Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua	
13 § Elinkaaren huomioiminen tietojärjestelmissä	versio 0.95/1.11.2019

13.1 § Tietoaineistojen ja tietojärjestelmien tietoturvallisuus

Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.

Hallituksen esitys HE 284/2018
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx

Tietojärjestelmällä tarkoitetaan järjestelmää, jonka tarkoitus on tietoja käsittelemällä palvella, helpottaa ja tehostaa jotakin toimintaa. Tietojärjestelmä koostuu ohjelmista, tietovarastoista, laitteista ja palveluista. Tietojärjestelmän elinkaari alkaa siihen liittyvästä tarvekartoituksesta ja päättyy tietojärjestelmän käytöstä poistoon. Tietojärjestelmän elinkaari kattaa kaikki tällä välillä olevat vaiheet, jotka ovat **määrittely** ja **suunnittelu**, **kilpailutus** ja **hankinta**, **toteutus** ja **kehitys**, **käyttöönotto**, **ylläpito** sekä **käytöstä poisto**. Tietojärjestelmien elinkaariajattelun lähtökohtana on järjestelmien suunnitelmallinen ja riskilähtöinen hallinta osana tiedonhallintayksikön toimintaa.

Tiedonhallintayksikkö varmistaa tietojärjestelmien tietoturvallisuuden koko niiden elinkaaren ajan tunnistamalla niihin kohdistuvat **riskit** ja mitoittamalla tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Riskienarvioinnissa tunnistetaan olennaiset riskit, jotka voivat vaikuttaa tietojärjestelmien käytettävyyteen ja saatavuuteen tai niissä käsiteltävien tietoaineistojen tietoturvallisuuteen.

Tietoturvallisuus tietojärjestelmien elinkaaressa muodostaa kokonaisuuden, johon kuuluvat riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella sekä tietoturvallisuustoimenpiteiden toteuttaminen. Tiedonhallintayksikkö arvioi tietojärjestelmiin liittyviä riskejä säännöllisesti niiden koko elinkaaren ajan sekä huomioi muuttuneiden riskien edellyttämät toimenpiteet tietoturvallisuuden suunnittelussa ja toteutuksessa. Tietojärjestelmien riskien arvioinnissa huomioidaan niiden toimintaympäristö ja järjestelmään liittyvät tietoturvavaatimukset.

Määrittely- ja suunnitteluvaihe
Määrittely- ja suunnitteluvaiheessa tehdään tarvekartoitus, jossa tunnistetaan ja määritellään tietojärjestelmä, sekä se mitä uuteen tai uudistettavaan tietojärjestelmään liittyy ja millaisia vaatimuksia siihen kohdistuu. Määrittely ja suunnitteluvaiheen aikana tunnistetaan tietoturvallisuuden kannalta keskeiset asiat, jotka on huomioitava toteutuksen myöhemmissä vaiheissa. Näihin kuuluvat aina tiedonhallintalaissa asetetut tietoturvallisuuden vähimmäisvaatimukset, jotka on lueteltu kortissa Suositukset tietoturvallisuudesta.

Määrittely- ja suunnitteluvaiheessa kuvataan tietojärjestelmän käyttötarkoitus sekä toimintaympäristö, kuten käyttäjät, ohjaava lainsäädäntö ja muut ulkoiset vaatimukset, järjestelmässä käsiteltävät tietoaineistot sekä liittymät muihin tietojärjestelmiin. Näiden pohjalta tehdään riskiarvio sekä määritetään tietojärjestelmään kriittisyys ja edellytetty tietoturvallisuuden taso, joiden perusteella tunnistetaan koko tietojärjestelmän elinkaaren aikana huomioitavat tietoturvavaatimukset. Tietojärjestelmään kohdistuvat toiminnalliset vaatimukset kuvataan ja niiden pohjalta laaditaan tietojärjestelmään kohdistuvat hyväksymiskriteerit. Tämä sisältää myös tietoturvallisuutta koskevat suunnitelmat ja vaatimukset, joiden määrittelyssä käytetään tarvittavaa tietoturvaosaamista. Määrittely- ja suunnitteluvaiheessa huomioidaan kortissa 13 § Tietoturvallisuus hankinnoissa tarkennukset koskien hankinnan suunnittelua ja valmistelua.

