
Tunne huominen.
XAMK
Kaakkois-Suomen
ammattikorkeakoulu

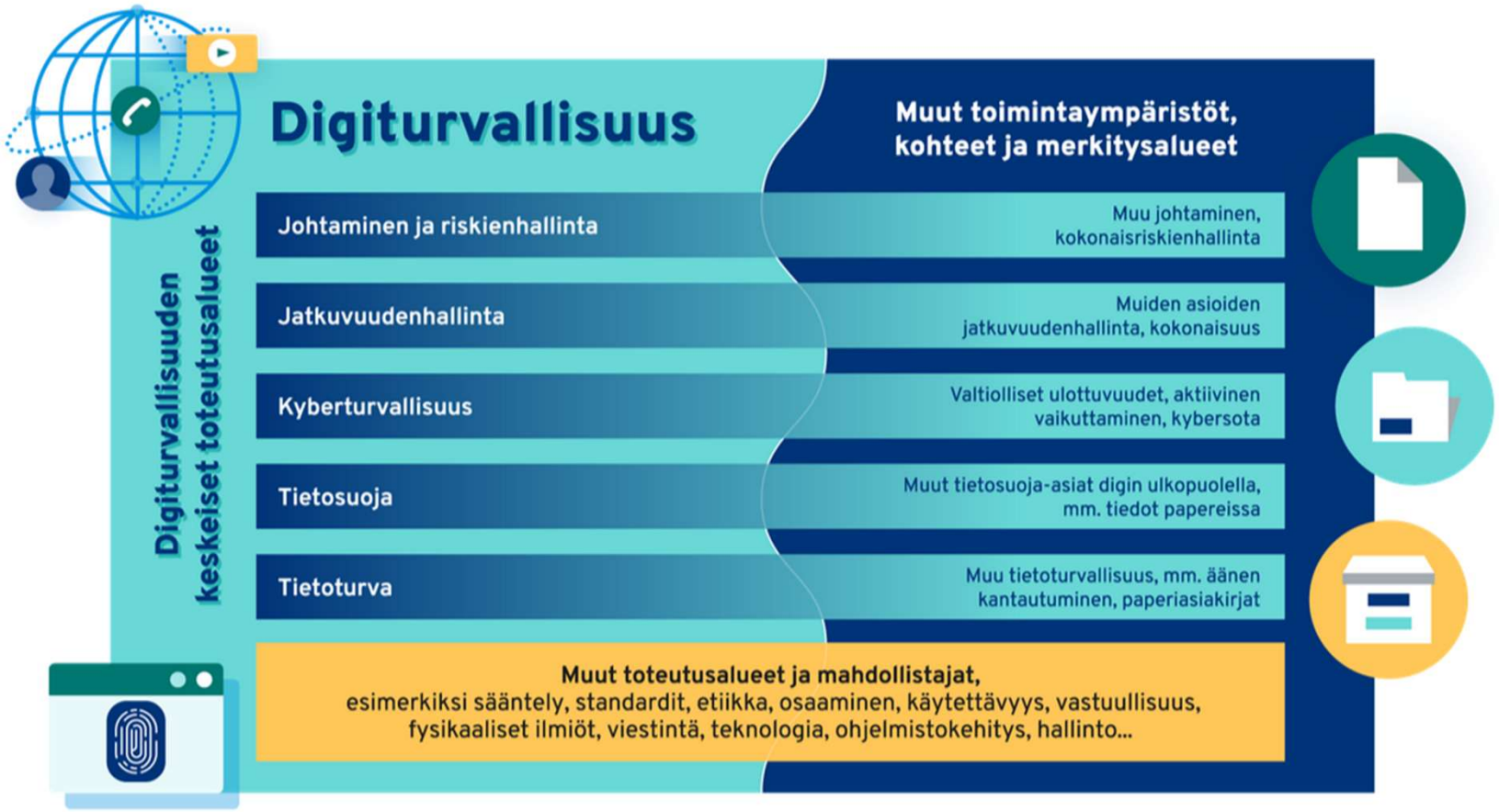
Digitaalinen Turvallisuus

Kaakkois-Suomen ammattikorkeakoulu
South-Eastern Finland University of Applied Sciences

www.xamk.fi

Kaakkois-Suomen ammattikorkeakoulu

Digitaalinen turvallisuus



Lähde: https://dvv.fi/mita-on-digiturva?

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Johtaminen ja riskienhallinta

- Johtaminen ja riskienhallinta luovat puitteet digitaalisen turvallisuuden onnistumiselle.

