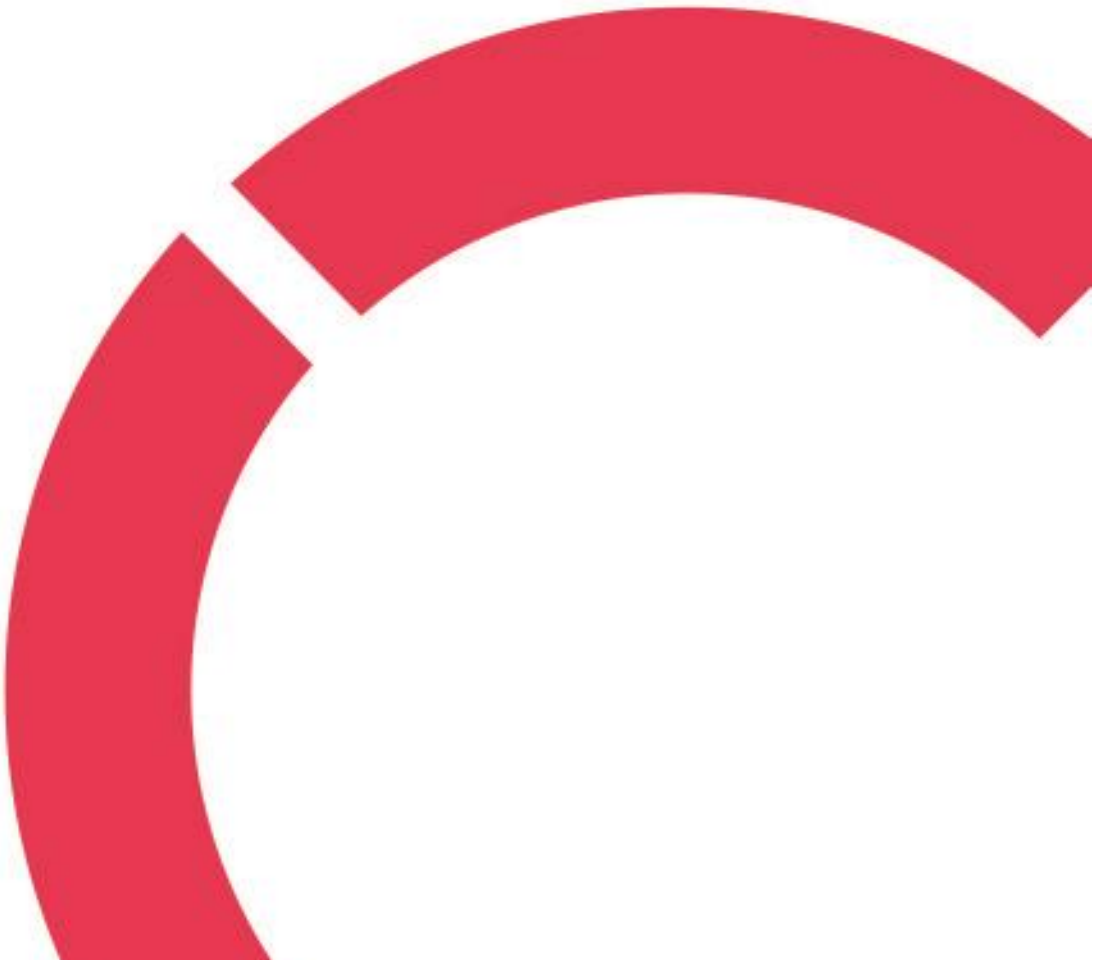
Milja Somero

HYVINVOINTIALUEEN LAITTEIDEN JA TIETOJÄRJESTELMIEN KRIITTISYYSLUOKITTELU

Pohjois-Pohjanmaan hyvinvointialue Pohde

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutus
Syyskuu 2024



TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Syyskuu 2024	**Tekijä/tekijät** Milja Somero
Koulutus Insinööri (AMK), tieto- ja viestintätekniikka		☒ AMK ☐ YAMK
Työn nimi HYVINVOINTIALUEEN LAITTEIDEN JA TIETOJÄRJESTELMIEN KRIITTISYYSLUOKITTELU. Pohjois-Pohjanmaan hyvinvointialue Pohde.		
Työn ohjaaja Ville Heikkiniemi		**Sivumäärä** 43+8
Työelämäohjaaja Anssi Huhtala		

Tehtävänä oli kehittää ja edistää Pohjois-Pohjanmaan hyvinvointialue Pohteen kriittisyysluokitteluprosessia laitteiden ja etenkin tietojärjestelmien osalta. Ongelmana oli aikaisemman prosessin hajanaisuus, eikä yhteistä selkeää linjaa luokittelulle ollut olemassa. Kriittisyysluokittelu toteutettiin ennen lähinnä vanhalla, sairaanhoitopiireistä totutulla tavalla ja yhdistäen eri työkaluja.

Opinnäytetyön tavoitteena oli saada aikaan vakaa pohja hyvinvointialueen kriittisyysluokittelulle ja itse prosessille alaan liittyvien teorioiden, säädösten, lakien, vanhojen materiaalien ja eri alojen kriittisyysluokittelutoteutuksien perusteella. Prosessia kehitettiin yhteistyössä Pohteen tietoturvatiimin ja eri ammattilaisten kanssa. Itse luokitteluprosessi lähtee käyntiin heti esiselvitysvaiheessa ja sen on tarkoitus olla valmis ennen kuin rahoitus ja budjetointi on varmistettu. Kriittisyysluokitteluprosessin suunnittelun pohjaksi määräytyi tietoturvaa, tietosuojaa ja terveydenhuoltoalaa koskevat lait, asetukset ja standardit, joiden tehtävänä oli antaa viitekehykset prosessin luomiseksi.

Toiminnallisessa osuudessa kriittisyysluokitteluprosessin tueksi kehitettiin ennakkokysely ja kriittisyysluokittelutyökalu. Ennakkokyselyn tarkoituksena oli jaotella laitteet ja tietojärjestelmät karkeasti eri luokkiin asiakkaan oman näkökulman mukaisesti. Kriittisyysluokitteluun tarkoitetun työkalun tehtävänä oli tarkentaa jo saatua arviota tarvittaessa. Ennakkokyselystä ja kriittisyysluokittelutyökalusta saatu arvio laitteen tai järjestelmän kriittisyysluokasta määrittäisi jatkotoimenpiteistä ja resursseista, joita laite tai tietojärjestelmä tarvitsee.

Opinnäytetyöprosessin jälkeen kriittisyysluokitteluprosessi tulee osaksi Pohteen laitteiden ja tietojärjestelmien kriittisyysluokittelua. Käytännössä tullaan näkemään tarkemmin, kuinka toimiva prosessi on ja mitä täytyy muuttaa tai kehittää. Opinnäytetyö antoi kuitenkin perustuksen hyvinvointialueen kriittisyysluokittelulle, joka muokkautuu ja tarkentuu käytäntöön pääsyn, tarpeiden ja ajan myötä.

Asiasanat
Hyvinvointialue, kriittisyysluokittelu, kriittisyysluokitteluprosessi, lääkinnälliset laitteet, potilasturvallisuus, tietojärjestelmät, tietoturva

ABSTRACT

Centria University of Applied Sciences	**Date** September 2024	**Author** Milja Somero
Degree programme Bachelor of Engineering, Communication and Information technology.		
Name of thesis THE CRITICALITY CLASSIFICATION PROCESS FOR THE DEVICES AND INFORMATION SYSTEMS OF THE WELLBEING SERVICES COUNTY. The wellbeing services county of North Ostrobothnia, Pohde.		
Centria supervisor Ville Heikkiniemi		**Pages** 43+8
Instructor representing commissioning institution or company Anssi Huhtala		

The task was to develop and advance the criticality classification process for devices and especially information systems within the Pohde Wellbeing Services County of North Ostrobothnia. The problem with the previous process was its fragmentation, and there was no clear common approach to classification. The criticality classification had been previously carried out mainly using old methods from the hospital districts by combining different tools.

The aim of the thesis was to establish a stable foundation for the criticality classification and the process itself within the wellbeing services county, based on relevant theories, regulations, laws, old materials, and criticality classification implementations from various fields. The process was developed in collaboration with Pohde's information security team and various professionals. The classification process starts at the preliminary investigation phase and is intended to be completed before funding and budgeting are confirmed. The design of the criticality classification process was based on laws, regulations, and standards related to information security, data protection, and the healthcare sector, which provided the frameworks for creating the process.

In the practical part of the thesis, a preliminary survey and a criticality classification tool were developed to support the criticality classification process. The purpose of the preliminary survey was to roughly categorize devices and information systems into different classes based on the client's own perspective. The purpose of the criticality classification tool was to refine the initial assessment if necessary. The assessment from the preliminary survey and the criticality classification tool would define the follow-up actions and resources needed by the device or information system.

After the thesis process, the criticality classification process will become part of Pohde's criticality classification for devices and information systems. In practice, it will be seen in more detail how functional the process is and what needs to be changed or developed. However, the thesis laid the foundation for the wellbeing services county's criticality classification, which will be shaped and refined over time based on practical application, needs, and experience.

Key words
Criticality classification, criticality classification process, information security, information systems, medical devices, patient safety, wellbeing services county

KÄSITTEIDEN MÄÄRITTELY

C2M2

(Cybersecurity Capability Maturity Model) on vapaaehtoinen organisaation kyberturvallisuuden kypsyyden arviointiprosessi.

CIA

(Confidentality, Integrity, Availability) on lyhenne kyberturvan kolmesta tukipilarista: Luotettavuus, Eheys ja Saatavuus.

CSF

(Cybersecurity Framework) on tietoturvallisuuden viitekehys.

DNS

(Domain Name System) on nimipalvelujärjestelmä, joka muuntaa www-osoitteet ip-osoitteiksi.

FIMEA

Lääkevalvontaviranomainen. Toimii osana eurooppalaista verkostoa.

GDPR

(General Data Protection Regulation) on tietosuoja-asetus, jonka tarkoituksena on suojata yksityishenkilöiden henkilötietoja niitä käsiteltäessä.

HTTP-/HTTPS

(Hypertext Transfer Protocol/ Hypertext Transfer Protocol Secure) ovat protokollia, joiden avulla voidaan jakaa resursseja. HTTPS-protokollan avulla tieto pysyy salattuna molempiin suuntiin.

HYPERVISOR

Virtualisointiohjelmisto, joka mahdollistaa useamman virtuaalisen palvelimen ajamisen yhden fyysisen palvelimen kautta ja jakaa tallennustilan, resurssit ja muistin näiden kanssa.

ICT

(Information And Communication Technology) tarkoitetaan suomeksi Tietotekniikkaa/Informaatiotekniikkaa (IT).

IEC

(International Electrotechnical Commission) on kansainvälinen sähkötekniikan standardointiorganisaatio, joka määrittää yhdessä ISO:n kanssa tietotekniikanalan standardit.

IP-OSOITE

(Internetin protokollaosoite) on numerosarja, joka yksilöi jokaisen internetissä liikennöivän laitteen.

ISO

(International Organization for Standardization) on kansainvälinen standardointiorganisaatio.

NIS2

(Network and Information Security Directive 2) on Euroopan parlamentin ja neuvoston luoma kyberturvallisuusdirektiivi.

NIST

(National Institute of Standards and Technology) on Yhdysvaltain standardisointi- ja teknologiainstituutti.

PPSHP

(Pohjois-Pohjanmaan sairaanhoitopiiri) oli kuntayhtymä ennen hyvinvointialueiden muodostumista, joka piti huolta alueen sosiaali- terveys- ja pelastustoimen palveluista.

PROXY

(Välityspalvelin) on palvelin, jonka tehtävänä on suodattaa ja varastoida verkossa siirrettäviä tiedostoja.

PSHP

(Pirkanmaan sairaanhoitopiiri) oli kuntayhtymä ennen hyvinvointialueiden muodostumista.

SFS

(Suomen Standardiliitto) on standardoinnin keskusjärjestö Suomessa.

SLA

(Service Level Agreement) on palvelutasosopimus, joka määrittää palvelulle tietyt vähimmäisvaatimukset. Se sisältää myös asiakkaan ja toimittajan väliset odotukset ja sitoumukset.

SOTE

(Sosiaali- ja terveysala) käytetään lyhenteenä Sosiaali- ja terveysalalle ja -palveluille.

SPOF

(Single Points of Failure) tarkoitetaan vikapistettä, jonka vuoksi koko järjestelmä lakkaa toimimasta, vaikka muuta vikaa ei olisi.

STM

(Sosiaali- ja terveysministeriö) vastaa Suomen sosiaali- ja terveyspolitiikan suunnittelusta, ohjauksesta ja toimeenpanosta.

TL (IV)

(Turvallisuusluokittelu (4)) on valtioneuvoston määräämä asetus valtiollisten turvallisuusluokiteltujen asiakirjojen merkitsemiseksi.

VALVIRA

Sosiaali- ja terveysalan lupa- ja valvontavirasto. Tehtävänä valvoa eri toimintojen asianmukaisuutta.

TIIVISTELMÄ
ABSTRACT
KÄSITTEIDEN MÄÄRITTELY
SISÄLLYS

1 JOHDANTO 1

2 TYÖN TAUSTAT 3
2.1 Hyvinvointialue Pohde 3
2.2 Työn lähtökohdat ja idea 4

3 LAIT JA ASETUKSET KRIITTISYYSLUOKITTELUN TUKENA 5
3.1 Standardit ja viitekehykset kriittisyysluokittelulle 5
3.1.1 ISO/IEC 27001 6
3.1.2 ISO/IEC 27002 6
3.1.3 ISO/IEC 27799 6
3.2 Muut tärkeät ISO-standardit 7
3.2.1 ISO 31000 7
3.2.2 ISO 22301 7
3.3 Tietosuoja-asetus GDPR 8
3.4 Kyberturvallisuusdirektiivi NIS2 8
3.5 NIST Cyber Security Framework 2.0 (CSF) 9
3.6 Kybermittari 9

4 KRIITTISYYSLUOKITTELU 11
4.1 Kriittisyysluokittelun ero eri aloilla 11
4.2 Terveydenhuollon kriittisyysluokittelu 12
4.3 Potilasturvallisuus osana kriittisyysluokittelua 13
4.4 Terveydenhuollon jatkuvan kehittämisen ylläpito 14
4.4.1 Häiriötilanteet 14
4.4.2 Häiriötilanteet terveydenhuollossa 14

5 KRIITTISYYDEN MÄÄRITYSPROSESSI LAITTEILLE JA TIETOJÄRJESTELMILLE 16
5.1 Ennakkokysely 17
5.2 Kriittisyysluokittelu työkalun avulla 18
5.3 Yhteispalaveri 18
5.4 Luokittelun varmistaminen ja ilmoittaminen 19
5.5 Jatkuvuuden toteuttaminen kriittisille laitteille ja tietojärjestelmille 19
5.5.1 Palvelimet 19
5.5.2 Kuormantasaus 21
5.5.3 Kahdennus 21
5.5.4 Testiympäristö ja testaus 22
5.6 Tulosten dokumentointi 23

6 ENNAKKOKYSELYN TOTEUTUS 24
6.1 Kriittisyysluokka itsearvioinnin avulla 24
6.2 Ennakkokyselyn kriittisyysarvio 26

7 TYÖKALUN TOTEUTUS 27
7.1 Toteutuksen lähtökohdat 27

7.2 Työkalun sisältö 28
7.3 Arviointikriteerit 29
7.4 Käyttökatkosarviointi 31
7.4.1 Suunniteltu käyttökatko 32
7.4.2 Suunnittelematon käyttökatko 33
7.5 Riippuvuudet 33
7.5.1 Pilviriippuvuus 34
7.5.2 Internetriippuvuus 34
7.5.3 Sairaalaympäristön ulkopuoliriippuvuus 35
7.6 Painoarvot 36

8 PROSESSIN TESTAAMINEN JA TULOKSET 37

9 YHTEENVETO 39

LÄHTEET 40
LIITTEET

KUVIOT

KUVIO 1. CSF:n sisältämät funktiot 9
KUVIO 2. Sairaalan toimintaympäristö potilaan hoidon ympärillä 12
KUVIO 3. Potilas- ja tietoturvallisuuden tasot 13
KUVIO 4. Esimerkki kriittisyysluokitteluprosessin alusta 16
KUVIO 5. Esimerkki kriittisyysluokitteluprosessin lopusta 17

KUVAT

KUVA 1. Hyvinvointialue Pohde, alueen kunnat 3
KUVA 2. Istekin kriittisyysluokittelun työkalu 28
KUVA 3. Kriittisyysluokittelutyökalun demoversio 29
KUVA 4. Työkalun painoarvomuutokset 36

1 JOHDANTO

Opinnäytetyön tavoitteena on ensiksi perehtyä jo olemassa oleviin työkaluihin, dokumentteihin ja materiaaleihin, jotka liittyvät terveydenhuoltoalan kriittisyysluokitteluun. Opinnäytetyössä keskitytään kehittämään kokonaisvaltaisesti kriittisyysluokitteluprosessia, ennakkokyselyä ja tietojärjestelmiin ja laitteisiin kohdistuvaa kriittisyysluokittelutyökalua, joita käytetään apuna kriittisyysluokittelun tekemisessä.

Opinnäytetyön lopputuloksen päämääränä on saada aikaan täysin toimiva kokonaisuus, jota voidaan käyttää hyvinvointialue Pohteen tietojärjestelmien ja laitteiden kriittisyysluokittelussa yhdessä tietojärjestelmien ja laitteiden omistajien kanssa. Prosessilla pyritään vähentämään tulkinnanvaraisuuksia ja parantamaan ymmärrystä järjestelmien ja laitteiden kriittisyyskokonaisuudesta. Tavoitteena on saada aikaan helposti ymmärrettävissä oleva työkalu, joka on nopea sisäistää ja ihanteellisessa tilanteessa ottaa osaksi hankintakokonaisuutta yhdessä ennakkokyselylomakkeen kanssa. Työkalun ja ennakkokyselyn keskiarvolla on tavoitteena antaa realistinen arvio laitteen tai tietojärjestelmän kriittisyydelle, jonka perusteella tarvittavat jatkotoimenpiteet voidaan tehdä.

Opinnäytetyössä valmistetaan ennakkokyselylomake, jonka avulla laitteen tai järjestelmän omistaja tekee oman karkean arvionsa tietojärjestelmän tai laitteen kriittisyydestä väliltä vähäinen (1) – kriittinen (4) esimerkkien ja kysymyksen vastausvaatimusten avulla. Ennakkokyselylomakkeen tarkoituksena on vähentää luokitteluun vaadittavaa työmäärää, antaa ennakkoarvio kriittisyydestä esiselvityksessä ja nopeuttaa kriittisyysluokittelun tekemisen prosessia. Jos jokainen uusi tietojärjestelmä tai laite käytäisiin läpi ammattilaisten kanssa, tulisi työmäärästä kohtuuton ja aikaa vievä. Tällä tavalla resurssit voidaan kohdistaa kriittisimpiin ja epäselviin tapauksiin, kun ne voidaan erikseen käydä läpi yhdessä ammattilaisten kanssa.

