



Fyysisen suojauksen opas



Sisältö

1 Johdanto	1	5.3. Pääsynhallintaprosessi	23	9 Hallinnollinen turvallisuus	41
2 Fyysisen suojaamisen edellytykset	2	5.4. Murtohälytysjärjestelmät	25	9.1. Turvallisuusjohtaminen	42
2.1. Vaatimustenmukaisuus	2	5.5. Analytiikkajärjestelmät	26	9.2. Turvallisuusosaaminen	42
2.2. Riskienhallinta	5	5.6. Tutkajärjestelmät	27	9.3. Turvallisuuskulttuuri	42
2.3. Organisaation jatkuvuudenhallinta ja valmiussuunnittelu	7	5.7. Droonit	27	9.4. Poikkeamienhallinta	42
3 Fyysisen turvallisuuden periaatteet	8	6 Vartiointipalvelut	28	9.5. Pääsynhallinta	43
3.1. Riskiperusteinen suojaaminen	8	6.1. Paikallisvartiointi	28	9.6. Turvallisuusauditoinnit	43
3.2. Kohteiden kriittisyysluokittelu	9	6.2. Aulavartiointi	29	9.7. Jatkuva parantaminen	44
3.3. Fyysisen turvallisuuden suunnitteluperiaatteet	9	6.3. Piirivartiointi	29	10 Työkalut	45
3.4. Suojattavat alueet	11	6.4. Etävalvontapalvelut	29	11 Liite 1 – Lait, standardit ja oheismateriaalit	46
3.5. Turvallisuuskartoitus	12	6.5. Hälytysvalvonta	29	Vaatimustenmukaisuus	46
3.6. Fyysisen suojauksen testaaminen	12	6.6. Hälytysvartiointi	29	11.1. Lait ja asetukset	46
4 Rakenteellinen suojaus	13	7 Suojaamisen kohde-esimerkit	30	11.2. Standardit	48
4.1. Aidat	14	7.1. Perustaso	31	11.3. Ministeriöiden julkaisemat suositukset ja ohjeet	49
4.2. Henkilöportit	14	7.2. Korotettu taso	32	11.4. Muut oppaat ja ohjeet	49
4.3. Ajoneuvoportit	15	8 Hankintaprosessi	33	11.5. Periaatepäätökset ja muut lähteet	50
4.4. Seinät, katot ja lattiat	15	8.1. Turvajärjestelmien tarvemäärittely	34		
4.5. Ovirakenteet	15	8.2. Hankittavat järjestelmät	34		
4.6. Ikkunat ja aukot	16	8.3. Turvajärjestelmiin liittyvät palvelut	34		
4.7. Valaistus	16	8.4. Hinta-arvion laatimien	35		
4.8. Arkkitehtuuriset ratkaisut	16	8.5. Rakenteellinen suojaus	35		
4.9. Lukitusratkaisut	16	8.6. Kameravalvontajärjestelmä	36		
5 Tekniset turvallisuusjärjestelmät	18	8.7. Kulunvalvontajärjestelmä	37		
5.1. Kameravalvontajärjestelmät	18	8.8. Murtohälytysjärjestelmä	38		
5.2. Kulunvalvontajärjestelmät	22	8.9. Lukitusratkaisut	39		
		8.10. Vartiointipalvelut	40		

Julkaisija: Huoltovarmuuskeskus
Laatinut: Huoltovarmuuskeskus ja Seclion Oy /
Mikko Oinonen (toim.)
Taitto: KMG Turku
Julkaisuvuosi: 2025

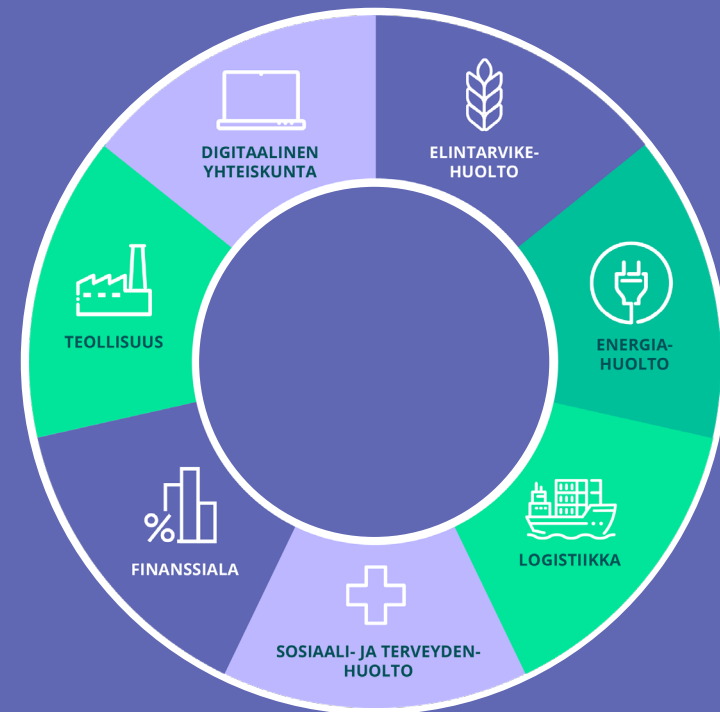
1 Johdanto

Huoltovarmuudella tarkoitetaan väestön toimeentulon ja suojaamisen, maan talouselämän, maanpuolustuksen sekä turvallisuuden kannalta välttämättömien taloudellisten toimintojen, välttämättömien tavaroiden, materiaalien ja palveluiden tuotannon ja saatavuuden sekä kriittisen infrastruktuurin turvaamista vakavien häiriötilanteiden ja poikkeusolojen varalta sekä niiden aikana.

Käytännön tasolla huoltovarmuuden turvaaminen perustuu pitkälti elinkeinoelämän varautumiseen sekä turvallisuuden varmistamiseen. Yksi keskeinen osa yrityksen turvallisuusjohtamista on yrityksen toiminnan fyysinen suojaaminen. Fyysisen suojauksen opas käsittelee sitä, miten fyysinen turvallisuus tulisi tarkoituksenmukaisesti ja riittävässä määrin huomioida osana turvallisuusjohtamista ja laajempaa varautumisen kokonaisuutta. Nämä kokonaisuudet antavat perusteet fyysisen suojaamiseen, mutta tässä

oppaassa niitä on tarkoituksenmukaista käsitellä vain keskeisiltä osin. Tarkemmin varautumisen perusteita käsitellään muun muassa Yrityksen varautumisen suositukset -oppaassa (julkaisu 2026 alussa, HVK). Turvallisuusjohtamisen perusteita on koottu esimerkiksi Elinkeinoelämän (EK) yritysturvallisuusmallissa.

Tämä ohje on suunnattu huoltovarmuuskriittisille yrityksille, mutta se tarjoaa kaikille organisaatioille keskeisiä tietoja ja valmiuksia, liittyen fyysisen turvallisuuden suunnitteluperiaatteisiin sekä eri suojautumisen keinoihin, kuten turvajärjestelmiin, rakenteelliseen suojaukseen, riskienhallintaan sekä hallinnollisiin prosesseihin. Ohjeessa ei ole tarkoitus käsitellä järjestelmien ja laitteiden yksityiskohtaisia tietoja, vaan antaa yleistason ymmärrys järjestelmistä, niiden käyttötarkoituksesta sekä tukea niiden hankintaa. Ohjeistuksen tavoitteena on parantaa huoltovarmuustoimijoiden fyysisen suojautumisen tasoa.



Kuva 1: Huoltovarmuuden sektorit (muuttumassa 2026).

2 Fyysisen suojaamisen edellytykset

2.1. Vaatimustenmukaisuus

Fyysisen suojauksen kehittäminen aloitetaan tunnistamalla vaatimukset, joita organisaatioon ja toimintaan kohdistuu. Kuvassa 2 on esitetty vaatimustenmukaisuuden (Compliance) keskeiset kokonaisuudet, joilla fyysisen turvallisuuden tasoa voidaan määritellä.

Vaatimustason määrittämiseen vaikuttavat sekä sisäiset että ulkoiset tekijät. Ulkoisia tekijöitä ovat esimerkiksi organisaatiota koskevat lakisääteiset velvoitteet, asetukset, standardit, huoltovarmuuteen tai varautumiseen liittyvät viranomaismääräykset, sekä olemassa olevat sopimusvelvoitteet muiden toimijoiden kanssa. Sisäisiä tekijöitä puolestaan ovat mm. liiketoiminnalliset ja strategiset tavoitteet, työjärjestys tai toimintasääntö, käytettävissä olevat voimavarat ja osaaminen.



Kuva 2: Vaatimustenmukaisuuden keskeiset kokonaisuudet



Lait ja asetukset

Lait ja asetukset määrittelevät organisaatioille velvollisuuksia fyysiseen turvallisuuteen liittyen. Näitä velvollisuuksia esiintyy niin yleisesti yksityishenkilöitä sekä toiminnanharjoittajia koskevassa lainsäädännössä, mutta myös toimialakohtaisissa laeissa ja asetuksissa.

Fyysisen suojaamisen perusteisiin vaikuttavia kansallisia lakeja ovat esimerkiksi:

- Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta 310/2025 (**CER-direktiivi**)
 - ▶ tavoitteena parantaa yhteiskunnan kriittisten palveluiden ja infrastruktuurien häiriönsietokykyä.
- Kyberturvallisuuslaki 124/2025 (**NIS2-direktiivi**)
 - ▶ tavoitteena parantaa kyberturvallisuuden tasoa.
- Tietosuojalaki 1050/2018 (**GDPR-asetus**)
 - ▶ sääntelee henkilötietojen käsittelyä, asettaa organisaatioille velvollisuuden osoittaa, että ne käsittelevät henkilötietoja lainmukaisesti, läpinäkyvästi ja turvallisesti.
- Asetus finanssialan digitaalisesta häiriönsietokyvystä (EU) 2022/2554 (DORA-asetus)
 - ▶ koskee rahoitusalan digitaalista häiriönsietokykyä, eli kykyä ennakoida riskejä, sekä toipua ja sopeutua teknologisiin häiriöihin ja kyberuhkiin.

Vaikka organisaatiolla ei olisi käytössään teknisiä turvajärjestelmiä, on fyysisen turvallisuuden ja varautumisen osalta tärkeää ottaa kuitenkin huomioon muun muassa **Työturvallisuuslaki** (738/2002), joka

velvoittaa työnantajan turvallisuusjärjestelyihin työssä, johon liittyy ilmeinen väkivallan uhka. Työ ja työolosuhteet on järjestettävä siten, että väkivallan uhka ja väkivaltilanteet ehkäistään mahdollisuuksien mukaan ennakolta. Tällöin työpaikalla on oltava väkivallan torjumiseen tai rajoittamiseen tarvittavat asianmukaiset turvallisuusjärjestelyt tai laitteet, sekä mahdollisuus avun hälyttämiseen (27 § Väkivallan uhka).

Lakien noudattamatta jättämisellä on aina negatiivisia seurauksia, joiden vaikutus riippuu noudattamatta jätetyn lain luonteesta, poikkeaman vakavuudesta, sekä muista mahdollisista tapauskohtaisista tekijöistä. Lain noudattamatta jättämisen seuraukset voivat vaihdella huomautuksista aina sakkorangaistuksiin, rikossyytteisiin tai jopa toimiluvan menetykseen.

Lait, asetukset, linkit ja muu syventävä tieto on koottu liitteeseen 1.

Standardit

Standardit eroavat lainsäädännöstä siten, ettei standardeilla lähtökohtaisesti ole oikeudellista asemaa. Standardit voivat kuitenkin saada tämän aseman, mikäli ne julkaistaan lakien ja asetusten kautta erikseen määritettyinä. Tyypillisesti standardeilla viitataan niin sanottuihin virallisiin standardeihin (esim. SFS, EN ja ISO), mutta myös yrityksillä ja eri organisaatioilla voi olla omia, joko sisäisesti tai ulkoisesti julkaistuja standardeja. Näiden noudattamista voidaan vaatia vain sopimuksellisin keinoin.

Viralliset standardit jakaantuvat kansallisiin, eurooppalaisiin sekä kansainvälisiin eli maailmanlaajuisiin standardeihin. Standardien käyttö lisää turvallisuutta sekä eri toimijoiden välisten toimintatapa menettelyiden yhteensopivuutta. Turvallisuutta ohjaavia standardeja ovat esimerkiksi:

- **ISO 31000** on kansainvälinen standardi, joka tarjoaa periaatteet, viitekehyksen ja prosessin organisaation riskienhallintaan
- **ISO 22301** on kansainvälinen standardi, joka käsittelee liiketoiminnan jatkuvuuden hallintajärjestelmää (BCMS). Tavoitteena on varmistaa häiriötilanteilta suojautuminen, niiden esiintymisen todennäköisyyden pienentäminen, niihin varautuminen ja reagoiminen sekä niistä palautuminen.
- **ISO 27001** on kansainvälinen standardi, joka määrittelee vaatimukset tietoturvallisuuden hallintajärjestelmälle (ISMS) joka kattaa riskienhallinnan, turvatoimet ja vaatimustenmukaisuuden varmistamisen, ja sitä voidaan soveltaa kaikenkokoisissa ja -tyyppisissä organisaatioissa.
- **SFS-EN 50131** on kansainvälinen standardi, joka määrittää vaatimukset rakennuksiin asennetuille murto- ja ryöstöhälytysjärjestelmille.



Kansalliset ohjaavat strategia-asiakirjat

Yhteiskunnan turvallisuusstrategia 2025

Valtioneuvoston periaatepäättös yhteiskunnan turvallisuusstrategiasta määrittelee Suomen varautumiseen liittyvät yleiset periaatteet. Toiminta perustuu suomalaiseen kokonaisturvallisuuden yhteistoimintamalliin, jossa valtionhallinto, viranomaiset, elinkeinoelämä, maakunnat ja kunnat sekä yliopistot ja tutkimuslaitokset, järjestöt ja yhteisöt sekä yksilöt muodostavat yhteistyöverkoston.

Suomen kyberturvallisuusstrategia 2024–2035

Suomen kyberturvallisuusstrategia on uudistettu 2025 hallitusohjelman mukaisesti vastaamaan muuttunutta toimintaympäristöä. Kyberturvallisuusstrategian uudistamisessa on otettu huomioon kyberturvallisuudirektiivin (NIS2) vaatimukset sekä muu aiheeseen liittyvä keskeinen strategia- ja selontekotyö.

Valtioneuvoston päätös huoltovarmuuden tavoitteista

Valtioneuvosto on asettanut yleiset tavoitteet huoltovarmuudelle. Päätös pitää sisällään huoltovarmuuden toteuttamisen periaatteiden ja kansallisten tavoitteiden lisäksi muun muassa kriittisen infrastruktuurin suojaamisen, varautumisen tavoitteet sekä kriittisen tuotannon ja palveluiden tuotannon turvaamisen tavoitteet.

Kansallinen ja alueellinen riskiarvio

Valtakunnallisen riskiarvion kokonaisuus koostuu sekä kansallisesta että alueellisista riskiarvioista. Niissä kartoitetaan säännöllisesti ihmisiä, ympäristöä, omaisuutta ja yhteiskunnan kriittisiä järjestelmiä uhkaavia riskejä, jotka edellyttävät viranomaistoimenpiteitä. Kansallinen ja alueelliset riskiarvot ovat saatavilla sisäministeriön Internetsivuilta.

- **Riskienhallintapolitiikka**, jonka tarkoituksena on ehkäistä vahinkoja ja minimoida niiden vaikutukset. Systemaattinen riskienhallinta tukee strategista ja operatiivista päätöksentekoa varmistamalla, että organisaatio tunnistaa ja hallitsee siihen kohdistuvat uhat ja riskit, säilyttää toimintakykynsä ja parantaa reagointikykyään. Riskit pidetään hallinnassa siten, ettei organisaation toiminta vaarannu.
- **Tietoturvapoliittika**, jonka tarkoituksena on suojata ja varmistaa tiedon luottamuksellisuus, eheys ja saatavuus. Se kattaa toimenpiteet, joilla suojataan tiedot vahingoilta, luvattomalta käytöltä ja tietovuodoilta.

Suosituksilla viitataan sellaisiin ulkoisiin tai sisäisiin suosituksiin, jotka eivät välttämättä velvoita tiettyyn tapaan toimia. Suosituksia voidaan julkaista sekä eri organisaatioiden, mutta myös viranomaisen toimesta. Edes viranomaisen julkaisema suositus ei ole oikeudellisessa asemassa tai muulla tavalla velvoittava. Kyseessä on kehote tai kannanotto liittyen tiettyyn tapaan toimia. Hyvänä esimerkkinä voidaan pitää Vakuutusyhtiöiden suojeluohjeita, jotka kuitenkin voivat olla sopimuksellisesti velvoittavia. Vakuutusyhtiöiden suojeluohjeet ja vakuutusehdot sisältävät muun muassa rikosten ennaltaehkäisyyn laadittuja ohjeistuksia, murtosuojaukseen liittyviä määräyksiä, toimialakohtaisia suosituksia ja velvoitteita. Niissä voi olla myös määritetty toimipaikkakohtaisia turvallisuusvelvoitteita.

Politiikat ja suositukset

Politiikalla tarkoitetaan organisaation sisäisiä linjauksia, joiden avulla järjestetään ja ohjataan organisaation harjoittamaa toimintaa. Organisaation politiikkojen on noudatettava voimassa olevaa lainsäädäntöä sekä kutakin organisaatiota mahdollisesti sopimuksellisesti velvoittavia vaatimuksia ja regulaatioita. Poliittika on organisaation sisäinen linjaus tai strategia. Esimerkkejä organisaatioiden turvallisuuteen liittyvistä strategioista:

- **Turvallisuuspolitiikka**, joka määrittelee, miten organisaatio suojaa henkilöstöään, tietojään, omaisuuttaan ja toimintaympäristöään. Tavoitteena on varmistaa toiminnan jatkuvuus, minimoida riskit ja noudattaa lakisääteisiä velvoitteita (kuten työturvallisuus-, pelastus- ja tietosuojalaki). Turvallisuuspolitiikka myös viestii turvallisuuden merkityksestä ja sitouttaa henkilöstön turvallisuustavoitteiden saavuttamiseen.