- Digitaalisen turvallisuuden johtaminen ja riskienhallinta tarjoavat rakenteet ja toimintamallit organisaation turvallisuusriskien hallinnalle. Lisäksi ne luovat perustan muille digitaalisen turvallisuuden osa-alueille.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Johtaminen digitaalisen turvallisuuden ytimessä

1. **Strateginen suunnittelu**
   - **Tavoitteena** digitaalisen turvallisuuden liittäminen organisaation yleiseen strategiaan ja liiketoiminnan tavoitteisiin.
   - **Toimet tavoitteiden saavuttamiseen:**
     - ✓ Turvallisuusstrategian laatiminen, joka kattaa organisaation mission, vision ja arvot.
     - ✓ Turvallisuustavoitteiden asettaminen ja niiden kytkeminen liiketoiminnnan tarpeisiin.
     - ✓ Turvallisuuskulttuurin edistäminen, jossa koko henkilöstö ymmärtää ja tukee turvallisuutta.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Johtaminen digitaalisen turvallisuuden ytimessä

2. **Johtajuus ja vastuunjako**
   - **Tavoitteena** selkeän johtorakenteen ja vastuiden määrittely turvallisuuteen liittyen.
   - **Toimet tavoitteiden saavuttamiseen:**
     - ✓ Digitaalisen turvallisuuden vastuuhenkilöiden nimeäminen, kuten tietoturvapäällikkö (CISO).
     - ✓ Johdon sitoutuminen turvallisuustoimenpiteisiin ja niiden rahoittamiseen.
     - ✓ Säännölliset turvallisuuskatselmukset ylimmän johdon tasolla.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Johtaminen digitaalisen turvallisuuden ytimessä

3. **Ohjeistus ja standardit**
   - **Tavoitteena** selkeät ja yhtenäiset toimintatavat, jotka varmistavat turvallisuusprosessien noudattamisen.
   - **Toimet tavoitteiden saavuttamiseen:**
     - ✓ Tietoturvapolitiikat ja niihin perustuvien sisäisten ohjeistusten laatiminen ja päivittäminen (katselmus ja hyväksyntä).
     - ✓ Säännölliset auditoinnit varmistamaan ohjeiden noudattaminen (sisäiset ja ulkoiset).
     - ✓ Kansainvälisten standardien (esim. ISO/IEC 27000 sarja) käyttöönotto.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Riskienhallinta osana johtamista

1. **Riskien tunnistaminen ja arviointi**
   - **Tavoitteena** tunnistaa ja priorisoida uhkia, jotka voivat vaikuttaa organisaation toimintaan.
   - **Toimet tavoitteiden saavuttamiseen:**
     - ✓ Uhkien kartoittaminen, kuten kyberhyökkäykset, tietovuodot, teknologiset viat (haavoittuvuudet) ja inhimilliset virheet (prosessit/toimintatavat).
     - ✓ Riskien vaikutusten ja todennäköisyyksien arviointi.
     - ✓ Riskirekisterin ylläpitäminen ja päivittäminen.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Riskienhallinta osana johtamista

2. **Riskienhallintastrategiat**
   - **Tavoitteena** vähentää riskien todennäköisyyttä ja vaikutuksia.
   - **Toimet tavoitteiden saavuttamiseen:**
     - ✓ Teknisten suojatoimenpiteiden (esim. palomuurit, varmuuskopiointi) käyttöönotto.
     - ✓ Organisatoristen prosessien, kuten varautumissuunnitelmien ja koulutusten kehittäminen.
     - ✓ Vakuutusten hankkiminen taloudellisten riskien varalle.

Riskienhallinta osana johtamista

3. **Jatkuva seuranta ja reagointi**
   - **Tavoitteena** varautua uusiin uhkiin ja reagoida nopeasti riskitilanteisiin.
   - **Toimet tavoitteiden saavuttamiseen:**
     - ✓ Riskimittareiden määrittäminen ja seuranta (esim. tapahtumine määrä, reaktiot nopeisiin uhkiin).
     - ✓ Säännölliset harjoitukset, kuten tietoturvaloukkausten simulaatiot.
     - ✓ Muutostenhallintaprosessit riskienhallinnan mukauttamiseksi uusiin tilanteisiin.

Johtamisen ja riskienhallinnan hyödyt

- Ennakoitavuus: Mahdolliset uhat ja haavoittuvuudet tunnistetaan ja niihin voidaan varautua etukäteen.
- Joustavuus: Organisaatio pystyy sopeutumaan nopeasti muuttuvaan uhkaympäristöön.
- Luotettavuus: Asiakkaiden ja sidosryhmien luottamus kasvaa, kun organisaatio osoittaa ottavansa turvallisuuden vakavasti.
- Kustannustehokkuus: Riskienhallinta vähentää merkittävästi mahdollisten turvallisuuspoikkeamien kustannuksia.

Johtaminen ja riskienhallinta toimivat digitaalisen turvallisuuden perustana. Ilman johdon tukea ja tehokasta riskienhallintaa muut turvallisuuden osa-alueet, kuten kyberturvallisuus ja tietosuoja, jäävät helposti hajanaisiksi tai tehottomiksi.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Jatkuvuudenhallinta

Kaakkois-Suomen ammattikorkeakoulu
South-Eastern Finland University of Applied Sciences

www.xamk.fi

Kaakkois-Suomen
ammattikorkeakoulu

Jatkuvuudenhallinta

Jatkuvuudenhallinta on keskeinen osa digitaalista turvallisuutta, joka varmistaa organisaation toiminnan jatkuvuuden ja nopean palautumisen häiriö- ja kriisitilanteissa. Tämä osa-alue keskittyy liiketoimintakriisien, kuten teknisten vikojen, kyberhyökkäysten, luonnonkatastrofien tai henkilöstöongelmien, hallintaan.