Ennakkokyselyn lisäksi opinnäytetyössä rakennetaan kriittisyysluokitteluun käytettävä työkalu, jonka tarkoituksena on antaa tarkempi arvio kriittisyydestä. Työkalun tulee olla helposti muunneltavissa painoarvojen sekä haluttujen kriteerien vuoksi, koska jokainen oma laite tai järjestelmänsä on omanlaisensa kokonaisuus, joka kattaa eri osa-alueita. Työkalun ohella pyritään noudattamaan ja ottamaan huomioon alaan liittyviä standardeja, ohjeistuksia sekä vaatimuksia, joista tärkeimmät käydään läpi tässä opinnäytetyössä lyhyesti. Työkalua on tarkoitus jatkokehittää tarpeiden ja vaatimusten muuttuessa käyttöönoton jälkeen.

Liikenne- ja viestintäviraston alainen viranomainen Kyberturvallisuuskeskus ja Suomen Standarditoimistoliiton sivut (SFS) oli iso apu opetellessani ja tutustuessani kriittisyysluokitteluun ja ylipäätään tietoturvaan liittyviin ohjeistuksiin, säädöksiin ja vaatimuksiin. Muuten kirjallisuudesta tai opinnäytetöistä ei löytynyt yhtäkään luokittelua, joka olisi suunnattu erityisesti suoraan sosiaali- ja terveysalan sektorille, vaan eri lähteitä täytyi soveltaa alalle sopiviksi ja ottaa erikseen huomioon potilasturvallisuuden säädökset.

Suurimpana apuna ja tietopankkina opinnäytetyössä on käytetty Pohteen tietoturvatiimin pitkäaikaisten ammattilaisten näkökulmia ja tietämystä. Isot kiitokset tietoturvapäällikkö Anssi Huhtalalle, tietoturvan kehittämispäällikkö Jukka Juntuselle, tietoturva-arkkitehtuuriasiantuntija Topias Mainiolle ja tietoturvasuunnittelija Antti Junttilalle, joiden tietämys, tuki ja apu oli korvaamatonta opinnäytetyön ja kriittisyysluokitteluprosessin kehittämisen aikana. Kiitokset kuuluvat myös koko Pohteen organisaatiolle, joka mahdollisti projektin toteutuksen ja mahdollisuuden kehittää omaa osaamistani.

2 TYÖN TAUSTAT

2.1 Hyvinvointialue Pohde

Sote- ja maakuntauudistusta koskevat sosiaali- ja terveysvaliokunnan laki- ja lausumaehdotukset hyväksyttiin eduskunnassa 23.6.2021 (Eduskunta 2024). Aiemmin kunnilla ja kuntayhtymillä oli päävastuu sosiaali- terveys- ja pelastuspalveluiden järjestämisestä, mutta vastuu siirtyi 1. tammikuuta 2023 erikseen määrätyille hyvinvointialueille (STM 2024).

Pohde, eli PPHVA (Pohjois-Pohjanmaan hyvinvointialue), on entinen PPSHP (Pohjois-Pohjanmaan sairaanhoitopiiri), mihin kuuluu yhteensä 30 kuntaa (KUVA 1). PPHVA on koko Pohjois-Pohjanmaan kattava hyvinvointialue. Yhteensä hyvinvointialueita on 21, joista Pohde on toiminta-alaltaan yksi Suomen suurimmista hyvinvointialueista. Pohde ja siellä työskentelevät yli 18 000 ammattilaista eri nimikkeillä vastaavat yli 400 000 asukkaan hyvinvoinnista, terveydestä ja turvallisuudesta Pohjois-Pohjanmaan alueella. (Pohde b, sivu ”Tietoa meistä”.)

KUVA 1. Hyvinvointialue Pohde, alueen kunnat (Pohde a, sivu ”Alueen kunnat”)

2.2 Työn lähtökohdat ja idea

Palveluiden ja ohjeistuksien päivittäminen PPSHP:n ajoilta tapahtuu Pohteen hyvinvointialueella asteittain, eivätkä kaikki muutokset tapahdu hetkessä. Sain tietoturvapäällikkö Anssi Huhtalalta toimeksiannon päivittää ja yhtenäistää nykyistä laitteistojen ja tietojärjestelmien kriittisyysluokitteluprosessia ja kehittää luokittelun apuna käytettävää Excel-taulukkotyökalua. Tarkoituksenani on hyödyntää jo olevassa olevia materiaaleja ja työkaluja opinnäytetyön tekemisessä, prosessin suunnittelussa ja työkalun kehittämisessä.

Aikaisemmin käytössä ovat olleet PPSHP:n, Istekin sekä Traficom kyberturvallisuuskeskuksen työkalut, joita yhdistämällä ja soveltamalla nykyiset järjestelmät Pohteella ovat kriittisyysluokiteltu, eikä yhteistä selvää linjaa luokittelulle ole vielä ollut käytössä. Tähän haluttiin muutosta, jotta tulevaisuudessa järjestelmien kriittisyysluokittelusta saataisiin yhtenäisempää, yksinkertaisempaa ja nopeampaa myös kaikkien luokittelussa mukana olevien toimijoiden näkökulmasta.

PPSHP:n aikainen ja Istekin omat kriittisyysluokittelutyökalut ovat tarpeeksi yksinkertaisia ja helposti muunneltavissa olevia kriittisyysluokittelutyökaluja, joiden muokkaamisesta on tarkoitus lähteä liikkeelle. Kyberturvallisuuskeskuksen teettämä kriittisyysluokittelutyökalu on hyvin kattava, joten tarkoituksenani on jättää se suunnittelun ulkopuolelle, mutta ottaa ideoita myös sitä kautta. Näistä kolmesta luokitteluapuvälineestä sovelletaan yhdessä teorioiden kanssa kokonaisuus, joka auttaa hyvinvointialueen laitteiden ja tietojärjestelmien kriittisyysluokittelussa.

3 LAIT JA ASETUKSET KRIITTISYYSLUOKITTELUN TUKENA

Tämän osuuden tarkoituksena on antaa luotettava pohjamateriaali kriittisyysluokitteluprosessin kehittämiselle. Osuudessa käydään läpi kansainvälisesti luokiteltuja standardeja tietoturvan tueksi, standardit liittyen riskien hallintaan ja jatkuvuuteen, terveydenhuollon toimialan tuomat säädökset ja kriittisyysluokittelulle hyödyllisiä standardeja. Kriittisyysluokitteluprosessin suunnittelemista sanelevat myös yleinen tietosuoja-asetus GDPR sekä kyberturvallisuusdirektiivi NIS2. Mukana on myös Suomen viranomaisten yhteistyössä kehittämä Kybermittari, joka on kohdistettu Suomessa toimivien yritysten ja organisaatioiden kriittisyysluokitteluun.

3.1 Standardit ja viitekehykset kriittisyysluokittelulle

Tässä osiossa käsitellään tärkeimpiä kansainvälisiä International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) standardeja, jotka määrittelevät vakaan pohjan tietoturvalle ja kriittisyysluokittelulle terveydenhuollon toimialalla. ISO/IEC 27000-sarja kattaa laajasti suosituksia tietoturvallisuuden standardeista, joita noudattamalla pystytään kontrolloimaan ja hallitsemaan tietoturvallisuutta organisaatiossa ja vähentämään tietoturvariskejä. Standardeilla pyritään suojaamaan organisaation tieto-omaisuus, joka voi kattaa esimerkiksi asiakkaiden potilastietoja tai organisaation työntekijöiden tietoja (SFS, ISO/IEC 27000).

Tässä osuudessa esiteltävät standardit ja asetukset sopivat hyvin kriittisyysluokittelun ja opinnäytetyössä tehtävän luokittelutyökalun tarkasteluun varautumistoimenpiteiden, esimerkiksi häiriötilanteiden hallinnan ja häiriötilasta toipumisen osalta. Kriittisyysluokitteluprosessin kehittämisen ohessa täytyy ottaa huomioon vähintään näiden standardien asettamat säädökset ja ohjeistukset, koska näiden avulla parannetaan laitteiden, järjestelmien ja resurssien priorisointia ja saadaan tukea päätöksien tekemiseen. (Mutanen, Tolonen & Vepsäläinen 2021, 10.)

Luokittelun taustalla käytetyistä viitekehyksistä huolimatta kriittisyysluokittelu edistää terveydenhuollon organisaatioiden kyber- ja kokonaisturvallisuuden hallintaa kokonaisvaltaisesti. Kyberturvallisuuteen liittyvien investointipäätöksien ja tarvittavia kehittämistoimenpiteitä voidaan perustella ja toteuttaa helpommin ja listata arvioinnin jatkuessa kohteet, jotka vaativat säännöllistä auditointia organisaation sisällä. (Mutanen, Tolonen & Vepsäläinen 2021, 10.)

3.1.1 ISO/IEC 27001

Kansainvälisesti tunnustetuin on ISO/IEC 27001-standardi, joka määrittää tietoturvan hallintajärjestelmän vaatimukset. Sen tärkeimmät periaatteet ovat tiedon luottamuksellisuuden varmistaminen, tiedon eheys ja tiedon saatavuuden varmistaminen. Standardi kattaa myös digitaalisen ja fyysisen tiedon ja laitteistojen tietoturvasuositukset ja -vaatimukset, sekä johdon, auditoinnin sekä riskienhallinnan näkökulmat. Standardia käytetään organisaation tietoturvallisuuden ja tietoturvariskien hallintapolitiikan, -järjestelmän ja -tavoitteiden luomisen ja ymmärtämisen tukena. (DNV, ISO/IEC 27001.)

3.1.2 ISO/IEC 27002

ISO 27002-standardia käytetään tietoturvajohtamisenjärjestelmän ja -prosessien tukena käytännön ohjeistuksena organisaatioissa, kuinka tietoturvariskien hallintakeinoja voidaan toteuttaa ja määrittää ISO/IEC 27001-standardissa määritellyn hallintajärjestelmän mukaisesti. Standardin pohjalta voidaan kehittää organisaation turvallisuusjohtamisen käytäntöjä sekä turvallisuusstandardeja. (SFS, ISO/IEC 27002.)

3.1.3 ISO/IEC 27799

ISO/IEC 27799-standardi on yksi osa tietoturvallisuuden standardeista, mutta se tuo mukanaan näkökulmia terveydenhuoltoon liittyvistä tietoturvavaatimuksista. Sen tarkoituksena on täydentää ISO 27002-standardin ohjeistuksia. (ISO, ISO/IEC 27799.) Tällä standardilla pyritään säilyttämään organisaation asiakkaiden henkilökohtaisten terveystietojen luottamuksellisuus, eheys ja saatavuus (CIA (Confidentality, Integrity, Availability)).

Luottamuksellisuudella (Confidentiality) tarkoitetaan tietojen käsittelemistä yksityisesti ja turvallisesti, kerättyjen tietojen pitämistä salassa ja tietojen käyttöä vain tiettyihin ennalta määritettyihin tarkoituksiin. Tietoja saa käsitellä ja päästä käsiksi vain siihen tarkoitukseen tarkoitetut henkilöt, jotka siihen on määrätty. (Jurvanen 2024a.) Terveydenhuoltoalalla tietoa kuitenkin voidaan tarvita antaa eteenpäin hoidon onnistumisen varmistamiseksi.

Eheydellä (Integrity) tarkoitetaan tiedon pysymistä yhtenäisenä, muuttumattomana ja luotettavana kaikissa olosuhteissa, kun tietoa tallennetaan, varastoidaan, siirretään tai haetaan. Eheys voidaan jakaa fyysiseen ja loogiseen eheyteen. Fyysisessä eheydessä on kyse tiedon tai datan rakenteellisen eheyden säilymisestä häiriötilanteessa, kun taas loogisella eheydellä tarkoitetaan tiedon tai datan sisällön hallintaa ja poikkeamattomuutta. (Jurvanen 2024b.)

Saatavuudella (Availability) tarkoitetaan tietojen saavutettavuutta ja hyödynnettävyyttä haluttuna aikana. Pääsyn tietoon, järjestelmään, ohjelmaan tai palveluun täytyy olla luotettavaa, häiriötöntä ja jatkuvaa tietojärjestelmän käyttäjän kannalta. (Jurvanen 2024c.)

3.2 Muut tärkeät ISO-standardit

3.2.1 ISO 31000

Yksi keskeisin ISO-standardi riskienhallinnan ja kriittisyysluokittelun näkökulmasta on ISO 31000. Se toimii ohjeistuksena eri aloilla kaikkiin organisaation toimiin liittyviin riskien hallintatoimiin sen sovellettavuuden ja laajuuden vuoksi. Standardi pyrkii painottamaan ja sitouttamaan jokaisen osallistumista riskienhallintatoimiin johtoportaasta aina organisaation toimijoihin. (SFS, ISO 31000.)

3.2.2 ISO 22301

Toinen tärkeä standardi, joka täytyy ottaa huomioon kriittisyysluokittelutyökalua suunnitellessa, on ISO 22301. Tämä standardi pitää sisällään vaatimuksia liittyen organisaation toimintojen jatkuvuushallintaan, joiden avulla tunnistetaan toimintoihin tai järjestelmiin liittyviä uhkia ja niiden vaikutuksia. Standardin avulla voidaan suunnitella ja toteuttaa toimintatavat häiriötilanteiden varalle. Hallintajärjestelmän tarkoituksena on auttaa kaiken kokoisia organisaatioita tunnistamaan ja minimoimaan riskien toteutumisen todennäköisyyttä sekä varautumaan ja reagoimaan toimintojen ja järjestelmien häiriöihin ja vikoihin, sekä palautumaan niistä normaalille tasolle mahdollisimman nopeasti. (SFS, ISO 22301.)

3.3 Tietosuoja-asetus GDPR

General Data Protection Regulation (GDPR) on tietosuoja-asetus, jonka tarkoituksena on suojata yksityishenkilöitä ja heidän henkilötietojaan niitä käsiteltäessä. Asetuksen tehtävänä on antaa viitekehykset henkilötietojen oikeanlaiselle käsittelylle, käsittelyiden lainmukaisuudesta, käsittelijän ja rekisteripitäjän velvoitteista, sopimuksista, vastuista ja arkaluontoisista tietojen käsittelystä. (Eur-lex 2022.)

GDPR vaikuttaa merkittävästi terveydenhuoltoon ja henkilö- ja potilastietojen käsittelyyn, koska terveydenhuollossa käsitellään suuria määriä henkilötietoja ja arkaluontoisia asioita. Potilaiden terveystiedot kuuluvat GDPR:n alaisiin erityisiin henkilötietoryhmiin, joihin GDPR asettaa tiukat vaatimukset näiden tietojen suojaamiselle. Terveydenhuollon organisaation vastuulla on suojata teknisin ja organisatorisilla toimenpiteillä henkilötietoja käsittelevät laitteet ja tietojärjestelmät.

Terveydenhuollossa on paljon laitteita ja tietojärjestelmiä, jotka hyödyntävät, sisältävät tai käsittelevät potilasdataa, joka vaikuttaa suoraan niiden kriittisyysluokitteluun. Tällaisten laitteiden ja tietojärjestelmien on noudatettava tiukkoja turvallisuusstandardeja ja hallintokäytäntöjä tietosuojan ja -turvan kannalta.

3.4 Kyberturvallisuusdirektiivi NIS2

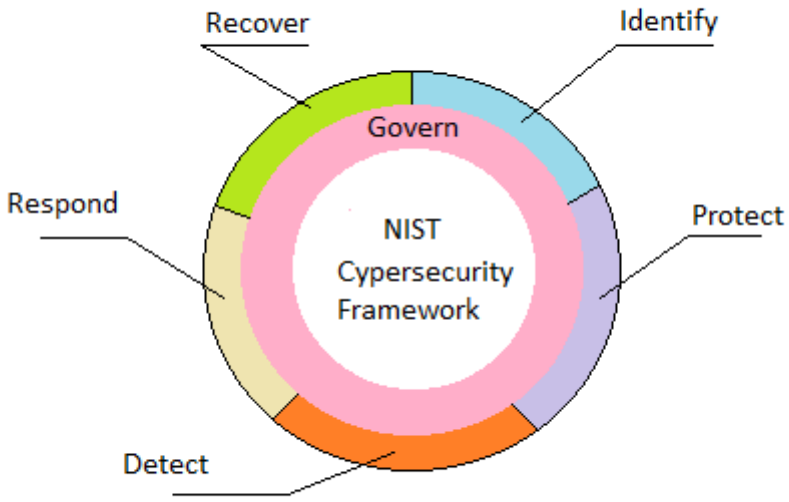
Network and Information Security Directive 2 (NIS2) on Euroopan parlamentin ja neuvoston direktiivi, joka asettaa kyberturvallisuuden riskienhallinnalle ja häiriöraportoinnille minimivaatimukset. NIS2-direktiivin on tarkoitus tulla osaksi kansallista lainsäädäntöä ja kumota aikaisempi verkko- ja tietoturvaa koskeva NIS-direktiivi. NIS2-direktiivillä pyritään parantamaan ja vahvistamaan kyberturvallisuutta koko Euroopan unionin alueella yhteiskunnallisesti. NIS2-direktiivin asettamien velvoitteiden soveltamisala laajenee koskemaan laajempaa osaa yrityksistä. (Valtioneuvosto.)

Kriittisyysluokittelu osuukin NIS2-direktiivin vaatimusten osaamisalueelle riskienhallinnan ja jatkuvuuden suojaamisen kannalta. Kriittisyysluokittelu on osa organisaation kokonaisvaltaista riskienhallintaa ja sen avulla laitteiden ja tietojärjestelmien jatkuvuutta häiriötilanteissa voidaan parantaa. NIS2-direktiivi edellyttää, että laitteet ja järjestelmät tunnistetaan ja luokitellaan niiden kriittisyyden perusteella. NIS2 velvoittaa terveydenhuollon organisaatiota raportoimaan kyberturvallisuuspoikkeamista, etenkin silloin, jos ne koskevat kriittiseksi luokiteltuja laitteita tai järjestelmiä.

3.5 NIST Cyber Security Framework 2.0 (CSF)

National Institute of Standards and Technology (NIST) on Yhdysvaltain standardisointi- ja teknologiainstituutti. Sen kehittämää Cybersecurity Framework (CSF) 2.0 viitekehystä käytetään ohjeena ja suosituksena kyberturvallisuusriskien hallintaan eri alojen organisaatioissa.

NIST CSF käyttää kypsyysmallimenetelmää, jolla organisaatio voi tehdä toimintaansa itsearviointeja ja auttaa kustannustehokkaasti organisaatiota tunnistamaan, arvioimaan ja hallitsemaan tietoturvariskejä. Kypsyysmalli sisältää viisi eri vaihetta: tunnistaminen, suojautuminen, havainnointi, reagointi ja palautuminen, jotka kaikki olennaisesti liittyvät kriittisyysluokitteluun (KUVIO 1). (NIST U.S. Department of commerce, 6–7.)