Asiakkaiden ja sidosryhmien vaatimukset

Usein asiakkaat ja sidosryhmät edellyttävät, että yrityksen tilat, henkilöstö ja kriittiset resurssit ovat suojattuja fyysisiltä uhkilta ja häiriöiltä. Turvallisuusratkaisujen tulee täyttää lainsäädännön, sopimusten ja alan standardien vaatimukset sekä varmistaa toiminnan jatkuvuus kaikissa olosuhteissa. Luottamus syntyy ennakkoivasta riskienhallinnasta ja selkeästä vastuunjaosta. Jotkut sidosryhmät saattavat edellyttää myös riittävän turvallisuustason ja pääsynhallinnan toteuttamista, sekä sen osoittamista dokumentoidusti, erityisesti tapauksissa, joissa organisaatio saa käsiteltäväksi ja säilytettäväksi turvallisuusluokiteltua viranomaisten tietoa tai muuten salassa pidettävää toisen organisaation tietoa.

Valvovan viranomaisen vaatimukset koskevat organisaatioita, jotka kuuluvat viranomaisvalvonnan piiriin esimerkiksi toimiluvan tai muun liiketoiminnan jatkuvuuden edellyttämän luvan perusteella.

Riittävän tasoista riskienhallintaa ja toiminnan fyysistä suojaamista on hyvä edellyttää myös omilta toimittajilta ja alihankkijoilta. Hyviä ohjeita tähän löytyy mm. Huoltovarmuuskeskuksen hankintojen ja sopimusperusteisen varautumisen SOPIVA-suosituksista (uudet ohjeet julkaistaan alkuvuodesta 2026).

2.2. Riskienhallinta

Riskienhallinta muodostaa perustan fyysisen suojauksen edellytyksille. Riskienhallinnan tavoite on tukea yrityksen johtamista, päätöksentekoa, henkilöstön koulutusta ja perehdytystä, jotta sen tavoitteisiin mahdollisesti vaikuttavat riskit ja riskien seuraukset tunnistetaan. Organisaation johto saa riskienhallinnan avulla kokonaiskuvan toimintansa merkittävimmistä riskeistä ja pystyy siten sovittamaan päätöksensä, ja riskejä rajoittavat toimenpiteet riskinkantokykynsä ja riskinottohalunsa puitteisiin. Samat periaatteet ovat sovellettavissa fyysisen suojauksen toteuttamiseen.

Fyysiseen toimintaympäristöön liittyvän riskienhallinnan toteuttaminen vaihtelee kunkin organisaation tarpeiden mukaan. Organisaation toimipaikkoja ja -tiloja tulee suojata riskiarvioihin perustuen kustannustehokkaasti. Tavoitteena on luoda häiriötön ja turvallinen työskentely- ja asiointiympäristö sekä organisaatiolle arvokkaan tiedon ja materiaalin anastamisen tai vahingoittamisen estämisen.

Liiketoimintalähtöisessä riskienhallinnassa turvallisuuden liittyvät riskit eivät välttämättä nouse suorilta vaikutuksiltaan kovin korkealle yrityksen riskiprofiilissa, verrattuna esimerkiksi liiketoiminnallisiin riskeihin. Turvallisuusriskien arvioinnissa onkin syytä kiinnittää huomiota taloudellisten vaikutusten ohella esimerkiksi yrityksen toimintavarmuuteen, henkilöstön ja asiakkaiden turvallisuuteen, vaatimustenmukaisuuteen sekä maineeseen vaikuttaviin riskeihin.

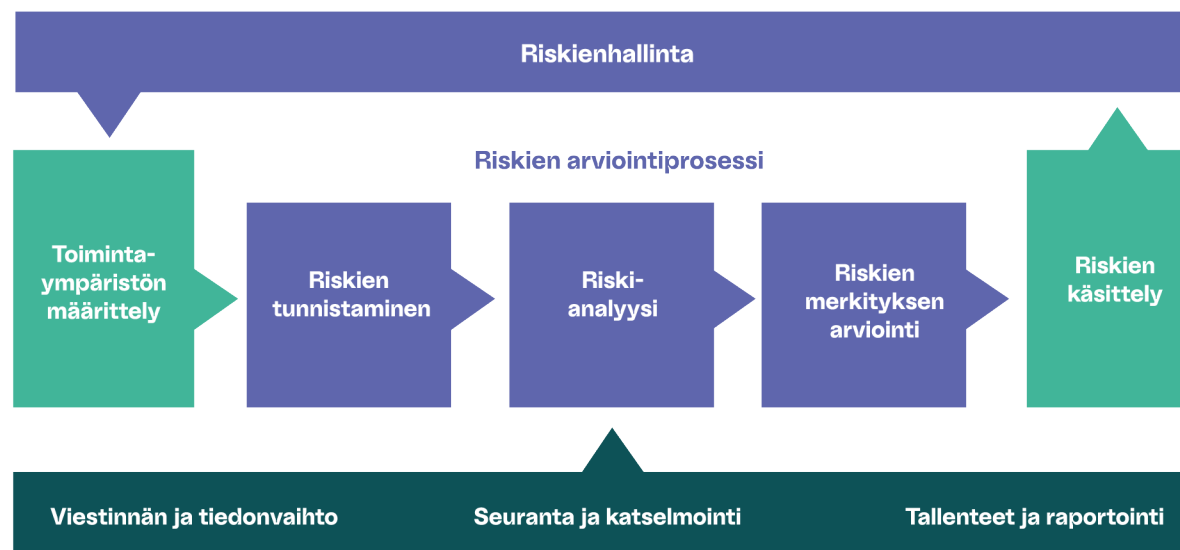
Riskienhallintaprosessi

Riskienhallintaprosessin perustana ovat ulkoisten ja sisäisten taustatietojen (ja muuttujien) määrittely. Taustatiedoissa määritellään sellaiset organisaatioon liittyvät tiedot ja olosuhteet, jotka vaikuttavat riskienhallintaprosessin toteuttamiseen. Riskienhallintaprosessin tarkoituksena on auttaa tunnistamaan yrityksen tavoitteita uhkaavia riskejä, edesauttaa yrityksen johtoa analysoimaan tunnistettuja riskejä ja niiden vaikutuksia sekä päättämään arvioinnin perusteella kullekin riskille parhaiten sopivista hallintakeinoista.

Riskienhallintaprosessi muodostuu yleensä kolmesta osaprosessista; toimintaympäristön määrittely, riskien arvioiminen ja riskien käsittely (Kuva 3). Näitä osaprosesseja tukevat niin sanotut tukiprosessit, joihin kuuluvat viestintä ja tiedonvaihto, seuranta ja katselmointi sekä tallenteet ja raportointi. Lisäksi riskien arvioiminen itsessään jakautuu kolmeen osaan; riskien tunnistamiseen, analysoimiseen ja merkityksen arvioimiseen. Kattavaa tietoa riskienhallinnan laadukkaasta toteuttamisesta saa esimerkiksi ISO 31000 Riskienhallinta -standardista.

Miksi turvallisuusriskejä arvioidaan?

- Pyritään varmistamaan toiminnan häiriöttömyys ja jatkuvuus
- Tuotetaan tietoa päätöksentekoa varten (miksi, mitä, miten?)



Kuva 3: Riskienhallinta ja riskien arviointiprosessi

2.3. Organisaation jatkuvuudenhallinta ja valmiussuunnittelu

Organisaation jatkuvuudenhallinta on strategista ja operatiivista toimintaa, jolla varmistetaan organisaation toiminnan jatkuminen häiriötilanteissa ja palautuminen niistä hyväksyttävällä tasolla. Se pohjautuu riskienhallintaan ja sisältää suunnitelmien ja menettelytapojen luomisen häiriötilanteiden varalle. Tavoitteena on suojata organisaation kriittisiä toimintoja, järjestelmiä, sekä varmistaa niiden ja liiketoiminnan jatkuvuus. Myös erilaisten turvallisuuteen ja fyysiseen suojaamiseen liittyvien toimintojen jatkuvuus on turvattava. Jatkuvuudenhallintaan on tarjolla hyviä malleja, esim. ISO 22301 -standardissa.

Jatkuvuudenhallinnan keskeiset vaiheet

- **Tunnistaminen ja analysointi:** Tunnistetaan kriittiset liiketoiminnot sekä niitä tukevat resurssit ja riippuvuudet.
- **Riskien arviointi:** Tunnistetaan potentiaaliset uhkat ja riskit. Arvioidaan niiden todennäköisyyttä ja merkittävyyttä sekä määritellään riskien hallintatoimenpiteet.
- **Strategian laatiminen:** Luodaan strategia, jossa määritellään, miten kriittisiä toimintoja suojataan ja miten niistä toivutaan.
- **Menettelytapojen ja suunnitelmien laatiminen:** Kehitetään menettelytavat häiriötilanteisiin. Näitä voivat olla esimerkiksi viestintäsuunnitelma, toipumissuunnitelma häiriön jälkeiseen toimintaan, turvallisuusjärjestelyt häiriötilanteissa sekä erilaiset varajärjestelyt, esim. suunnitelma vaihtoehtoihin toimitiloihin siirtymiseksi.
- **Toteutus, testaus ja ylläpito:** Toteutetaan suunnitelmat, testataan niitä säännöllisesti harjoitusten avulla ja kehitetään niitä tarvittaessa, jotta ne kyetään pitämään ajantasaisina ja vaikuttavina.

Jatkuvuudenhallinta painottuu normaaliolojen häiriöiden hallintaan ja liiketoiminnan keskeytysten minimoimiseen, kun taas valmiussuunnittelu varmistaa toiminnan jatkumisen vakavissa häiriötilanteissa ja poikkeusoloissa, joissa resurssit ja olosuhteet voivat muuttua merkittävästi. Valmiussuunnittelulla varaudutaan kriiseihin, jotka voivat uhata yhteiskunnan toimintakykyä. Se keskittyy turvaamaan lakisääteiset tehtävät ja kriittiset palvelut myös äärimmäisissä olosuhteissa. Yrityksen on syytä huomioida fyysisen suojauksen suunnittelussa ja tason mitoituksessa myös sen rooli ja tehtävät yhteiskunnallisten kriittisten palveluiden arvoketjussa.



3 Fyysisen turvallisuuden periaatteet

3.1. Riskiperusteinen suojaaminen

Riskiperusteisella suojaamisella viitataan sellaiseen turvallisuuden suunnitteluun, jossa suojaustoimenpiteiden valinta perustuu tapauskohtaisesti suoritettuun riskiarvioon ja hyväksyttyyn riskitasoon. Tyypillisiä vaihtoehtoisia tapoja turvallisuuden suunnittelulle ovat esimerkiksi yleismallisten suunnitteluohjeiden tai niin sanottujen yleisesti alalla hyväksi todettujen käytänteiden mukaan suojaaminen. Se ei kuitenkaan ole suositeltavaa, sillä kaikki kohteet ja niissä harjoitettava toiminta sekä organisaatioissa vallitsevat toimintatavat ovat lähtökohtaisesti erilaisia. Ilman riskiperusteista suojaimista merkittäviäkin tapauskohtaisia muuttujia jää helposti huomioimatta.



3.2. Kohteiden kriittisyysluokittelu

Turvallisuuden ja toiminnan jatkuvuuden näkökulmasta, eri tilojen kriittisyys kiinteistöissä ja toimitiloissa vaihtelee. Tämä vaikuttaa keskeisesti tilojen suojaustarpeisiin; turvallisuuden ja toiminnan jatkuvuuden kannalta kriittisimmät tilat edellyttävät lähtökohtaisesti korkeampaa suojauksen tasoa, kun taas vähemmän kriittisille tiloille riittää matalampi suojauksen taso.

Kriittisyysluokittelussa kohteen tilat jaetaan tyypillisesti eri kriittisyysluokkiin, joilla on toisistaan eriävät suojaustarpeet. Nämä kriittisyysluokat muodostetaan arvioimalla tilojen kriittisyyden määrittäviä tekijöitä, joita ovat muun muassa tilan käyttötarkoitus, tiloissa harjoitettava toiminta, sekä tiloissa säilytettävät laitteet ja järjestelmät, omaisuus sekä tietoaaineisto.

Kriittisyysluokittelu mahdollistaa tilan kriittisyyteen nähden oikein suhteutetun, tarkoituksenmukaisen ja kustannustehokkaan suojaamisen. Lisäksi sen avulla vältetään mahdollisilta suojauksen ylimitoituksilta, jotka nostavat kustannuksia tarpeettomasti sekä voivat hankaloittaa jokapäiväistä toimintaa kohteella.

3.3. Fyysisen turvallisuuden suunnitteluperiaatteet

Kohteen fyysisen suojaamisen tarkoituksena on suojata organisaation tahtotilan tai toiminnan kannalta tärkeitä arvoja erinäisiltä uhilta. Organisaatioiden suojattavat kohteet jaetaan tyypillisesti seuraaviin kategorioihin: ihmiset, tieto, laitteisto, omaisuus, toiminta ja maine. Näitä kohteita on mahdollista suojata tunnistamalla, estämällä ja havaitsemalla ennakkoon haitallinen toiminta tai negatiiviset tapahtumat, reagoimalla niihin ja suunnittelemalla ennalta keinot organisaation toiminnan tai tilanteen palauttamiseksi normaalitilaan häiriö- tai poikkeustilanteen jälkeen.

Lähtökohtana kohteen suojaamiseen toimii suojattavien arvojen tunnistaminen – mikä meille on tärkeää? Näitä seikkoja voidaan tunnistaa esimerkiksi edellä mainituista kuudesta kategoriasta. Tyypillisiä suojattavia kohteita ovat jokapäiväisen toiminnan mahdollistava työntekijöiden terveys, toiminnan häiriöttömyyden kannalta kriittiset laitteet, järjestelmät ja prosessit, organisaation vakavaraisuuteen vaikuttava tai muu omaisuus, salassa pidettävät tietoaaineistot sekä organisaation maine.

Monitasoisen suojaamisen ja siinä sovellettavien eri kontrollien tavoitteena on varmistaa suojattavien kohteiden turvaaminen hyödyntäen vasteaika-ajattelua. Tarkoituksena on vahingollisen toiminnan pysäyttäminen määritellyssä vasteajassa. Periaate perustuu kolmeen pääelementtiin:

Hidaste

Hidasteiden tehtävä on lisätä aikaa, jonka tunkeutuja tarvitsee päästäkseen seuraavaan suojaustasoon. Jokainen lisätty sekunti kasvattaa mahdollisuutta estää rikos tai tunkeutuminen ja aiheuttaa viivytyksiä tunkeutujalle. Hidasteet voivat olla esimerkiksi:

- Rakenteellisia ratkaisuja: aidat, portit, lukot, ovet, lasit ja rakenteet
- Teknisiä järjestelmiä: kulunvalvonta
- Prosessuaalisia keinoja: tarkastuspisteet ja henkilöllisyystarkastukset

Havaitseminen

Havaitsemisen tarkoituksena on mahdollistaa, että poikkeamat havaitaan ajoissa. Havainnointi on kriittistä, sillä hidaste ilman havaintoa ei johda vasteeseen. Havaitsemiskeinoja ovat esimerkiksi:

- Ihmisten tekemät havainnot: Henkilökunnan tai vartiointin toimesta
- Tekniset järjestelmät: kulunvalvonta, -kamera- ja murtohälytysjärjestelmät

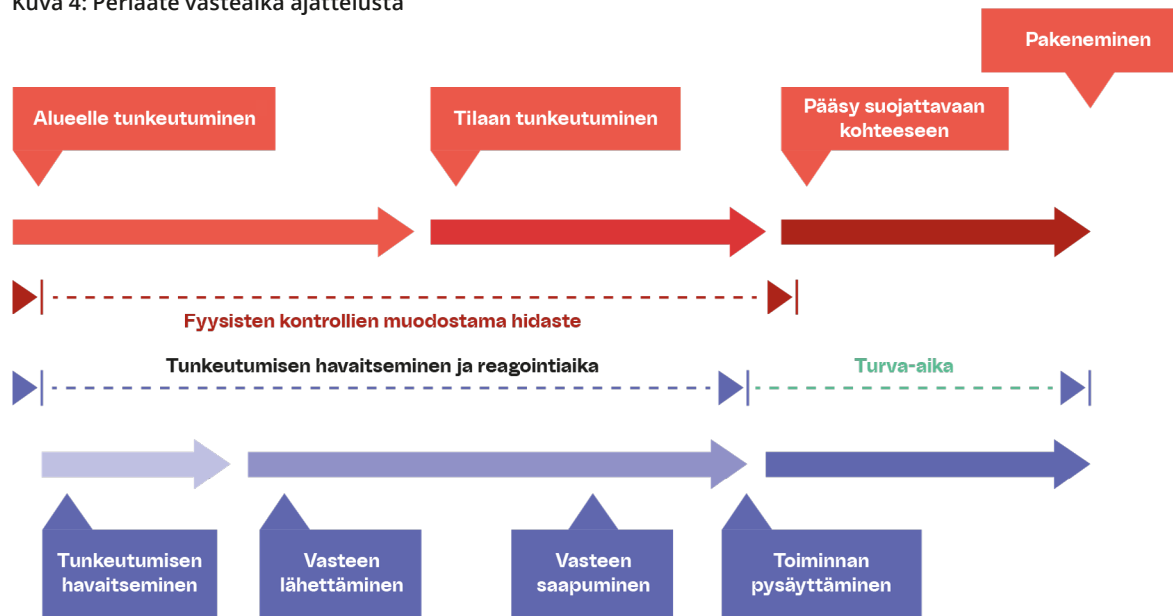
Vaste

Vaste tarkoittaa toimintaa, joka käynnistyy havainnosta ja tavoitteellisesti toteutuu hidasteen mahdollistamassa ajassa.

- Hälytyksen siirto valvontakeskukseen tai vartijalle
- Vartijan tai poliisin vaste kohteeseen saapumiselle
- Automaattiset toimenpiteet: ovien lukitus, kameravalvonnan kohdistus ja tilan eristäminen.

Vasteen tehokkuus riippuu siitä, kuinka nopeasti tieto kulkee ja kuinka hyvin resurssit on organisoitu. Hidaste ja havaitseminen ilman vastejärjestelmää ei riitä – kaikki ovat välttämättömiä.