Jatkuvuudenhallinnan tarkoitus ja tavoitteet

- **Tarkoituksena** varmistaa, että organisaatio pystyy jatkamaan kriittisiä toimintojaan häiriöistä huolimatta.
- **Tavoitteena:**
  - ✓ Vähentää häiriöiden vaikutusta liiketoimintaan ja palveluihin.
  - ✓ Turvata kriittiset resurssit, kuten tiedot, henkilöstö, tilat ja teknologia.
  - ✓ Nopea palautuminen normaaliin toimintaan kriisitilanteiden jälkeen.

Jatkuvuudenhallinta: Keskeiset prosessit ja vaiheet

1. **Riskien arviointi ja kriittisyysanalyysi**
   - **Tarkoitus:** Tunnistaa organisaation toiminnan kannalta kriittiset resurssit ja prosessit sekä niihin kohdistuvat riskit.
   - **Toimet:**
     - ✓ **Business Impact Analysis (BIA):** Analysoi, mitkä prosessit ovat välttämättömiä ja kuinka nopeasti niiden toiminta on palautettava.
     - ✓ **Riskien arviointi:** Kartoitus mahdollisista häiriöistä, kuten verkkohyökkäykset, laitteistoviat tai luonnonmullistukset.

Jatkuvuudenhallinta: Keskeiset prosessit ja vaiheet

2. Jatkuvuussuunnitelman laatiminen

- **Tarkoitus:** Dokumentoida käytännön toimenpiteet, joilla varmistetaan kriittisten toimintojen jatkuvuus.
- **Toimet:**
  - ✓ Priorisoidaan toiminnot ja määritellään palautumisaikataulut (RTO - Recovery Time Objective, RPO - Recovery Point Objective).
  - ✓ Määritellään vastuut ja roolit kriisitilanteissa.
  - ✓ Laaditaan selkeät toimintamallit eri häiriötilanteiden varalle.

3. Teknologiset varautumistoimet

- **Tarkoitus:** Turvata teknologiset järjestelmät ja tiedot häiriöiden varalta.
- **Toimet:**
  - ✓ Varmuuskopiointi: Säännöllinen tiedostojen ja järjestelmien varmuuskopiointi, mielellään eri sijaintiin (esim. pilvipalvelut, ulkoiset varmuuskopiot)
  - ✓ Katastrofipalautussuunnitelma (Disaster Recovery Plan): Tiedot ja prosessit, joilla palautetaan tekniset järjestelmät mahdollisimman nopeasti.
  - ✓ Kaksinkertainen infrastruktuuri: Ylijäämäkapasiteetin ja redundanssin lisääminen kriittisiin järjestelmiin.

Jatkuvuudenhallinta: Keskeiset prosessit ja vaiheet

4. **Testaus ja harjoittelu**
   - **Tarkoitus:** Varmistaa suunnitelman toimivuus käytännössä ja henkilöstön valmiudet toimia kriisitilanteessa.
   - **Toimet:**
     - ✓ Säännölliset häiriötilannesimulaatiot, kuten palvelinrikkojen tai kyberhyökkäysten harjoittelu.
     - ✓ Palautusprosessien testaaminen (esim. varmuuskopioiden palautus).

5. **Jatkuva kehittäminen**
   - **Tarkoitus:** Pitää jatkuvuudenhallinta ajan tasalla muuttuvassa toimintaympäristössä.
   - **Toimet:**
     - ✓ Seurataan ja analysoidaan todellisia häiriötilanteita.
     - ✓ Päivitetään jatkuvuussuunnitelmaa uusien uhkien, teknologioiden ja liiketoimintatarpeiden mukaisesti.
     - ✓ Otetaan käyttöön uusia teknologisia ratkaisuja ja toimintamalleja.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Jatkuvuudenhallinta: Keskeiset työkalut ja menetelmät

- **Varmuuskopiointijärjestelmät:** Automaattiset järjestelmät, jotka varmistavat tietojen säilymisen häiriötilanteissa.
- **Pilvipohjaiset palvelut:** Tarjoavat skaalautuvuutta ja vaihtoehtoisia tallennuspaikkoja.
- **Jatkuvuudenhallinnan ohjelmistot:** Työkalut, jotka tukevat suunnitelmien laatimista, riskien arviointia ja seurantaa (esim. Everbridge, Fusion Framework System).
- **Tietoturvavalvontajärjestelmät:** Tunnistavat ja reagoivat häiriöihin reaaliajassa.

Jatkuvuudenhallinta: Hyödyt ja merkitys

- **Liiketoiminnan jatkuvuus:** Mahdollistaa palveluiden ja toimintojen jatkumisen keskeytyksettä.
- **Sidosryhmien luottamus:** Asiakkaat ja yhteistyökumppanit arvostavat organisaatiota, joka on varautunut häiriöihin.
- **Vahva kilpailuasema:** Hyvin hoidettu jatkuvuudenhallinta voi olla kilpailuetu markkinoilla.
- **Riskienhallinnan osana:** Tukee laajempaa digitaalisen turvallisuuden strategiaa ja parantaa organisaation resilienssiä.