Laki julkisen hallinnon tiedonhallinnasta
Suosituskortti
Kohderyhmä: Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät
Käyttötarkoitus: Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua

13 § Elinkaaren huomioiminen tietojärjestelmissä	versio 0.95/1.11.2019

Tietojärjestelmän tai sen osan määrittelyvaiheessa arvioidaan sekä kokonaisuuden että järjestelmän eri osien tietoturvallisen toteuttamisen riskejä. Sellaisten osa-kokonaisuuksien sisällyttämistä järjestelmään on vältettävä, joiden tietoturvallinen toteuttaminen tai ylläpito vaativat runsaasti resursseja. Keskeistä on kiinnittää myös huomioita tietoriskien arvioinnissa koko palvelu- ja toimitusketjun kaikkien osapuolien ja heidän ympäristöjensä huomioimiseen, jotta tietojärjestelmään kohdistuvat riskit tulee kokonaisvaltaisesti hallittua. Organisaation johto sitoutuu tietoriskien hallintaan perustuvaan tietoturvallisuuden toteuttamiseen jo määrittely- ja suunnitteluvaiheesta lähtien. Johdolle on myös tarkoituksenmukaista antaa realistinen kuva tietoturvallisuuden rakentamisen ja ylläpidon vaatimista resursseista.

Lisäksi ennen hankintaa tai toteutusta suunnitteluvaiheessa laaditaan alustava suunnitelma hankinnan ja toteutuksen aikaisista tietoturvaan liittyvistä tehtävistä, vastuista ja aikataulutuksesta.

Kilpailutus- ja hankintavaihe
Kilpailutus- ja hankintavaiheessa suunnitellaan ja toteutetaan tietojärjestelmään liittyvä hankinta kortissa 13 § Tietoturvallisuus hankinnoissa mukaisesti.

Kilpailutus- ja hankintavaiheessa on keskeistä, että hankintavaatimuksiin, tarjouspyyntöihin ja sopimuksiin sisällytetään myös tietoturvaa koskevat vaatimukset. Ne kohdistuvat sekä hankinnan kohteena olevaan tietojärjestelmään että sen toteuttavaan ja tarjoavaan toimittajaan.

Toteutusvaihe
Toteutusvaiheen sisältö riippuu hankittavasta tietojärjestelmästä sekä sen toteutusmallista. Kyseessä voi olla esimerkiksi täysin räätälöity järjestelmä ja siihen liittyvä laajempi kehitysprojekti tai valmisohjelmisto, johon tehdään toteutusvaiheen aikana ainoastaan tiettyjä konfigurointeja.

Toteutusvaiheessa tehdään uudelleen tarkastelu määrittelyvaiheessa laadittuun riskiarviointiin sekä tehdään tarvittavat tarkentavat uhkamallinnukset ja riskiarviot tietojärjestelmään liittyvien riskien ja uhkaskenaarioiden tunnistamiseksi.

Määritetyt tietoturvavaatimukset suunnitellaan ja dokumentoidaan tietoturvakontrolleiksi, jotka toteutetaan tämän vaiheen aikana. Toteutusvaiheessa tunnistetaan myös tietojärjestelmän liittymät muihin järjestelmiin sekä niistä muodostuvat riippuvuudet ja tietovirrat. Nämä dokumentoidaan osaksi arkkitehtuuri- ja integraatiosuunnitelmia, joiden mukaisesti toteutetaan tarvittavat integraatiot muuhun ympäristöön varmistaen myös tietoturvallisuuden toteutuminen niissä.

Tietojärjestelmät koostuvat usein lukuisista, mahdollisesti hajautetuista ja usean osapuolen tekemistä komponenteista. Tällöin on tietoriskien hallinnassa hyvä kiinnittää huomiota rajapintojen hallintaan sekä palvelujärjestelmän ja taustajärjestelmän välisen tiedonsiirron hallintaan.