Kuva 4: Periaate vasteaika ajattelusta



Tavoitteena on, että tunkeutumiseen kuluva aika on suurempi kuin sen pysäyttämiseen kestävä aika, jossa: **Laskukaava: $T_k > T_h + T_r + T_p$**

- T_k = Tunkeutumiseen kestävä aika
- T_h = Aika tunkeutumisen alkamisesta ja havaitsemisesta
- T_r = Aika havaitsemisesta reagointiin
- T_p = Toiminnan pysäyttämisen kuluva aika

3.4. Suojattavat alueet

Toimitilaturvallisuuden tärkeimpiä peruseriaatteita on kerroksittain suojaaminen, jolla pyritään estämään asiaton pääsy kohteeseen ja sen alueille, sekä rajoittamaan mahdollisia tunkeutumisyrityksiä. Kullekin vyöhykkeelle asetettavilla suojauskeinoilla pyritään havaitsemaan ja/tai hälyttämään mahdollisesta tunkeutumisyrityksestä tai estämään tai hidastamaan niitä. Suunnittelun perustana toimii suojattavien arvojen tunnistaminen ja kohteisiin suoritettut riskiarviot.

Fyysisen turvallisuuden suunnittelun kohde ja sen alueet jaetaan kehämäisesti esimerkiksi viiteen suojattavaan vyöhykkeeseen, mitä kutsutaan myös sipuliperiaatteeksi. Tyypillisesti suojauksen taso nousee mitä lähemmäksi sisintä vyöhykettä lähestytään. Kullekin vyöhykkeelle asetetaan tarkoituksenmukaisia suojauskeinoja, jotka yhdessä muodostavat vaikuttavan suojauskokonaisuuden. Vyöhykkeille asetettavat suojauskeinot voivat olla niin rakenteellisia kuin teknisiäkin ratkaisuja. Lisäksi kohteen suojaamiseen voidaan käyttää erinäisiä vartiointipalveluja. Tärkeää on kuitenkin huomioida, etteivät jokaisen kohteen tarpeet ole samanlaiset. Voi siis olla kohteita, joissa ei ole toimintaympäristö huomioiden tarkoituksenmukaista tai ylipäättään mahdollista hyödyntää kaikkia esitettyjä suojattavia vyöhykkeitä.

Suojattavien alueiden jako viiteen eri suojausvyöhykkeeseen:

Kehäsuojaus

Kiinteistön ulkokehän, kuten aitalinjojen suojaaminen, sekä valvonta.

Aluesuojaus

Kiinteistöä ympäröivän maa-, meri-, tai ilma-alueen suojaaminen, sekä valvonta.

Kuorisuojaus

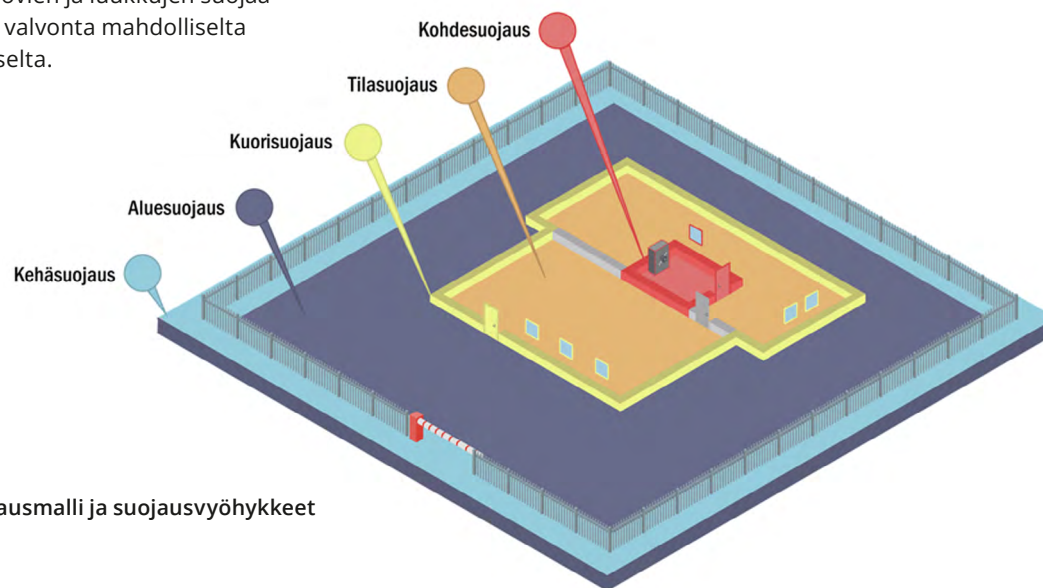
Rakennuksen ulkokuoren eli seinien, katon, ikkunoiden, ovien ja luukkujen suojaaminen, sekä valvonta mahdolliselta tunkeutumiselta.

Tilasuojaus

Rakennuksen sisätilojen suojaaminen. Tilat ovat suositeltavaa jakaa eri kriittisyysluokkiin, joille määritellään omat suojaustasot ja toimenpiteet.

Kohdesuojaus

Organisaation kriittisimpien toimintojen, tilojen tai kohteiden suojaaminen. Pääsy kohdesuojauksen alueelle rajataan usein hyvin tiukaksi.



Kuva 5: Suojausmalli ja suojausvyöhykkeet

3.5. Turvallisuuskartoitus

Fyysiseen suojaukseen liittyvää lähtötilanteen selvittäminen on hyvä aloittaa suojattavien kohteiden tunnistamisesta sekä niiden suojaustarpeen arvioinnista, eli turvallisuuskartoituksesta. Tavoitteena on kerätä tietoa suojausta vaativista seikoista ja niiden kriittisyydestä toiminnassa.

Mikäli kohteessa on olemassa fyysisen suojauksen menettelyjä, kuten turvajärjestelmiä, voidaan usein hyödyntää olemassa olevia suunnitelmia ja materiaaleja turvallisuuskartoituksen tueksi. Olemassa olevien menettelyiden ja ratkaisujen turvallisuuskartoituksessa korostuu niiden riittävyyden ja tarkoituksenmukaisuuden arviointi, sekä toimintaympäristössä tapahtuvien muutosten myötä ilmenevien uusien tarpeiden tunnistaminen.

- Mitä tässä nimenomaisessa kohteessa on tarkoituksenmukaisinta suojata ja miksi se on tärkeää?
- Millaisia tiloja on käytössä ja mikä on niiden käyttötarkoitus?
- Mikä on kohteen nykyisen suojauksen taso?
- Ovatko tilamuutokset vaikuttaneet suojaustarpeisiin?

Turvallisuuskartoitus voidaan joko tilata palveluna tai suorittaa organisaation sisäisen asiantuntijan toimesta. Tärkeintä kuitenkin on se, että turvallisuuskartoituksen suorittaa henkilö, jolla on riittävä asiantuntemus turvallisuuskartoituksista ja kartoitettavasta aihealueesta. Näin tarvekartoituksessa ja sitä kautta hankinnoissa voidaan välttyä turvallisuuden yli- sekä alimitoituksia, mutta varmistetaan myös se, ettei nykyisissä järjestelyissä tai toiminnassa ole havaittavissa puutteita.

3.6. Fyysisen suojauksen testaaminen

Fyysisen suojaamisen testaamisen tarkoituksena on arvioida yrityksen tai sen kohteen fyysisen suojauksen tasoa ja suorituskykyä. Se on niin sanotusti hyökkäysmulaatioon perustuvaa auditointia, jonka tavoitteena on antaa yritykselle tietoa mahdollisista fyysisen suojauksen puutteista ja haavoittuvuuksista. Testaaminen voi olla tiedustelua, jossa tavoitteena on kerätä mahdollisimman paljon tietoa avoimista lähteistä (OSINT – Open Source Intelligence), jota voitaisiin myöhemmin hyödyntää yritystä vastaan vahingollisesti. Vaihtoehtoisesti testaamisella voidaan pyrkiä

tunkeutumaan esim. yrityksen tiloihin ja saamaan haltuun tietoa tai materiaalia.

Tunkeutumisharjoitus on suunniteltu testi, jossa simuloidaan kohteeseen tunkeutumista organisaation fyysisten suojausten toimivuuden ja tehokkuuden arvioimiseksi. Harjoituksessa ulkopuoliset tai ennalta nimetyt henkilöt pyrkivät luvatta pääsemään alueelle, tilaan tai rakennukseen hyödyntäen mahdollisia suojausten heikkouksia. Tavoitteena on tunnistaa järjestelmien, rakenteiden ja toimintatapojen puutteet sekä kehittää organisaation valmiuksia torjua todellisia uhkia. Harjoitus tulee toteuttaa suunnitellusti ja hallitusti, ja siitä tulee aina sopia etukäteen vastuuhenkilöiden kanssa.

Harjoituksen jälkeen käydään läpi havaintoja ja tuloksia, joiden pohjalta voidaan päivittää turvallisuussuunnitelmia, ohjeistaa henkilöstöä sekä parantaa rakenteellisia ja teknisiä ratkaisuja. Näin varmistetaan, että mahdolliset haavoittuvuudet tunnistetaan ajoissa eikä turvallisuudessa luoteta pelkästään teoreettisiin arvioihin.

4 Rakenteellinen suojaus

Rakenteellisen suojauksen tarkoituksena on estää tai hidastaa alueelle tai tilaan tunkeutuminen. Teknisten ratkaisuiden avulla voidaan edellä mainittujen lisäksi havaita ja viestiä eteenpäin mahdollisista luvattomista tunkeutumisista esimerkiksi vartioimisliikkeen hälytyskeskukseen ja viranomaisille. Kohteessa voidaan käyttää myös erilaisia vartiointipalveluja fyysisen turvallisuuden parantamiseksi.

Turvateknisiin ratkaisujen hankinnassa ja suunnittelussa tulee aina huomioida järjestelmiin ja laitteisiin liittyvät huolto- ja ylläpitotarpeet sekä näihin liittyvät kustannukset.

	Ennaltaehkäisy	Havaitseminen	Hidastaminen	Estäminen
Kameravalvontajärjestelmä	✓	✓	✗	✗
Kulunvalvontajärjestelmä	✓	✓	✓	✓
Rikosilmoitinjärjestelmä	✓	✓	✗	✗
Rakenteellinen suojaus	✓	✗	✓	✓
Lukitustekniikka	✓	✗	✓	✓

Kuva 5: Teknisten ja rakenteellisten ratkaisujen käyttötarkoitukset fyysisessä suojautumisessa

4.1. Aidat

Aidan tehtävänä on suojata kohteen maa-alueita tai tonttia ja viestiä siitä, että pääsy alueelle on rajattua, eikä sitä tulisi ilman asianmukaista tarkoitusta ylittää. Aidan suojausvaikutus perustuu mahdollisten tunkeutumisyritysten hidastamiseen. Parhaimmassa tapauksessa aidoilla voidaan jopa ennaltaehkäistä tai estää äkillisestä mielenjohteesta tehtyjä tai matalan motivoituneisuuden tunkeutumisyrityksiä. Lisäksi aitalinja voi toimia osana luonnollista valvontaa asiattoman kulun havainnoimiseksi, ja sitä voidaan valvoa teknisillä turvallisuusjärjestelmillä.

Aitatyyppejä on lukuisia erilaisia, heiveröisemmistä työmaa-aidoista lähtien aina kiinteämpiin, maahan kiinnittyviin ja seinämäisiin rakenteisiin asti. Aitojen rakentaminen turvallisuustarkoituksessa, on kuitenkin melko korkeakustanteista, sillä tämä lisää aidan ominaisuuksiin kohdistuvia vaatimuksia. Tämä tarkoittaa sitä, että aidan on oltava riittävän korkea, lujarakenteinen sekä mahdollisesti sisältää sen ylittämistä tai alittamista vaikeuttavia elementtejä.

Myös muiden aitalinjan rakenteiden, kuten porttien ja puomien, tulee vastata aidalle asetettuja vaatimuksia, sillä aitalinja on ainoastaan yhtä vahva kuin sen heikoin lenkki. Aitalinja vaatii myös jatkuvaa huolenpitoa; sen kummallakaan puolella ei saa olla näkösuojaa antavia tai aidan ylittämistä mahdollistavia puita, pensaita tai muita elementtejä. Aitalinjan kasvillisuus tai lumi-

kuormat saattavat myös vaurioittaa aita tai aiheuttaa vääriä hälytyksiä, mikäli aitalinjaa valvotaan aitavalvonnalla tai muilla turvajärjestelmillä.

Suosittelut aidan vähimmäisvaatimukset:

- Korkeus 2400 mm
- Materiaali: teräs
- Kolmilanka-aita 6 mm pysty – 2 x 8 mm vaaka
- Kiinnitys metallitolppiin, joiden väli korkeintaan 2400 mm
- Metallitolpat kiinnitetty luotettavasti maahan, joko valulla tai riittävän syväälle kallioon tai muuhun kiinteään ainekseen

Yleisesti ottaen alueen uloimman aitauksen yläosia ei ole tarpeen suojata erillisillä kiipeily- tai turvaesteillä, tai teknisellä aitavalvonnalla. Sen sijaan rajattujen tai kriittisten alueiden osalta tätä voidaan harkita osana kokonaisratkaisua.

4.2. Henkilöportit

Aidatulle alueelle kulku mahdollistetaan käyttäen erilaisia portteja osana aitarakennetta. Portin avulla alueelle kulku rajataan vain henkilöille, joilla on asianmukainen syy kulkea alueelle. Kulkuliikennettä alueelle pystytään rajaamaan ja seuraamaan porttien lukituksen ja kulunvalvonnan avulla. Kulunvalvontaa voidaan hyödyntää myös turvateknisen valvonnan rajapintana. Aitojen tavoin, myös erilaisia portteja on laaja

kirjo. Porttityypin valinnan tulee ominaisuuksiltaan myötäillä valittua aitatyyppiä, jotta aitalinjan suojauksen taso olisi yhdenmukainen.

Suosittelut portin minimivaatimukset:

Henkilöportti

Henkilöportin tulee olla osa aitalinjaa ja rakenteeltaan yhtä vahva kuin muu aita. Porttiympäristöjen toteutuksessa tulee aina huomioida mahdolliset hätäpoistumistiet ja -portit, jotka ovat turvallisesti käytettävissä, mutta samalla turvassa luvattomalta käytöltä.

Henkilöportit varustetaan sähköisellä kulunvalvonnalla tai elektromekaanisella lukituksella sekä vähintään vierailijoille tarkoitettut portit porttipuhelinjärjestelmän soittokojeella.

Käyntiportti / Kulkuportti / Henkilöportti / Saranaportti:

- 1-lehtinen käyntiportti (käsiikäyttöinen)
- Kulkuaukon leveys: 1100 – 1200 mm
- Käyntiportin korkeudet: 2200 – 2400 mm

Pyöröportti

Pyöröportilla on mahdollista valvoa alueelle kulkua, koska pyöröportti annostelee kulun siten, että vain yksi henkilö pääsee läpi kerralla. Kortinlukijalla tai muilla tunnistimilla varustettuna se varmistaa, että vain lähtökohtaisesti luvalliset henkilöt pääsevät alueelle.

Henkilöportit varustetaan sähköisellä kulunvalvonnalla tai elektromekaanisella lukituksella sekä vähintään vierailijoille tarkoitetut portit porttipuhelinjärjestelmän soittokojeella. Alueelta ulospäin kulku tapahtuu joko avauspainikkeen tai kulunvalvontajärjestelmän avulla. Myös pyöröportissa tulee huomioida hätäpoistumistie-määräykset.

- Kuumasinkitty teräsrakenne
- Kulkukäytävän leveys min. 600 mm
- Kiertokulma 120 astetta
- Optiona kattovalo sekä lämmitys

4.3. Ajoneuvoportit

Ajoneuvoporttien valinnassa on hyvä huomioida vaadittavan aukon leveys, liikenteen määrä, avautumisnopeus, haluttu suojaustaso ja porttiympäristön talvikunnossapito. Yleisimmät ajoneuvoportit ovat tyypiltään liukuportti sekä taittoportti, jotka molemmat soveltuvat henkilö-, ja raskaanliikenteen tarkoituksiin. Ajoneuvoportin yhteyteen voidaan asentaa myös puomikoneistot, jotka nopeuttavat entisestään ruuhka-aikaista käyttöä.

Suosittelut vähimmäisvaatimukset:

- Materiaali: Teräs tai alumiini
- Korkeus: Aitalinjan mukainen
- Avautumisaika: 3–30 s
- Lisätoiminnot: hätäpysäytys ja esteen tunnistus
- Integrointi: Kulunvalvontaan ja/tai rekisterikilventunnistukseen

4.4. Seinät, katot ja lattiat

Rakennuksen seinät, katto ja lattiat ovat tilaa rajaavia rakenteita, jotka voivat olla rakennuksen ulkopintoja tai muihin sisätiloihin rajoittuvia seiniä, lattiaita tai kattoja. Rakenteiden on kiinnityksineen oltava sellaisia, ettei tilaan pysty tunkeutumaan rakenteita rikkomatta ja murtautumisesta tai niiden yrityksistä tulee jäädä jälki. Rakenteet tai niiden osat eivät saisi myöskään olla ulkopuolelta rikkomatta irrotettavissa. Uudis- tai korjauskentämisen aikana tehtävillä rakenteellisilla ratkaisuilla voi olla suurikin vaikutus kohteen turvallisuuteen, minkä vuoksi turvallisuusasiantuntija onkin hyvä ottaa mahdollisimman aikaisessa vaiheessa osaksi suunnitteluprosessia.

Seinä, katto tai lattiarakenteita ei tyypillisesti vahvisteta erikseen turvallisuustason korottamiseksi, mutta korkean turvallisuustason kohteissa se kannattaa ottaa huomioon. Näiden rakenteiden vahvistaminen on mahdollista esimerkiksi metalli- tai vanerilevyillä, joilla pyritään estämään tai vähintäänkin hidastamaan tilaan mahdollisesti kohdistuvia tunkeutumisyrityksiä. Tämä on tyypillistä etenkin kohdesuojauksessa, kun tilassa tiedetään säilytettävän kallisarvoista omaisuutta, suojattavaa tietoa, turvallisuuskriittisiä laitteita ja järjestelmiä tai harjoitettavan kriittistä toimintaa.

Rakenteiden turvallisuusominaisuuksien tasosta ja sen vahvuudesta tunkeutumisyrityksiä vastaan, voidaan hyödyntää SFS-EN 1627 standardin mukaisista RC-luokituksista (RC1-RC6). Korkeamman RC-luokan rakenteet kestävät kauemmin korkeamman tason murtotyökaluja vastaan.