Jatkuvuudenhallinta vaatii sekä teknistä että organisatorista valmistautumista. Se on tehokas tapa minimoida häiriöiden vaikutuksia ja varmistaa liiketoiminnan toimivuus kaikissa tilanteissa.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Kyberturvallisuus

Kaakkois-Suomen ammattikorkeakoulu
South-Eastern Finland University of Applied Sciences

www.xamk.fi

Kaakkois-Suomen
ammattikorkeakoulu

Kyberturvallisuus

Kyberturvallisuus on digitaalisen turvallisuuden ydinosa-alue, joka keskittyy suojaamaan organisaation digitaalista infrastruktuuria, tietojärjestelmiä, dataa ja palveluita kyberuhkilta. Se kattaa laajan joukon teknisiä, organisatorisia ja hallinnollisia toimenpiteitä, joiden tavoitteena on varmistaa tiedon ja järjestelmien luottamuksellisuus, eheys ja saatavuus.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Kyberturvallisuuden peruspilarit

1. **Luottamuksellisuus (Confidentiality)**
   - **Tavoitteena** varmistaa, että tieto on vain valtuutettujen henkilöiden, järjestelmien tai prosessien saatavilla.
   - **Toimenpiteitä** tavoitteiden saavuttamiseksi:
     - ✓ Tiedon salaaminen (esim. AES, SSL/TLS).
     - ✓ Pääsynhallinta ja käyttöoikeuksien rajaus (esim. roolipohjainen pääsynhallinta, RBAC).
     - ✓ Monivaiheinen tunnistautuminen (MFA).

Kyberturvallisuuden peruspilarit

2. **Eheys (Integrity)**
   - **Tavoiteena** suojata tieto manipuloinnilta ja varmistaa sen oikeellisuus.
   - **Toimenpiteitä** tavoitteiden saavuttamiseksi:
     - ✓ Kryptografiset tarkistussummat ja digitaaliset allekirjoitukset.
     - ✓ Lokien ja tiedostojen muokkauksen seuranta (esim. SIEM-järjestelmät).
     - ✓ Varastoidun ja siirrettävän tiedon suojaaminen.

3. **Saatavuus (Availability)**
   - **Tavoiteena** varmistaa, että järjestelmät, palvelut ja tiedot ovat käytettävissä aina tarvittaessa.
   - **Toimenpiteitä** tavoitteiden saavuttamiseksi:
     - ✓ Redundanssin ja varajärjestelmien käyttö (esim. klusteroinnit, pilvipalvelut).
     - ✓ Suojautuminen palvelunestohyökkäyksiltä (esim. DDoS-suojausratkaisut).
     - ✓ Automaattinen varmuuskopiointi ja nopea palautus (DRP, Disaster Recovery Plan).

Kyberturvallisuuden osa-alueet

a) **Verkkoturvallisuus**
- **Tavoitteena** suojata verkkoja ja niiden välityksellä kulkevaa tietoa luvattomalta käytöltä ja hyökkäyksiltä.
- **Toimenpiteitä** tavoitteiden saavuttamiseksi:
  - ✓ Palomuurit ja tunkeutumisenestojärjestelmät (IPS/IDS).
  - ✓ VPN-yhteydet etätyöntekijöille.
  - ✓ Segmentointi ja erillisten verkkovyöhykkeiden käyttö (esim. DMZ).

b) **Sovellusturvallisuus**
- **Tavoitteena** suojata ohjelmistot ja sovellukset haavoittuvuuksilta, jotka voivat johtaa hyökkäyksiin.
- **Toimenpiteitä** tavoitteiden saavuttamiseksi:
  - ✓ Sovellusten haavoittuvuustestaukset (esim. OWASP ASVS).
  - ✓ Turvallisen ohjelmistokehityksen periaatteet (esim. DevSecOps).
  - ✓ Päivitysten ja korjausten (patch management) hallinta.

Kyberturvallisuuden osa-alueet

c) **Päätelaite- ja laiteturvallisuus**
- **Tavoitteena** suojata yksittäiset laitteet, kuten tietokoneet, älypuhelimet ja IoT-laitteet.
- **Toimenpiteitä** tavoitteiden saavuttamiseksi:
  - ✓ Endpoint Detection and Response (EDR) -ratkaisut.
  - ✓ Antivirusten ja haittaohjelmasuojauksen käyttö.
  - ✓ Laitteiden salaaminen ja etätyhjennysmahdollisuus.

d) **Identiteetin ja pääsynhallinta (IAM)**
- **Tavoitteena** hallita käyttäjien ja järjestelmien käyttöoikeuksia ja estää luvaton pääsy.
- **Toimenpiteitä** tavoitteiden saavuttamiseksi:
  - ✓ SSO (Single Sign-On) -ratkaisujen käyttö.
  - ✓ Tunnistautumisprosessien vahvistaminen (esim. biometria, MFA).
  - ✓ Privileged Access Management (PAM) -ratkaisut.