Toteutuksen aikana suoritetaan suunnitellut katselmoinnit ja testaukset pohjautuen riskiarvioon ja tarveharkintaan; mm. arkkitehtuurikatselmointi, koodikatselmointi, toiminnallisuuksien testaus, väärinkäyttötapausten testaus/ tietoturvatestaus ja suorituskykytestaus.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua	
13 § Elinkaaren huomioiminen tietojärjestelmissä	versio 0.95/1.11.2019

Toteutusvaiheessa huomioidaan sille etukäteen laaditut suunnitelmat ja vaiheet. Tavoitteena on, että tarvittavat toimenpiteet tehdään riskilähtöisesti ja suunnitelmallisesti asianmukaisen tietoturvallisuuden sisään rakentamiseksi.

Toteutetut tietoturvakontrollit ja ratkaisut dokumentoidaan osaksi tietojärjestelmän turvallisuuskuvausta ja muuta laadittua dokumentaatiota.

Tietoturvallisuusvastuiden epäselvyydet toteutuksen aikana ovat tavallinen ongelma, etenkin monitoimittajaympäristössä. Tähän voidaan varautua tietoriskien jatkuvalla hallinnalla ja riskien hallintaan tähtäävien toimenpiteiden toteuttamisella, huomioiden erityisesti sopimuksiin kirjatut tavoitteet ja toimenpiteet riskien hallinnan osalta. Sopimuksiin liittyviä tyypillisiä riskejä ovat IRP-kysymykset, tekijänoikeudet, lisenssit ja kaikki vielä tunnistamaton immateriaalioikeuden alla oleva aineisto, omistajan vaihdokset ja fuusiot.

Käyttöönottovaihe

Käyttöönottovaihetta varten laaditaan käyttöönottosuunnitelma tuotantoon viennin toteuttamiseksi. Osana tietojärjestelmän käyttöönottoa suoritetaan käyttöönottohyväksyntä, jossa varmistetaan aiemmin kuvattujen vaatimusten toteutuminen tietojärjestelmässä. Hyväksyntä edellyttää tarvittavien toiminnallisuuksien ja tietoturvakontrollien todentamista. Tietojärjestelmien, laitteiden ja sovellusten käyttöönottoasennuksen tehdään määritetyn prosessin ja ohjeistuksen mukaisesti huomioiden esimerkiksi organisaation laatimat arkkitehtuuriperiaatteet, yhteensopivuuden muuhun ympäristöön sekä määritetyt suojausvaatimukset ja kovennukset. Näiden toteuttamiseksi on määritetty määrämuotoiset konfiguraatiot eri asetuksille ja parametreille sekä tarpeettomat palvelut on poistettu käytöstä. Kovennetun, määritetyt tietoturva-asetukset sisältävän, asennuksen toteuttamisessa voidaan hyödyntää ylläpidettyä luotettua levykuvaa (golden image), jonka avulla asennus tehdään. Nämä levykuvat katselmoidaan, testataan ja päivitetään säännöllisesti niiden asianmukaisuuden varmistamiseksi. Myös itse tietojärjestelmien, laitteiden ja sovellusten konfiguraatioiden säännöllinen katselmointi ja valvonta suunnitellaan osaksi ylläpitovaihetta.

Tietojärjestelmän tietoturvakuvaus päivitetään tarvittavien muutosten osalta käyttöönottovaiheessa.