4.5. Ovirakenteet

Tilojen ovet tulisi olla rakenteeltaan sellaisia, joista tunkeutuminen ei ole mahdollista ilman työkaluin tapahtuvaa rakenteiden rikkomista. Murtautumisista tai niiden yrityksestä tulee jäädä jälki. Fyysisen suojaamisen suunnittelussa tulee ottaa huomioon suojatavan kohteen kriittisyys ja sen mukana tulevat suojausvaatimukset. Lisäksi on syytä huomioida erityisesti myös se, että oven vaikutus turvallisuuteen riippuu myös ikkunoiden sekä seinä, lattia ja kattorakenteiden vahvuudesta.

Ovityypin valinta tapahtuu usein sekä rakennusteknisestä että esteettisestä näkökulmasta, mutta yhtä lailla tärkeää on myös turvaominaisuuksiltaan vahvan ovityypin valitseminen. Oven ja sen rakenteiden materiaali on keskeinen osa tätä vahvuutta. Tyypillisimmin käytettäviä materiaaleja ovat puu, teräs, alumiini ja lasi. Turvaominaisuuksiltaan vahvat ovet ovat tyypillisesti metallisia. Korkeamman turvaluokituksen kohteissa niissä voidaan käyttää vahvisteita, kuten luodinkestäviä materiaaleja. Uusitut ovet ja uusittu lukitus saattavat alentaa vakuutusmaksuja, mistä on kuitenkin aina neuvoteltava yhteistyössä vakuutusyhtiön kanssa.

Ovityypin turvallisuusominaisuuksien tasosta ja sen vahvuudesta tunkeutumisyrityksiä vastaan, voidaan hyödyntää SFS-EN 1627 standardin mukaisista RC-luokituksista (RC1-RC6). Korkeamman RC-luokan ovet kestävät kauemmin korkeamman tason murtotyökaluja vastaan.



4.6. Ikkunat ja aukot

Rakennuksen ikkunat ovat tärkeä suunnitella ja suojata siten, ettei niitä pystytä rikkomatta irrottamaan ulkopuolelta. On syytä pohtia myös murtosuojattujen lasielementtien tarvetta. Ikkunoihin liittyen tulee huomioida salakatselun mahdollisuus myös ylemmissä kerroksissa droonien yleistessä, ja täten estää näkyvyys etenkin sellaisiin tiloihin, joissa käsitellään salassa pidettäviä aineistoja.

Rakennuksessa olevat aukot kuten esimerkiksi katto- ja ilmastointiluukut tulee suunnitella siten, että kulku näiden aukkojen ääreen tapahtuu vain valvotuista tiloista. Vaihtoehtoisesti aukot suojataan esimerkiksi teräksisin kalterein. Ikkunoita ja muita aukkoja on mahdollista valvoa turvatekniikan avulla, esimerkiksi murtohälytysjärjestelmän magneettikoskettimilla tai lasin rikkoutumiseen reagoivilla ilmaisimilla.

Ikkunat luokitellaan standardissa SFS-EN 356 luokkiin P1A-P5A, jotka ovat iskunkestäviä lasia, sekä luokkiin P6B-P8B, jotka ovat murransuojalaseja. Luokka P1A on kevyin versio ja P8B järein. Näiden lisäksi standardista EN-13124 löytyy räjähdysuojalaseja luokituksella EXR1-EXR5 ja luodinkestäviä lasia standardista EN1063 luokituksella BR1-BR7.

Aukkojen suojaamisessa hyödynnettävät ratkaisut luokitellaan standardin SFS-EN 1627 mukaisesti luokkiin RC1-RC6.

4.7. Valaistus

Riittävän voimakas, tasalaatuinen sekä muilta ominaisuuksiltaan sijoitettavaan toimintaympäristöön tarkoituksenmukainen valaistus on yksi keskeisistä rakenteellisen suojauksen komponenteista. Valaistus on sellaisenaan tehokas keino muun muassa rikollisuuden sekä vaaratilanteiden ehkäisemiseksi. Sillä on merkittävä vaikutus etenkin tapaturmien ennaltaehkäisemisessä.

Lisäksi valaistuksella on merkittävä rooli eri turvajärjestelmien tukena toimimisessa. Muun muassa kameravalvontajärjestelmiin liitettyjen valvontakameroiden riittävän kuvanlaadun varmistaminen edellyttää riittävän valaistuksen suunnittelua. Sitä voidaan hyödyntää tehokkaasti myös osana muita turvajärjestelmiä integraatioiden avulla esimerkiksi niin, että murtoilmaisu- tai kulunvalvontajärjestelmän hälytys ohjaa valaistuksen hälyttävälle alueelle, mikä voi osaltaan häiritä mahdollista tunkeutujaa tai jopa saada tämän perääntymään aikeistaan kiinnijäämisriskin kasvaessa.

4.8. Arkkitehtuuriset ratkaisut

Rakenteellinen murtosuojaus ei rajoitu pelkästään hankittavien rakenteiden tyyppiin ja turvallisuusominaisuuksien tarvearviointiin. Fyysinen turvallisuus on syytä huomioida myös arkkitehtuurisilla ratkaisuilla tila- ja pihasuunnittelussa. Muun muassa kasvien ja kasvuston sekä erinäisten pihaelementtien sijoittelulla

voidaan saada aikaan merkittäviäkin turvallisuusvaikutuksia. Niitä voidaan hyödyntää muun muassa eri alueiden ja kulkuteiden rajaamisessa, näköesteenä tai esteenä tunkeutumiselle. Aulatilojen tilaratkaisuilla, kuten aulapalvelutiskin ja sitä ympäröivien rakenteiden valinnalla ja sijoittelun suunnittelulla on mahdollista parantaa henkilöturvallisuutta. Kulkturvallisuutta voidaan parantaa sijoittamalla kulkuportit näiden yhteyteen.

Tila- ja pihasuunnitteluun liittyvien ratkaisujen lisäksi on olemassa myös varta vasten turvallisuustarkoitukseen suunniteltuja arkkitehtuurisia ratkaisuja, kuten ajohidasteet, pollarit ja törmäyssuojat. Myös näiden avulla on mahdollista rajata alueita sekä kulkutietä, mutta niillä voidaan myös estää ajoneuvolla pääsy alueelle sekä suojata kiinteistöä sekä sen alueita ja siellä käyskenteleviä ihmisiä.

4.9. Lukitusratkaisut

Lukitus-termillä viitataan sekä mekaanisiin että sähkölukitusratkaisuihin, kuten moottoroituihin lukitusjärjestelmiin ja elektromekaanisiin lukitusjärjestelmiin. Mekaanisessa lukituksessa oveen asennetaan perinteinen mekaaninen avainpesä. Avainpesä estää kulun ovesta ilman avainpesään sopivaa avainta. Sähkölukitusjärjestelmillä hallitaan ovien sähkölukkoja sekä valvotaan ovien asentotiloja (kiinni/auki). Sähkötoimiset lukot liitetään tyypillisesti kulunvalvonta-, murtoilmaisu- ja paloilmoinjärjestelmiin.



Mikäli avaimen haltija kadottaa avaimensa, kasvaa riski lukituksen eheydestä kadotetun avaimen väärinkäytön vuoksi ja kaikki lukot, joihin kadonnut avain on käynyt, tulee sarjoittaa uudelleen. Mekaanisten lukitusratkaisujen haittoina ovatkin täten pitkän aikavälin kustannukset, jotka johtuvat lukituksen uudelleen sarjoittamisesta sekä manuaalisen avaintenhallinnan hallinnoinnista. Mekaanisen avainpesän varustelluista ovista ei ole saatavilla tietoa, onko ovi auki tai kiinni tai kuka on ovesta kulkenut.

Suosituksena on, että lukkojen heloineen tulee perustua standardeihin SFS 5970 ja SFS 7020, joissa standardin mukaan hyväksytyt tuotteet jaetaan käyttökohteiden mukaan luokkiin 1-4.

Elektromekaaniset lukitusjärjestelmät

Elektromekaaniset lukitusratkaisut ovat mekaaniselle lukitukselle vaihtoehtoinen tapa toteuttaa lukitus kiinteistössä. Se toimii kiinteistön niin sanottuna kevyenä kulunhallinta- ja lukitusjärjestelmänä, jonka avulla mahdollistetaan kulkuoikeuksien hallinta sekä lokitietojen kerääminen ovista kulkemisesta. Elektromekaanisesta lukituksesta käytetäänkin myös termejä kevyt kulunhallinta ja sähkömekaaninen lukitus. Elektromekaaninen lukitus on mahdollista toteuttaa joko kaapeloituna tai ilman kaapelointia. Kaapeloitu toteutus on lähtökohtaisesti kustannuksiltaan korkeampi tapa toteuttaa elektromekaaninen lukitus, mutta se on vastaavasti toiminnaltaan luotettavampi sekä häiriösietokyvyltään varmempi toteutustapa.

Elektromekaaniset lukitusratkaisut mahdollistavat valmistajasta ja toteutustavasta riippuen ovien tilatiedot, kulkutapahtumista lokitiedot sekä keskitetyn avainten kulkuoikeuksien hallinnan verkkokäyttöliittymän kautta. Avaintenhallinta onkin elektromekaanisessa lukitusjärjestelmässä huomattavasti tehokkaampaa verrattuna mekaaniseen lukitukseen. Esimerkiksi kadonneet avaimet voidaan kuolettaa, jolloin lukitukset eivät vaadi korkeakustanteista uudelleensarjoittamista. Avaimiin asetettuja kulkuoikeuksia on helppo muuttaa, joten avainten vaihtaminen käyttäjältä toiselle onnistuu vaivatta, esimerkiksi henkilöstöön liittyvien muutoksien tai vaihdosten yhteydessä.

Mekaaninen lukitus

Mekaaninen lukitus on toimiva ratkaisu etenkin silloin, kun kyseessä on matalan riskitason tilan lukitseminen kustannustehokkaasti. Perinteiset mekaaniset lukitukset ovat toimintavarmoja, pitkäikäisiä lukitusratkaisuja, joiden toiminta perustuu avaimen kääntöliikkeestä syntyvään mekaaniseen liikevoimaan, joka avaa lukon kielen. Mekaaniset lukitusratkaisut ovat hankintakustannukseltaan edullisin tapa toteuttaa lukitusratkaisu verrattuna sähkölukitus- ja elektromekaanisiin lukitusjärjestelmiin. Lukitusratkaisu ei vaadi erillisiä lisenssejä, kaapelointeja tai virtalähteitä toimiakseen.

Mekaanisen lukituksen ongelmakohtana on sen manuaalinen hallinnointi, joka vaatii erillisen kirjanpidon jokaisen avaimen haltijasta sekä avainten sarjoituksen eri lukkoihin. Mikäli avaimen haltija kadottaa avai-

mensa, kasvaa riski lukituksen eheydestä, kadotetun avaimen väärinkäytön vuoksi; tässä tilanteessa kaikki lukot, joihin kadonnut avain on käynyt, tulee sarjoittaa uudelleen. Mekaanisen avainpesän varustelluista ovista ei ole myöskään saatavilla tietoa siitä, onko ovi auki tai kiinni tai kuka on ovesta kulkenut. Lisäksi mekaanista lukitusta hankkiessa on huomioitava lukitusratkaisun patentin voimassaolo. Mikäli patentti on umpeutunut, tarkoittaa se sitä, että avaimesta on mahdollista teettää kopiot viemällä se tätä palvelua tuottavaan liikkeeseen.

Sähkölukitus ja moottorilukot

Sähkölukitusratkaisuja löytyy vastaamaan useisiin eri käyttötarkoituksiin. Sähkölukituksessa tulee ottaa huomioon oven oletettu käyttöaste, tilaolosuhteet, paloturvallisuusasetukset sekä poistumistiemääräykset ja erinäisiin kiinteistön automaatiikka- ja ohjausjärjestelmiin liittäminen. Sähkölukitusratkaisuissa hyödynnetään avainpesän osalta joko mekaanisia tai elektromekaanisia lukitusratkaisuja, joilla ovesta päästään kulkemaan avainta käyttämällä.

Moottorilukkojen toimintaperiaate perustuu lukon sisällä olevaan sähkömoottoriin, joka työntää lukon kielen sisään ovea avatessa ja palautuu takaisin ulospäin jousivoimalla, kun oven moottorilukko lukkiutuu.

5 Tekniset turvallisuusjärjestelmät

5.1. Kameravalvontajärjestelmät

Kameravalvontajärjestelmän tarkoituksena on valvoa sille ennalta suunniteltuja valvonta-alueita tai kohteita. Kameravalvontaa voidaan hyödyntää turvallisuusteen (security) liittyvän valvonnan lisäksi prosessien ja tuotantolinjastojen valvonnassa sekä analytiikan tuottamisessa. Valvonta-alue suunnitellaan riskiperusteisesti kohteen käyttötarkoituksen, luonnon ja suojattavat arvot huomioiden.

Kameravalvontajärjestelmä koostuu tyypillisesti tallentimesta tai videohallintaohjelmistosta, verkkokytymistä sekä valvontakameroista. Kameravalvontajärjestelmään liittyvien laitteiden valinnassa, sekä niihin liittyvien teknisten vaatimusten määrittelyssä, on tärkeää huomioida toimintaympäristöön liittyvät muuttujat, kuten esimerkiksi sää- ja valoisuusolosuhteet, valvonta-alueen laajuus, tarvittava valvontakuvan tarkkuus (yleiskuva/tunnistuskuva/yksilöntikkuva).

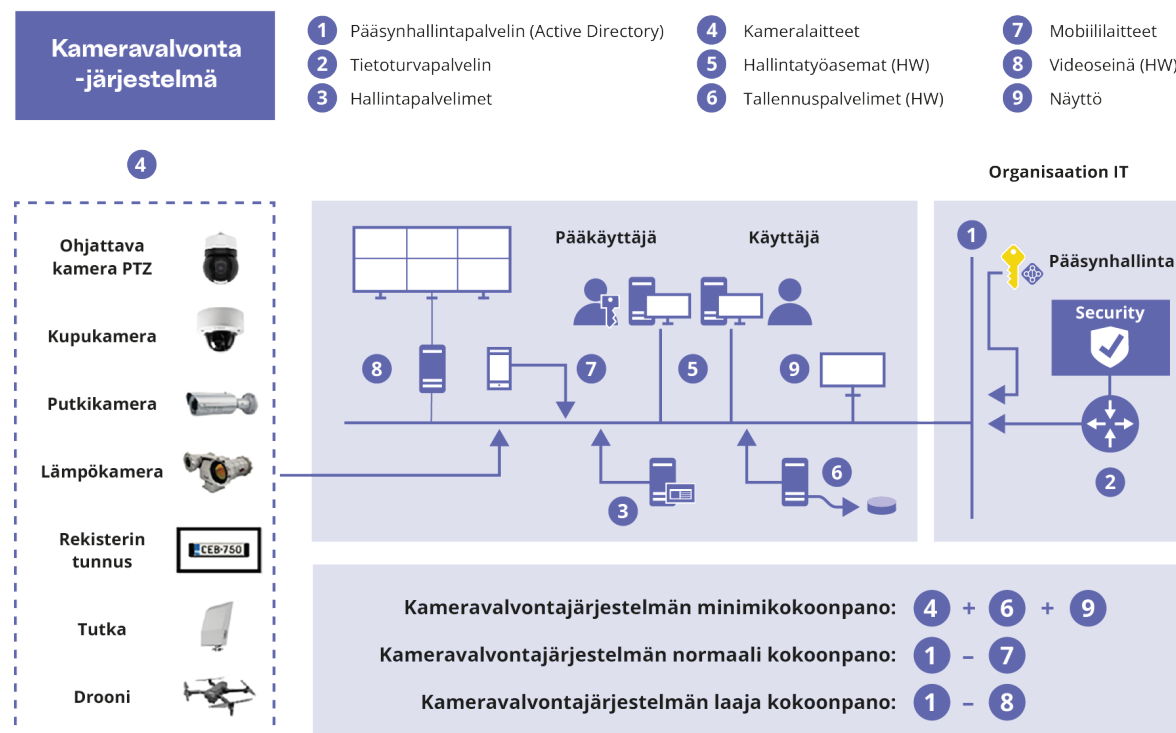
Kameravalvontajärjestelmä ei teknisiltä ominaisuuksiltaan ole itsenäisesti rikoksia estävä tilaturvallisuusjär-

jestelmä, vaikkakin usein sitä käsitelläänkin vastaavien järjestelmien ohessa. Kameravalvontajärjestelmällä on kuitenkin myös rikoksia ja väärinkäytöksiä ennaltaehkäisevä vaikutus kiinnijäämisriskin vuoksi. Kameravalvontajärjestelmän päätarkoituksena on saada tilanteen mukaan joko reaaliaikaista tai tallentavaa (tai molempia) kuvamateriaalia määritellyltä alueelta. Kuvan antaman tilannetiedon perusteella voidaan esimerkiksi lähettää tapahtumapaikalle vartiointiliikkeen edustaja. Tallennemateriaalia voidaan hyödyntää tapahtumaketjujen selvittämiseen ja todentamiseen jälkikäteen ja sitä voidaan hyödyntää esimerkiksi poliisin tekemässä rikostutkinnassa.

Kameravalvontajärjestelmän pääsynhallinta, tietoturva ja versionhallinta tulee perustua organisaation turvallisuuspolitiikkaan. Tallenteiden säilytysaika tulee täyttää organisaation GDPR- ja selosteen käsittelytoimista mukaiset vaatimukset. Nykyinen tietosuoja-asetus ei edellytä entisen kaltaista rekisteri- tai tietosuojaselostetta. Seloste käsittelytoimista on organisaation sisäinen asiakirja, jossa kuvataan henkilötietojen käsittelyä.