KUVIO 1. CSF:n sisältämät funktiot (mukaillen NIST U.S. Department of commerce, 10)

3.6 Kybermittari

Huoltovarmuuskeskus ja Traficomin Kyberturvallisuuskeskus ovat luoneet yhdessä viranomaisten, yritysten, organisaatioiden ja riskienhallinnan asiantuntijoiden kanssa kriittisyysluokitteluun liittyvän työ-

kalun, Kybermittarin. Kybermittari on kehitetty kansainvälisien NIST CSF:n ja Cybersecurity Capability Maturity modelin pohjalta (C2M2) Suomessa toimivien organisaatioiden ja yrityksien tarpeisiin (Kyberturvallisuuskeskus 2024a, luku "Mikä on kybermittari?").

Kybermittarin tehtävänä on mitata kyberturvallisuuden kokonaisvaltaista tasoa ja investointien hyötyä kyberturvallisuuden kehittämisessä ja ylläpitämisessä. Arviointimalli tapahtuu itsearviointi- ja haastattelutyyppisesti, joilla mitataan organisaation eri toimintamalleja, sisäisiä prosesseja ja tekniikoita. Saatavilla tuloksilla voidaan määrittää kokonaiskuva siitä, mitä eri riskejä organisaatio pystyy itse hallitsemaan ja mitä olennaisia riskejä on tunnistettu. Niin kuin NIST CSF, myös Kybermittari antaa arvion organisaation tasosta tunnistaa, suojata, havainnoida ja reagoida riskeihin sekä tasosta palautua riskien aiheuttamista häiriöistä. (Mutanen, Tolonen & Vepsäläinen 2021, 9–10 [Kyberturvallisuuskeskus 2024b].)

4 KRIITTISYYSLUOKITTELU

Kriittisyysluokittelulla tarkoitetaan prosessia, jossa voidaan arvioida ja luokitella eri kohteita tärkeys- ja kriittisyysjärjestykseen. Kohteilla voidaan tarkoittaa esimerkiksi laitteita, järjestelmiä, toimintoja tai tietoja, ja näiden kriittisyyttä verrataan suhteessa niiden toimintaan ja organisaation tavoitteisiin. (Mutanen, Tolonen & Vepsäläinen 2021, 3.) Luokittelu antaa organisaatiolle apua resurssien oikeasta priorisoinnista ja auttaa ylläpitämään elintärkeiden toimintojen, laitteiden ja järjestelmien toiminnan jatkuvuuden, turvallisuuden ja laadun (Mutanen, Tolonen & Vepsäläinen 2021, 10). Jos kriittisyysluokittelua ei toteuteta yhtenäisesti kaikkien laitteiden ja järjestelmien varalta, voidaan olla siinä käsityksessä, että kaikki ovat kriittisesti luokiteltuja (Mutanen, Tolonen & Vepsäläinen 2021, 4). Olen ymmärtänyt kriittisyysluokittelun olevan itsessään jatkuvaa työtä, jota pyritään uudistamaan esimerkiksi ympäristön tai säädöksien muuttuessa. Kriittisyysluokittelukokonaisuus vaatii laajaa tuntemusta sairaalaympäristön kokonaiskuvasta ja siihen vaaditaan eri alojen ammattilaisia. Kriittisyysluokitteluarvio antaa suuntaa sopimuksien laatimiseen ja sen tulee olla yhteensopiva toimittajan ja asiakkaan välisen Service Level Agreement (SLA)-palvelutasosopimuksen kanssa (Huhtala 2024).

4.1 Kriittisyysluokittelun ero eri aloilla

Priorisoivattavat asiat riippuvat paljon alasta, jossa työskennellään, ja kriittisyysluokittelu auttaa kohdistamaan käytössä olevat resurssit esimerkiksi tuotannon sujuvan pyörimisen tai potilasturvallisuuden kannalta tärkeimpiin kohteisiin. Kriittisyysluokittelulla voidaan myös löytää, havainnoida ja ennakoida turvallisuuden kehittämistarpeita (Mutanen, Tolonen & Vepsäläinen 2021, 9).

Tuotannossa kriittisyysluokittelussa kyse on lähinnä toiminnan sujuvasta toimimisesta. Tuotantoympäristössä kriittisyydessä voi olla kyse varaosien saatavuudesta ja korjaamisesta, laitteen luotettavuudesta ja vikaantumisvälistä tai henkilöturvallisuusriskin mahdollisuudesta laitteen vikaantuessa. (Tuomisalo 2021.) Tuotannossa noudatetaan eri standardeja kuin terveydenhuoltoalalla. Tällainen standardi on esimerkiksi PSK 6800, joka toimii osana teollisuuden riskienhallintaa ja määrittelee sen alan kriittisyysluokittelun tekemistä.

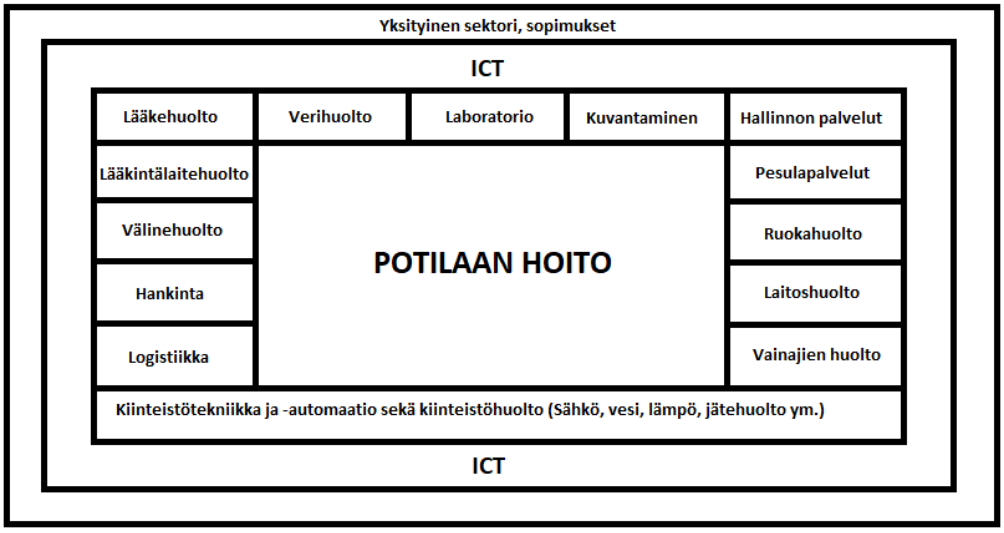
Terveydenhuoltoalalla tilanne on hieman eri, koska kriittisyysluokittelua tarkastellaan aina potilaan hoidon näkökulmasta. Häiriön sattuessa sairaalaympäristössä kyse voi olla pahimmassa tapauksessa

laitteen käyttökatkon aiheuttama potilaan vammautuminen tai jopa kuolema. Ainakin muutama asia yhdistää kaikkia aloja kriittisyysluokittelun näkökulmasta: laite- tai järjestelmäviasta johtuvat kustannukset, ydintoimintojen häiriöt ja mahdolliset mainehaitat yritykselle tai organisaatiolle.

4.2 Terveydenhuollon kriittisyysluokittelu

Terveydenhuollossa laitteiden ja järjestelmien kriittisyysluokittelua varten täytyy olla selkeä kokonaiskuva potilaan hoitoon liittyvistä toiminnoista ja prosesseista, koska kaikki toiminnot ovat riippuvuussuhteessa toisiinsa nähden (Mutanen, Tolonen & Vepsäläinen 2021, 11). Joissakin toiminnoissa jokin laite tai järjestelmä voi olla kriittinen, mutta kun siirrytään eri toimintoihin, ei sama laite tai järjestelmä välttämättä enää olekaan kriittinen sillä alueella (Mainio 2024).

Potilaan hoitoon ja sen onnistumiseen liittyvät toiminnot ovat määrältään paljon isommat, mitä äkkiseltään voitaisiin kuvitella, eikä kokonaisuuden hahmottaminen ole yksinkertaista (KUVIO 2). Toiminnot lähtevät organisaation tieto- ja viestintätekniikasta (ICT) ja yksityisen sektorin palveluista aina potilaan ruokahuoltoon ja hallinnon tukipalveluihin saakka ja kattavat kaiken tältä väliltä. Jos yksikin asia vaarantuu matkan varrella, voi sillä olla vaikutusta potilaan turvalliseen hoitoon. Siksi kokonaisuuden hahmottamisessa tarvitaan jokaisen osa-alueen hallintaa ja ymmärtämistä. (Mutanen, Tolonen & Vepsäläinen 2021, 12.)

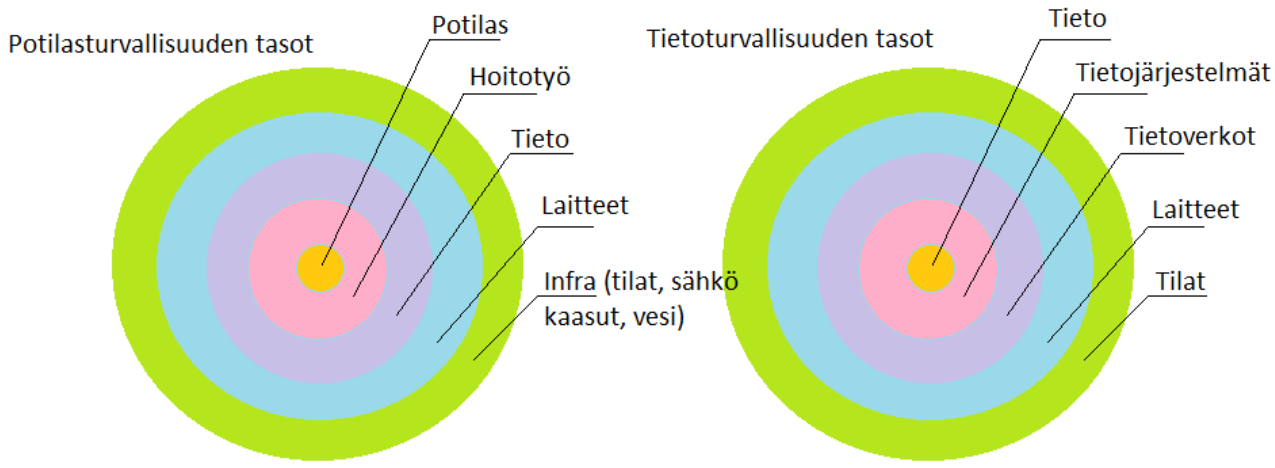


KUVIO 2. Sairaalan toimintaympäristö potilaan hoidon ympärillä (mukaillen Mutanen, Tolonen & Vepsäläinen 2021, 11)

4.3 Potilasturvallisuus osana kriittisyysluokittelua

Potilasturvallisuus on yksi iso osa terveydenhuollon toimintoja. Potilaan kuuluisi saada oikeaa hoitoa ilman ylimääräistä haittaa, viivytyksiä tai muita ongelmia. Potilaiden terveyden- ja sairaanhoidon tulisi olla turvattuna, joka pyritään varmistamaan terveydenhuollon toimintayksiköiden, ammattihenkilöiden ja organisaation käytäntöjen ja periaatteiden avulla. Potilaan turvallisuus käsittää esimerkiksi oikeanlaisen hoidon, kuntoutuksen, sairauksien ehkäisemisen ja diagnostiikan. (Mutanen, Tolonen & Vepsäläinen 2021, 12.)

Terveydenhuollon toimintojen digitalisoituminen on johtanut siihen, että tietojärjestelmät ja digitaaliset palvelut ovat potilashoitotyön keskiössä (KUVIO 3). Sairaaloiden tietojärjestelmät ja suuri osa nykyaikaisista lääkintälaitteista, jotka mahdollistavat mutkattomamman ja tehokkaamman hoitotyön, ovat jollain tavalla kytköksissä eri tietojärjestelmiin, pilviratkaisuihin ja tietoverkkoihin. Kytkökset kasvattavat riskiä joutua kyberuhan kohteeksi. Potilastietojärjestelmä ei ole ainoa, joka on kriittinen osa potilasturvallisuutta, vaan potilasturvallisuudelle ja hoitotyölle voi olla muita yhtä kriittisiä laitteita tai järjestelmiä. Jos joihinkin laitteisiin tai järjestelmiin ei kiinnitetä tarpeeksi huomiota ja resursseja, voivat häiriöt aiheuttaa potilasturvallisuuteen liittyviä riskejä. Terveydenhuollossa tapahtuvalla kriittisyysluokittelulla pyritään vaikuttamaan kokonaisvaltaisesti potilasturvallisuuden ylläpitämiseen. (Mutanen, Tolonen & Vepsäläinen 2021, 12.)



KUVIO 3. Potilas- ja tietoturvallisuuden tasot (mukaillen Mutanen, Tolonen & Vepsäläinen 2021, 13)

4.4 Terveydenhuollon jatkuvan kehittämisen ylläpito

Jatkuva kehittäminen on tärkeä osa terveydenhuoltoa hyvinvointialueen toimintojen digitalisoinnin myötä. Koskaan ei pidä luottaa siihen, ettei mitään tarvitsisi enää tehdä, vaan kehittämisen täytyy olla jatkuvaa työtä. Terveydenhuolto kokee jatkuvasti muutospaineita ja -tarpeita lainsäädännön, taloudellisten rakennemuutosten ja yhteiskunnan muuttuessa, jotka pitää ottaa huomioon kehittämisen ylläpidossa ja jatkuvuudessa. Jatkuvalla kehittämisellä pyritään minimoimaan näiden muodostamia riskejä ja välttämään ongelmien kasaantumisen liian suureksi ja sen avulla voidaan parantaa kaikkien tyytyväisyyttä, kehittää asiakaspalvelua ja kustannustehokkuutta. Kaiken keskiössä tulee kuitenkin jatkuvasti pitää potilaan hoidon mutkaton onnistuminen, häiriötilanteiden ja riskien minimointi ja potilasturvallisuus. (Mutanen, Tolonen & Vepsäläinen 2021, 13.)

4.4.1 Häiriötilanteet

Yleisesti häiriötilanteella voidaan tarkoittaa yhteiskunnan elintärkeiden toimien ja tehtävien turvallisuutta vaarantavia uhkia tai tapahtumia, jotka vaativat eri toimijoiden ja viranomaisten tiivistä yhteistyötä ja viestintää. Häiriötilanteet voivat syntyä luonnonkatastrofien seurauksena, mihin luokitellaan esimerkiksi sään aiheuttamat tuhot, joihin ihmiset eivät voi itse vaikuttaa. Sään aiheuttamat tuhot voivat syntyä esimerkiksi tulvista, sähkökatkoksista, myrskyistä tai muista luonnonilmiöistä. Ihmisten itseaiheutettuihin häiriötilanteisiin kuuluu esimerkiksi inhimilliset virheet, terrori-iskut, kyberhyökkäykset ja mellakat. Jokin häiriötilanne voi koskea pelkästään tiettyä aluetta tai pahimmillaan koko Suomea. (Termipankki 2024.) Harvinaisissa tapauksissa häiriön laajuus voi koskea koko maanosaa tai maailmaa.

4.4.2 Häiriötilanteet terveydenhuollossa

Sosiaali- ja terveydenhuoltoympäristössä laitteistojen ja tietojärjestelmien häiriöt voivat johtua useasta eri asiasta. Häiriötilanteet voivat syntyä ennalta-arvaamattomasti esimerkiksi kyberhyökkäyksen tai luonnonkatastrofin seurauksena, tai inhimillisesti, kun järjestelmiä ja laitteistoja päivitetään, muokataan tai muutetaan. Aina ei tiedetä, onko häiriö syntynyt vahingossa inhimillisten virheiden takia,

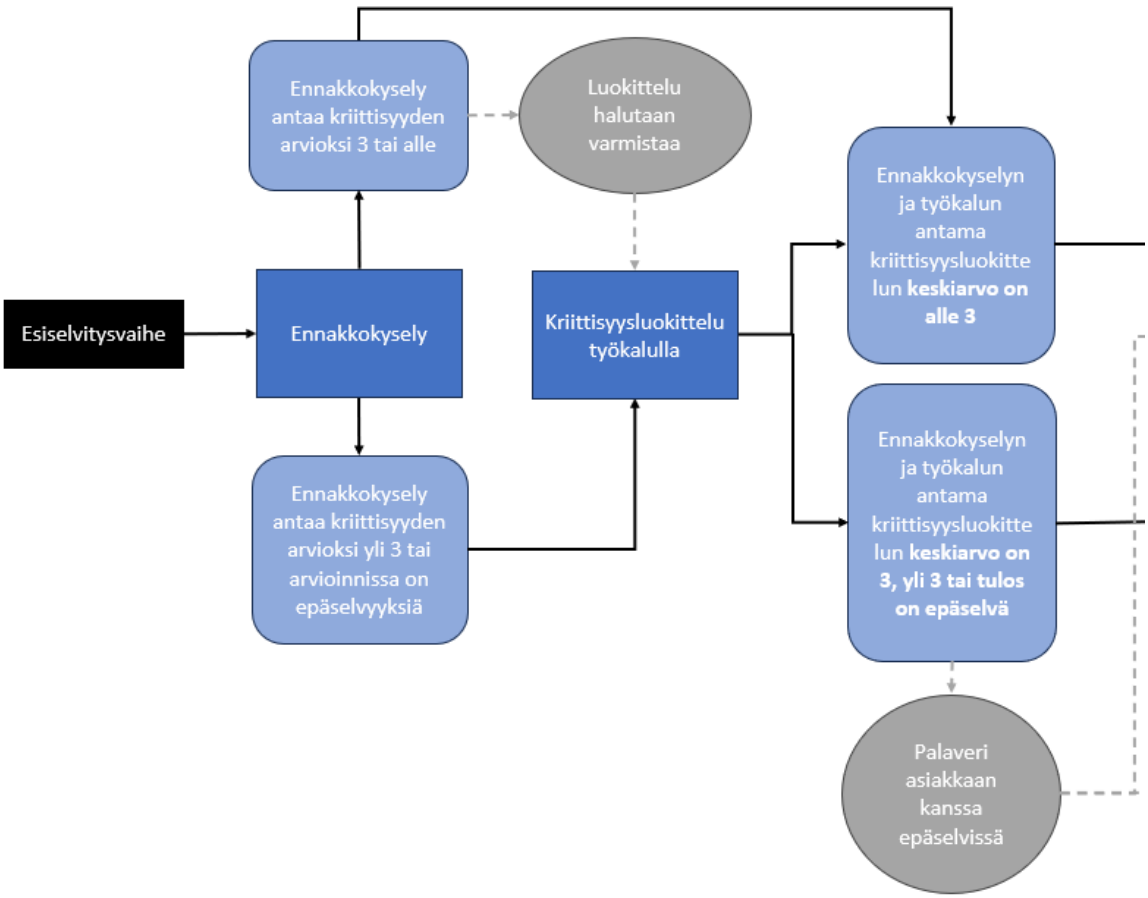
vaiko tahallisesta toiminnasta. Jos potilasturvallisuus vaarantuu tietojärjestelmän, laitteiston tai toiminnon häiriön vuoksi, on palveluntuottajan ja järjestelmän omistajan velvollisuus tehdä siitä erillinen ilmoitus Valviralle ja/tai Fimealle (Kanta 2024, luku ”Ilmoitus muille viranomaisille”).