Ylläpitovaihe

Osana ylläpitoa tunnistetaan käsittely-ympäristössä tai vaatimuksissa tapahtuvien muutosten vaikutus tietojärjestelmään sekä niiden edellyttämät muutokset tietoturvakontrolleihin. Tehtävissä muutoksissa noudatetaan määritettyjä muutoshallintamenettelyitä. Tietojärjestelmään kohdistetaan säännöllisiä riskiarvioita sekä suojaustason asianmukaisuuteen kohdistuvia arvioita, jotta varmistutaan siitä, että tietojärjestelmään kohdistuvat riskit ja vaatimukset ovat huomioitu. Arvioinneissa hyödynnetään muun muassa katselmointeja sekä automaattisia ja manuaalisia tietoturvatestauksia. Toteutustavasta riippuen myös tietojärjestelmän palvelutoimittajaan kohdistetaan tarvittavia auditointeja ja heiltä voidaan edellyttää tietojärjestelmän turvallisuustason seurantaa sekä siihen liittyvää raportointia. Ylläpitovaiheen yhtenä tavoitteena on varmistaa määritettyjen tietoturvavaatimusten ja suojauskeinojen ajantasaisuus ja asianmukainen toiminta tehtyihin suunnitelmiin pohjautuen sekä näitä koskevan dokumentaation ja kuvausten ylläpito.

Laki julkisen hallinnon tiedonhallinnasta
Suosituskortti
Kohderyhmä: Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät
Käyttötarkoitus: Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua

13 § Elinkaaren huomioiminen tietojärjestelmissä	versio 0.95/1.11.2019

Tietojärjestelmien ylläpidossa noudatetaan organisaatiossa määritettyjä prosesseja ja toimintatapoja, kuten muutoshallinta, poikkeamienhallinta ja riskienhallinta, kun huolehditaan tietojärjestelmien haavoittuvuuksien hallinnasta, päivityksistä, varmuuskopioinnista, konfiguraation hallinnasta ja kovennuksista, haittaohjelmasuojauksesta sekä valvonnasta. Ylläpitovaiheessa pitää huolehtia myös toiminnan jatkuvuuden edellyttämästä tietojärjestelmän toivuttamisen suunnittelusta ja varmistamisesta harjoittelulla.

Osana tietojärjestelmien ylläpitoa toteutetaan tarvittava valvonta ja seuranta muun muassa tietojärjestelmän toimivuuden, suorituskyvyn ja tietoturvallisuuden seuraamiseksi ja ylläpitämiseksi. Valvonnassa huomioidaan kortissa 17 § Lokitietojen kerääminen suositukset.

Varmuuskopiot otetaan tehdyn suunnitelman mukaisesti huomioiden organisaation toiminnan ja käsitellyn tiedon pohjalta määritetyt varmuuskopioitavat tiedot, varmuuskopiointiin käytetyt menetelmät ja sen tiheys sekä varmuuskopioiden suojaamiseen liittyvät keinot. Varmuuskopiointi toteutetaan

- käyttäen siihen tarkoitettua ratkaisua,
- kirjaten lokiin tiedot varmuuskopioiduista tiedoista, varmuuskopioinnin ajankohdasta ja varmuuskopion kohteesta sekä merkiten varmuuskopiot asianmukaisesti,
- varmistaen varmuuskopioinnin onnistuminen ja palauttaminen esimerkiksi raportein sekä palautustestein, sekä
- suojaten varmuuskopiot vahingoilta ja väärinkäytöksiltä, kuten ylikirjoittamiselta, muuttamiselta tai tuhoutumiselta sekä niiden siirron että säilytyksen aikana.

Päivitystenhallinnassa noudatetaan määritettyä prosessia, jossa määritetään päivitystarpeen tunnistaminen ja havaitseminen, päivitysten asentamiseen liittyvät toimintamallit (huomioiden erityyppiset tietojärjestelmät ja ympäristöt sekä niiden mahdollisesti muodostamat erityistarpeet), päivitysten epäonnistumiseen ja palautumiseen liittyvät käytännöt, päivitystilanteen seurantaan ja siitä raportointiin liittyvät toimintatavat sekä vaihtoehtoiset suojaustavat ja toimenpiteet, kun haavoittuvuutta ei voida korjata päivityksellä (esimerkiksi päivitystä ei ole vielä julkaistu tai jokin sovellus ei toimi päivitetyssä versiossa).