Kameravalvontajärjestelmän periaate:



Kuva 7: Kameravalvontajärjestelmä periaatekuva

Kameravalvontajärjestelmän periaatekuvassa on kuvattu yleisimmin käytettyjä toteutustapoja. Näiden lisäksi kameravalvontajärjestelmän voi toteuttaa:

- **Monitoimipaikkainen malli:** Jossa hallintapalvelimet ja työasemat sijaitsevat paikassa A ja paikalliset kuvaa tallentavat tallentimet kiinteistöissä B.
- **Pilvipalveluna:** Jossa kiinteistössä tai kiinteistöissä sijaitsevat kameralaitteet tallentavat kuvan pilvipalvelimelle ja livekuvan katselu sekä tallenteiden haku tapahtuu palvelualustan kautta siihen myönnettyillä oikeuksilla.
 - Pilvipalvelu toteutuksessa on suositeltavaa hyödyntää ns. edge-tallennusta kuvahäviön välttämiseksi. Palvelin yhteyden katketessa kamera kuva tallennetaan kameralaitteeseen asennetulle muistikortille. Yhteyden palautuessa tallennettu materiaali siirretään pilvipalvelimelle.

Kameravalvontajärjestelmän tietoliikenneyhteydet ja laitteet on suositeltavaa eriyttää organisaation muista tietoliikenneverkkoista verkkoa loogisesti segmentoimalla, esimerkiksi virtualisoimalla (VLAN).

Valvonta-alueet voidaan suunnitella esimerkiksi seuraavasti:

Yleiskuvan kameralla on tarkoitus kuvata nimensä mukaisesti yleisesti aluetta, joka halutaan kameravalvonnan piiriin. Yleiskuvan alueita voivat olla mm.

- Aulatilat
- Kiinteistöjen ulkokuori ja sen seinustat
- Laajat piha- sekä pysäköintialueet

Tunnistuskuvan kameran tarkoituksena on havaita valvotulla alueella sellaisella tarkkuudella tapahtuva asia, henkilö, esine tai ajoneuvo, jotta valvontakuvan perusteella voidaan tunnistaa esimerkiksi vaatepuksen väri sekä tapahtumien tarkka kulku. Tunnistuskuvan valvonta-alueita voivat olla mm.

- Käytävät
- Sisäänkäyntien edustat
- Kriittisten kohteiden tai tilojen välitön läheisyys

Yksilöintikuvalla tarkoitetaan kameraa, jonka tekniset ominaisuudet mahdollistavat tarkan valvontakuvan halutusta valvonta-alueesta siten, että valvonta-alueella liikkuvat henkilöt sekä ajoneuvot voidaan yksilöidä. Yksilöintikuvan kameroiden valvonta-alueita voivat olla mm:

- Henkilöportit
- Ajoneuvoportit ja luiskat
- Sisäänkäyntiovet
- Kriittiset tilat tai alueet

On huomioitava, että kameroiden kuvan tarkkuuteen vaikuttaa ympäristö, johon se asennetaan (valaistuksen määrä sekä esimerkiksi sääolosuhteet). Kameravalvontajärjestelmän suunnittelussa tulee siis määritellä tarkkuuden tarve kamerakohtaisesti, eikä yleisiä tarkkuusmäärittelyjä ole em. syystä järkevää tehdä. Kameravalvonnan suunnittelu tulisi toteuttaa aina asiantuntevan henkilön toimesta, huomioiden asiaankuuluva lainsäädäntö sekä muut mahdolliset vaatimukset:

Yleinen tietosuoja-asetus (GDPR)

<https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32016R0679>

Laki yksityisyyden suojasta työelämässä

<https://www.finlex.fi/fi/laki/ajantasa/2004/20040759>

Turva-alan yrittäjien kameravalvontaopas

<https://turva-alanyrittajat.fi/kameravalvontaopas>



Kameramallit ja niiden käyttötarkoitus

Kameramalli	Käyttötarkoitus	Ominaisuuksia
Kääntöpääkamerat, PTZ	Aktiivinen valvonta, tehokas käyttö tarvitsee operaattorin / valvomon, joka ohjaa kameraa.	Automaattinen liikkeenseuranta yhdistettynä analytiikkaan tai tutkaan. Analytiikalla voidaan myös havaita lämpötila eroja.
Kiinteät kupukamerat	Yleisvalvonta sisällä ja ulkona.	Analytiikka mm.: liikkeentunnistus, virtuaalinen aitalinja, ihmisten ja ajoneuvojen luokittelu, esineen katoaminen
Kiinteät putkikamerat	Yleisvalvonta sisällä ja ulkona.	Analytiikka mm.: liikkeentunnistus, virtuaalinen aitalinja, ihmisten ja ajoneuvojen luokittelu, esineen katoaminen
Lämpökamerat	Laajojen alueiden yleisvalvonta. Kriittisten järjestelmien lämpötilan seuranta	Lämpötilan pistemittaus
ANPR-kamerat	Rekisterikilpien lukemiseen hyödynnettävä kamera. Mahdollistaa esim. ajoneuvoporteista alueelle sisään ajamisen	Ajoneuvojen luokittelu, kilpien tallennus aikaleimalla
Dronekamerat	Laajojen alueiden aktiivinen turvallisuusvalvonta, kohteiden tarkistamis- tai etsintätehtävät, kattojen turvallisuusvalvonta	Lämpökamera, automatisoidut valvontakierrokset, ei vaadi välttämättä lainkaan ihmisen hallintaa, automaattinen kohteen seuranta
Ex-kamerat	Kamerat räjähdysriskille tiloille / alueille.	Räjähdyssuojattu kotelointi, ATEX- ja IECEx-sertifioituja, korroosion kestäviä
360 Kamerat	Yleisvalvonta sisällä ja ulkona, lyhyt kantama, kiinteä objektiivi, tuottaa pyöreän kuvan, jonka voi muuttaa ns. normaalikuvaksi VMS järjestelmässä	Liikkeentunnistus, ihmisten ja ajoneuvojen luokittelu, virtuaalinen aitalinja, lämpökartta
Multisensori	Laajojen alueiden yleisvalvonta. Sisältää 2-4 objektiivia.	Liikkeentunnistus, ihmisten ja ajoneuvojen luokittelu, virtuaalinen aitalinja, virtuaalinen PTZ
Tutkat (lisälaite)	Laajojen alueiden yleisvalvonta. Kriittisten järjestelmien lämpötilan seuranta.	Nopeuden mittaus, kulkureitin seuranta, aikainen havainnointi myös sumussa

5.2. Kulunvalvontajärjestelmät

Kulunvalvontajärjestelmät ovat älykkäitä ja verkotettuja kokonaisuuksia, joiden tarkoituksena on hallita ja valvoa tiloihin pääsyä sekä seurata kulkutapahtumia. Kulunvalvontajärjestelmän perusajatuksena on määrittää ja hallita, kenellä on oikeus liikkua missäkin tiloissa ja milloin. Järjestelmä mahdollistaa kulkueuryhmien ja -alueiden määrittelyn, henkilöiden eritasoisten oikeuksien asettamisen sekä ovien tilatietojen ja kulkutapahtumien valvonnan.

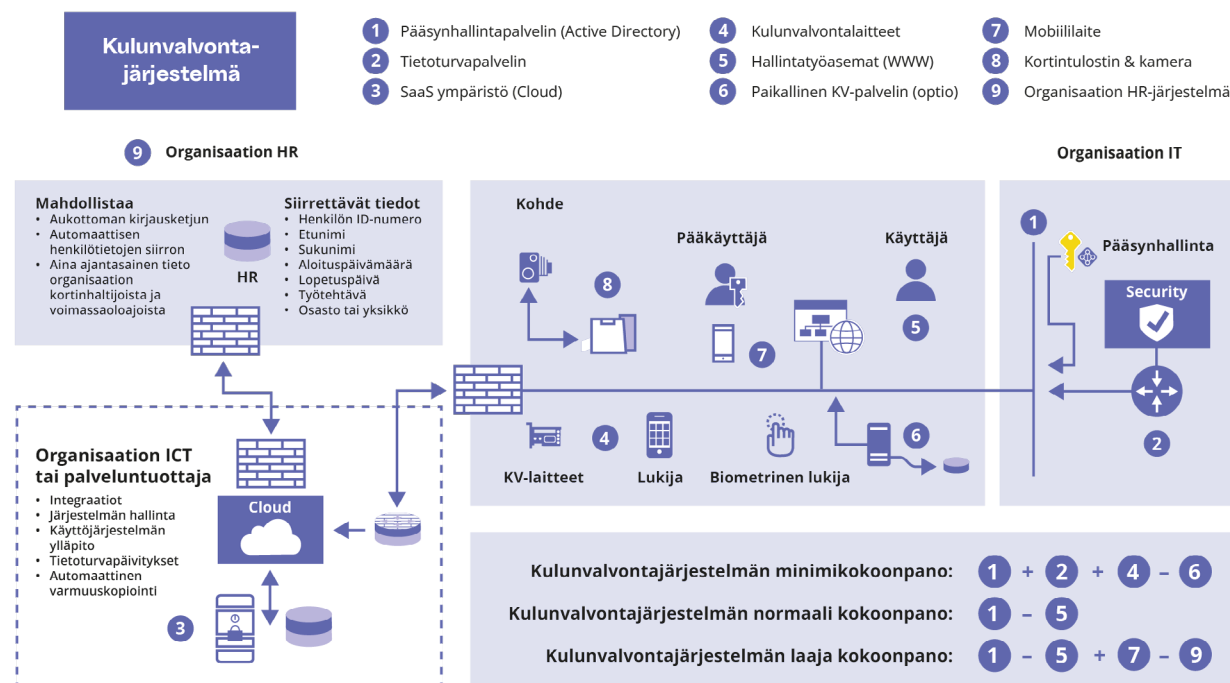
Kulunvalvontajärjestelmien järjestelmäkokoaisuudet ja niiden hallinnointi voidaan toteuttaa:

- SaaS ympäristöstä, joka voi fyysisesti sijaita Suomen tai EU:n alueella ja jota tuotetaan palveluna Tilaa-jalle. Vaihtoehtoisesti voidaan käyttää Tilaaajan omaa tai palveluna ostettua datakeskus- tai pilviympäristöä.
- Paikalliselta palvelimelta tai työasemalta
 - Vähemmän suositeltu ratkaisu ellei paikalliset palvelimet ole ICT yksikön hallinnoimia sekä tietoturva- ja SOC valvonnan piirissä.

Kulunvalvontajärjestelmien henkilötietojen käsittely perustuu tietosuojalainsäädäntöön, erityisesti EU:n yleiseen tietosuojalakiin (GDPR) sekä kansalliseen tietosuojalakiin. Järjestelmässä käsitellään usein työntekijöiden ja muiden tiloihin oikeutettujen henkilöiden tunnistetietoja, kuten nimiä, veronumeroa, ID-numeroa, kulkulupia, kulkutapahtumia. Näiden tietojen käsittelyn tulee olla asianmukaisesti dokumentoitua ja rajattua vain niihin tietoihin, jotka ovat välttämättömiä kulunvalvonnan toteuttamiseksi.

Kulunvalvontajärjestelmät luokitellaan standardin SFS-EN 60839-11 mukaan luokkiin 1-4. Luokka 1 on tarkoitettu matalan suojaustason kohteisiin ja luokka 4 erittäin korkean suojaustason kohteisiin.

Kulunvalvontajärjestelmän periaate:



Kuva 8: Kulunvalvontajärjestelmä periaatekuva

5.3. Pääsynhallintaprosessi

Kulunvalvonnan pääsynhallintaprosessi on jatkuva prosessi, jolla varmistetaan, että vain oikeutetut henkilöt pääsevät organisaation tiloihin ja resursseihin tiettyinä aikoina. Se koostuu tyypillisesti neljästä päävaiheesta: valtuutus, tunnistautuminen, pääsy ja auditointi/hallinta. Pääsynhallinnan prosessissa voidaan hyödyntää organisaation henkilöstöhallinnon (HR) ja kulunvalvonnan välistä integraatiota tai tuottaa pääsynhallinnan prosessi erillisellä PIAM (Physical Identity and Access Management) hallintasovelluksella.

Valtuutus

1. Määritellään, kenellä on oikeus päästä millekin alueelle ja milloin. Tämä perustuu usein roolipohjaiseen pääsynhallintaan (RBAC – Role-Based Access Control) jossa henkilöille myönnetään pääsy heidän tehtäviensä tai roolinsa perusteella.
2. Muille kuin organisaation yleisille alueille tarvitaan aina alueesta tai tilasta vastaavan valtuutuksen.
3. Luodaan selkeät käytännöt ja säännöt, jotka määrittävät pääsyolosuhteet ja -tasot (esim. fyysinen pääsy tiettyyn huoneeseen tai tilaan).

Tunnistautuminen

1. Henkilö esittää kulkutietonsa (esim. kulkukortti, PIN-koodi, biometrinen tunnus tai mobiiliavain) järjestelmälle todistaakseen henkilöllisyytensä
2. Järjestelmä tarkistaa tunnistetietojen aitouden ja varmistaa, että ne vastaavat valtuutettua identiteettiä.

Pääsy

1. Kun henkilöllisyys on varmistettu ja järjestelmä on todennut hänellä olevan tarvittavat luvat, pääsy myönnetään (esim. ovi aukeaa).
2. Jos lupaa ei ole, pääsy evätään ja järjestelmä voi tarvittaessa laukaista hälytyksen.

Auditointi ja hallinta

1. Järjestelmä kirjaa kaikki kulkutapahtumat, mukaan lukien onnistuneet ja epäonnistuneet yritykset, keskitettyyn tietokantaan.
2. Säännölliset auditoinnit ja raporttien tarkastelu auttavat havaitsemaan luvattomat pääsy-yritykset, mahdolliset tietoturva-aukot ja varmistamaan käytäntöjen noudattamisen.
3. Käyttöoikeuksia hallitaan ja päivitetään jatkuvasti henkilöstön vaihtuessa (pohjautus ja poishallinta) ja organisaation tarpeiden muuttuessa.



Kulunvalvontajärjestelmän aktiivinen, ajantasainen ja ammattitaitoinen hallinnointi vaikuttaa merkittävästi kulunvalvontajärjestelmän vaikuttavuuteen. Järjestelmän hallinnointiohjelmistossa voidaan laatia kulkuoikeusryhmiä ja -alueita, nimetä eritasoisia oikeuksia henkilöille, valvoa lokitietoja ovien kulkutapahtumista, sekä valvoa ovien tilatietoa ja asettaa oville aikaohjelmia. Aikaohjelmilla määritellään esimerkiksi se, kuinka ovesta pääsee kulkemaan; riittääkö pelkkä tunniste vai vaaditaanko lisäksi henkilökohtainen PIN-koodi, tai milloin ovesta kulkeminen aiheuttaa hälytyksen.

Kulunvalvontajärjestelmän hälytystoimintoja ei pidä kuitenkaan sekoittaa murtohälytysjärjestelmiin, sillä ne eivät täytä murtohälytysjärjestelmille asetettuja vaatimuksia.

Kulunvalvontajärjestelmän laitekoonpano koostuu:

- Paikallisesta, virtuaalisesta- tai pilviympäristön palvelimesta
- Keskuslaitteesta, eli väyläohjaimesta
- Ovikohtaisista ovi/pääteohjaimista
- Kulunvalvonnan lukijoista
- Kulkutunnisteista ja avaimista
- Kytkimistä
- Integraatioista, esim.:
 - ▶ HR, vierailijahallinta, porttipuhelin, korttitulostus ja avainkaapit

Lukijatyypit

Lukijan malli	Käyttötarkoitus	Ominaisuuksia
Normaali lukija	Ei kriittiset ovet	Ns. peruslukija, ei mahdollista kaksoistodennusta
PIN-lukija	Ulko-ovet ja kriittisten tilojen ovet	Varustettu koodinäppäimistöllä. Mahdollistaa kaksoistodennuksen (Tunniste + koodi)
BLE- / NFC-lukija	Ulko-ovet ja kriittisten tilojen ovet	Mahdollistaa kaksoistodennuksen (Tunniste + sormenjälki / kasvot). Tunniste sekä tunnistautuminen mobiililaitteella.
Biometrinen	Kriittisten tilojen ovet	Mahdollistaa kaksoistodennuksen (Tunniste + biometrinen)

Huomioitava lukijoiden valinnassa

- Nykyaikainen teknologia
- Organisaatiokohtaiset applikaatiot (salaustiedostot)
- Riittävä salaus (vähintään AES 128)
- Soveltuvuus käyttöympäristöön (IP- ja käyttölämpötilat)
- Asennusmahdollisuudet (ovi- vai seinäpintaan)

5.4. Murtohälytysjärjestelmät

Murtohälytysjärjestelmä on tekninen tilaturvallisuusjärjestelmä, jonka päätarkoituksena on valvoa rakennusta. Murtohälytysjärjestelmän ilmaisimista voidaan välittää hälytystieto järjestelmää valvovalle taholle, ensisijaisesti vartioimisliikkeelle ja toissijaisesti mobiililaitteeseen tai paikalliselle valvomolle. Järjestelmä koostuu tyypillisesti keskuslaitteesta, varmennetusta ilmoituksensiirtolaitteesta, käyttölaitteesta ja ilmaisinkannasta.

Murtohälytysjärjestelmä tunnetaan myös nimillä:

- Rikosilmoitinjärjestelmä
- Tunkeutumisen ilmaisujärjestelmä
- Murtohälytinjärjestelmä
- Murtoilmaisujärjestelmä
- Hälytysjärjestelmä

Murtohälytysjärjestelmällä voidaan suorittaa

- Tilavalvontaa
- Kohdevalvontaa
- Kuorivalvontaa
- Kehävalvontaa

Itsenäisenä järjestelmänä murtohälytysjärjestelmä ei ole teknisiltä ominaisuuksiltaan kyvyllinen ennaltaehkäisemään tai estämään rikoksia tai väärinkäytöksiä. Järjestelmän käyttö perustuu hälytyksen ilmaisuun ja hälytyksen siirtoon. Murtohälytysjärjestelmällä voi kuitenkin olla ennaltaehkäisevä vaikutus ilkivaltaan tai rikoksiin. Murtohälytysjärjestelmä on myös mahdollista integroida osaksi kulunvalvonta- sekä kameravalvontajärjestelmiä, jolloin valvontaa saadaan suoritettua tehokkaammin sekä helpokäyttöisemmin.