Lääkintälaitteistojen viat saattavat olla ennakoitavissa, joka nopeuttaa niiden korjaamista. Usein laitteen omistajalla on näkemys mahdollisista riskeistä, jotka laitteeseen liittyvät. Laitteistot sisältävät usein ohjelmistoja, jotka pyörivät laitteen ohessa ja nämä saattavat sisältää vikoja, viallisia päivityksiä, vanhoja päivityksiä tai muita riskejä ja sitä kautta tuoda haavoittuvuuksia esille, joka mahdollistaa häiriöiden synnyn. (Vuorinen 2019, 19–20.) Suuri riski laitteissa on myös terveydenhuollon toimijoiden avaamat yhteydet oman sisäverkkonsa ja internetin välille, joka tuo omat riskinsä ja häiriön mahdollisuudet esille, jollei riskejä kartoiteta ja suojata tarpeellisin keinoin. (Vuorinen 2019, 10).

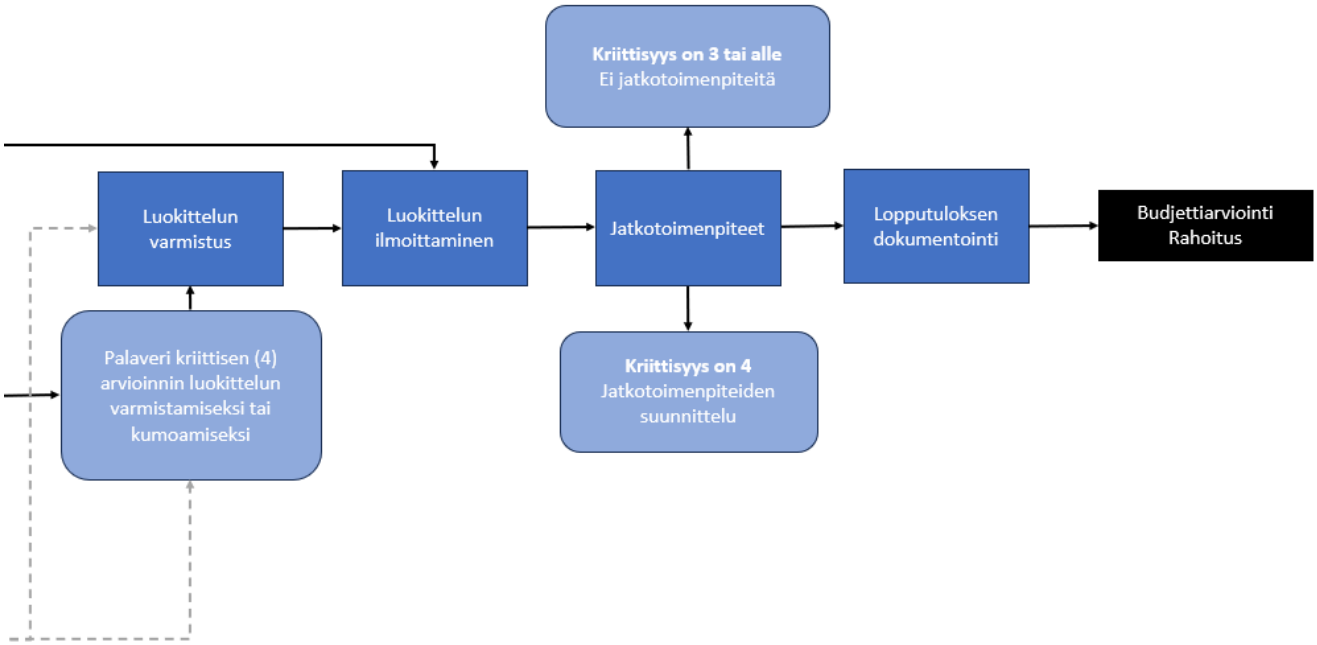
Pohteella havaituista ja suunnitelluista häiriötilanteista informoidaan työntekijöitä tarvittaessa sähköpostitse ja Pohteen Ilona-lähiverkossa, jota käytetään organisaation sisäiseen viestintään ja tietojenkäsittelyyn. Työntekijät voivat myös itse ilmoittaa huomatessaan häiriötilanteen, jos häiriö liittyy suoraan tai edes osittain Pohteen järjestelmiin, toimintoihin tai laitteistoihin.

5 KRIITTISYYDEN MÄÄRITYSPROSESSI LAITTEILLE JA TIETOJÄRJESTELMILLE

Jotta kriittisyysluokittelutyö onnistuisi ja tavoitteet täytettäisiin, on yhtenäistettävä ja sovittava käytettävistä työmenetelmistä ja toimintatavoista. Kriittisyysluokittelu ei saisi olla liian raskas ja aikaa vievä, vaan helposti sujuva ja selkeä toteuttaa. Luokittelussa hyödynnetään mahdollisimman paljon jo kerättyä tietoa eri kriittisyysluokittelutavoista ja työkaluista. Luokittelu pyritään hoitamaan siten, että laitteiston tai tietojärjestelmän omistaja pystyy selvissä tapauksissa tekemään luokittelun itsenäisesti. Ihanteellisessa tilanteessa prosessi lähtee käyntiin heti, kun Pohteen asiakaspalveluyksikkö tai tietojärjestelmistä tai laitteistoista vastaavat yksiköt aloittavat asiakkaan kanssa esiselvitysvaiheen (KUVIO 4) ja luokittelun tulisi olla valmiina ennen budjettiarviointia ja rahoituksen hakemista (KUVIO 5) (Huhtala 2024).



KUVIO 4. Esimerkki kriittisyysluokitteluprosessin alusta



KUVIO 5. Esimerkki kriittisyysluokitteluprosessin lopusta

Kriittisyysluokittelua voidaan helpottaa jaksottamalla eri työvaiheet kategorioihin esimerkiksi näin: ennakkokysely ja kriittisyysluokittelu työkalulla, toimenpiteet, luokittelun varmistaminen/ilmoittaminen, jatkuvuuden toteutus, tulosten dokumentointi.

5.1 Ennakkokysely

Tietojärjestelmien ja laitteiden kriittisyydestä asiakas ohjataan tekemään itsenäisesti ennakkokysely esiselvitysvaiheessa, jonka avulla selvitetään alustava kriittisyyden taso tietojärjestelmälle tai laitteelle. Kysymykset muotoillaan sopimaan mahdollisimman laajasti eri tietojärjestelmiin ja laitteisiin, jonka voi lähettää tai ohjata omistajalle ennakkoon uuden laitteen tai järjestelmän tullessa esiselvitettäväksi. Asiakas antaa oman arvionsa kriittisyydestä esimerkkien ja kysymyksen vastausvaatimuksien mukaisesti.

5.2 Kriittisyysluokittelu työkalun avulla

Tapauksissa, joissa ennakkokyselyn perusteella luokitteluarvioksi saadaan tärkeä (3) tai kriittinen (4), ohjataan asiakas tekemään luokittelu vielä työkalun avulla, jotta laitteen tai tietojärjestelmän kriittisyysluokittelusta saadaan mahdollisimman tarkka ja laaja näkemys.

Jos halutaan, niin alemmat ennakkokyselystä saadut luokittelut, vähäinen (1) ja normaali (2), voidaan varmistaa vielä työkalulla tehtävän kriittisyysluokittelun avulla, tai siirtyä suoraan luokitteluarvion ilmoittamiseen ja jättää tämä vaihe kokonaan välistä.

Jos asiakas epäilee ennakkokyselyn perusteella saadun kriittisyysarvion todenmukaisuutta tai tilanne on muuten epäselvä, voi asiakas tehdä kriittisyysluokittelun työkalun avulla ennakkokyselyn lisäksi ja vertailla tuloksia keskenään. Jos tulokset poikkeavat paljon toisistaan, esimerkiksi ennakkokysely antoi tuloksen normaali (2), mutta työkalu tuloksen kriittinen (4), voidaan tuloksen varmistamiseksi pitää yhteispalaveri tietoturvatiimin ja laitteeseen tai tietojärjestelmään liittyvän ammattihenkilöstön kanssa.

5.3 Yhteispalaveri

Riippuen saadusta luokitteluarviosta, voidaan määrätä yhteispalaveri liittyen järjestelmään tai laitteeseen. Jos annettavista ennakkotiedoista selviää ja ollaan varmoja, ettei laite tai tietojärjestelmä ole kriittinen, ei palaveria välttämättä tarvita. Kuitenkin, jos ennakkoon tehdyssä kriittisyysluokittelussa esiintyy minkäänlaisia epäselvyyksiä, voidaan pitää yhteinen palaveri laitteen tai tietojärjestelmän omistajan kanssa selvyyden saamiseksi.

Jos järjestelmä tulee luokitelluksi kriittiseksi (4) tai tärkeäksi (3) ennakkokyselyn ja/tai työkalusta saatavan kriittisyysarvion keskiarvon perusteella, voidaan tietojärjestelmän tai laitteen omistajan kanssa käydä yhteispalavereita ja varmistaa yhdessä laitteen tai järjestelmän kriittisyyden taso. Apuna voidaan käyttää roolikohtaisia haastatteluja tai moniammatillista tiimiä liittyen käsiteltävissä olevaan järjestelmään tai laitteeseen, jotta saadaan parempi kokonaiskuva ja eri näkemyksiä käsiteltävästä kriittisestä järjestelmästä tai laitteesta ja siitä, ovatko ne oleellisia potilasturvallisuuden kannalta.

5.4 Luokittelun varmistaminen ja ilmoittaminen

Kriittisen luokittelun varmistamisen avuksi voidaan palavereiden mukaan kutsua tarvittaessa esimerkiksi johdon-, lääkäri-, kliinisen yksikön tai hoitotyön edustajia tai ICT- ja tietoturva-asiantuntijoita, jotka yhdessä laitteiston tai järjestelmän omistajan kanssa käyvät läpi prosessin ja saavat kattavan kokonaiskuvan laitteen tai järjestelmän kriittisyydestä. Tarkoituksena on, että pääsääntöisesti tietoturvatiimi vastaa luokittelun varmistamisesta ja tarvittaessa avuksi voidaan ottaa muita, enemmän siltä osa-alueelta tietäviä henkilöitä. Jos laitteen tai tietojärjestelmän kriittisyysluokaksi varmistetaan korkein mahdollinen kriittisyystaso (4) ja joissakin tapauksissa myös tärkeän tason (3), täytyy miettiä ratkaisuja laitteen tai järjestelmän jatkuvuuden varalle.

Ennakkokyselyn ja työkalulla tehdyn kriittisyysluokitteluarvion keskiarvo täytyy ilmoittaa tietoturvatiimille, joka siirtää järjestelmän tai laitteen tiedot ja saadun luokittelun erikseen sovittuun paikkaan odottamaan sitä, tuleeko laite tai tietojärjestelmä Pohteen käyttöön. Tietoturvatiimi kuittaa luokittelun oikeaksi ja määrää jatkotoimenpiteistä tärkeiden (3) ja kriittisten (4) laitteiden ja tietojärjestelmien kohdalla. Terveydenhuoltoympäristössä pyritään siihen, ettei kriittisiksi määriteltyjä laitteistoja tai järjestelmiä olisi kovinkaan montaa (Mainio 2024).

5.5 Jatkuvuuden toteuttaminen kriittisille laitteille ja tietojärjestelmille

Kaikista korkeimman tason (4) ja osalle tärkeän tason (3) kriittisyysluokittelun saaneille laitteille ja tietojärjestelmille täytyy tehdä erillinen suunnitelma sen toiminnan sujuvalle jatkuvuudelle erilaisissa häiriötilanteissa. Jatkuvuutta voidaan parantaa useilla eri menetelmillä, joilla varmistetaan potilaiden turvallinen ja sujuva hoito sekä terveydenhuoltotoiminnan häiriöttömyys. Jos luokittelu on tehty väärin tai kriittisen laitteen tai järjestelmän toiminnan jatkuvuutta ei ole turvattu tarpeeksi vahvasti, voi hetkellinenkin häiriötilanne aiheuttaa pahimmillaan potilaan hoidon vaarantumisen, vammautumisen tai jopa hengenvaaran. Jatkuvuuden toteuttaminen on jatkuvaa työtä luokitteluprosessin tekemisen jälkeen. (Mainio 2024.) Alla muutama esimerkki, joiden avulla voidaan parantaa laitteen tai tietojärjestelmän toiminnan jatkuvuutta häiriötilanteen sattuessa.

5.5.1 Palvelimet

Palvelimilla on useita eri tehtäviä digimaailmassa. Palvelimien tarkoituksena on toimia esimerkiksi verkkosivujen isännöinnissä Hypertext Transfer Protocol ja Hypertext Transfer Protocol Secure-protokollien (HTTP- ja HTTPS) avulla tai hallinnoimassa tietokantapalveluita ja vastaamassa tietokantakyselyihin. Se voi toimia proxy-palvelimena asiakkaan ja muiden palvelimien välillä tai Domain Name System-palvelimena (DNS), jonka tehtävänä on muuttaa verkkotunnukset IP-osoitteiksi (Internetin protokollaosoite). Yksinkertaistettuna palvelimet toimivat kaiken taustalla vastaamassa pyyntöihin, käsittelemässä tietoja, hallitsemassa verkkoja ja yhteyksiä ja tarjoamassa tarvittavia palveluita tai resursseja asiakkaille. Palvelimet voivat olla joko fyysisiä tai virtuaalisia. (Mainio 2024.)

Fyysinen palvelin on tietokonejärjestelmä, jota ajetaan yleensä omasta konesalista käsin. Fyysinen palvelin on laite, joka sisältää tehokkaita komponentteja, jotka on suunniteltu kestämään ja ajamaan raskaita työkuormia. Laitteen komponentteja ovat esimerkiksi prosessorit, verkkokortit, liitäntäportit, kiintolevyt ja keskusmuistit. Fyysinen palvelin sisältää palvelinkäyttöjärjestelmän ja on yleensä kytkettynä luotettaviin ja nopeisiin verkkoyhteyksiin. (Lavanko 2019a.)

Virtuaalinen palvelin on ohjelmallisesti luotu ympäristö, joka joko ajetaan fyysisen palvelimen päällä olevan virtualisointiohjelmiston (Hypervisor) avulla. Virtuaalipalvelinta voidaan ajaa suoraan isäntäkäyttöjärjestelmän päällä (Hosted, type 2) tai ajetaan suoraan laitteiston päällä ilman isäntäkäyttöjärjestelmää (Bare-metal, type 1). Yhdellä fyysisellä palvelimella voi samanaikaisesti olla käynnissä useita eri virtuaalipalvelimia, jotka ovat eristetty toisistaan. Virtuaalisen palvelimen etuja ovat sen tehokas fyysisen palvelimen resurssien jakaminen muiden virtuaalisten palvelinten kesken, kustannussäästöt virrankulutuksessa, tilan tarpeessa ja fyysisissä komponenteissa, se nopeuttaa toipumista ongelmatilanteissa ja parantaa järjestelmän vikasietoisuutta ja virtuaalisen palvelimen käyttöönotto on nopeampaa verrattuna fyysisen palvelimen konfigurointiin ja asentamiseen. Virtuaalisia palvelimia on helppo luoda lisää ja poistaa tarpeen mukaan, kun on tarve testata ja kehittää uutta. (Lavanko 2019b.)

Jos laite tai järjestelmä luokitellaan kriittiseksi (4), ja joissakin tapauksissa myös tärkeäksi (3), tulee sen toiminta turvata molemmilla, fyysisellä ja virtuaalisella palvelimella. Kun toiminta on suojattu usealla palvelimella, ei yhden virtuaalipalvelimen ongelmat vaikuta saman fyysisen palvelimen tai sitä kautta pyöriviin muihin virtuaalisiin palvelimiin. Jos virtuaalipalvelinta pyörittävä fyysinen palvelin vaurioituu tai lakkaa toimimasta, voidaan kaikki virtuaalipalvelimet automaattisesti ja nopeasti käynnistää toisessa fyysisessä palvelimessa. Tällä tavoin voidaan turvata järjestelmän tai laitteen palvelinten häiriöttömyys, minimoida riskejä ja reagoida nopeasti ongelmatilanteen sattuessa. Muissa kuin

kriittiseksi luokitelluissa laitteissa ja järjestelmissä riittää, että palvelin ajetaan joko fyysisenä omasta konesalista tai virtuaalisena palvelimena. (Mainio 2024.)

5.5.2 Kuormantasaus

Kuormantasauksen tarkoituksena on tasapainottaa esimerkiksi verkkosivujen dataliikennettä kahden eri palvelimen ja maantieteellisesti eri paikassa olevien asiakaskuntien välillä (Tapio 2023, 1). Kuormantasauksella vältetään palvelimen ylikuormittuminen, jolla taas parannetaan palvelimen skaalautuvuutta, viansieto- ja kantokykyä ja palvelun saatavuutta. (Tapio 2023, Tiivistelmä).

Jos laite tai järjestelmä luokitellaan kriittiseksi (4) tai tärkeäksi (3) ja näiden toimintaa pyörittävät palvelimet on varmistettu kuormantasauksella, ei tarvitse pelätä suuren dataliikenteen aiheuttamaa laitteen tai järjestelmän ylikuormittumista. Ylikuormittuminen voi hidastaa laitteen tai järjestelmän toimivuutta, aiheuttaa vikoja tai pahimmillaan kaataa koko laitteen tai järjestelmän.

5.5.3 Kahdennus

Kahdennuksella voidaan pyrkiä tasaamaan kuormaa. Kahdennuksella voidaan tarkoittaa jonkin palvelun, kriittisen osan tai laitteen tuplaamista järjestelmässä, laitteissa tai verkossa. Kahdennuksen tarkoituksena on estää Single Point of Failure (SPOF)-pisteiden syntymistä ja maksimoimaan palvelun käyttöajan. Tällaisen pisteen syntyminen johtaa koko järjestelmän vikaantumiseen, vaikka muuta vikaa järjestelmässä ei olisi toimivuuden kannalta. (Avinetworks.) Kahdennus avulla voidaan toteuttaa joko aktiivi/passiivi tai aktiivi/aktiivi -tavoilla.

Aktiivi/passiivi -tilalla tarkoitetaan sitä, kun passiivilaite odottaa, että aktiivilaite vikaantuu. Laitteiden välinen yhteys havaitsee heti, mikäli aktiivitilassa oleva laite vikaantuu ja passiivitilassa oleva laite voi ottaa aktiivilaitteen paikan ja aloittaa toimintansa. Laitteiden asetukset synkronoituvat keskenään, jotta passiivilaitteen aloittama toiminta käynnistyy yliheiton seurauksena. (Palo Alto Networks 2014.)