Kyberturvallisuuden osa-alueet

e) **Tietoturvavalvonta ja -reaktio (SOC ja IR)**
- **Tavoitteena** valvoa järjestelmien toimintaa ja reagoida nopeasti mahdollisiin turvallisuusuhkiin.
- **Toimenpiteitä** tavoitteiden saavuttamiseksi:
  - ✓ SIEM (Security Information and Event Management) -järjestelmät.
  - ✓ Kyberuhkien seuranta ja tiedustelu.
  - ✓ Incident Response -tiimien ja -prosessien luominen.

f) **Kyberuhkien tiedustelu ja hallinta**
- **Tavoitteena** ennakoida ja tunnistaa uusia kyberuhkia.
- **Toimenpiteitä** tavoitteiden saavuttamiseksi:
  - ✓ Uhkatiedon kerääminen (Threat Intelligence).
  - ✓ Haavoittuvuusskannaukset ja penetraatiotestaukset.
  - ✓ Uusien haittaohjelmien analysointi.

Kyberturvallisuuden osa-alueet

g) **Koulutus ja tietoisuuden lisääminen**
- **Tavoitteena** varmistaa, että henkilöstö tunnistaa kyberuhkat ja osaa toimia turvallisesti.
- **Toimenpiteitä** tavoitteiden saavuttamiseksi:
  - ✓ Säännölliset koulutukset ja simulaatiot (esim. phishing-harjoitukset).
  - ✓ Turvallisuuspolitiikkojen selkeä kommunikointi.
  - ✓ Käyttäjien ohjeistaminen turvalliseen salasanakäytäntöön.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Kyberturvallisuuden uhkatyypit

- **Haittaohjelmat:** Virukset, troijalaiset, kiristysohjelmat.
- **Tietojenkalastelu (Phishing):** Tietojen varastaminen valesähköposteilla tai verkkosivustoilla.
- **Palvelunestohyökkäykset (DDoS):** Järjestelmien saatavuuden estäminen.
- **Tietomurrot:** Luvaton pääsy tietoihin tai järjestelmiin.
- **Sisäiset uhkat:** Henkilöstön tahallinen tai tahaton toiminta, joka aiheuttaa turvallisuusriskin.

Kyberturvallisuuden hallintamalleja ja standardeja

- **ISO/IEC 27001:** Kansainvälinen standardi tietoturvan hallintajärjestelmille.
- **NIST Cybersecurity Framework:** Ohjeistus riskienhallinnan ja kyberturvallisuuden kehittämiseen.
- **GDPR ja muut tietosuojalait:** Tietosuojan integrointi kyberturvallisuuteen.

Kyberturvallisuuden merkitys

- **Liiketoiminnan jatkuvuus:** Estää taloudelliset menetykset ja mainehaitat.
- **Lainsäädännön noudattaminen:** Varmistaa tietosuojalainsäädännön vaatimusten täyttymisen.
- **Luottamus ja maine:** Asiakkaat ja sidosryhmät luottavat organisaatioon, joka panostaa kyberturvallisuuteen.

Kyberturvallisuus on dynaaminen ja jatkuvasti kehittyvä ala, joka vaatii jatkuvaa valvontaa, päivityksiä ja sopeutumista uusiin uhkiin. Kokonaisvaltainen kyberturvallisuusstrategia on välttämätön nykyaikaisessa digitaalisessa toimintaympäristössä.

Tietosuoja

Kaakkois-Suomen ammattikorkeakoulu
South-Eastern Finland University of Applied Sciences

www.xamk.fi

Kaakkois-Suomen
ammattikorkeakoulu

Tietosuoja

Tietosuoja on keskeinen osa digitaalista turvallisuutta, ja sen tarkoituksena on varmistaa henkilötietojen suojaaminen ja yksityisyyden turvaaminen. Tietosuojan painopiste on erityisesti henkilötietojen käsittelyn laillisuudessa, turvallisuudessa ja läpinäkyvyydessä.

Tietosuojan tarkoitus ja tavoitteet

- **Tarkoituksena** suojata yksilöiden oikeuksia heidän henkilötietoihinsa liittyen ja varmistaa, että organisaatiot käsittelevät henkilötietoja lainmukaisesti.
- **Tavoitteena**:
  - ✓ Estää tietojen luvaton käyttö, pääsy ja vuotaminen.
  - ✓ Varmistaa henkilötietojen käsittelyn oikeellisuus ja turvallisuus.
  - ✓ Edistää luottamusta organisaation ja asiakkaiden välillä.