Haittaohjelmasuojausta koskevat toimintamallit on määritetty kuvaten muun muassa haittaohjelmasuojaukseen käytettyjen ratkaisujen asennuksen ja konfiguroinnin sekä päivittämisen käytännöt, ratkaisujen ajantasaisuuden ylläpitämisen sekä niiden toimivuuden varmistamisen.

Ylläpitoyhteydet ja -oikeudet on toteutettu vähimpien oikeuksien periaatteen mukaisesti, jolloin ylläpitotoimiin on käytössä lievimmät mahdolliset tarvittavat oikeudet. Tietojärjestelmien ylläpitoyhteydet tehdään käyttäen salattuja yhteyksiä sekä looginen ja fyysinen pääsy on rajattua.

Käytöstä poisto
Käytöstä poistoa varten laaditaan riskiarviointi, jossa tunnistetut riskit huomioidaan poiston toteuttamisessa. Käytöstä poistolle laaditaan suunnitelma, jossa huomioidaan muun muassa säilytettävän tiedon migraatio, tuhottavien laitteiden ja muistivälineiden sanitointi sekä käytöstä poistuvan tietojärjestelmän osien tuhoaminen.

Laki julkisen hallinnon tiedonhallinnasta
Suosituskortti
Kohderyhmä: Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät
Käyttötarkoitus: Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua

13 § Elinkaaren huomioiminen tietojärjestelmissä	versio 0.95/1.11.2019

Käytöstä poiston yhteydessä tietoaineistojen tuhoamisen tulee tapahtua tunnistettuihin riskeihin nähden riittävän luotettavalla tavalla. Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen joutuminen oikeudettomien henkilöiden haltuun. Tietoaineistojen elinkaaren osalta huomioidaan kortin 13 § Elinkaaren huomioiminen tietoaineistojen käsittelyssä periaatteet.

Kortti Suositukset tietoturvallisuudesta
Kortti 13 § Elinkaaren huomioiminen tietoaineistojen käsittelyssä
Kortti 13 § Tietoturvallisuus hankinnoissa
Kortti 17 § Lokitietojen kerääminen

Sanasto

Kyberturvallisuussanasto
https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf
Kokonaisturvallisuussanasto
http://www.tsk.fi/tiedostot/pdf/Kokonaisturvallisuuden_sanasto_2.pdf
Valtionhallinnon tietoturvasanasto
https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto

Alusta on ohjelmiston tai tietojärjestelmän tekninen toimintaympäristö. Alustalla tarkoitetaan yksinkertaisimmillaan laitteistoa ja sen varusohjelmistoa. Yleisemmässä tapauksessa alustalla saatetaan tarkoittaa tiettyä laajempaa sovellusten ajoympäristöä erilaisine tukiohjelmistoineen, tietokantoineen, tietoliikennevalmiuksineen.

Arviointi on sen selvittäminen, täyttääkö tietty kohde eri osiltaan sille asetetun tavoitetilan (vaatimukset, suositukset ja parhaat käytännöt). Arviointiprosessi on usein hyväksyntäprosessin osaprosessi.

Auditointi on riippumattoman tahon suorittama kohteen, sen toiminnan ja toiminnan tulosten yleensä määräajoin tapahtuva tutkiminen sen selvittämiseksi, vastaako kohde siihen kohdistuvia vaatimuksia.

Haavoittuvuudet ovat alttiuksia turvallisuutta uhkaaville tekijöille, puutteita ja heikkouksia turvatoimissa sekä suojauksissa. **Tietoturvahaavoittuvuudet** ovat tietojärjestelmän tai sen osan heikkous, joka vaarantaa tietoturvan Haavoittuvuus voi olla seurausta ohjelmavirheestä tai siitä, että jotakin erityistapausta ei ole otettu huomioon. Haittaohjelmat hyödyntävät levitessään tietoturvahaavoittuvuuksia.

Haavoittuvuusskannaus on tietoverkossa kohdejärjestelmän palveluissa olevien tunnettujen haavoittuvuuksien automaattinen haku, esimerkiksi murtokokeilla tai tutkimalla palvelimen ohjelmistoversiota.