Aktiivi/aktiivi -tilalla tarkoitetaan sitä, että laitteiden asetukset ja istunnot synkronoituvat jatkuvasti. Laitteet tarkastelevat jatkuvasti myös toistensa tilaa, ja mikäli yhteydessä havaitaan ongelmia, toimiva

laite ottaa itselleen ajettavaksi kaikki toiminnot toiselta laitteelta. Aktiivi/aktiivi -tilassa laitteet tukevat kuormantasausta. (Palo Alto Networks 2014.)

Jos laite tai järjestelmä luokitellaan kriittiseksi (4) tai tärkeäksi (3) ja kahdennetaan niiden toimintaan vaadittavat komponentit, ei laitteen kaatuminen, käyttökatkos tai vikaantuminen haittaa, koska toiminta on varmistettu kahdennuksen avulla.

5.5.4 Testiympäristö ja testaus

Tärkeiden (3) ja kriittisten (4) laitteiden ja tietojärjestelmien uudet päivitykset ja asennukset täytyy testata ennen käyttöönottoa. On mahdollista, että uusien päivitysten tai asennuksien mukana tulee ennalta-arvaamattomia ongelmia, jotka voivat aiheuttaa katkoksia, hitautta tai muita häiriötilanteita laitteen tai tietojärjestelmän toimintaan. Siksi on tärkeää, että uudet asennukset ja päivitykset testataan hyvin ennen käyttöönottoa etenkin tärkeiden ja kriittisten laitteiden ja järjestelmien kohdalla.

Testaaminen voidaan toteuttaa erilaisilla tavoilla. Ensimmäisessä tavassa testiympäristö toteutetaan kopioimalla järjestelmä tai laite. Uudet päivitykset ja asennukset tehdään ensiksi kopioversioon ja pidetään käynnissä esimerkiksi useita päiviä. Jos järjestelmän tai laitteen toiminta jatkuu normaalisti eikä häiriöitä synny, voidaan uudet päivitykset ja asennukset ladata myös olemassa olevaan järjestelmään tai laitteeseen. Nykyään ei ole niin tärkeää, vaikka uusinta viruspäivitystä ei saada käyttöön heti saman päivän aikana. (Mainio 2024.)

Toisessa tavassa uudet päivitykset ja asennukset tehdään suoraan vähemmän kriittisille järjestelmille, joiden vikaantuminen ei haittaa sairaalaympäristön toimintaa. Testaamiseen voidaan käyttää esimerkiksi kymmeniä laitteita tai järjestelmiä sairaalaympäristössä, johon uudet päivitykset ja asennukset tehdään suoraan. Viikon pyörimisen jälkeen tilanne tarkastetaan, ja jos niiden toiminta on jatkunut normaalina eikä häiriöitä ole syntynyt, voidaan päivitykset ja asennukset ladata muihin järjestelmiin ja laitteisiin. (Mainio 2024.)

5.6 Tulosten dokumentointi

Tulosten dokumentoinnin tarkoituksena on tallentaa käytössä olevien kriittisyysluokiteltujen laitteiden ja tietojärjestelmien kriittisyysluokka yhteen paikkaan, josta tämän tiedon saatavuus on helposti saatavilla joka tilanteessa. Häiriötilanteen tai katkoksen aikana laitteiden ja järjestelmien luokat voidaan nopeasti saada selville ja keskittää käytössä olevat resurssit kaikista kriittisimpien laitteiden ja järjestelmien toimintaan, jotta isoilta vahingoilta vältyttäisiin.

Kun laitteen tai tietojärjestelmän kriittisyysluokittelu on saatu päätökseen ja kriittisten (4) ja tärkeiden (3) luokittelu on saatu varmistettua, tulee tulokset dokumentoida yhteiseen sovittuun paikkaan. Ennen kuin järjestelmää tai laitetta otetaan käyttöön, täytyy tulokset dokumentoida erilliseen paikkaan odottamaan järjestelmän tai laitteen mahdollista käyttöön tuloa. Arvioita ei voida siirtää Pohteelle ennen kuin käyttöönotto on täysin varmistettuna (Huhtala 2024).

Jos järjestelmä tai laite tulee käyttöön, voidaan tiedot siirtää Pohteen omaan käyttöön. Pohteella yhteiseksi paikaksi on suunniteltu Digiturva-sivustoa, jonne käytössä olevat laitteet ja järjestelmät kootaan kriittisyysluokittelun perusteella. Digiturva on yhdistetty Teams-sovellukseen, jolloin tiedot ovat aina saatavilla häiriöistä huolimatta. Tuloksia tulisi päivittää säännöllisesti, koska laitteiden ja järjestelmien sisältö ja riippuvuudet saattavat muuttua esimerkiksi päivitysten myötä.

6 ENNAKKOKYSELYN TOTEUTUS

Ennakkokyselyn toteutus tehdään laitteiden ja tietojärjestelmien esiselvitysvaiheessa. Ennakkokyselyn avulla saadaan karkea arvio laitteen tai järjestelmän kriittisyydestä, kun laitteen tai tietojärjestelmän omistaja tekee itsearvioinnin ennakkokyselyn avulla. Koko hankintaprosessin näkökulmasta laitteen tai järjestelmän kriittisyyden arviointi tulee aloittaa heti esiselvitysvaiheessa asiakaspalveluyksikössä ja luokittelun tulee olla tehtynä ennen rahoituksen hakemista, koska kriittisimmät järjestelmät ja laitteet aiheuttavat muita suuremmat kustannukset ja ne tulisi pystyä ennakoimaan budjettiarvioinneissa (Huhtala 2024).

6.1 Kriittisyysluokka itsearvioinnin avulla

Ennakkokysely tietojärjestelmän kriittisyysluokasta yhdistetään jo olemassa olevaan tietojärjestelmien esiselvitysvaiheeseen. Asiakas ohjataan antamaan oma arvionsa tietojärjestelmän kriittisyydestä sairaalaympäristössä, kun kysymyksenä on: ” Millaisia vaikutuksia tietojärjestelmän 2 tunnin virka-aikana tapahtuvalla käyttökatkolla saattaa olla?” (LIITE 2).

Asiakas saa neljä vaihtoehtoa, joista valita yksi esimerkkijärjestelmien ja kysymyksen vastauksen perusteella. Jos asiakas punnitsee kahden vaihtoehdon välillä, kannattaa hänen valita niistä kriittisemmän tason vaihtoehto.

Vähäinen (1)

”Vähäisen tason tietojärjestelmän toimimattomuus voi vaikeuttaa potilaan hoitoa. Tietojärjestelmän toimintakatkos saattaa aiheuttaa alle kymmenen tuhannen euron vahingot, olla merkittävän mainehaitan riskitekijä, vaikeuttaa lakisääteisten tehtävien hoitamista tai aiheuttaa riskin ydintoimintojen häiriölle. Asiakas joutuu käyttämään varajärjestelyitä tai ratkaisuja.

Vähäisiä, tason 1 tietojärjestelmiä voivat olla esimerkiksi työaikaleimaus ja taukojumppasovellus.”

Normaali (2)

”Normaalin tason tietojärjestelmän toimimattomuus voi estää potilaan kiireettömän hoidon. Tietojärjestelmän toimintakatkos saattaa aiheuttaa yli kymmenen tuhannen euron vahingot tai merkittävän mainehaitan, estää lakisääteisten tehtävien hoitamisen tai aiheuttaa häiriön ydintoimintoihin. Asiakas on täysin riippuvainen tietojärjestelmän toiminnasta.

Normaaleja, tason 2 tietojärjestelmiä voivat olla esimerkiksi digisanelu, materiaalintilausjärjestelmät ja hoitajakutsujärjestelmä.”

Tärkeä (3)

”Tärkeän tason tietojärjestelmän toimimattomuus voi estää potilaan kiireellisen hoidon tai aiheuttaa väliaikaisen terveydellisen haitan. Tietojärjestelmän toimintakatkos saattaa aiheuttaa yli sadantuhannen euron vahingot. Tietojärjestelmä on oleellinen ydintoimintojen toiminnassa, ja katkos voi estää ydintoimintojen toiminnan kokonaan yhdessä tai useammassa yksikössä.

Tärkeän, tason 3 tietojärjestelmiä voivat olla esimerkiksi Verso (verien tilausjärjestelmä) ja Nearis (kuvantamisjärjestelmä).”

Kriittinen (4)

”Kriittisen tason tietojärjestelmän toimimattomuus voi aiheuttaa mahdollisuuden potilaan hengenvaaraan tai pysyvään haittaan. Tietojärjestelmän toimintakatkos saattaa aiheuttaa yli 1 miljoonan euron vahingot. Tietojärjestelmä on oleellinen ydintoimintojen toiminnassa, ja katkos voi estää ydintoimintojen toiminnan kokonaan yhdessä tai useammassa yksikössä.

Kriittisen, tason 4 tietojärjestelmä voi olla esimerkiksi Esko-potilastietojärjestelmä.”

Alustavien suunnitelmien mukaan laitteiden kriittisyysluokittelu itsearvioinnin avulla tullaan toteuttamaan lähes samalla tavalla ja samoilla vaatimuksilla kuin tietojärjestelmien (LIITE 3). Laiteinvestoinneilla ei kuitenkaan tällä hetkellä ole käytössä selkeää esiselvitysvaihetta tai -lomaketta, joten laitteiden kriittisyysluokittelun ennakkokysely jää vielä suunnitteluasteelle ja otetaan käsittelyyn, kun tietojärjestelmien kriittisyysluokitteluprosessi on saatu valmiiksi.

6.2 Ennakkokyselyn kriittisyysarvio

Selvissä tapauksissa, jossa laitteelle tai järjestelmälle saadaan kriittisyydeksi vähäinen (1) tai normaali (2) ennakkokyselyn avulla, voidaan luokittelu lyödä lukkoon. Ennakkokyselynlomakkeen tarkoituksena on eritellä kriittiset (4) ja tärkeät (3) laitteet ja järjestelmät erilleen muista. Ennakkokyselyn tuloksen vahvistamiseksi asiakas voi käyttää kriittisyysluokittelutyökalua kyselyn ohella ja verrata näiden tuloksia keskenään. Jos ennakkokyselyn ja Excel-työkalun antamat tulokset eroavat paljon toisistaan tai ylittävät keskiarvoltaan arvon 3 (Tärkeä) tai ovat yhtä suuria kuin 3, on hyvä olla yhteydessä ja keskustella ammattilaisten kanssa laitteen tai järjestelmän kriittisyysluokittelun vahvistamiseksi tai kumoamiseksi.

Ennakkoselvityksen lähtökohtana oli muotoilla se siten, ettei ristiriitoja tai muita epäselvyyksiä synny, ja sen tuli olla selkeä ja itsenäisesti täytettävissä asiakkaan näkökulmasta. Kysymyksen, esimerkkien ja vastauksien täytyi olla tarpeeksi selkeitä, jotta kriittisyysarviosta saatiin mahdollisimman realistinen.

Kävimme yhdessä läpi eri vaihtoehtoja ennakkokyselyn toteutukselle, ottaen huomioon asiakaspalveluyksikön ja laite- ja tietojärjestelmäpuolen investoinneista vastaavien mielipiteet ja näkökulmat. Tällä tavoin vältyimme päällekkäisyyksiltä heidän laatimien kysymyksien kanssa. Tulimme siihen lopputulokseen, että asiakkaalle on tarpeellista antaa esimerkkejä kyseisen luokan tietojärjestelmistä ja laitteista, joka parantaa asiakkaan oman tietojärjestelmän kriittisyyden hahmottamista. Kysymyksessä puhutaan virka-ajalla tapahtuvasta kahden tunnin katkoksesta, jonka tarkoituksena on rajata käyttökatko tiettyyn hetkeen. Asiakkaan on helpompi tunnistaa tästä aiheutuvat häiriötilanteet ja yhdistää oma laitteensa tai tietojärjestelmänsä vastaamaan oikeaa kriittisyysluokkaa ja tilannetta ja siitä aiheutuvia riskejä.

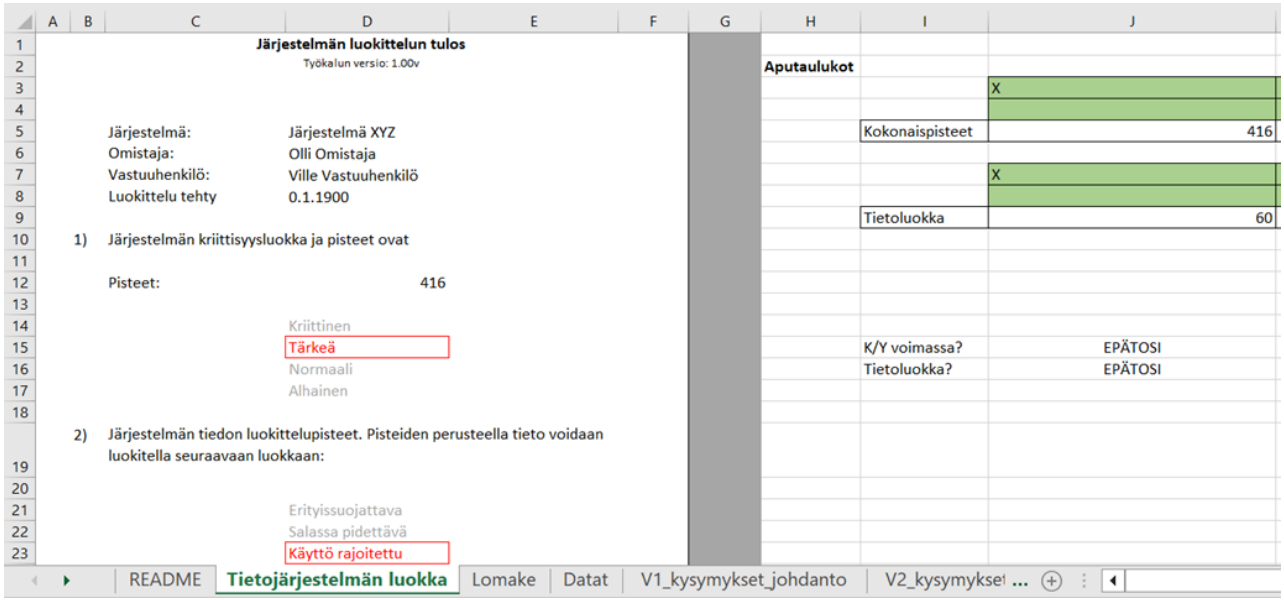
7 TYÖKALUN TOTEUTUS

Perehdyn kriittisyysluokitteluun eri aloilla muiden opinnäytetöiden kautta, joista peilaan ja sovellan kehittämisideoita luokittelutapoihin ja kriteereihin sote-alalla. Käymme yhdessä tietoturvatiimin sisällä keskustelua ja palavereita halutusta projektin lopputuloksesta, joka opinnäytetyön yhteydessä rakennetaan toimivaksi kokonaisuudeksi. Tutustun alan standardeihin ja niiden asettamiin vaatimuksiin sekä ohjeistuksiin, joita voidaan hyödyntää työkalun suunnittelussa mahdollisimman tehokkaasti.

Excel-pohjaisen laitteiden ja järjestelmien kriittisyysluokitteluun tarkoitetun työkalun tarkoituksena on tukea kriittisyysluokitteluarviota yhdessä ennakkokyselyn kanssa. Työkalu on tarkoitus toteuttaa jo olemassa olevien kriittisyysluokitteluun tarkoitettujen apuvälineiden pohjalta (KUVA 2) ja soveltaa siitä uusi, yksinkertainen työkalu kriittisyyden määrittämiseksi ja tarvittaessa tuodaan myös uusia näkökulmia kriittisyysluokittelun tueksi.

7.1 Toteutuksen lähtökohdat

Lähtökohtana on rakentaa työkalu tyhjään Excel-pohjaan, johon tehdään prototyyppi kriittisyysluokittelutyön työkalusta. Prototyyppiä kehitetään ja päivitetään yhdessä tietoturvatiimin kanssa kohti haluttua lopputulosta. Työkalua on tarkoitus testata myöhemmin käytännössä esimerkkijärjestelmillä yhdessä ennakkokyselyn kanssa, jotta kriittisyysluokittelu ja koko siihen liittyvä prosessi saadaan hiottua mahdollisimman realistiseksi. Testauksessa tullaan käyttämään apuna jo luokiteltuja järjestelmiä, jolloin painoarvot ja kriteerit saadaan skaalattua oikeanlaisiksi.

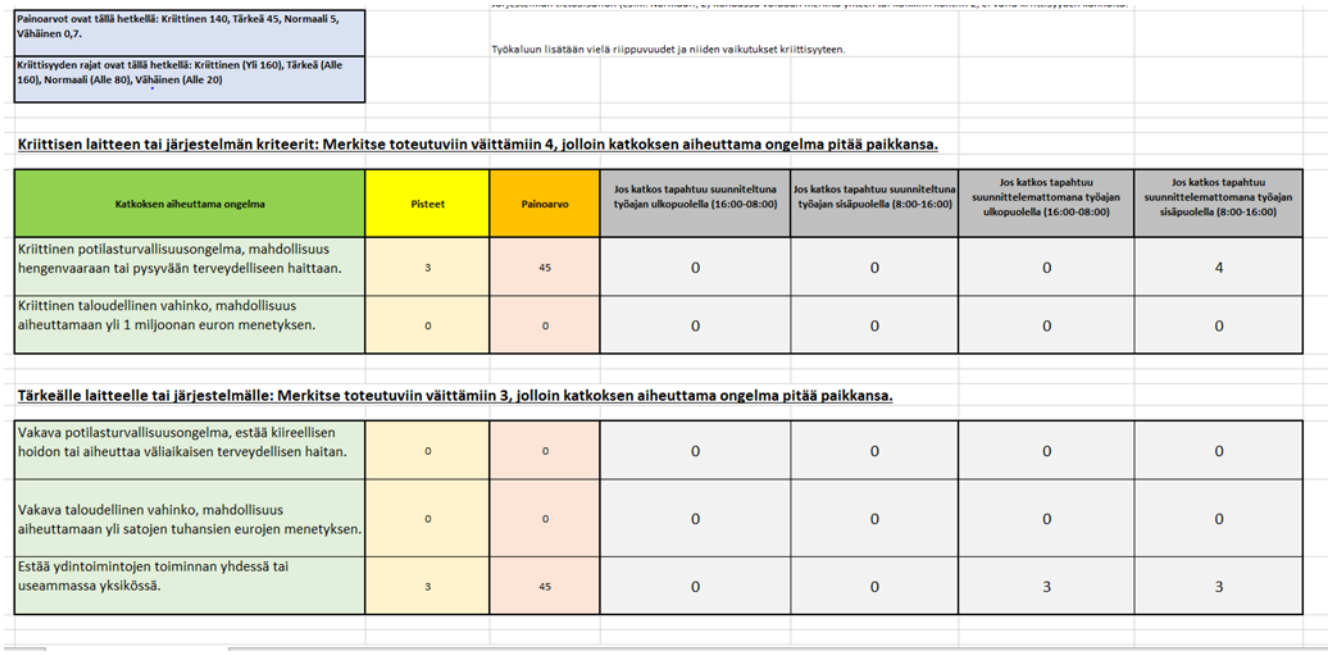


KUVA 2. Istekin kriittisyysluokittelun työkalu. Työkalu pohjautuu VAHTI-ohjeeseen ja PSHP:n dokumentointiin. Yksi opinnäytetyössä apuna olleista työkaluista (Liikamaa 2021)

7.2 Työkalun sisältö

Kriittisyysluokittelutyöhön tarkoitettu työkalu (LIITE 1) sisältää useita määritelmiä, riippuvuuksia ja arvoja, jotka vaikuttavat saatavaan kriittisyysluokitteluarvoon ja joilla koetaan olevan merkitystä kriittisyysluokittelua tehtäessä. Määritelmiä voidaan halutessa muokata, muuttaa, poistaa tai lisätä riippuen kriittisyysluokiteltavasta laitteesta tai järjestelmästä. Kuitenkin laitteen tai järjestelmän ennakkoon tehtävässä kriittisyysluokittelussa olisi arvot ja määritelmät hyvä pitää vakiona, jotta saadaan mahdollisimman yhtenäinen kuva kriittisyyden ennakkoarviosta laitteiden ja järjestelmien välillä.