Tietosuojan keskeiset periaatteet

Tietosuoja perustuu kansainvälisesti tunnustettuihin periaatteisiin, kuten EU:n yleisessä tietosuoja-asetuksessa (GDPR):

a) Laillisuus, kohtuullisuus ja läpinäkyvyys
- Henkilötietoja käsitellään laillisesti ja oikeudenmukaisesti, ja käsittelyn on oltava läpinäkyvää rekisteröidyille.

b) Tarkoitussidonnaisuus
- Henkilötietoja kerätään ja käytetään vain ennalta määriteltyihin, laillisiin tarkoituksiin.

c) Tietojen minimointi
- Kerätään ja käsitellään vain tarpeellinen määrä henkilötietoja.

d) Oikeellisuus
- Tiedot on pidettävä paikkansapitävinä ja ajan tasalla.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Tietosuojan keskeiset periaatteet

e) Säilytyksen rajoittaminen

- Henkilötietoja säilytetään vain niin kauan kuin on tarpeen niiden käsittelyn tarkoitusten saavuttamiseksi.

f) Luottamuksellisuus ja turvallisuus

- Henkilötietoja käsitellään tavalla, joka varmistaa niiden turvallisuuden, mukaan lukien suojaus luvattomalta käsittelyltä ja vahingoittumiselta.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Tietosuojan keskeiset osa-alueet

a) **Henkilötietojen tunnistaminen ja hallinta**
   - **Tarkoitus:** Selvittää, mitä henkilötietoja organisaatio käsittelee ja miten niitä hallinnoidaan.
   - **Toimenpiteitä:**
     - ✓ Tietovarantojen kartoittaminen.
     - ✓ Henkilötietojen luokittelu (esim. arkaluonteiset tiedot).
     - ✓ Rekisteriselosteiden ja tietojen käsittelydokumentaation ylläpito.

b) **Oikeusperusteet ja tietojen keruu**
   - **Tarkoitus:** Varmistaa, että tietojen käsittely perustuu lailliseen oikeusperusteeseen.
   - **Toimenpiteitä:**
     - ✓ Tietojen käsittelyperusteiden määrittely (esim. suostumus, sopimus, lakisääteinen velvoite).
     - ✓ Läpinäkyvien tietosuojailmoitusten laatiminen.

Tietosuojan keskeiset osa-alueet

c) Tietojen suojaaminen

- **Tarkoitus:** Estää tietojen luvaton käyttö ja turvata tietojen eheys ja saatavuus.
- **Toimenpiteitä:**
  - ✓ Tietojen salaus (esim. AES-salaus).
  - ✓ Pääsynhallinta ja käyttöoikeuksien rajoittaminen.
  - ✓ Laitteiden ja tietojen fyysinen suojaaminen.

d) Rekisteröityjen oikeudet

- **Tarkoitus:** Varmistaa, että rekisteröidyt voivat käyttää oikeuksiaan henkilötietoihinsa liittyen.
- **Oikeuksia:**
  - ✓ Oikeus saada tietoa omista tiedoistaan.
  - ✓ Oikeus tietojen oikaisemiseen ja poistamiseen.
  - ✓ Oikeus siirtää tiedot järjestelmästä toiseen (datansiirrettävyys).
  - ✓ Oikeus vastustaa tietojen käsittelyä tai rajoittaa sitä.

Tietosuojan keskeiset osa-alueet

e) Tietosuojaloukkausten hallinta

- **Tarkoitus:** Reagoida tietoturvaloukkauksiin nopeasti ja tehokkaasti.
- **Toimenpiteitä:**
  - ✓ Loukkausten tunnistaminen ja ilmoittaminen valvontaviranomaisille (esim. 72 tunnin sisällä GDPR:n mukaan).
  - ✓ Rekisteröityjen informointi vakavien loukkausten tapauksessa.
  - ✓ Loukkausten analysointi ja prosessien parantaminen.

f) Tietosuojakoulutus ja -tietoisuus

- **Tarkoitus:** Varmistaa, että henkilöstö ymmärtää tietosuojavelvoitteet ja toimii niiden mukaisesti.
- **Toimenpiteitä:**
  - ✓ Säännöllinen henkilöstön kouluttaminen.
  - ✓ Tietosuojakäytäntöjen ja ohjeistusten kommunikointi.
  - ✓ Käytännön simulaatiot, kuten tietosuojaloukkauksen harjoitukset.

Tietosuojan keskeiset osa-alueet

g) Tietosuoja osana suunnittelua

- **Tarkoitus:** Integroida tietosuoja kaikkiin prosesseihin ja järjestelmiin niiden suunnitteluvaiheessa.
- **Toimenpiteitä:**
  - ✓ Privacy by Design -periaatteen noudattaminen.
  - ✓ Riskiperusteinen lähestymistapa uusien palveluiden tai tuotteiden suunnittelussa.

Tietosuojaa ohjaavaa lainsäädäntöä ja standardeja

Tietosuoja perustuu usein kansainväliseen ja kansalliseen lainsäädäntöön:

- **EU:n yleinen tietosuoja-asetus (GDPR):** Asettaa tiukat vaatimukset henkilötietojen käsittelylle EU:ssa.
- **ePrivacy-asetus:** Täydentää GDPR:ää erityisesti sähköisen viestinnän osalta.
- **ISO/IEC 27701:** Tietosuojan hallintajärjestelmästandardi.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Tietosuojan hyödyt ja merkitys

- **Luottamus:** Asiakkaat ja yhteistyökumppanit arvostavat organisaatiota, joka käsittelee henkilötietoja vastuullisesti.
- **Lainsäädännön noudattaminen:** Estää oikeudelliset seuraamukset ja sakot.
- **Kilpailuetu:** Hyvin hoidettu tietosuoja voi toimia erottautumisena kilpailijoista.
- **Riskienhallinta:** Vähentää henkilötietojen vuotamiseen ja väärinkäyttöön liittyviä riskejä.