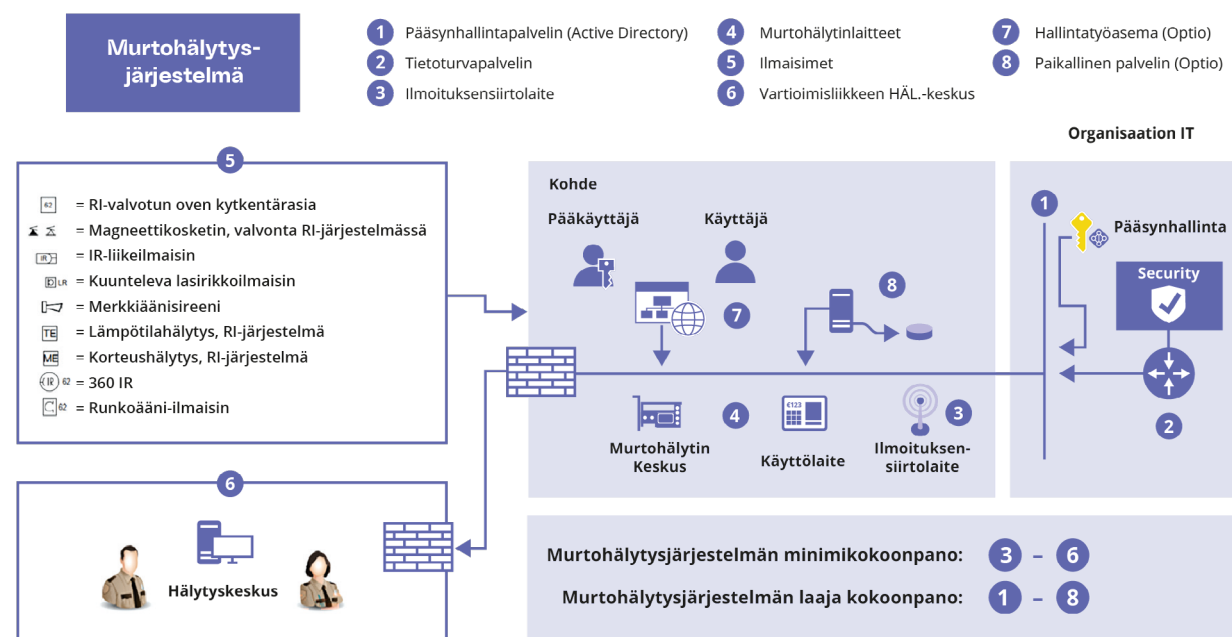
Teknisenä tilaturvallisuusjärjestelmänä murtohälytysjärjestelmä ei itsenäisesti kykene tunnistamaan alueella liikkuvia henkilöitä. Sillä saadaan kuitenkin välitön hälytys ilmaisimen havaitsemasta poikkeavasta tapahtumasta, kuten havaitusta liikkeestä aikana, jolloin tilan tulisi olla tyhjä, hälytyksiä valvovalle taholle.

Murtohälytysjärjestelmät luokitellaan standardin SFS-EN 50131 mukaan luokkiin 1–4.

Luokissa 1–2 saa hyödyntää kauttaaltaan langattomia ilmaisimia. Luokassa 3 langattomia ilmaisimia saa hyödyntää ainoastaan kohdevalvonnassa ja hälytyspaiknikeissa. Luokassa 4 langattomia ilmaisimia ei sallita.

Murtohälytysjärjestelmien ilmoituksensiirtolaitteet luokitellaan standardin SFS-EN 50136-1:2012 mukaan luokkiin SP1-SP6 ja DP3-DP4.

Murtohälytysjärjestelmän periaatekuva



Kuva 9: Murtohälytysjärjestelmä periaatekuva

Ilmainen	Käyttötarkoitus	Ominaisuuksia
Ovikosketin (magneettikosketin)	Ovet, nosto- ja liukuovet ja luukut	Uppo-, tai pintakosketin, nosto-oven koskettimet
Liikeilmainen	Tilavalvonta sisätiloissa	Voi käyttää myös ulkona - virrehälytysten todennäköisyys erittäin korkea
Kuunteleva lasirikkoilmainen	Lasipintojen valvonta	Reagoi lasin rikkoutumisen ääneen
Runkoääni- ja värinäilmaisimet	Rakenteiden valvonta (esim. Seinät, lattiat ja katot) Kohde valvonta, esim. Kassakaapit	Rakenteisiin, jotka voivat olla betonia tai terästä
Vesivuotoilmaisimet	Vesivuodolle alttiit tilat tai kriittiset tilat	Koteloituja, teippianturi tai yksittäisantureita langallisena tai langattomina ilmaisimina.
Ryöstö- ja hätäkutsuilmaisimet	Ryöstö- tai hätäkutsuhälytykseen	Äänekäs tai äänetön hälytys. Painike tai kahva mallisia.
Linjailmaisimet	Pitkien suorien linjojen valvonta, esim. Pitkät käytävät ja aitalinjat	50 M – 300 m ir-linjavaltvonta
Aitavalvontajärjestelmät	Kehäsuojauksen aitarakenteet ja ylitykset	Aitarakenteisiin asennettavat, virtuaalisen aitalinjan valvonta tai maahan upotettavat
Lidar-tutkat	Laajojen ulkoalueiden valvonta ja objektien tunnistus	Tutkien kantamat väliltä 20 m – 300 m
Sireenit ja vilkut	Paikallishälytyksen ilmaisemiseen	Huomioitava desibelit ja niiden mahdollinen säätö tilan mukaisesti

5.5. Analytiikkajärjestelmät

Tekoälyyn perustuvan keskeisiä ominaisuuksia ovat kyky integroida erilaisten järjestelmien, kuten kamera-valvonnan ja IoT-laitteiden, tuottama data yhdeksi kokonaisuudeksi. Tekoäly hyödyntää koneoppimista ja kehittyntä analytiikkaa esimerkiksi kasvojen ja ajoneuvojen tunnistukseen, kulkutapahtumien kartoitukseen sekä automaattihälytysten luomiseen mustalle listalle asetetuista kohteista.

Analytiikkajärjestelmän edut ilmenevät erityisesti sen automaattisessa reagoinnissa ja tiedon yhdistämisessä, mikä mahdollistaa nopean ja tarkan hälytysjärjestelmän toiminnan sekä valvottujen alueiden tehokkaan seurannan. Älykäs analytiikka vähentää manuaalisen työn tarvetta ja parantaa turvallisuutta, sillä järjestelmä tunnistaa poikkeavuudet ja reagoi niihin

välittömästi. Lisäksi järjestelmä tukee sujuvaa integraatiota olemassa oleviin turvajärjestelmiin, mikä tekee siitä joustavan ja laajennettavan ratkaisun erilaisiin kiinteistöympäristöihin.

5.6. Tutkajärjestelmät

Tutkajärjestelmiä voidaan hyödyntää muita teknisiä turvallisuusjärjestelmiä tukevana järjestelmänä muun muassa aluevalvonnassa. Ne ovat suunniteltu laaja-alaiseen passiiviseen tai puolipassiiviseen valvonta-alueen valvontaan. Tutkat perustuvat verkkoon kytkettävään keskuslaitteeseen, tutkaohjelmistoon, tutkapaneeliin tai useampaan tutkapaneeliin sekä niihin liitettävään kiinteistön kameravalvontajärjestelmään.

Tutkien tarkoitus on valvoa niille valmiiksi suunniteltuja valvonta-alueita, joihin rakennetaan etäisyyksien perusteilla eri sektoreja, joille puolestaan asetetaan omat hälytysasteensa. Tutkapaneeleitten mukaan, tutkien kantama vaihtelee sadasta metristä (100 m) yli neljään sataan metriin asti (400 m). Valvontasektorit ohjelmoidaan kohdekohtaisesti ja olosuhteet huomioiden siten, että:

Uloin sektori

- Tutka tunnistaa henkilön tai ajoneuvon liikkeen, antaa liikkeelle yksilöidyn ID:n, joka tallentuu järjestelmän lokitietoihin. Järjestelmä piirtää liikkeen aiheuttajan liikuntaradan kartalle.

Keskimmäinen sektori

- Mikäli hälytyksen aiheuttaja, ajoneuvo tai henkilö saapuu keskimmäiselle sektorille, laukaisee liike hiljaisen hälytyksen järjestelmässä, jolloin järjestelmä automaattisesti ohjaa liikettä lähimmän tutkajärjestelmään liitetyn PTZ kameran kohti liikkeen aiheuttajaa. Kamera seuraa liikettä keskisektorilla automaattisesti.

Sisimmäisin sektori

- Mikäli hälytyksen aiheuttaja etenee kohti kiinteistöä keskimmäisen sektorin yli sisimmäiselle hälytyssektorille, laukaisee liike hälytyksen järjestelmässä. Hälytys siirretään valvonnasta vastaavalle taholle. Sisimmäisellä hälytyssektorilla tapahtuva liikettä järjestelmä seuraa automaattisesti sitä lähimmillä PTZ kameroilla.

Maatutkat ja droonien havainnointitutkat eroavat käyttöominaisuuksiltaan tutkapaneelien käyttöominaisuuksiltaan. Maatutkassa tutkapaneeli on kiinteä kiinteistön seinään tai katolle tolppaan asennettava paneeli, kun taas droonien havainnointitutkassa paneeli on katolle asennettava aktiivinen, automatisoitu pyörivä paneeli. Pyörivän paneelin ansiosta droonien havainnointitutka kykenee valvomaan oikein katolle asennettuna ja ilmaan suunnattuna kiinteistön yläpuolen ilmatilan.

Tutkien hankinnassa tulee kuitenkin huomioida, että tutkat toimivat luvallisilla taajuuksilla, sillä muuten ne muuttuvat luvanvaraisiksi. Luvallisia tutkia löytyy mm. kameravalmistajilta tai tutkalaitteisiin erikoistuneilta laitevalmistajilta.

Yleisimpiä käytössä olevia tutkateknologioita ovat LiDAR (Light Detection and Ranging) ja RADAR (Radio Detection and Ranging). RADAR on luotettava pitkällä kantamalla ja huonossa säässä, mutta sen tarkkuus on rajallinen. LiDAR tarjoaa huipputarkkuuden ja 3D-kuvauksen, mutta on herkempi sääolosuhteille ja lisäksi se on kalliimpi verrattuna RADAR:iin.

5.7. Droonit

Droonivalvonnalla tarkoitetaan yleensä mobiilia, drooniin perustuvaa valvontaa organisaation toimesta, jossa miehittämättömiä ilma-aluksia käytetään esimerkiksi alueiden, tapahtumien tai kiinteistöjen valvontaan reaaliaikaisella kuvantamisella ja muilla sensoreilla. Valvontaa voidaan toteuttaa myös autonomisesti, jolloin drooni valvoo aluetta itsenäisesti, tallentaen materiaalin muistikortille jälkikäteen tarkasteltavaksi tai lähettäen live-kuvadatan valvomoon.

Droonien havaitsemisen ja erityisesti niihin vaikuttaminen on useille toimijoille taloudellisesti ja juridisesti haastavaa. Tärkeämpää on tiedostaa miten drooneilta voidaan suojautua käytössä olevien resurssien puitteissa.

- Suojaa salainen tai suojattava tieto aina salakatselulta
 - ▶ Huolehdi, että esim. työaseman tai mobiililaitteen näyttö ei ole luettavissa ja tallennettavissa droonien toimesta.
- Hyödyntämällä droonien havaitsemisteknologiaa
 - ▶ Havaitsemista on mahdollista toteuttaa hyödyntäen tutkia, RF-analyysia, kamera- ja akustista valvontaa, sekä infrapunaan perustuvia järjestelmiä
- Suomen lainsäädäntö ei mahdollista tällä hetkellä drooneihin vaikuttamista organisaatioiden toimesta, pl. viranomaiset ja puolustusvoimat.

6 Vartiointipalvelut

Kohteen fyysistä turvallisuutta pystytään parantamaan ja uhkia ennaltaehkäisemään myös erilaisin turvallisuuspalveluratkaisuin. Palveluja voidaan räätälöidä toimijan ja kohteen fyysisen suojaamisen tarpeiden mukaisesti. Vartiointipalveluiden kustannusrakenne määräytyy pitkälti vartioinnin palkkakustannuksista, sekä lisäksi piirivartioinnissa ajoneuvokustannuksista ja hälytysten valvonnassa ja tarkastamisessa hälytysvalmiudesta.

Huomioitavaa on, että vartiointia voidaan tarvittaessa tilata vain määrääjäksi, esimerkiksi kahdeksi viikoksi remontin ajalle tai turvallisuutta edistämään, jos on havaittu turvallisuuteen liittyvän uhkatason nousua.

Yleisesti vartiointipalveluiden osalta on hyvä pitää mielessä kaksi asiaa:

1. Vartiointipalveluiden joustavuus

- Palvelusopimusten joustavuuteen kannattaa kiinnittää erityistä huomiota sopimuksia laadittaessa. Mikäli sopimusehdot ovat liian tiukat, voi käydä niin, että pienetkin muutostarpeet vartiointipalveluissa johtavat lisäkustannuksiin tai muutosten toteuttaminen viivästyy huomattavasti alkuperäisestä tarpeesta.

2. Vartiointipalveluiden raportointi

- Palvelusopimuksia laadittaessa on hyvä sopia myös raportoinnin riittävästä tasosta palveluntarjoajan kanssa, sillä raportointi tuo ostetuille palveluille lisäarvoa. Nykyään useimmilla palveluntarjoajilla on käytössään sähköiset raportointijärjestelmät, joiden ansiosta raportointi on käytännössä reaaliaikaista.

6.1. Paikallisvartiointi

Paikallisvartiointinnissa vartija on kohteessa läsnä sovituina kellonaikoina. Vartijan ollessa läsnä kohteessa, mahdollistetaan nopea reagointi uhkatilanteisiin. Jo pelkällä vartijan läsnäololla on turvallisuutta edistävä ja ennaltaehkäisevä vaikutus.

Paikallisvartiointin yhteydessä voidaan suorittaa tarkastuskierroksia, kuten julkisivun, teknisten tilojen ja tuotannon tilojen tarkastuskierroksia. Tarkastuskierroksille voidaan ennalta määritellä tarkastettavat asiat, kuten ovien lukitus, ikkunoiden lukitus tai esimerkiksi sisätilojen valojen sulkeminen tai palovartiointi.

Paikallisvartijan tehtäviin voidaan sisällyttää useita eri päivittäisiä tehtäviä, kuten ajoneuvo- ja henkilöportin hallinnointitehtävät, vierailijakirjanpidolliset tehtävät, turvallisuusjärjestelmien käyttö- ja valvonta tehtävät, avainten hallinta- ja luovutus sekä näkyvän vartiointin suorittaminen kohteella.

Paikallisvartiointin kustannukset määräytyvät tuotettujen volyymien mukaan, eli sen mukaan, kuinka paljon vuorokaudesta vartija on kohteella läsnä.



6.2. Aulavartiointi

Aulavartiointin avulla kohteeseen saadaan aulan vastaanottotehtävien hoidon lisäksi liitettyä esimerkiksi kohteen valvontakameroiden tarkkailu palveluntarjoajan toimesta. Riippuen palvelukokonaisuudesta, aula-vartiointiin voi kuulua myös kohteen turvajärjestelmien hallintaa sekä kulunvalvonnan tehtäviä.

Aulavartiointia kutsutaan usein myös termillä aulapalvelu, siihen usein liitettävien eri palvelutehtävien takia. Aulavartiointin tehtävänkuvaan usein liitetään vierailijoiden hallintaa ja asiakaspalveluun liittyvät tehtävät, kuten vierailijoiden vastaanotto ja sisään kirjaustehdävät, opastus ja neuvontatehtävät sekä päivittäiset postinjakot, avaintenhallinta- ja kiinteistöhuoltoon liittyvät koordinoitutehtävät.

6.3. Piirivartiointi

Piirivartiointinissa palveluntarjoaja suorittaa vuorokauden ympäri, tai vain tiettyinä kellonaikoina, kohteeseen (alue, kiinteistö, tilat) ennalta sovitusti vartiointikierroksia ja sovitun mukaisia toimenpiteitä.

Vartiointikierroksella suoritettavat tehtävät ovat voivat olla esimerkiksi hälytyslaitteiden kytkeminen valvontaan tai avaus- ja sulkukierrokset sekä tarkastuskierrokset, joilla vartija varmistaa, että alueella tai tilassa ei ole luvattomia henkilöitä. Piirivartiointi suorittaa myös

hälytystehtäviä, jossa esimerkiksi kiinteistön murtohälytyslaitteen hälyttäessä, vartija lähetetään paikalle tarkastamaan tilanne sekä selvittämään hälytyksen syytä.

Piirivartiointin hyöty on tarjota kustannustehokkaasti ja säännöllisen epäsäännöllisesti valvontaa kohteelle. Huomioitavaa on, että vartija ei kuitenkaan ole kohteella jatkuvasti, joten valvonta ja tarkastuskierrokset yhdistetään usein tekniseen valvontaan. Jos kohteella tarvitaan jatkuvaa vartijan paikalla oloa, voidaan harkita paikallis- tai aulavartiointipalvelua.

6.4. Etävalvontapalvelut

Etävalvonta käsittää erilaisten turvallisuusjärjestelmien aktiivisen valvonnan etäyhteyksin. Tyypillisin vartiointiliikkeen suorittama etävalvontapalvelu on kameravalvontapalvelu, joka toteutetaan esimerkiksi kamerakierroksin.

Kamerakierroksilla tarkoitetaan kohteen sisä- ja ulkoalueiden etävalvontaa. Vartija tarkkailee kohteessa olevien valvontakameroiden kuvaa ja mahdollisissa poikkeamatilanteissa reagoi hälytyksiin tarvittavilla toimenpiteillä tilanteen hoitamiseksi. Kamerakierrokset ovat usein kustannustehokas valvontaratkaisu paikallis- tai piirivartiointiin verrattuna mutta on hyvä huomioda, että kohteen turvallisuusjärjestelmien tulee olla ajantasaisia ja toimintakykyisiä, jotta etävalvonnasta saadaan toivottu hyöty.

6.5. Hälytysvalvonta

Hälytysvalvonnalla tarkoitetaan kohteen rikosilmoitinjärjestelmän lähettämien hälytysten vastaanottamista palveluntarjoajan hälytyskeskukseen sekä hälytysten välittämistä edelleen joko sovitulle yhteyshenkilölle ja/ tai vartijalle.

Palveluntarjoajan hälytyskeskuksen tulee olla Finanssiala ry:n hyväksymä.