Havaitseva kontrolli pyrkii havaitsemaan suojaavan kerroksen läpi päässeen jäännösriskin aiheuttamat vaikutukset. Valvonta ei enää estä vahinkoa tapahtumasta, vaan ainoastaan saattaa sen näkyväksi.

Hyväksymistarkastus kattaa toimet, joilla todetaan, täyttääkö tuote tai työn tulos asetetut vaatimukset.

Komponentti on itsenäinen ohjelmistoyksikkö, joka tarjoaa palveluja hyvin määritellyn rajapinnan kautta.

Kontrolli on riskien hallinnan tavoite, keino tai menetelmä, suunnitelmallinen jatkuva toiminta, kertaluonteinen tai toistuva toimenpide, jolla varaudutaan tai suojaudutaan (tieto)turvaloukkauksia tai haitallisia tapahtumia vastaan. Kontrollit ovat ehkäiseviä, havaitsevia (ilmaisevia) tai korjaavia. **Suojauksella** tarkoitetaan haitallisen ulkopuolisen vaikutuksen torjumista tai ennalta ehkäisyä.

Kriteeri on arviointiperuste, jolla todetaan tavoitteen täyttyminen.

Pääsynhallinta käsittää ne menettelyt, joilla varmistetaan, että käyttäjät, laitteet, sovellukset ja järjestelmät pääsevät käyttämään tietojärjestelmissä olevaa tietoa roolinsa mukaisesti.

Pääsynvalvonta kattaa ne tiedot, toiminnot ja menettelyt, joiden avulla palvelujärjestelmän tai sen palvelulelementtien käyttö mahdollistetaan vain valtuutetuille käyttäjille.

Salakirjoittaa eli käyttää menetelmää tiedon esityksen muuttamiseksi sellaiseksi, että tiedon alkuperäinen sisältö on mahdollista saada selville vain samaa tai soveltuvaa käänteistä menetelmää käyttäen. Salakirjoittaminen tapahtuu salausavainta käyttäen tietyn salausalgoritmin mukaisesti.

Salattu yhteys on salausmenetelmällä ulkopuolisilta suojattu tietojärjestelmien välinen yhteys.

Salaus on tiedon, esimerkiksi toiselle henkilölle lähetettävän viestin käsittelyä niin, että ulkopuolinen ei saisi haltuunsa tietoa tai viestiä tai sen sisältämää informaatiota. Salaus tarkoittaa myös salakirjoitusta eli salakirjoittamista tai sen tulosta.

Salausmenetelmä on salaukseen ja salauksen purkamiseen käytettävä menetelmä.

Suojattava kohde on organisaation toiminnan kannalta merkityksellinen kohde, joka halutaan suojata riskien varalta. Suojattava kohde voi olla esimerkiksi tieto, tietojärjestelmä, prosessi, fyysinen tila, yksittäinen asiakirja tai työasema.

Testaus on järjestelmän toimivuuden, käytettävyyden, suorituskyvyn, määritysten mukaisuuden tai muun ominaisuuden selvittämiseksi tehtävä toimenpidesarja.

Tietojärjestelmä on ihmisistä, tietojenkäsittelylaitteista, datansiirtolaitteista ja ohjelmista koostuva järjestelmä, jonka tarkoitus on tietoja käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi sekä abstrakti systeemi, jonka muodostavat tiedot ja niiden käsittelysäännöt.