Tietosuoja ei ole pelkästään tekninen kysymys, vaan se vaatii organisaatiolta kokonaisvaltaista lähestymistapaa, joka yhdistää lainsäädännön noudattamisen, turvallisuuskäytännöt ja henkilöstön sitoutumisen.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Tietoturva

Kaakkois-Suomen ammattikorkeakoulu
South-Eastern Finland University of Applied Sciences

www.xamk.fi

Kaakkois-Suomen
ammattikorkeakoulu

Tietoturva

Tietoturva on digitaalisen turvallisuuden osa-alue, joka keskittyy suojaamaan tietoa sen **luottamuksellisuuden**, **eheyden** ja **saatavuuden** näkökulmasta. Tietoturva käsittää teknisiä, organisatorisia ja hallinnollisia toimenpiteitä, jotka suojaavat tietoa ja tietojärjestelmiä sekä fyysisessä että digitaalisessa muodossa.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Tietoturvan peruspilarit

Tietoturva rakentuu **kolmen keskeisen periaatteen** varaan:

1. **Luottamuksellisuus (Confidentiality)**
   - **Tavoitteena** estää luvaton pääsy tietoihin.
   - **Toimenpiteitä** tavoitteiden saavuttamiseksi**:**
     - ✓ Tiedon salaaminen (esim. AES, SSL/TLS).
     - ✓ Käyttäjien tunnistaminen ja pääsynhallinta (esim. käyttäjätunnukset, salasanat, kaksivaiheinen tunnistautuminen).
     - ✓ Fyysinen tietojen suojaaminen (esim. suojatut tilat ja lukitut kaapit).

2. **Eheys (Integrity)**
   - **Tavoitteena** varmistaa, että tieto pysyy muuttumattomana ja luotettavana.
   - **Toimenpiteitä** tavoitteiden saavuttamiseksi:
     - ✓ Kryptografiset tarkistussummat ja digitaaliset allekirjoitukset.
     - ✓ Tiedostojen muokkaushistorian seuranta ja lokitus.
     - ✓ Kontrollit, jotka estävät luvattomat muutokset.

Tietoturvan peruspilarit

3. **Saatavuus (Availability)**
   - **Tavoitteena:** Taata, että tieto ja järjestelmät ovat käytettävissä tarvittaessa.
   - **Toimenpiteitä** tavoitteiden saavuttamiseksi:
     - ✓ Palvelinten redundanssi ja ylijäämäkapasiteetti.
     - ✓ Palautussuunnitelmat ja varmuuskopiointi.
     - ✓ Palvelunestohyökkäyksiltä (DDoS) suojautuminen.

Tietoturvan osa-alueet

a) **Verkkoturva**
   - **Tavoitteena:** Suojata organisaation tietoverkot ja niiden välityksellä siirrettävä tieto.
   - **Toimenpiteitä** tavoitteiden saavuttamiseen:
     - ✓ Palomuurit ja tunkeutumisenestojärjestelmät (IPS/IDS).
     - ✓ Verkkoliikenteen salaaminen (esim. VPN).
     - ✓ Verkkojen segmentointi, kuten DMZ-alueiden käyttö.

b) **Sovellusturvallisuus**
   - **Tavoitteena:** Suojata ohjelmistot ja sovellukset haavoittuvuuksilta ja väärinkäytöksiltä.
   - **Toimenpiteitä** tavoitteiden saavuttamiseen:
     - ✓ Turvallinen ohjelmistokehitys (esim. DevSecOps).
     - ✓ Haavoittuvuuksien skannaus ja korjaaminen (patch management).
     - ✓ Sovellusten käytönvalvonta ja lokitus.

Tietoturvan osa-alueet

c) **Päätelaiteturvallisuus**
- **Tavoitteena** suojata käyttäjien päätelaitteet (esim. tietokoneet, älypuhelimet, IoT-laitteet).
- **Toimenpiteitä** tavoitteiden saavuttamiseen:
  - ✓ Haittaohjelmasuojaus ja palomuurit.
  - ✓ Endpoint Detection and Response (EDR) -ratkaisut.
  - ✓ Laitteiden salaus ja etätyhjennysominaisuudet.

d) **Tiedonhallinta ja -suojaus**
- **Tavoitteena** suojata tieto sen koko elinkaaren ajan.
- **Toimenpiteitä** tavoitteiden saavuttamiseen:
  - ✓ Tietojen luokittelu (esim. arkaluonteiset, julkiset).
  - ✓ Tietojen salaaminen ja pseudonymisointi.
  - ✓ Tietojen hallittu hävittäminen (esim. tietoturvallinen tuhoaminen).