Työkalu (KUVA 3.) sisältää ohjeet kriittisyysluokittelun tekemiseen. Väittämän kohdan perusteella annetaan arvo haluttuun kohtaan väliltä 1–4, jonka painoarvot työkalu laskee automaattisesti ja määrittää laitteelle tai järjestelmälle kriittisyyden näiden vastattujen kohtien perusteella. Osa arvoista saattaa muuttua riippuen häiriön suunnittelemattomuudesta tai suunnitellun käyttökatkon vuoksi, mutta työkalu toteutetaan siten, että se automaattisesti huomio ne laskuissa eikä käyttäjän itse tarvitse miettiä asiaa tarkemmin. Vaikka samalle riville tulisi koko rivi täyteen nelosia, ei työkalu laske niitä yhteen, vaan ottaa huomioon vain yhden suurimman riviin kuuluvan luvun.



Painoarvot ovat tällä hetkellä: Kriittinen 140, Tärkeä 45, Normaali 5, Vähäinen 0,7.
Kriittisyyden rajat ovat tällä hetkellä: Kriittinen (Yli 160), Tärkeä (Alle 160), Normaali (Alle 80), Vähäinen (Alle 20)

Työkaluun lisätään vielä riippuvuudet ja niiden vaikutukset kriittisyyteen.

Kriittisen laitteen tai järjestelmän kriteerit: Merkitse toteutuviin väittämiin 4, jolloin katkoksen aiheuttama ongelma pitää paikkansa.

Katkoksen aiheuttama ongelma	Pisteet	Painoarvo	Jos katkos tapahtuu suunniteltuna työajan ulkopuolella (16:00-08:00)	Jos katkos tapahtuu suunniteltuna työajan sisäpuolella (8:00-16:00)	Jos katkos tapahtuu suunnittelemattomana työajan ulkopuolella (16:00-08:00)	Jos katkos tapahtuu suunnittelemattomana työajan sisäpuolella (8:00-16:00)
Kriittinen potilasturvallisuusongelma, mahdollisuus hengenvaaraan tai pysyvään terveydelliseen haittaan.	3	45	0	0	0	4
Kriittinen taloudellinen vahinko, mahdollisuus aiheuttamaan yli 1 miljoonan euron menetyksen.	0	0	0	0	0	0

Tärkeälle laitteelle tai järjestelmälle: Merkitse toteutuviin väittämiin 3, jolloin katkoksen aiheuttama ongelma pitää paikkansa.

Vakava potilasturvallisuusongelma, estää kiireellisen hoidon tai aiheuttaa väliaikaisen terveydellisen haitan.	0	0	0	0	0	0
Vakava taloudellinen vahinko, mahdollisuus aiheuttamaan yli satojen tuhansien eurojen menetyksen.	0	0	0	0	0	0
Estää ydintoimintojen toiminnan yhdessä tai useammassa yksikössä.	3	45	0	0	3	3

KUVA 3. Kriittisyysluokittelutyökalun demoversio. Testailin pisteiden ja painoarvojen toimivuutta ja automatisointia halutun lopputuloksen mukaan. Lopulliset painoarvot saattavat poiketa kuvassa olevista

7.3 Arviointikriteerit

Laitteiden ja tietojärjestelmien arviointikriteerit, joista kaikkia kohtia ei tarvitse täyttää täyttääkseen tietyn kriittisyyden arvion. Jos johonkin kohtaan on annettu jo kriittisempi arvio, sitä ei tule merkata enää lievempien väittämien kohdalle. Arviointikriteerit on otettu Istekin kriittisyysluokittelutyökalusta ja PPSHP:n työkalusta ja nidottu yhdeksi, sovelletuksi kokonaisuudeksi. Arviointikriteerien tarkoituksena on erotella laitteet ja järjestelmät kriittisyyden perusteella. Arviointikriteerit ovat pääsääntöisesti samat kuin ennakkokyselyssä, mutta antavat tarkemman arvion kriittisyydelle automaattisesti. Työkalussa on myös otettu huomioon laitteen tai tietojärjestelmän sisältämä tietosisältö ja muut vaikuttavat tekijät.

Kriittiselle laitteelle tai järjestelmälle:
- Kriittinen potilasturvallisuusongelma, mahdollisuus hengenvaaraan tai pysyvään terveydelliseen haittaan.
- Kriittinen taloudellinen vahinko, mahdollisuus aiheuttaa yli 1 miljoonan euron menetyksen.

Tärkeälle laitteelle tai järjestelmälle:

- Vakava potilasturvallisuusongelma, estää kiireellisen hoidon tai aiheuttaa väliaikaisen terveydellisen haitan.
- Vakava taloudellinen vahinko, mahdollisuus aiheuttaa yli satojen tuhansien eurojen menetyksen.
- Estää ydintoimintojen toiminnan yhdessä tai useammassa yksikössä.

Normaalille laitteelle tai järjestelmälle:
- Kohtalainen potilasturvallisuusongelma, estää kiireettömän hoidon.
- Kohtalainen taloudellinen vahinko, mahdollisuus aiheuttaa yli kymmenien tuhansien eurojen menetyksen.
- Kohtalainen mainehaitta, aiheuttaa merkittävän mainehaitan.
- Järjestelmän tietosisältö, sisältää potilastietoja tai sosiaalihuollon asiakastietoja.
- Estää lakisääteisen tehtävän hoitamisen.
- Aiheuttaa häiriön tai saattaa aiheuttaa riskin ydintoimintojen toimimisen estymiselle yhdessä tai useammassa yksikössä.
- Asiakkaan toiminta on täysin riippuvainen laitteesta tai järjestelmästä.

Vähäisesti kriittiselle laitteelle tai järjestelmälle:
- Vähäinen potilasturvallisuusongelma, vaikeuttaa potilaan hoitoa.
- Vähäinen taloudellinen vahinko, mahdollisuus aiheuttamaan alle kymmenien tuhansien eurojen menetyksen.
- Vähäinen mainehaitta, aiheuttaa riskin merkittävälle mainehaitalle.
- Järjestelmän tietosisältö, sisältää TL IV tai muita salassa pidettäviä tietoja.
- Vaikeuttaa lakisääteisen tehtävän hoitamista.
- Saattaa aiheuttaa riskin ydintoimintojen häiriölle yhdessä tai useammassa yksikössä.
- Asiakas joutuu käyttämään varajärjestelyjä tai ratkaisuja.

7.4 Käyttökatkosarviointi

Käyttökatkon ajankohta ja pituus vaikuttaa laitteen ja järjestelmän kriittisyyteen huomattavasti. On täysin eri asia, jos järjestelmä on poissa käytössä normaalin toimistotyöajan (8.00–16.00) sisällä kuin sen ulkopuolella. Laitetta tai järjestelmää on hankalampi lähteä nopeasti korjaamaan työajan ulkopuolella, jos sen ylläpitoon ei olla erikseen varauduttu. Jos laitteen tai tietojärjestelmän täytyy olla käytössä 24/7, se tulee ottaa huomioon toimittajasopimuksissa. Käyttökatko saattaa potilasturvallisuuden kannalta vaikuttaa hoitopäätöksiin, hoitoon pääsy voi hidastua, hidastuttaa diagnooseja tai viivästyttää lääkkeiden jakelua ja aiheuttaa riskin virheille. Joskus joudutaan turvautumaan varajärjestelmiin, resursoimaan henkilökuntaa ja käyttämään manuaalisia prosesseja.

Käyttökatkon vaikutusarviointi on vaikea toteuttaa yksinkertaisesti kriittisyysluokitteluun. Täytyy ottaa huomioon käyttökatkon ajankohta, luokittelu, tapahtuuko katkos toimistotyöaikana tai sen ulkopuolella, ja kuinka kauan käyttökatkos voi olla yhteensä päällä ilman, että se aiheuttaa vakavaa haittaa. Käyttökatkon suunnittelulla ja suunnittelemattomuudella on myös vaikutuksia luokitteluun.

Suuntaa antavat arviot, kuinka kauan laite tai järjestelmä voi olla poissa käytöstä ilman merkittävää haittaa:

Työaikana (klo. 8.00–16.00):
- Kriittisessä laitteessa tai järjestelmässä alle 30 minuuttia.
- Tärkeässä alle 2 tuntia

- Normaalissa noin 4 tuntia.
- Vähäisessä noin 8 tuntia.

Työajan ulkopuolella (klo. 16.00–8.00):
- Kriittisessä laitteessa tai järjestelmässä alle 1 tunti.
- Tärkeässä alle 4 tuntia.
- Normaalissa noin 8 tuntia.
- Vähäisessä noin 16 tuntia.

7.4.1 Suunniteltu käyttökatko

Suunnitellun käyttökatkon aiheuttama ongelma pyöristää laitteen tai järjestelmän väittämän kriittisyyden ylöspäin. Tämä on otettu huomioon myös työkalun suunnittelussa, joka nostaa kyseistä arvoa ja samalle sen tuottamaa painoarvoa automaattisesti näissä tilanteissa. Jos samalla rivillä on muitakin numeroita täytettynä luvun tai lukujen ylentämisen jälkeen, ottaa taulukko huomioon laskuissa vain uuden, muita korkeamman luvun.

Jos suunnitellun käyttökatkon aikana laite tai järjestelmä aiheuttaa vakavan potilasturvallisuusongelman (Luokittelu vähintään: Tärkeä, 3), vakavan taloudellisen menetyksen (Luokittelu vähintään: Tärkeä, 3) tai estää täysin ydintoiminnan toimimisen (Luokittelu: Tärkeä, 3), pyöristää työkalu laitteen tai järjestelmän automaattisesti kriittiseksi (4) käyttökatkoarvioinnin kriittisyyden perusteella oikean väittämän kohdalle.

Jos suunnitellun käyttökatkon aikana laite tai järjestelmä aiheuttaa kohtalaisen potilasturvallisuusongelman (Luokittelu: Normaali, 2), kohtalaisen taloudellisen menetyksen (Luokittelu: Normaali, 2), häiriön tai riskin ydintoimintojen toimimisen estymiselle yhdessä tai useammassa yksikössä (Luokittelu: Normaali, 2), kohtalaisen mainehaitan (Luokittelu: Normaali, 2), estää lakisääteisten tehtävien hoitamisen (Luokittelu: Normaali, 2) tai jos asiakkaan toiminta on täysin riippuvainen laitteesta tai järjestelmästä (Luokittelu: Normaali, 2), pyöristää se laitteen tai järjestelmän automaattisesti tärkeäksi (3) käyttökatkoarvioinnin kriittisyyden perusteella oikean väittämän kohdalle.

7.4.2 Suunnittelematon käyttökatko

Suunnittelemattoman käyttökatkon ongelma pyöristää laitteen tai järjestelmän väittämän kriittisyyden alaspäin tai pitää sen samana. Tämä on otettu huomioon myös työkalun suunnittelussa, joka alentaa kyseistä arvoa ja samalla sen tuottamaa painoarvoa automaattisesti näissä tilanteissa. Jos samalla rivillä on muitakin numeroita täytettynä luvun tai lukujen alentamisen jälkeen, ottaa taulukko huomioon laskuissa aina vain korkeimman luvun kyseiseltä riviltä.

Jos suunnittelemattoman käyttökatkon aikana laite tai järjestelmä aiheuttaa kriittisen tai vakavan potilasturvallisuusongelman (Luokittelu: Tärkeä, 3 tai kriittinen, 4), kriittisen tai vakavan taloudellisen menetyksen (Luokittelu: Tärkeä, 3 tai kriittinen, 4) tai estää täysin ydintoiminnan toimimisen (Luokittelu: Tärkeä, 3), pyöristää se laitteen tai järjestelmän automaattisesti tärkeäksi (3) tai pitää sen samana käyttökatkoarvioinnin kriittisyyden perusteella oikean väittämän kohdalla.

Kuitenkin, jos suunnittelemattoman käyttökatkon aikana laite tai järjestelmä aiheuttaa kohtalaisen potilasturvallisuusongelman (Luokittelu: Normaali, 2), kohtalaisen taloudellisen menetyksen (Luokittelu: Normaali, 2), häiriön tai riskin ydintoimintojen toimimisen estymiselle yhdessä tai useammassa yksikössä (Luokittelu: Normaali, 2), kohtalaisen mainehaitan (Luokittelu: Normaali, 2), estää lakisääteisten tehtävien hoitamisen (Luokittelu: Normaali, 2) tai jos asiakkaan toiminta on täysin riippuvainen laitteesta tai järjestelmästä (Luokittelu: Normaali, 2), pitää se laitteen tai järjestelmän kriittisyyden samana (Normaali, 2) käyttökatkoarvioinnin kriittisyyden perusteella oikean väittämän kohdalla.

7.5 Riippuvuudet

Riippuvuudella tarkoitetaan sitä, kun laitteen tai tietojärjestelmän toiminta on riippuvainen joistakin toiminnoista. Riippuvuudet vaikuttavat kriittisyysluokkaan ja tietoturvavaatimuksiin laitteen tai järjestelmän osalta, sekä määrittävät jatkotoimenpiteistä näiden sujuvan häiriöttömän toiminnan turvaamiseksi. Riippuvuuksien aiheuttamat riskit tulee kartoittaa ja suojata, häiriötilanteiden varalle tulee tehdä varautumissuunnitelmat, valvonnan tulee olla jatkuvaa, toimintaa täytyy seurata ja näistä täytyy kerätä lokitietoja. Jokaisen toimijan täytyy noudattaa lainsäädäntöä, standardeja, sopimuksia ja vaatimuksia. Sairaalan kriittinen toiminta ja potilasturvallisuus eivät saa milloinkaan vaarantua riippuvuuksista huolimatta. (Mainio 2024.)

7.5.1 Pilviriippuvuus

Jos laite tai tietojärjestelmä on riippuvainen pilvipalveluista, vaatii se huolellista suunnittelua, ylläpitoa, valvontaa, seurantaa ja lainsäädännön tuntemusta. Pilveen kulkeva ja sieltä tuleva liikenne täytyy salata ja itse pilvessä säilytettävät tiedot tulee olla salattuina jatkuvasti, niin siirrossa kuin säilytyksessä. Myös rajapintaintegraatiot muihin järjestelmiin täytyy olla turvallisia ja säädösten mukaisia. Pilviympäristön täytyy olla varautunut häiriötilanteisiin varajärjestelmillä ja tietojen palautusmekaniikoilla. Lokitietojen kerääminen ja säilyttäminen pilviympäristöstä täytyy tehdä kattavasti tutkintojen, auditointien sekä seurannan vuoksi. (Mainio 2024.)

Pilvipalveluntarjoajan täytyy täyttää kaikki asiaankuuluvat lainsäädännölliset vaatimukset ja datan käsittelyn tulee tapahtua asiamukaisesti suojatussa ympäristössä. Pilvipalveluntarjoajan täytyy olla luotettava ja on varmistettava, että he tarjoavat riittävät tietoturvatoimenpiteeet ja tietojen varmuuskopiot. Heidän on noudatettava vaadittuja standardeja, sertifikaatteja ja tietosuoja- sekä tietoturvavaatimuksia. Pilvipalveluntarjoajan ja organisaation välille määritellään tarkat sopimukset, esimerkiksi SLA-sopimus, mihin määritellään tarkat palvelutasovaatimukset. Tietojen tulisi fyysisesti olla säilytettävänä Suomessa ja niihin pääsyn tapahtua Suomen sisällä, koska eri maiden väliset tietosuoja- ja tietoturvavaatimukset voivat vaihdella. (Mainio 2024.)

7.5.2 Internetriippuvuus

Jos laite tai tietojärjestelmä on riippuvainen internetistä, edellyttää se vahvoja teknisiä suojauksia, käyttäjien valvontaa ja seurantaa. Häiriötilanteiden varalle täytyy olla varautumissuunnitelma ja päivitykset kaikkiin kytköksissä oleviin laitteisiin tulee toteuttaa säännöllisin väliajoin, jotta haavoittuvuuksia ei päästä käyttämään hyväksi. (Mainio 2024.)

Kaikki internetin kautta tapahtuva tiedonsiirto tulee suojata vahvan salauksen avulla käyttämällä protokollia ja palomuureja. Järjestelmiin tai laitteisiin pääsyä rajoitetaan tietyille valtuutetuilla käyttäjille käyttäjäoikeuksin esimerkiksi roolien tai vastuiden mukaan, ja tunnistautumiseen tulisi vaatia monivaiheista Multi-factor Authentication-tunnistautumista (MFA). Myös internetin lokitietojen kerääminen ja säilyttäminen täytyy tehdä kattavasti tutkintojen, auditointien sekä seurannan vuoksi. Laitteilla on oltava varajärjestelmät, offline-toimintamahdolllisuudet ja huolto tai korjaus saatavilla mahdollisimman nopeasti, jos internetyhteys pääsee katkeamaan. (Mainio 2024.)

Kriittiset laitteet ja tietojärjestelmät tulee sijoittaa omille suojatuille verkkoalueilleen segmentoidun verkkoarkkitehtuurin mukaisesti, mikä mahdollistaa laitteiden ja tietojärjestelmien eristämisen muista verkon osista. (Mainio 2024.)

7.5.3 Sairaalaympäristön ulkopuoliriippuvuus

Sairaalaympäristön ulkopuoliriippuvuudella tarkoitetaan sitä, että laite tai tietojärjestelmän toiminta on jollain tavoin riippuvainen ulkopuolisesta toimijasta. Tällöin on tärkeää tehdä perusteellinen riskianalyysi kartoittamaan ulkopuolisiin riippuvuuksiin liittyvät tietoturvariskit ja niiden vaikutukset sairaalan toimintaan. (Mainio 2024.)