6.6. Hälytysvartiointi

Hälytysvartiointinalla tarkoitetaan tilannetta, jossa palveluntarjoajan hälytyskeskus lähettää kohteelle vartijan tarkistamaan ilmaantuneen hälytyksen syyn sekä aloittamaan tilannekohtaiset toimenpiteet.

Hälytysvartiointinista käytetään usein sen arkisempaa termiä – *hälytyskäynnit*.

7 Suojaamisen kohde-esimerkit

Kriittisillä toimijoilla voi olla useita eri kiinteistökokonaisuuksia, joissa turvallisuuteen liittyvät tarpeet vaihtelevat kohteiden välisten muuttujien vuoksi. Tästä syystä kaikille kiinteistöille sellaisenaan sopivaa turvallisuusratkaisujen muuttia ei ole olemassa, mutta suuntaviivoja voidaan kuitenkin esittää. Seuraavat kolme kohde-esimerkkiä perustuvat kokoluokan perusteella tehtyyn turvallisuustarpeiden jaotteluun. Esimerkkien tarkoituksena on luoda yleisen tason ymmärrys kunkin kokoluokan kohteen vaatimista turvallisuustoimista, ja antaa suuntaa niiden hinnoittelusta.

7.1. Perustaso

Perustason kohteessa on normaaleja toimistoja, tuotantotiloja tai vastaavia. Tiloissa ei säilytetä salassa pidettäviä dokumentteja tai siellä ei ole huoltovarmuuden kannalta kriittisiä toimintoja, järjestelmiä tai laitteita.

Murtovalvontajärjestelmä

- Tilojen murtovalvonta toteutetaan riskienarvioinnin perusteella.
- Valvonnan laajuus on kuori ja tarvittaessa tila. Valvonnassa hyödynnetään ovikoskettimia, liikeilmaisimia ja lasirikkoilmaisimia.

Suositus järjestelmän luokasta:

- Vähintään EN50131 luokka (grade) 2

Hälytysten siirto:

- 24h miehitetty vartioimisliike

Kulunvalvontajärjestelmä

- Kulunvalvontajärjestelmä ei ole välttämätön.

Lukitusjärjestelmä

- Lukitus suositeltavaa toteuttaa **patenttisuojatulla** mekaanisella tai elektromekaanisella lukituksella. Avainhallinta vastuutettu nimetylle henkilölle.

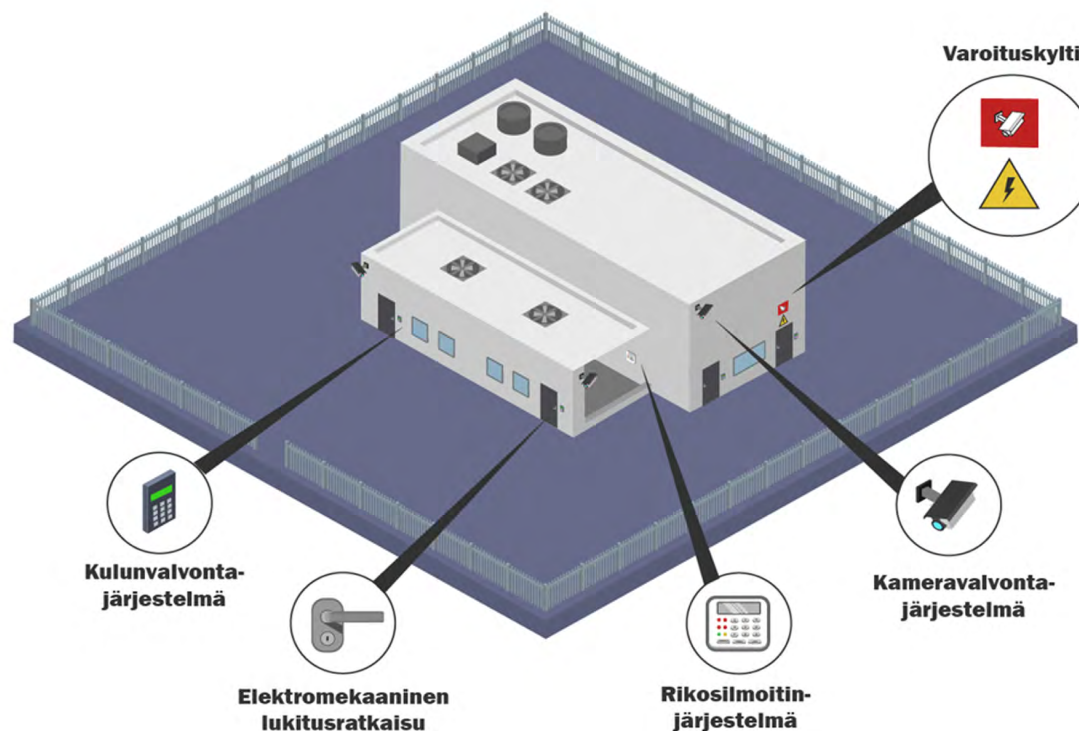
Kameravalvontajärjestelmä

- Kameravalvontajärjestelmä toteutetaan riskienarvioinnin perusteella. Valvonnan laajuus voi olla esimerkiksi rakennuksen kuori ja piha-alue, sekä sisäänkäyntiovet tarvittaessa.

Rakenteelliset ratkaisut

- Ei erityisiä vaatimuksia, ns. normaalit rakenteet soveltuvat. Suosituksena toteuttaa rakenteelliset ratkaisut ja rakenteiden vahventamiset tarvittaessa Finanssialan ”**Rakenteellinen murtosuojaus I**” mukaisesti.

<https://www.finanssiala.fi/wp-content/uploads/2024/01/rakenteellinen-murtosuojaus-i.pdf>



Kuva 10: Havainnollistava esimerkki perustasoisen kohteen valvonta- ja suojauskokonaisuudesta

7.2. Korotettu taso

Korotetun tason kohteessa säilytetään organisaation tai viranomaisten (TL-luokiteltua) salassa pidettävää tietoa tai kohteessa sijaitsee organisaation tai huoltovarmuuden kannalta kriittisiä toimintoja, järjestelmiä tai laitteita.

Organisaation säilyttäessä ja käsiteltäessä turvallisuusluokiteltua tietoa, on suositeltavaa hyödyntää rakenteellisessa ja teknisessä suunnittelussa, sekä toteutuksessa Katakriin ohjeistuksia, Valtioneuvoston asetusta asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), sekä tiedonluovuttajan ohjeistuksia ja mahdollisia vaatimuksia.

Murtovalvontajärjestelmä

- Tilat varustetaan murtovalvontajärjestelmällä.
- Valvonnan laajuus on vähintään kuori ja tila, sekä tarvittaessa kohde- ja kehäsuojaus.
- Eriyishuomioita tulee kiinnittää tiloihin, joissa säilytetään salassa pidettävää tietoa tai tilassa sijaitsee kriittisiä järjestelmiä tai laitteita.
- Valvonnassa hyödynnetään esimerkiksi ovikoskettimia, liikeilmaisimia, lasirikkoilmaisimia ja tarvittaessa tärinä- ja seismisiä ilmaisimia.

Suositus järjestelmän luokasta:

- Vähintään EN50131 luokka (grade) 3

Hälytysten siirto:

- Standardit SFS-EN ISO 9001:2015 ja SFS-EN 50518:2019 täyttävään hälytyskeskukseen

Kulunvalvontajärjestelmä

- Suosituksena varustaa tilat kulunvalvonnalla.
- Kulunvalvonnan laajuus vähintään kuoren ovet, tilojen väliset raja-ovet, sekä tunnistetut kriittiset tilat.
- Kulkeminen tapahtuu henkilökohtaista tunnistetta käyttäen.
- Kriittisten tilojen ja kuoren ovilla suosituksena hyödyntää PIN-näppäimistöllä varustettuja lukijoita, jotka mahdollistavat kaksoistunnistamisen.

Lukitusjärjestelmä

- Patenttisuojaattu mekaaninen lukitus tai kulunvalvonnan puuttuessa elektromekaaninen lukitus. Avainhallinta vastuutettu nimetyille henkilölle.

Kameravalvontajärjestelmä

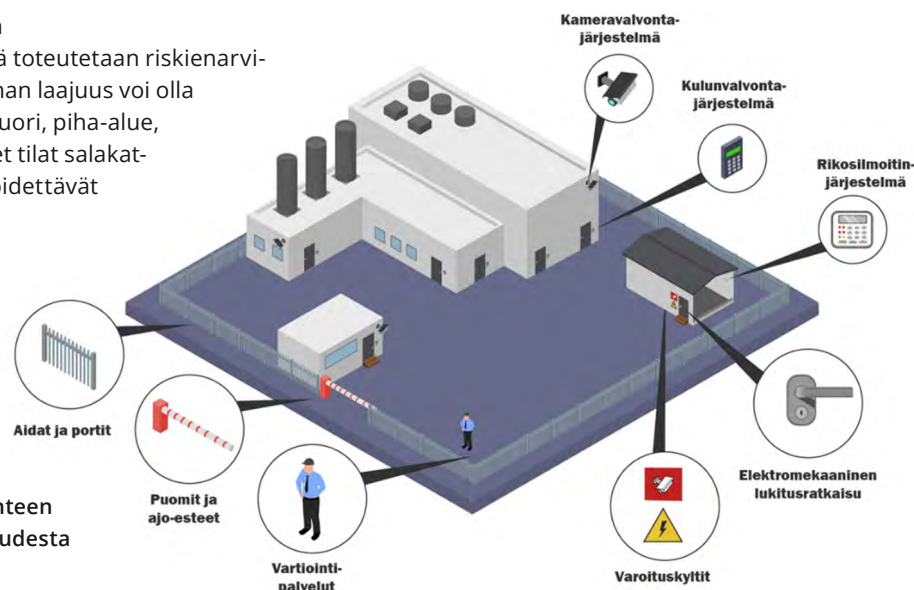
- Kameravalvontajärjestelmä toteutetaan riskienarvioinnin perusteella. Valvonnan laajuus voi olla esimerkiksi rakennuksen kuori, piha-alue, sisäänkäyntiovet ja kriittiset tilat salakatselu huomioiden (salassa pidettävät materiaalit).

Rakenteelliset ratkaisut

- Suosituksena toteuttaa rakenteelliset ratkaisut ja rakenteiden vahventamiset tarvittaessa Finanssialan ”Rakenteellinen murto suojausohje II” tai ”Rakenteellinen murto suojausohje III” mukaisesti. Organisaation tulee itse määrittää vaadittava taso, esimerkiksi säilytettävän salassa pidettävän tiedon tai järjestelmien kriittisyyden mukaisesti - riskienarvioinnin tuloksiin perustuen.

<https://www.finanssiala.fi/wp-content/uploads/2024/01/rakenteellinen-murto suojaus-ii.pdf>

<https://www.finanssiala.fi/wp-content/uploads/2024/01/rakenteellinen-murto suojaus-iii.pdf>



Kuva 11:
Havainnollistava
esimerkki korotetun tason kohteen
valvonta- ja suojauskokonaisuudesta

8 Hankinta-prosessi

Yksityisissä hankinnoissa yritys voi tehdä päätöksiä joustavammin ja hankintaprosessi on usein nopeampi, sillä sääntely ja kilpailutuksen velvoitteet ovat vähäisemmät kuin julkisella sektorilla. Yksityiset toimijat voivat painottaa esimerkiksi innovatiivisuutta tai nopeaa käyttöönottoa valinnoissaan. Yksityisissä hankinnoissa ei sovelleta julkisia hankintoja koskevaa hankintalakia.

Julkisissa hankinnoissa korostuvat avoimuus, tasapuolisuus ja kilpailuttaminen, koska hankinnat rahoitetaan julkisista varoista. Prosessiin liittyy tiukemmat säännöt, kuten hankintalain noudattaminen, mikä varmistaa läpinäkyvyyden ja reilun kilpailun tarjoajien kesken. Lisäksi julkisissa hankinnoissa riskienhallinta ja pitkäaikainen kustannustehokkuus ovat usein erityisen tärkeitä tavoitteita. Molemmissa hankintatavoissa on kuitenkin sama tavoite turvallisuuden näkökulmasta.

Fyysiseen suojaamiseen liittyvissä hankinnoissa on syytä huomioida myös varautumiseen liittyvät näkökulmat. Tähän liittyen on koottu ohjeistusta, mm. Huoltovarmuuskeskuksen hankintojen ja sopimusperusteisen varautumisen SOPIVA-suositukseen (uudet ohjeet julkataan alkuvuodesta 2026).

8.1. Turvajärjestelmien tarvemäärittely

Turvajärjestelmien hankinnan lähtökohtana on huolellinen tarvemäärittely, jossa kartoitetaan kiinteistön tai organisaation toimintaan, riskeihin ja suojaustarpeisiin liittyvät vaatimukset. Tarvemäärittelyssä tunnistetaan muun muassa suojattavat kohteet, arvot ja toiminnot sekä arvioidaan mahdolliset uhkatekijät ja niiden todennäköisyys. On tärkeää ottaa huomioon kiinteistön käyttötarkoitus, henkilöstön määrä, sijainti sekä muut erityispiirteet, jotka vaikuttavat järjestelmävalintoihin.

Tarvemäärittelyyn kannattaa osallistaa eri sidosryhmiä, kuten käyttäjiä, ylläpitoa ja turvallisuusasiantuntijoita, jotta lopputulos vastaa todellisia tarpeita ja käytännön toimintaa. Hyvin laadittu tarvemäärittely auttaa valitsemaan oikeat tekniset ratkaisut ja varmistaa, että järjestelmät tukevat organisaation arkea sekä täyttävät mahdolliset viranomaisvaatimukset ja standardit. Perusteellinen määrittely ehkäisee turhia kustannuksia ja mahdollistaa järjestelmien tehokkaan käytön sekä tulevaisuuden laajennukset ilman merkittäviä muutoksia.

Tarvemäärittely tulee dokumentoida, jotta kaikki osapuolet ovat tietoisia tavoitteista ja vaatimuksista hankintaprosessin aikana sekä järjestelmien ylläpidossa. Hyvä suunnittelu on puoli työtä – kun perusteukset ovat kunnossa, myös turvajärjestelmien käyttöönotto ja hallinta sujuvat jouhevasti.

8.2. Hankittavat järjestelmät

Turvajärjestelmät muodostavat kiinteistön ja organisaation suojaamisen teknisen perustan. Näihin järjestelmiin kuuluvat esimerkiksi kulunvalvontajärjestelmät, jotka rajoittavat ja seuraavat henkilöiden liikkumista tiloissa, sekä murtohälytysjärjestelmät, jotka havaitsevat luvattomat sisään tulot ja välittävät hälytyksen vartiointiliikkeelle tai hälytyskeskukseen. Videovalvontajärjestelmät mahdollistavat tilojen reaaliaikaisen valvonnan ja tapahtumien tallentamisen, mikä tukee sekä ennaltaehkäisevää turvallisuutta että jälkikäteistä selvittelyä.

Lisäksi fyysisiin turvajärjestelmiin voidaan lukea tekniset esteet, kuten portit, aidat ja lukitusratkaisut, jotka vaikeuttavat pääsyä suojattuihin alueisiin. Kaikien järjestelmien yhteensovitus, integrointi tai analysointi mahdollistavat kattavan turvallisuustason ja tukevat kiinteistön arjen toimintaa sekä riskienhallintaa.

8.3. Turvajärjestelmiin liittyvät palvelut

Turvajärjestelmien hankintaan kuuluu olennaisena osana myös niihin liittyvät palvelut, jotka varmistavat järjestelmien toimivuuden ja tukevat niiden käyttöä arjessa. Tyypillisiä palveluita ovat esimerkiksi järjestel-

mien pääkäyttäjä-, korjaushuolto-, ja ennakko- huolto- palvelut sekä tekninen tuki ja käyttäjien koulutus. Näillä palveluilla varmistetaan, että turvajärjestelmät toimivat suunnitellusti ja käyttäjät osaavat hyödyntää niiden ominaisuuksia tehokkaasti.

Lisäksi palveluihin voi sisältyä järjestelmien palvelunalustat ohjelmistointeen (SaaS), etävalvonta, ylläpito ja ohjelmistopäivitykset, joiden avulla turvajärjestelmiä voidaan kehittää ja mukauttaa muuttuvien tarpeiden mukaisesti.

Vartiointipalvelut, hälytyskeskusyhteydet sekä järjestelmien auditointi ja testaus ovat myös tärkeitä osia kokonaisvaltaista turvallisuutta. Hyvän palveluntarjoajan valinta ja selkeät palvelusopimukset auttavat ehkäisemään ongelmia sekä takaavat järjestelmien pitkäikäisyyden ja kustannustehokkaan käytön.



8.4. Hinta-arvion laatimien

On tärkeää muistaa, että esitetyt hinta-arviot ovat puhtaasti suuntaa antavia; budjetoinnin tulee aina perustua saatuihin tarjouksiin. Lisäksi muutokset markkinatilanteissa voivat vaikuttaa voimakkaasti hintoihin. Hinta-arviot eivät myöskään sisällä järjestelmien tai rakenteellisten suojausmekanismien toimintaan saattamiseksi yleistä tasoa vaativampien asennustöiden lisäkustannuksia.

Alla esitetyt kustannukset ovat sidottu Q4/2025 hintatasoon ja myöhemmin tarkasteltuna hintaan tulee lisätä vähintään 5 % / vuosi.

Hankintavaiheessa tulee huomioida kohdekohtaiset asennustyön haasteet, vaadittavat aputyöt sekä tarvittavat lisävarustukset kuten:

- Perustukset sekä maadoitukset
- Kaapelointitapa ja kaapeloinnissa käytettävä materiaali (MHS, kuitu ja CAT6)
- Keskusten virransyöttö ja varmistukset (UPS tai varavoima)
- Verkkoyhteyksien luominen
- Laitekaappien sekä vaadittavien kenttälaitteiden lämmitys tai viilennys
- Nostinkulut
- Suunnittelukustannukset
- Matkakulut ja yöpyminen (kohteiden sijainti verrattuna asennusliikkeeseen)

8.5. Rakenteellinen suojaus

Suojausmalliin perustuen, kohteen rakenteellinen suojaus tulisi toteuttaa niin, että kiinteistön kehä varustetaan aidoilla, henkilökulku- ja ajoneuvoporteilla sekä puomeilla. Kehä- ja aluesuojauksessa suositellaan hyödynnettäväksi valvontaa tehostavia valaisinylväitä, joita tulee asentaa siten, että kohteen aidattu alue on katettu myös pimeään aikaan.