Tietoturvan osa-alueet

e) **Identiteetin ja pääsynhallinta (IAM)**
- **Tavoitteena** estää luvaton pääsy järjestelmiin ja tietoihin.
- **Toimenpiteitä** tavoitteiden saavuttamiseen:
  - ✓ Roolipohjainen pääsynhallinta (RBAC).
  - ✓ Privileged Access Management (PAM) -ratkaisut.
  - ✓ Monivaiheinen tunnistautuminen (MFA).

f) **Tietoturvavalvonta ja uhkien hallinta**
- **Tavoitteena** tunnistaa ja reagoida nopeasti tietoturvauhkiin.
- **Toimenpiteitä** tavoitteiden saavuttamiseen:
  - ✓ SIEM (Security Information and Event Management) -järjestelmät.
  - ✓ Uhkatiedustelu ja haavoittuvuusskannaukset.
  - ✓ Reagointi- ja palautusprosessit (Incident Response).

Tietoturvan osa-alueet

g) **Fyysinen turvallisuus**
- **Tavoitteena** suojata laitteistot, tilat ja fyysiset tietovarannot.
- **Toimenpiteitä** tavoitteiden saavuttamiseen**:**
  - ✓ Pääsytilojen valvonta (esim. kulunvalvonta, kameravalvonta).
  - ✓ Laitteistojen sijoittaminen turvallisiin paikkoihin.
  - ✓ Suojattujen tilojen varmistaminen hätätilanteissa.

h) **Katastrofipalautus ja jatkuvuudenhallinta**
- **Tavoitteena** palauttaa tietojärjestelmät ja tiedot häiriöiden jälkeen.
- **Toimenpiteitä** tavoitteiden saavuttamiseen:
  - ✓ Automaattiset varmuuskopiointijärjestelmät.
  - ✓ DRP (Disaster Recovery Plan) -suunnitelmien laatiminen.
  - ✓ Säännöllinen testaus ja harjoittelu.

Tietoturvaan kohdistuvat uhkat

- **Teknologiset uhkat**
  - ✓ Haittaohjelmat (virukset, troijalaiset, ransomware).
  - ✓ Palvelunestohyökkäykset (DDoS).
  - ✓ Verkkohyökkäykset (man-in-the-middle, phishing).

- **Inhimilliset virheet**
  - ✓ Heikot salasanat.
  - ✓ Tahattomat tietovuodot (esim. väärin lähetetyt sähköpostit).
  - ✓ Puutteellinen tietoturvatietoisuus.

- **Fyysiset uhkat**
  - ✓ Laitteiden varkaudet tai vahingot.
  - ✓ Tulipalot, luonnonmullistukset.
  - ✓ Valvomaton pääsy tiloihin.

Tietoturvatoimenpiteet

- **Tekniset ratkaisut**
  - ✓ Palomuurit ja virustorjuntaohjelmat.
  - ✓ Salauksen käyttöönotto (esim. VPN, TLS).
  - ✓ Automaattiset päivitykset ja haavoittuvuuksien korjaukset.

- **Hallinnolliset ratkaisut**
  - ✓ Tietoturvapolitiikat ja ohjeistukset.
  - ✓ Riskienhallintasuunnitelmat ja tietoturva-auditoinnit.
  - ✓ Henkilöstön koulutus ja tietoisuuden lisääminen.

- **Organisatoriset ratkaisut**
  - ✓ Tietoturvan integrointi liiketoimintastrategiaan.
  - ✓ Selkeät vastuut ja roolit tietoturvan hallinnassa.
  - ✓ Säännölliset tietoturvaharjoitukset ja simulaatiot.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Tietoturva standardeja ja lainsäädäntöä

- **ISO/IEC 27001:** Tietoturvan hallintajärjestelmien standardi.
- **NIST Cybersecurity Framework:** Ohjeistus riskienhallintaan ja tietoturvan parantamiseen.
- **GDPR:** Tietosuojalainsäädäntö, joka edellyttää tietoturvallisia henkilötietojen käsittelytapoja.
- **Kyberturvallisuuslaki (Suomi):** Vaatimukset kriittisten toimijoiden tietoturvasta.

Tietoturvan hyödyt

- **Tietojen ja järjestelmien suojaaminen**: Estää luvattoman pääsyn, tietovuodot ja manipuloinnin.
- **Liiketoiminnan jatkuvuus:** Suojaa keskeytyksiltä ja kriisitilanteilta.
- **Luottamuksen lisääminen:** Asiakkaat ja yhteistyökumppanit luottavat tietoturvallisiin toimijoihin.
- **Lainsäädännön noudattaminen:** Välttää sakot ja oikeudelliset seuraamukset.

Tietoturva on laaja ja jatkuvasti kehittyvä osa-alue, joka vaatii proaktiivista asennetta, monipuolisia toimenpiteitä ja henkilöstön sitoutumista. Kokonaisvaltainen tietoturva on organisaation toiminnan perusta.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Tunne huominen.