Tällaisissa tilanteissa sopimukset, esimerkiksi SLA-sopimus, ovat tärkeitä. Ne määrittelevät laitteen tai tietojärjestelmän toimintaan vaadittavat palvelutasovaatimukset ja muut vaadittavat vaatimukset. Palvelutasovaatimukset voivat sisältää tietoa, vastuita, tietoturvatoimenpiteitä ja käytettävyyteen tai vasteaikoihin liittyviä vaatimuksia. Kaikkien ulkopuolisten toimijoiden on noudatettava tietosuojalainsäädäntöä eli GDPR:ää, jos he käsittelevät tai säilyttävät tietoja sairaalan ulkopuolella. Tietoja tulee säilyttää Suomen sisäpuolella, koska lait ja vaatimukset voivat riippuvat maasta, missä niitä käytetään. Ulkopuolisten toimijoiden kanssa täytyy laatia SLA:n lisäksi myös tarvittavat Data Processing Agreement (DPA) tietojenkäsittelysopimukset. Kolmansien osapuolien täytyy noudattaa sairaalan tietoturvakäytäntöjä, sisältäen tietoturva-arvioinnit ja auditoinnit kolmansien osapuolten toiminnasta. (Mainio 2024.)

Häiriötilanteita varten täytyy ottaa huomioon varajärjestelmät ja palautumissuunnitelmat. Jos tiedot ovat riippuvaisia sairaalan ulkopuolisesta palvelusta, täytyy tiedot varmuuskopioida säännöllisin väliajoin ja säilyttää sairaalaympäristössä. (Mainio 2024.)

Voi olla tapauksia, että laite tai tietojärjestelmä on riippuvainen esimerkiksi ulkoisesta palveluntarjoajasta. Tällöin laitetta tai tietojärjestelmää ei voida luokitella kriittiseksi (4), koska sairaala ei itsessään pysty vaikuttamaan ulkopuolisten palveluntarjoajien kykyyn tarjota jatkuvaa palvelua ilman keskeytyksiä. Laitteen tai järjestelmän ollessa kriittinen (4), sen toiminta tulee toteuttaa pääsääntöisesti siten, että se ei ole riippuvainen sairaalaympäristön ulkopuolisesta toiminnasta. Joissakin tapauksissa voidaan käyttää VPN:ää tai muita suojattuja kanavia ulkoisten palveluiden ja järjestelmien välillä. (Mainio 2024.)

7.6 Painoarvot

Painoarvolla tarkoitetaan sitä, kuinka paljon jokin tietty asia vaikuttaa kriittisyyteen. Jokaisen arviointikriteerin, käyttökatkon vaikutusarvioinnin ja riippuvuuden arviointi tehdään kriittisyysasteikolle 1–4, jossa 1 (vähäinen), 2 (normaali), 3 (tärkeä) ja 4 (kriittinen). Painoarvojen yhteenlaskettu summa antaa laitteelle tai tietojärjestelmälle sen kriittisyysarvion. Jos arvo ylittää tärkeän (3) tai kriittisen (4) kriittisyyden rajan, tulee laitteen kriittisyys varmistaa ammattilaisten kanssa.

Työkalussa kriittisen kriteerin painoarvo on 80, tärkeän 20, normaalin 5 ja vähäisen 1. Tällä hetkellä työkalussa kriittisyysluokittelun rajoina on kriittiselle järjestelmälle yli 230, tärkeälle sama tai alle 230, normaalille sama tai alle 165 ja vähäiselle sama tai alle 86. Painoarvot ovat määritelty siten, että suurin osa järjestelmistä ja laitteista lajiteltaisiin alle kriittisen luokittelun.

Työkalun painoarvot olisi hyvä pitää ennakkoarvioinnissa vakiona. Painoarvojen muuttaminen tehdään myös mahdolliseksi, riippuen laitteesta tai järjestelmästä ja tilanteesta, koska joissakin tilanteissa painoarvot saattavat olla järkevä muuttaa. Arvojen muuttaminen tehdään mahdolliseksi siksi, että vaikka jokin laite tai järjestelmä voisi olla tietyssä ympäristössä kriittinen, ei se kuitenkaan aina päde, jos sama laite tai järjestelmä toimiikin jossain toisessa ympäristössä. Painoarvojen muuttaminen tehdään työkaluun siten, että koodit muokkautuvat muokattavien painoarvojen mukaan G-sarakkeelta, jolloin näitä on helpompi muuttaa halutuiksi. Tällä tavalla vältytään siltä, että jokainen koodi pitäisi erikseen käydä muuttamassa halutunlaiseksi. Painoarvot muuttuvat joissain tapauksissa suunnittelemattoman ja suunnitellun käyttökatkon mukaan (KUVA 4).

Kriittisen laitteen tai järjestelmän kriteerit: Merkitse toteutuviin väittämiin 4, jolloin katkoksen aiheuttama ongelma pitää paikkansa.

Katkoksen aiheuttama ongelma	Pisteet 1-4	Painoarvo 1-80	Jos katkos tapahtuu suunniteltuna työajan ulkopuolella (16:00-08:00)	Jos katkos tapahtuu suunniteltuna työajan sisäpuolella (8:00-16:00)	Jos katkos tapahtuu suunnittelemattomana työajan ulkopuolella (16:00-08:00)	Jos katkos tapahtuu suunnittelemattomana työajan sisäpuolella (8:00-16:00)
Kriittinen potilasturvallisuusongelma, mahdollisuus hengenvaaraan tai pysyvään terveydelliseen haittaan.	3	20	0	0	4	0
Kriittinen taloudellinen vahinko, mahdollisuus aiheuttamaan yli 1 miljoonan euron menetyksen.	4	80	4	0	0	0

KUVA 4. Työkalun painoarvomuutokset

8 PROSESSIN TESTAAMINEN JA TULOKSET

Kriittisyysluokitteluprosessia lähdettiin koeponnistamaan verien tilauspalvelujärjestelmän avulla. Pidimme palaverin (Hintsanen, Huhtala, Kuismin, Mainio, Rautio, Somero & Vahtola 2024) yhdessä kolmen verien tilauspalvelun käyttäjän kanssa kriittisyysluokitteluprosessista testataksemme, mihin luokkaan järjestelmä tulee luokitelluksi tämänhetkisen prosessin kautta. Kävimme keskustelua prosessista kokonaisuudessaan, kuinka luokittelua on tarkoitus hyödyntää ja mikä on prosessin keskeinen tarkoitus. Järjestelmä oli luokiteltu kriittiseksi (4) jo PPSHP:n ajoilta, joten päätimme ohittaa tässä tapauksessa ennakkokyselyyn vastaamisen ja oletimme, että ennakkokyselyssä verien tilauspalvelu on luokiteltu kriittiseksi (4).

Esittelin kriittisyysluokitteluun tehdyn työkalun ja ohjeistin sen käytössä ja olimme apuna kysymyksiin vastaamisessa. Jotkin väittämät aiheuttivat ristiriitoja, esimerkiksi tarkoitetaanko asiakkaalla potilasta vai järjestelmän omistajaa ja taloudellinen vahinko- osio tuntui tuottavan hankaluuksia. Taloudellinen vahinko- osuudessa täytyy miettiä, kuinka paljon järjestelmän tai laitteen 2 tunnin käyttökatkos saattaa aiheuttaa ja vastausvaihtoehdot ovat 1 miljoonan ja alle kymmenentuhannen euron vahinkojen välillä. On siis hankala arvioida tarkasti ennakkoon, kuinka paljon esimerkiksi ihmisen pysyvä vammautuminen katkoksen seurauksena tulisi tuottamaan taloudellista vahinkoa.

Saimme yhdessä täytettyä vaaditut kohdat ja työkalu laski automaattisesti verien tilauspalvelulle kriittisyysluokaksi normaali (2), vaikka todellisuudessa järjestelmä on tärkeän (3) ja kriittisen (4) välimaastossa. Painoarvojen yhteissummaksi tuli 94, joka ohitti vähäisen (1) vain 8 pisteellä, mutta jäi jälkeen tärkeästä (3) järjestelmästä jopa 71 pistettä.

Tuloksista voitiin helposti päätellä, että painoarvoja joudutaan vielä tarkastelemaan sekä kriittisyysrajoja laskemaan, jotta lopputulos vastaisi realistisemmin oikeaa kriittisyysluokkaa. Saimme samalla myös arvokasta tietoa ja uusia näkökulmia kriittisyysluokittelun ja työkalun parantamiseen. Suunnittelemattoman ja suunnitellun käyttökatkon aiheuttamat pisteiden muutokset olivat näkyvissä väittämän rivillä siihen vastatessa ja saimme kommenttia, että se saattaa vaikuttaa vastaajan näkökulmasta realistisesti vastaamiseen, koska tällöin vastaaja saattaa vastata siten, että saa mahdollisimman korkeat pisteet. Työkalusta poistetaan pisteiden näkyvyys, mutta jätetään vielä pisteiden yhteismäärä näkyviin yhteenvetoon, jotta vältytään pisteiden näkyvyyden aiheuttamalta vaikutukselta vastaamiseen. Työkalusta

muutetaan asiakas- nimikettä käyttävät kohdat ja potilas- nimikkeeksi, jotta vältytään epäselvyyksiltä, ketä asiakkaalla oikein tarkoitetaan.

Lopulta palaverista saatujen rakentavien keskustelujen, mielipiteiden ja kommenttien avulla lähdettiin kehittämään ja uusimaan työkalua pelkistetymmäksi ja helppokäyttöisemmäksi täyttäjän näkökulmasta. Lopputuloksesta tuli mielestäni paljon parempi versio kuin ensimmäisestä demoversiosta (LIITE 4). Testaaminen antoi arvokasta tietoa prosessin jatkokehityksestä ja suunnasta, johon prosessia lähdetään viemään tulevaisuudessa.

9 YHTEENVETO

Opinnäytetyöni aiheena oli kehittää kriittisyysluokitteluprosessia hyvinvointialue Pohteen laitteille ja tietojärjestelmille ja tehdä ennakkokysely ja työkalu kriittisyysluokittelutyön tueksi. Kriittisyysluokittelun tarkoituksena on antaa arvio laitteen tai tietojärjestelmän kriittisyydestä, jolloin pysytään paremmin perillä siitä, minkälaisia riskejä häiriötilanteet saattavat aiheuttaa, minne resurssit ovat kannattavinta kohdistaa ja minkälaista vahinkoa katkos voi saada aikaan. Luokittelun avulla voidaan myös määrittää laitteen tai tietojärjestelmän toiminnan jatkuvuuden varalle varmistavia toimia, jolloin mahdolliset riskit voidaan minimoida.

Opinnäytetyössä ei vältytty hankalilta tilanteilta tai ongelmilta. Suurin ongelma oli ehdottomasti koko kriittisyysluokitteluprosessin kokonaisuuden ymmärtäminen ja sisäistäminen. Aluksi aihe tuntui todella laajalta ja vaadittiin ymmärrystä sieltä ja täältä, mutta onneksi lähdin tutustumaan aiheeseen hitaasti tietoturvatiimin kanssa ja apuna olivat myös jo olemassa olevat materiaalit ja muille aloille tehdyt opinnäytetyöt kriittisyysluokittelusta, jotka avasivat aihetta pala palalta. Alkukankeuksien jälkeen pääsin onneksi hyvin vauhtiin prosessin ymmärtämisen lisäydyttyä ja sain tarvittaessa apua ja arvokasta tietoa tiimiltä. Toiseksi isommaksi ongelmaksi koitui kriittisyysluokittelun apuna käytettävän työkalun painoarvot, joista oli haastavaa saada järkeviä. Työkalua piti testailla useasti eri painoarvoilla ja tilanteilla, tehdä laskelmia mahdollisista yhdistelmistä ja tasapainottaa se siten, ettei korkein kriittisyys tulisi kuin harvoin. Olen toiminnallisten tehtävien lopputulokseen mielestäni ihan tyytyväinen, vaikka parannettavaa löytyy aina ja koko kriittisyysluokitteluprosessi ja työkalut mukautuu tarpeen mukaan käyttöön pääsyn myötä.

Opinnäytetyöprosessina kriittisyysluokittelu uutena aiheena itselleni oli sopivan haastava, mutta opinnoista saadut valmiudet tietoturvan osalta auttoivat opinnäytetyön tekemisessä ja antoivat hyvän pohjan lähteä työstämään uutta aihetta. Sosiaali- ja terveysala on itselleni täysin uusi aluevaltaus, jota koskevien lakien ja säädöksien oppiminen toivat omat haasteensa opinnäytetyön suorittamiseen, mutta osaltaan uuden oppiminen ja tiedonjano piti mielenkiintoa yllä aina alkumetreiltä loppuun saakka. Kahden hyvin erilaisen alan yhdistäminen toisiinsa on monimutkaista ja vaatii joko tietämystä molemmilta aloilta, laajat kontaktit tai hyvät taustajoukot, jotka auttavat ymmärtämään molempien alojen käytäntöjä ja prosesseja. Kävimme monta kallisarvoista ja mieleenpainuvaa keskustelua tietoturvatiimin ja henkilöstön kanssa. Esittelin monelle henkilölle kriittisyysluokitteluprosessin myös aivan uu-

tena asiana ja sain heiltä mahtavia parannusehdotuksia ja kannustavia kommentteja. Olen opinnäytetyöhöni, kehitykseeni ja lopputulokseen erittäin tyytyväinen, ottaen huomioon lähtökohdat ja alkukankeudet.

Sosiaali- ja terveysalalta ei löydy kattavasti jo tehtyjä opinnäytetyön aiheita liittyen kriittisyysluokitteluun, joten jatkotutkimukset ovat tarpeen. Hyviä jatkotutkimusaiheita voisivat olla esimerkiksi sosiaali- ja terveysalaan liittyvien toimintojen ja siellä käsiteltävien tietojen kriittisyysluokittelun kehittäminen, kriittisten laitteiden ja järjestelmien jatkuvuuden varmistamisen suunnitteluun perehtyminen ja perehtyminen etenkin lääkinnällisten laitteiden laajempaan ja tarkempaan luokitteluun ja luokitteluprosessiin.

Ikinä ei voi olla liian luottavainen järjestelmien tai laitteiden jatkuvaan toimivuuteen, vaikka kaikki mahdolliset skenaariot olisi käyty läpi ja varmistettu, koska teknologia on alati kehittyvä ja muuttuva ala niin positiivisessa, kuin negatiivisessakin mielessä. Tietoturvakollegoitani lainaten: ”On aina hyvä pitää foliohattu käden ulottuvilla tietoturva-asioissa, koska ikinä ei voida tuudittautua olemassa olevien ratkaisujen kestävyyteen tai sulkea eri skenaarioita täysin pois.” Kaikin puolin kriittisyysluokittelu opinnäytetyön aiheena oli erittäin opettavainen, sopivan haastava ja uutta asiaa tuli paljon, vaikka opittavaa varmasti jäi ja oppiminen aiheen parissa on jatkuvaa.

LÄHTEET

Avinetworks. Single Point of Failure Definition. *What is a Single Point of Failure?* Saatavissa: https://avinetworks.com/glossary/single-point-of-failure/. Viitattu 15.8.2024.

DNV. ISO/IEC 27001. *Tietoturvallisuuden hallintajärjestelmä.* 2022. Saatavissa: https://www.dnv.fi/services/iso-iec-27001-tietoturvallisuuden-hallintajarjestelma-3327/. Viitattu 17.7.2024.

Eduskunta. 2024. *Eduskunta hyväksyi hyvinvointialueiden perustamista ja sosiaali- ja terveydenhuollon sekä pelastustoimen järjestämisen uudistusta koskevan lainsäädännön.* Saatavissa: https://www.eduskunta.fi/FI/tiedotteet/Sivut/eduskunta-aanestaa-sote-uudistuksesta-keskiviikkona.aspx. Viitattu 2.7.2024.

Eur-lex. 2022. *Yleinen tietosuoja-asetus (GDPR).* 27.4.2016/679. Saatavissa: https://eur-lex.europa.eu/FI/legal-content/summary/general-data-protection-regulation-gdpr.html. Viitattu 3.9.2024.

Hintsanen, J., Huhtala, A., Kuismin, M., Mainio, T., Rautio, K., Somero, M., & Vahtola, P. Verien tilauspalvelujärjestelmän luokittelun testaaminen prosessin kautta, Teams-palaveri. 23.9.2024.

Huhtala, A. 2024. Tietoturvapäällikön henkilökohtainen tiedonanto, Teams-keskustelu. 6.8.2024.

ISO. ISO/IEC 27799. *Health informatics — Information security management in health using ISO/IEC 27002.* 2016. Saatavissa: https://www.iso.org/obp/ui/en/#iso:std:iso:27799:ed-2:v1:en. Viitattu 18.7.2024.

Jurvanen, L. 2024a. *Mitä tarkoittaa tietoturvan luottamuksellisuus?* Saatavissa: https://www.savelan.fi/mita-tarkoittaa-tietoturvan-luottamuksellisuus/. Viitattu 21.8.2024.

Jurvanen, L. 2024b. *Mitä tarkoittaa tietojen eheys?* Saatavissa: https://www.savelan.fi/mita-tarkoittaa-tietojen-eheys/. Viitattu 21.8.2024.

Jurvanen, L. 2024c. *Mitä tarkoittaa tietoturvan käytettävyys eli saatavuus?* Saatavissa: https://www.savelan.fi/mita-tarkoittaa-tietojen-eheys/. Viitattu 21.8.2024.

Kanta. 2024. *Toiminta häiriötilanteissa*. Saatavissa: https://www.kanta.fi/ammattilaiset/hairiotilanne-ohje. Viitattu 7.7.2024.

Kyberturvallisuuskeskus. 2024a. *Mikä on kybermittari?* Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari?toggle=Mik%C3%A4%20on%20Kybermittari%3F. Viitattu 5.8.2024.

Kyberturvallisuuskeskus. 2024b. *Kybermittari.* Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari. Viitattu 8.8.2024.

Lavanko, H. 2019a. Oikeat alustat yrityksesi työkuormille, osa 1: Vertailussa fyysinen palvelin ja virtuaalipalvelin. *Mitä etuja on fyysisellä palvelimella?* Saatavissa: https://www.advania.fi/blogi/oikeat-alustat-yrityksesi-tyokuormille-osa-1. Viitattu 19.8.2024.

Lavanko, H. 2019b. Oikeat alustat yrityksesi työkuormille, osa 1: Vertailussa fyysinen palvelin ja virtuaalipalvelin. *Mitä etuja on virtuaalipalvelimella?* Saatavissa: https://www.advania.fi/blogi/oikeat-alustat-yrityksesi-tyokuormille-osa-1. Viitattu 19.8.2024.

Liikamaa, M. 2021. *Istekin kriittisyysluokittelun työkalu*. Saatavissa: Istekki, Pohteen dokumentit. Viitattu: 31.7.2024.

Mainio, T. 2024. Tietoturva-arkkitehdin henkilökohtainen tiedonanto, Teams-palaveri. 5.8.2024.

Mutanen, J., Tolonen, P. & Vepsäläinen, P. 2022. *Toimintojen ja tietojärjestelmien kriittisyysluokittelu. Kyber-terveys-hanke.* Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Sote_toimintojen_ja_tietoj%C3%A4rjestelmien_kriittisyyden_luokittelu_v1.0.pdf. Viitattu 8.8.2024.