Vaatimus on kohteelle asetettu yksittäinen tavoite, joka kohteen tulee pystyä toteuttamaan.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua	
13 § Elinkaaren huomioiminen tietojärjestelmissä	versio 0.95/1.11.2019

Koko elinkaari	Tietojärjestelmiin liittyvät riskit arvioidaan säännöllisesti
Määrittely ja suunnittelu	Tunnistetaan tietojärjestelmän merkitys tiedonhallintayksikön toiminnalle ja sen jatkuvuudelle sekä siinä käsiteltävät tiedot ja niiden merkitys
	Tunnistetaan tietojärjestelmään kohdistuvat ulkoiset vaatimukset
	Arvioidaan tietojärjestelmään kohdistuvat riskit
	Määritetään tietojärjestelmän kriittisyys ja tietoturvataso
	Määritetään ja kuvataan tietojärjestelmään ulkoisista vaatimuksista, sisäisestä luokituksesta ja tunnistetuista riskeistä muodostuvat tietoturvavaatimukset
	Määritetään tietojärjestelmän hyväksymiskriteerit
	Suunnitellaan hankinnan ja toteutuksen aikaiset tietoturvaan liittyvät tehtävät ja niiden aikataulutus
Kilpailutus ja hankinta	Tietojärjestelmään liittyvä hankinta tehdään suunnitelmallisesti
	Hankinnassa huomioidaan kortin 13 § Tietoturvallisuus hankinnoissa periaatteet
	Kilpailutukseen- ja hankintaan liittyviin kuvauksiin, vaatimuksiin, tarjouspyyntöihin ja sopimuksiin sisällytetään myös tietoturvaa koskevat vaatimukset
	Tietoturvavaatimukset kohdistuvat sekä hankinnan kohteena olevaan tietojärjestelmään että sen toteuttavaan ja tarjoavaan toimittajaan
Toteutus	Tehdään uhkamallinnus ja tunnistetaan tietojärjestelmään liittyvät riskit ja uhkaskenaariot
	Valitaan ja dokumentoidaan tietoturvakontrollit
	Tunnistetaan tietojärjestelmän liittymät muihin järjestelmiin sekä näihin liittyvät riippuvuudet osana kokonaisarkkitehtuuria
	Toteutetaan valitut tietoturvakontrollit osana tietojärjestelmän kehitystä
	Toteutetaan määritetyt katselmoinnit ja testaukset (arkkitehtuurikatselmointi, koodikatselmointi, toiminnallisuuksien testaus, väärinkäyttötapausten testaus/ tietoturvatestaus, suorituskykytestaus)
	Laaditaan tietojärjestelmän turvallisuuskuvaus ja muu dokumentaatio
Käyttöönotto	Laaditaan käyttöönottosuunnitelma
	Toteutetaan tarvittavat integraatiot ja liittymät muuhun ympäristöön varmistaen myös integraatioiden tietoturvallisuus
	Suoritetaan tietojärjestelmän hyväksyntätestaus
	Tehdään hyväksyntä tietojärjestelmän käyttöönotosta
Ylläpito	Katselmoidaan ja arvioidaan riskejä sekä suojaustason asianmukaisuutta säännöllisesti
	Tunnistetaan käsittely-ympäristössä ja vaatimuksissa tapahtuvien muutosten vaikutuksen tietojärjestelmään sekä niiden edellyttämät muutokset tietoturvakontrolleihin; muutoksissa noudatetaan määritettyjä muutoshallintamenettelyitä

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua	
13 § Elinkaaren huomioiminen tietojärjestelmissä	versio 0.95/1.11.2019

	Suoritetaan tietojärjestelmän ylläpitoa tehtyjen suunnitelmien mukaisesti huolehtien muun muassa päivityksistä, varmuuskopioinnista, konfiguraation hallinnasta ja kovennuksista sekä haittaohjelmasuojauksesta
	Ylläpidetään ja päivitetään tietojärjestelmää koskevaa dokumentaatiota ja kuvauksia tehtyjen muutosten mukaisesti
	Suoritetaan tietojärjestelmän jatkuvaa valvontaa tunnistettujen riskien mukaisesti
Käytöstä poisto	Laaditaan ja hyväksytään käytöstä poistolle suunnitelma
	Suunnitellaan ja toteutetaan säilytettävän tiedon migraatio
	Sanitoidaan tuhottavat laitteet poistaen niissä olevat tiedot luotettavasti
	Tuhotaan käytöstä poistuvan tietojärjestelmän osat