NIST U.S. Department of commerce. 2024. *The NIST Cybersecurity Framework (CSF) 2.0.* Saatavissa: https://doi.org/10.6028/NIST.CSWP.29. Viitattu 1.8.2024.

Palo Alto Networks. 2014. *Redundancy and Resiliency Features for Your Firewall.* Saatavissa: https://www.paloaltonetworks.com/products/features/redundancy.html. Viitattu 27.8.2024.

Pohde a. *Alueen kunnat.* Saatavissa: https://pohde.fi/tietoa-meista/pohjois-pohjanmaan-hyvinvointialue/alueen-kunnat/. Viitattu 9.7.2024.

Pohde b. *Tietoa meistä.* Saatavissa: https://pohde.fi/tietoa-meista/. Viitattu 8.7.2024.

SFS. ISO 22301. *Turvallisuus ja kriisinkestävyys.* 2019. Saatavissa: https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-22301-turvallisuus-ja-kriisinkestavyys/. Viitattu 24.7.2024.

SFS. ISO 31000. *Riskienhallinta.* 2018. Saatavissa: https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-31000-riskienhallinta/. Viitattu 22.7.2024.

SFS. ISO/IEC 27000. *Tietoturvallisuuden standardisarja*. 2022. Saatavissa: https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/. Viitattu 17.7.2024.

SFS. ISO/IEC 27002. *Tietoturvallisuuden standardisarja*. 2022. Saatavissa: https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/. Viitattu 17.7.2024.

STM. 2024. *Hyvinvointialueet vastaavat sote-palvelujen ja pelastustoimen järjestämisestä*. Saatavissa: https://stm.fi/hyvinvointialueet. Viitattu 8.7.2024.

Tapio, J. 2023. *Kuormantasaus pilvipalveluissa.* Tampere: Tampereen yliopisto. Informaatioteknologian ja viestinnän tiedekunta. Kandidaatin tutkielma. Saatavissa: https://urn.fi/URN:NBN:fi:tuni-202305065345. Viitattu 20.8.2024.

Termipankki. 2024. *Häiriötilanne.* Saatavissa: https://termipankki.fi/tepa/fi/haku/h%C3%A4iri%C3%B6tilanne. Viitattu 23.7.2024.

Tuomisalo, J. 2021. *Kriittisyysluokittelun hyödyt ja kompastuskivet teollisuuden kunnossapidon arjessa*. Saatavissa: https://www.caverion.fi/blogi/teollisuus/kriittisyysluokittelun-hyodyt-ja-kompastuskivet-teollisuuden-kunnossapidon-arjessa/. Viitattu 30.7.2024.

Valtioneuvosto. *Kyberturvallisuusdirektiivin (NIS2-direktiivi) kansallista toimeenpanoa tukeva työryhmä.* Saatavissa: https://valtioneuvosto.fi/hanke?tunnus=LVM044:00/2022. Viitattu 4.9.2024.

Vuorinen, S. 2019. *Sosiaali- ja terveysministeriön julkaisuja.* 2019:14. Kyberturvallisuus. Ohje sosiaali- ja terveydenhuollon toimijoille. Helsinki: Valtioneuvoston hallintoyksikkö, julkaisutuotanto. Saatavissa: http://urn.fi/URN:ISBN:978-952-00-4085-7. Viitattu 15.7.2024.

Kriittisyysluokittelu tietojärjestelmille ja lääkintälaitteille demo - Milja Somero 2024

Painoarvot, muokkaa G soluista:	Kriittinen 4:	80
	Tärkeä 3:	20
	Normaali 2:	5
	Vähäinen 1:	1

Ohje luokittelun tekemiseen:

Kaikkiin kohtiin ei välttämättä tarvitse vastata, vaan jätä ne tyhjäksi. Haluttuun kohtaan vastataan katkoksen aiheuttaman ongelman kriittisyyden arvolla, esim. "Tärkeä"kohdan väittämä pitää paikkansa, merkitään haluttuun paikkaan 3. Ota huomioon, milloin ongelma on olemassa ja merkitse oikea numero 0 paikalle vain siihen kohtaan tai kaikkiin kohtiin, jotka pitävät paikkansa siltä riviltä. Lomake laskee kriittisyyden automaattisesti. Painoarvoihin ei tarvitse koskea, mutta niitä voi muuttaa halutessaan. Rivin kokonaispisteet ja painoarvo tulevat näkyviin pisteet ja painoarvo kohtiin. Taulukko laskee vain korkeimman painoarvon mukaan per rivi. Taulukon lopussa näet kokonaispisteet, kokonaispainoarvon ja niistä saadun kriittisyysluokittelun arvon.

Kriittisyyden rajat ovat tällä hetkellä: Kriittinen (Yli 230), Tärkeä (Alle 230), Normaali (Alle 165), Vähäinen (Alle 86)

HUOMIO!

Suunnittelematon katkos laskee arvot 4 -> 3
Suunniteltu katkos nostaa arvot 3 -> 4 ja 2 -> 3

Merkitse toteutuviin väittämiin 4, jolloin katkoksen aiheuttama ongelma pitää paikkansa.

Katkoksen aiheuttama ongelma	Pisteet 1-4	Painoarvo 1-80	Jos katkos tapahtuu suunniteltuna työajan ulkopuolella (16:00-08:00)	Jos katkos tapahtuu suunniteltuna työajan sisäpuolella (8:00-16:00)	Jos katkos tapahtuu suunnittelemattomana työajan ulkopuolella (16:00-08:00)	Jos katkos tapahtuu suunnittelemattomana työajan sisäpuolella (8:00-16:00)
Kriittinen potilasturvallisuusongelma, mahdollisuus hengenvaaraan tai pysyvään terveydelliseen haittaan.	3	80	4	0	4	4
Kriittinen taloudellinen vahinko, mahdollisuus aiheuttamaan yli 1 miljoonan euron menetyksen.	4	80	4	0	0	0

Merkitse toteutuviin väittämiin 3, jolloin katkoksen aiheuttama ongelma pitää paikkansa.

Vakava potilasturvallisuusongelma, estää kiireellisen hoidon tai aiheuttaa väliaikaisen terveydellisen haitan.	4	80	0	3	3	0
Vakava taloudellinen vahinko, mahdollisuus aiheuttamaan yli satojen tuhansien eurojen menetyksen.	0	0	0	0	0	0
Estää ydintoimintojen toiminnan yhdessä tai useammassa yksikössä.	4	80	0	3	0	0

Merkitse toteutuviin väittämiin 2, jolloin katkoksen aiheuttama ongelma pitää paikkansa.

Kohtalainen potilasturvallisuusongelma, estää kiireettömän hoidon.	0	0	0	0	0	0	
Kohtalainen taloudellinen vahinko, mahdollisuus aiheuttamaan yli kymmenien tuhansien eurojen menetyksen.	0	0	0	0	0	0	
Kohtalainen mainehaitta, aiheuttaa merkittävän mainehaitan.	0	0	0	0	0	0	
Järjestelmän tietosisältö, sisältää potilastietoja tai sosiaalihuollon asiakastietoja.	2	5	2	2	2	0	JOS JÄRJESTELMÄ SISÄLTÄÄ KYSEISIÄ TIETOJA, MERKITSE RIVILLE VÄHINTÄÄN YHTEEN KOHTAAN 2!
Estää lakisääteisen tehtävän hoitamisen.	2	5	0	0	2	0	
Aiheuttaa häiriön tai saattaa aiheuttaa riskin ydintoimintojen toimimisen estymiselle yhdessä tai useammassa yksikössä.	3	20	0	2	2	0	
Asiakkaan toiminta on täysin riippuvainen laitteesta tai järjestelmästä.	2	5	0	0	0	2	

Merkitse toteutuviin väittämiin 1, jolloin katkoksen aiheuttama ongelma pitää paikkansa.

Vähäinen potilasturvallisuusongelma, vaikeuttaa potilaan hoitoa.	0	0	0	0	0	0	
Vähäinen taloudellinen vahinko, mahdollisuus aiheuttamaan alle kymmenen tuhannen euron menetyksen.	0	0	0	0	0	0	
Vähäinen mainehaitta, aiheuttaa riskin merkittävälle mainehaitalle.	0	0	0	0	0	0	
Järjestelmän tietosisältö, sisältää TL IV tai muita salassa pidettäviä tietoja.	1	1	1	0	0	0	JOS JÄRJESTELMÄ SISÄLTÄÄ KYSEISIÄ TIETOJA, MERKITSE RIVILLE VÄHINTÄÄN YHTEEN KOHTAAN 1!
Vaikeuttaa lakisääteisen tehtävän hoitamista.	0	0	0	0	0	0	
Saattaa aiheuttaa riskin ydintoimintojen häiriölle yhdessä tai useammassa yksikössä.	0	0	0	0	0	0	
ratkaisuja.	1	1	0	1	1	1	

YHTEENSÄ:	Pisteet	Painoarvot
	26	357
KRIITTISYYSLUOKKA:	KRIITTINEN	4

Kriittisyysluokka, tietojärjestelmät

Anna oma arviosi tietojärjestelmän kriittisyydestä sairaalaympäristössä. Millaisia vaikutuksia tietojärjestelmän 2 tunnin virka-aikana tapahtuvalla käyttökatkolla saattaa olla?

Vähäinen 1:

- *Vähäisen tason tietojärjestelmän toimimattomuus voi vaikeuttaa potilaan hoitoa. Tietojärjestelmän toimintakatkos saattaa aiheuttaa alle kymmenen tuhannen euron vahingot, riskin merkittävälle mainehaitalle, vaikeuttaa lakisääteisten tehtävien hoitamista, aiheuttaa riskin ydintoimintojen häiriölle. Asiakas joutuu käyttämään varajärjestelyitä tai ratkaisuja.*

- Vähäisiä, tason 1 tietojärjestelmiä voi olla esimerkiksi työaikaleimaus ja taukojumppasovellus.

Normaali 2:

- *Normaalin tason tietojärjestelmän toimimattomuus voi estää potilaan kiireettömän hoidon. Tietojärjestelmän toimintakatkos saattaa aiheuttaa yli kymmenen tuhannen euron vahingot, merkittävän mainehaitan, estää lakisääteisten tehtävien hoitamisen tai aiheuttaa häiriön ydintoimintoihin. Asiakas on täysin riippuvainen tietojärjestelmän toiminnasta.*

- Normaaleja, tason 2 tietojärjestelmiä voi olla esimerkiksi digisanelu, materiaalintilausjärjestelmät ja hoitajakutsujärjestelmä.

Tärkeä 3:

- *Tärkeän tason tietojärjestelmän toimimattomuus voi estää potilaan kiireellisen hoidon tai aiheuttaa väliaikaisen terveydellisen haitan. Tietojärjestelmän toimintakatkos saattaa aiheuttaa yli sadantuhannen euron vahingot. Tietojärjestelmä on oleellinen ydintoimintojen toiminnassa, ja katkoksen aikana voi estää ydintoimintojen toiminnan kokonaan yhdessä tai useammassa yksikössä.*

- Tärkeän, tason 3 tietojärjestelmiä voi olla esimerkiksi Verso (verien tilausjärjestelmä) ja Nearis (kuvantamisjärjestelmä)

- järjestelmäpalvelut (Nearis, digisanelu)

- Verso (vahtola paula, tietohallinto)

Kriittinen 4:

- *Kriittisen tason tietojärjestelmän toimimattomuus voi aiheuttaa mahdollisuuden potilaan hengenvaaraan tai pysyvään haittaan. Tietojärjestelmän toimintakatkos saattaa aiheuttaa yli 1 miljoonan euron vahingot. Tietojärjestelmä on oleellinen ydintoimintojen toiminnassa, ja katkoksen aikana voi estää ydintoimintojen toiminnan kokonaan yhdessä tai useammassa yksikössä.*

- Kriittisen, tason 4 tietojärjestelmä voi olla esimerkiksi Esko-potilastietojärjestelmä.

Voit varmistaa tietojärjestelmän kriittisyysluokan työkalun avulla:

(Linkki kriittisyysluokittelutyökaluun)

HUOM! Mikäli tietojärjestelmän pitää olla käytössä 24/7, se pitää ottaa huomioon toimittajasopimuksissa.

Kriittisyysluokka, laitteet

Anna oma arviosi laitteen kriittisyydestä sairaalaympäristössä. Millaisia vaikutuksia laitteen 2 tunnin virka-aikana tapahtuvalla käyttökatkolla saattaa olla?

Vähäinen 1:

- *Vähäisen tason laitteen toimimattomuus voi vaikeuttaa potilaan hoitoa. Laitteen toimintakatkos saattaa aiheuttaa alle kymmenen tuhannen euron vahingot, riskin merkittävälle mainehaitalle, vaikeuttaa lakisääteisten tehtävien hoitamista, aiheuttaa riskin ydintoimintojen häiriölle. Asiakas joutuu käyttämään varajärjestelyitä tai ratkaisuja.*

- Vähäisiä, tason 1 laitteita ovat esimerkiksi sykemittari, toimistolaitteet, tulostin ja itseilmottautumislaite.

Normaali 2:

- *Normaalin tason laitteen toimimattomuus voi estää potilaan kiireettömän hoidon. Laitteen toimintakatkos saattaa aiheuttaa yli kymmenen tuhannen euron vahingot, merkittävän mainehaitan, estää lakisääteisten tehtävien hoitamisen tai aiheuttaa häiriön ydintoimintoihin. Asiakas on täysin riippuvainen laitteen toiminnasta.*

- Normaaleja, tason 2 laitteita ovat esimerkiksi asiakkaan itsenäisesti käyttämät laitteet ja verenpainemittari. Myös osa laitteista, jotka ovat automatisoineet manuaalisesti suoritettavat tehtävät.

Tärkeä 3:

- *Tärkeän tason laitteen toimimattomuus voi estää potilaan kiireellisen hoidon tai aiheuttaa väliaikaisen terveydellisen haitan. Laitteen toimintakatkos saattaa aiheuttaa yli sadantuhannen euron vahingot. Laite on oleellinen ydintoimintojen toiminnassa, ja katkoksen aikana voi estää ydintoimintojen toiminnan kokonaan yhdessä tai useammassa yksikössä.*

- Tärkeän, tason 3 laitteita ovat esimerkiksi leikkauskoneet, kuvantamisen laitteet ja EKG-laite. Myös osa laitteista, jotka ovat automatisoineet manuaalisesti suoritettavat tehtävät.

Kriittinen 4:

- *Kriittisen tason laitteen toimimattomuus voi aiheuttaa mahdollisuuden potilaan hengenvaaraan tai pysyvään haittaan. Laitteen toimintakatkos saattaa aiheuttaa yli 1 miljoonan euron vahingot. Laite on oleellinen ydintoimintojen toiminnassa, ja katkoksen aikana voi estää ydintoimintojen toiminnan kokonaan yhdessä tai useammassa yksikössä.*

- Kriittisen, tason 4 laitteita ovat esimerkiksi hengityskone ja muut tehohoidon onnistumisen kannalta oleelliset laitteet.

Voit varmistaa laitteen kriittisyysluokan työkalun avulla:

(Linkki kriittisyysluokittelutyökaluun)

HUOM! Mikäli laitteen pitää olla käytössä 24/7, se pitää ottaa huomioon toimittajasopimuksissa.

Ohje luokittelun tekemiseen työkalulla:	Työkalun painoarvot:	
Täytä kohdat, joissa laitteen/järjestelmän katkoksen vaikutus pätee alla olevaan kysymykseen. Ota huomioon, tapahtuuko katkos suunniteltuna vai suunnittelemattomana. Kun olet täyttänyt toteutuvat kohdat, näet laitteen/järjestelmän kriittisyysluokan ja kriittisyysarvioon liittyvät huomiot työkalun lopusta. Painoarvot ovat muokattavissa F-sarakkeelta.	Kriittinen (4)	80
	Tärkeä (3)	20
	Normaali (2)	5
	Vähäinen (1)	1

Mitä vaikutuksia laitteen tai järjestelmän 2 tunnin käyttökatkolla saattaa olla?

Vaikutus	Pisteet	Suunniteltu käyttökatko	Suunnittelematon käyttökatko
Potilasturvallisuus			
Mahdollisuus potilaan hengenvaaraan tai pysyvään terveydelliseen haittaan.	4	x	x
Estää potilaan kiireellisen hoidon tai aiheuttaa väliaikaisen terveydellisen haitan.	0		
Estää potilaan kiireettömän hoidon.	0		
Vaikeuttaa potilaan hoitoa.	0		

Vaikutus	Pisteet	Suunniteltu käyttökatko	Suunnittelematon käyttökatko
Taloudellinen vahinko			
Voi aiheuttaa yli 1 miljoonan euron menetyksen.	0		
Voi aiheuttaa yli satojen tuhansien eurojen menetyksen.	3		x
Voi aiheuttaa yli kymmenien tuhansien eurojen menetyksen.	0		
Voi aiheuttaa alle kymmenen tuhannen euron menetyksen.	0		

Vaikutus	Pisteet	Suunniteltu käyttökatko	Suunnittelematon käyttökatko
Ydintoiminta			
Estää ydintoimintojen toiminnan yhdessä tai useammassa yksikössä.	0		
Aiheuttaa riskin ydintoimintojen toimimisen estymiselle yhdessä tai useammassa yksikössä.	3	x	
Aiheuttaa riskin ydintoimintojen häiriölle yhdessä tai useammassa yksikössä.	0		

Vaikutus	Pisteet	Suunniteltu käyttökatko	Suunnittelematon käyttökatko
Mainehaitta			
Aiheuttaa merkittävän mainehaitan.	3	x	x
Voi aiheuttaa riskin merkittävälle mainehaitalle.	0		

Vaikutus	Pisteet	Suunniteltu käyttökatko	Suunnittelematon käyttökatko
Lakisääteisest tehtävät			
Estää lakisääteisen tehtävän hoitamisen.	0		
Vaikeuttaa lakisääteisen tehtävän hoitamista.	1	x	

Vaikutus	Pisteet	Suunniteltu käyttökatko	Suunnittelematon käyttökatko
Potilaan toiminta			
Potilaan toiminta on täysin riippuvainen laitteesta tai järjestelmästä.	0		
Potilas joutuu käyttämään varajärjestelyitä tai ratkaisuja.	1		x

Tietosisältö/henkilötietoryhmä	Pisteet	Laite/järjestelmä sisältää näitä tietoja
Tietosisältö ja henkilötietoryhmä		
Laite/järjestelmä sisältää tai käsittelee potilastietoja tai muita erityisiä henkilötietoryhmiä.	3	x
Laite/järjestelmä sisältää tai käsittelee työntekijöiden tai asiakkaiden henkilötietoja.	2	x

Kriittisyysluokka	Pisteet yhteensä	Painoarvot yhteensä	Huomiot
Yhteenveto ja tulokset			
Tärkeä (3). Laitteen/järjestelmän käyttökatkolla on vakavia vaikutuksia.	20	167	Saattaa vaatia erityisjärjestelyitä jatkuvuuden varalle. Ole yhteydessä tietoturvatiimiin, jotta kriittisyysarviota voidaan käydä yhdessä läpi ja tarkentaa tarvittaessa.