Kuorisuojauksessa kiinteistön kaikki ovet, ikkunat ja muut aukot tulee varustaa asianmukaisilla, murtosuojatuilla ovilla, ikkunoilla tai luukuilla. Kuoren rakenteel-

linen suojaus tulee suunnitella niin, ettei kiinteistöön päästä tunkeutumaan luvattomasti. Tila ja kohdevyöhykkeellä rakenteellisen suojauksessa tulee huomioida tilakohtaiset turvallisuusvaatimukset. Ovien kustannuksiin vaikuttaa, valitaanko esimerkiksi sellaiset ovet, joilla suojataan joko murtautumiselta tai palolta tai molemmilta.

Alla esitetty esimerkkikohteen hinta-arvio sisältää kohteen kehän aidan, ajoneuvo- ja henkilökulkuportit, ajoneuvopuomit, aluesuojauksen ulkovalaisinylväät sekä palonkestävät ovet ja murtosuojatut ikkuna-aukot.

Rakenteellinen suojaus	Määrä	Hinta-arvio EUR
Teräs tai alumiini verkkoaita (metriä)	1	25–45 €
Ajoneuvopuomi (kpl)	1	4 000–6 000 €
Manuaalinen käyntiportti (kpl)	1	1 500–2 500 €
Automaattinen ajoneuvoportti (kpl)	1	9 000–20 000 €
Ulkovalaisinylväs (kpl)	1	2 000–4 500 €
Palonkestävä profiiliovi (kpl)	1	1 500–2 500 €
Palonkestävä umpiovi (kpl)	1	1 000–1 500 €
Ikkunoiden murtosuojakalvo (m ²)	1	150–250 €

8.6. Kameravalvontajärjestelmä

Kameravalvontajärjestelmän toiminta kohteessa perustuu henkilön, tapahtuman tai alueen valvontaan, käyttäen joko aktiivista (kuvaa seurataan esimerkiksi valvomosta) tai passiivista (kuva tallennetaan myöhemmin katsottavaksi) kameravalvontaa. Kamera-valvontajärjestelmä koostuu pääosin tallentimesta, aktiivilaitteista kuten kytkimistä ja niihin liitettävistä kameroista ja mahdollisesta erillisestä palvelimesta.

Kameravalvontajärjestelmän osalta suojausmallin mukaisessa suojauksessa kameravalvontajärjestelmän tarkoituksena on tuottaa yleistä kuvaa kiinteistön ympäristöstä, kuten aidoilta ja sisäänkäyntien porteilta. Sisäänkäyntien porttien ja muiden sisäänkäyntien kulkuväylien osalta on suositeltavaa, että kameravalvonnalla saadaan valvottua alue tunnistamisen tarkkuudella.

Sisätiloissa tapahtuva kameravalvonta on suositeltavaa toteuttaa siten että sillä saadaan valvottua prosesseihin ja henkilöstön työturvallisuuteen kuuluvat riskialueet sekä muutoin yleiskuvaa käytäviltä, auloista ja

asiakastiloista. Kameravalvontajärjestelmän käyttö ei kuitenkaan sovellu henkilökunnan työnteon seuraamiseen, josta on määritelty laissa.

Alla esitetty esimerkkikohteen kameravalvontajärjestelmän hinta-arvio sisältää vaadittavat palvelimen, työaseman, kytkimet, ohjelmistot ja lisenssit, asennustyöt, kaapeloinnin sekä palvelut.

Kameravalvontajärjestelmä	Määrä	Hinta-arvio EUR
Kameravalvonnan tallennin	1	2 000–12 500 €
Ohjelmistot ja Kameralisenssit / Kamera	1	70–200 €
Kiinteä ulkokamera	1	450–950 €
Kiinteä sisäkamera	1	200–500 €
PTZ kääntöpääkamera	1	600–2 500 €
CAT tai Kuitukaapelointi / Piste	1	140 €
Ohjelmiston ylläpito tai lisenssimaksu / kamera	1	20–40 €
Huolto ja ylläpitopalvelut / kk	1	100–250 €



8.7. Kulunvalvontajärjestelmä

Kohteen kulunvalvontajärjestelmä koostuu palvelimesta, yhdestä tai useammasta keskuslaitteesta, keskuslaitteisiin liitettävistä oviohjaimista, oviohjaimiin liitettävistä lukijoista sekä hallinnointityöasemasta. Kulunvalvontajärjestelmän palvelin voidaan sijoittaa fyysisesti kohteeseen, tai vaihtoehtoisesti palveluntuottajien hallinnoimaan pilvipalveluun. Suositeltavaa on, että suurien organisaatioiden kulunvalvontajärjestelmän hallinnointi on keskitettyä, helpottaen täten kulkemista eri kohteiden välillä, samaa kulkutunnistetta käyttäen.

Alla esitetty esimerkkikohteen kulunvalvontajärjestelmän hinta-arvio sisältää vaadittavat oviohjaimet, virtalähteet, palvelimen, työaseman, erillisen varavirtalähteen, kulunvalvontajärjestelmän lisenssit, asennustyöt, kaapeloinnin sekä palvelut.

Kulunvalvontajärjestelmä	Määrä	Hinta-arvio EUR
Kulunvalvontapiste, yksipuoleinen lukija	1	800–1 200 €
Kulunvalvontapiste, kaksipuoleinen lukija	1	1 000–1 400 €
Ohjelmistot ja lisenssit / Ovi	1	10–35 €
Palvelinympäristö / kk (SaaS)	1	600–1 250 €
MHS kaapelointi / Piste	1	170 €
Huolto ja ylläpitopalvelut / kk	1	100–250 €
Ohjelmiston ylläpito ja lisenssimaksut / kk	1	50–800 €
Pääkäyttäjäpalvelut / kk	1	100–350 €



8.8. Murtohälytysjärjestelmä

Suojausmallin mukaisesti, murtohälytysjärjestelmällä valvotaan kohteen vyöhykkeitä erilaisin ilmaisimin. Kohteen murtohälytysjärjestelmä koostuu yhdestä tai useammasta keskuslaitteesta, johon murtohälytysjärjestelmän ilmaisimet kaapeloidaan. Ilmaisimien kaapelointi keskuslaitteen väylään voidaan tehdä osoitteellisesti tai silmukkapäätteillä. Osoitteellinen valvonta mahdollistaa tiedon saamisen siitä, mikä tietty ilmaisimien kyseisessä väylässä hälyttää.

Kehän ilmaisimien tarkoituksena on valvoa aita- ja portteja sekä muita kehällä olevia kulkureittejä. Aluesuojauksessa ilmaisimien keskeisin tehtävä on valvoa yleiskuva sisäpihalla liikkuvista henkilöistä aikoina, jolloin henkilökunnan toiminta alueella on vähäistä. Aidan ja raja-alueen valvontaan voidaan käyttää linjailmaisimia sekä aita- ja porttivalvontaa.

Kiinteistön sisätiloissa murtohälytysjärjestelmällä pyritään valvomaan kaikkia kiinteistön murtorajapinnassa olevia ovia, ikkunoita ja luokkuja magneettikoskettimin, lasirikkokäyttöilmaisimien sekä IR-ilmaisimien. Kiinteistön kuoren tilat on syytä valvoa kahdennetuoin keinoin,

mikäli se nähdään tarpeelliseksi tilojen kriittisyysluokan tai muun turvallisuusnäkökulmaan perustuen. Kahdennetulla valvonnalla tarkoitetaan esimerkiksi magneettikoskettimia ovissa, sekä tilailmaisimia tai lasirikkokäyttöilmaisimia, jotka valvovat sisäänkäyntejä.

Hinta-arvio pitää sisällään myös järjestelmän vaatimat silmukkakortit, virtalähteet, käyttöpaneelit, tiedonsiirtolaitteen ja järjestelmän asennustyöt, kaapeloinnin sekä palvelut.

Murtohälytysjärjestelmä	Määrä	Hinta-arvio EUR
Keskuslaite	1	500–1 200 €
Käyttölaite	1	200–450 €
Ilmoituksensiirtolaite	1	300–700 €
Ohjelmistot ja lisenssit / kk (tarvittaessa)	1	15–20 €
Murtohälytysjärjestelmän ilmaisimet	1	30–180 €
Murtohälytysjärjestelmän ovikoskettimet	1	15–30 €
MHS kaapelointi / Piste	1	140 €
Huolto ja ylläpitopalvelut / kk	1	100–250 €

8.9. Lukitusratkaisut

Lukituksen tarkoituksena on estää luvaton pääsy rajatuille alueille ja kiinteistöön. Lukituksessa tulee huomioida kiinteistön käyttöaste, tarvittavien avainten määrä, avaintenhallinnan toteutus sekä erityistä valvontaa mahdollisesti vaativat kiinteistön tilat.

Kulunvalvontajärjestelmään sekä rakennusautomaatiikkaan liitettävät ovet tulee varustaa sähköluukoilla, kuten moottori- tai solenoidilukoilla, jotka ovat käyttötarkoitukseltaan tilaan soveltuvat sekä ohjausjärjestelmiin sopivat. Lukituksessa on suositeltavaa käyttää kulunvalvontaa tai elektromekaanisia avainpesiä kohteen ulkokuoren ovissa, porteissa, sekä kiinteistön sisätiloissa. Kulunvalvonnan tai elektromekaanisen lukituksen tavoitteena on sujuvoittaa avaintenhallintaa ja kulkeamista kiinteistössä sekä korottaa turvallisuuden tasoa.

Alla esitetty esimerkkikohteen hinta-arvio sisältää kaikkien ovien avainpesien toteutuksen elektromekaanisella lukitusratkaisulla.

Lukitusratkaisut	Määrä	Hinta-arvio EUR
Sisäoven lukitus (mekaaninen)	1	150–300 €
Sisäoven lukitus (elektromekaaninen)	1	250–450 €
Ulko-oven lukitus (mekaaninen)	1	200–350 €
Ulko-oven lukitus (elektromekaaninen)	1	300–550 €
Sähköinen moottorilukko (Ulko-ovet)	1	1 000–1 400 €
Sähköinen Solenoidilukko (Sisäovet)	1	700–900 €
Avaimet	1	30–80 €
Lisenssimaksut / kk	1	10 €
Huolto ja ylläpitopalvelut / kk (Lukoston hallinta)	1	50 €



8.10. Vartiointipalvelut

Kohteen fyysistä turvallisuutta voidaan parantaa eri vartiointipalveluilla. Suurille kohteille suunnattuja vartiointipalveluita ovat mm. paikallis- ja aulavartiointipalvelut, kun taas keski- ja pienikokoisille kohteille suunnattuja vartiointipalveluita ovat piiri- ja hälytysvartiointipalvelut sekä hälytysvalvontapalvelut.

Vartiointipalveluiden kustannusten muodostumiseen vaikuttaa olennaisesti tilattavien vartiointipalveluiden määrä. Esimerkiksi paikallisvartiointipalvelussa tilattava palvelu saattaa olla hyvinkin räätälöity asiakkaan ilmoittamiin tarpeisiin kohdistuen vain sovittujen asioiden tarkkailuun ja valvontaan.

Alla olevassa taulukossa on esitetty suuntaa antavia kustannusarvioita eri vartiointipalveluiden osalta.

Vartiointipalvelu	Tarkennus	Määrä	Hinta-arvio EUR
Paikallisvartiointipalvelu	Ympäri vuorokautinen (24 h)	1	25 000–30 000 €
Paikallisvartiointipalvelu	Arkipäivisin 12 h	1	8 000–9 500 €
Piirivartiointipalvelu	Kolme kierrosta joka päivä (ma–su)	1	1 000–1 500 €
Aulavartiointipalvelu	Arkipäivisin 8 h	1	5 000–6 500 €
Etävalvontapalvelu	Kaksi kierrosta joka päivä (ma–su)	1	400–700 €
Hälytysvalvontapalvelu	Ympäri vuorokautinen (24 h)	1	40–70 €
Hälytysvartiointipalvelu (hälytyskäynnit)	Arkisin (huom. veloitetaan toteuman mukaan)	1	70–100 € (kertakustannus)
Hälytysvartiointipalvelu (hälytyskäynnit)	Viikonloppuisin ja pyhinä (huom. veloitetaan toteuman mukaan)	1	120–200 € (kertakustannus)

9 Hallinnollinen turvallisuus

Liiketoiminnan jatkuvuus, turvallisuus ja vaatimuksenmukaisuus muodostavat yhdessä kestävä ja vastuullisen yritystoiminnan perustan. Kun nämä osa-alueet ovat asianmukaisesti huomioituja, organisaatio kykenee toimimaan tehokkaasti, turvallisesti ja luotettavasti muuttuvassa toimintaympäristössä.



Kuva 12: Elinkeinoelämän keskusliiton yritysturvallisuusmalli jatkuvaan parantamiseen (sovellettuna)



9.1. Turvallisuusjohtaminen

Turvallisuusjohtaminen on organisaatitasoinen, systemaattinen lähestymistapa, jolla varmistetaan turvallisuustoimien suunnittelu, toteutus ja jatkuva kehittäminen. Siihen kuuluu riskien tunnistaminen ja arviointi, selkeiden vastuualueiden määrittely sekä johdon sitoutuminen turvallisuuskulttuuriin ylläpitämiseen. Turvallisuusjohtaminen edellyttää säännöllistä seurantaa, auditointeja sekä henkilöstön osallistamista, jotta turvallisuuskäytännöt pysyvät ajan tasalla ja organisaatio kykenee reagoimaan nopeasti muuttuviin uhuihin. Hyvin johdettu turvallisuustoiminta vahvistaa organisaation resilienssiä ja tukee pitkän aikavälin liiketoiminnan jatkuvuutta.

9.2. Turvallisuusosaaminen

Olenaisena osana tätä on henkilöstön ohjeistaminen ja turvallisuusosaamisen ylläpito. Henkilöstön turvallisuusosaamisen ja tietoisuuden kehittämiseksi ja ylläpitämiseksi on monenlaisia keinoja. Henkilöstön osamisen perustana toimii kattava ja toisteinen turvallisuuskoulutus. Henkilöstölle perehdytetään toimintamallit fyysisen turvallisuuden osalta, ja määritellään, miten nämä vaikuttavat yksilön ja työyhteisön toimintaan jokapäiväisessä toiminnassa sekä mitä henkilöstöltä odotetaan fyysisen turvallisuustason ylläpidon suhteen.

Henkilöstölle annettavat turvallisuusohjeistuksien tulisi kattaa kaikki oleellinen heidän toimintansa kannalta. Turvallisuusohjeistuksissa on hyvä käyttää visuaali-

suutta ja esimerkkejä esitettävien asioiden havainnollistamiseksi. Ohjeistusten osalta tulee varmistua niiden saatavuudesta ja päivittämisen käytänteistä.

9.3. Turvallisuuskulttuuri

Henkilöstön rooli halutun fyysisen turvallisuustason ylläpidossa on tärkeä, mutta yleiseen suhtautumiseen turvallisuutta kohtaan vaikutetaan ennen kaikkea organisaation johdon toimesta. Johdon suhtautuminen fyysiseen turvallisuuteen korreloi suoraan henkilöstön asenteisiin ja tekoihin. Ilmentämällä fyysisen turvallisuuden tärkeyttä ja viestimällä tästä läpi koko organisaation, johto kertoo tahtotilastaan ja siitä, millaista turvallisuuskäyttäytymistä organisaatiossa edellytetään ja miksi fyysisestä turvallisuudesta on tärkeää jokaisen omalta osaltaan huolehtia. Organisaation turvallisuuskulttuuri tulee saattaa tasolle, jolla se tukee tehokkaasti fyysisen turvallisuuden rakenteellisia ja teknisiä ratkaisuja.

Henkilöstöön riittyviä riskejä voidaan vähentää turvallisuusselvitysten myötä. On kuitenkin hyvä huomioda, että turvallisuusselvitykset ovat vain yksi työkalu, jonka avulla voi vaikuttaa yritysturvallisuuteen.

9.4. Poikkeamienhallinta

Poikkeamilla viitataan sellaisiin tilanteisiin tai tapahtumiin, joissa organisaation toiminta ei ole suunnitellun tai vaatimusten mukaista. Organisaatioilla on hyvä olla olemassa poikkeamien ja korjaavien toimenpiteiden

prosessi, jolla varmistetaan, että mahdollisia poikkeamia tunnistetaan osana organisaation ja sen henkilöstön jokapäiväistä toimintaa, ja että tunnistetut poikkeamat käsitellään systemaattisesti niin, että tarvittavat poikkeaman korjaavat toimenpiteet toteutetaan. Poikkeamia on mahdollista tunnistaa muun muassa henkilöstön toimesta esimerkiksi katselmoimalla järjestelmistä saatua dataa, mutta myös ulkopuolisten tahojen toimesta muun muassa asiakasvalitusten muodossa. Poikkeamatilanteiden varalle on syytä määritellä toimintatavat ja poikkeama- tai turvallisuushavainnoista ilmoittamisen prosessi. Henkilöstön tulee pystyä helposti ilmoittamaan tapahtuneista toimitilaturvallisuuden poikkeamatilanteista, jotta niihin voidaan reagoida.

Kun organisaation toiminnassa havaitaan poikkeamia, tulee organisaation:

1. reagoida poikkeamaan tilanteen edellyttämällä laajuudella
2. ryhtyä toimiin poikkeaman hallitsemiseksi ja korjaamiseksi
3. käsitellä poikkeamasta johtuvia seurauksia
4. arvioida toimenpiteiden tarve poikkeaman syiden poistamiseksi ja poikkeaman toistumisen estämiseksi
5. selvittää toistuuko sama poikkeama organisaation toiminnan eri osa-alueilla
6. säilyttää dokumentoitua tietoa näyttönä poikkeamien luonteesta, poikkeamien takia tehdyistä toimenpiteistä, sekä tehtyjen korjaavien toimenpiteiden tuloksista.



Poikkeamaan reagointi ja sitä seuraavien toimenpiteiden laajuus tulisi arvioida aina tapauskohtaisesti. Kaikkia poikkeamia eivät välttämättä edellytä korjaustoimenpiteitä, eikä kaikkia poikkeamia tai niiden syitä ole taloudellisesti kannattavaa poistaa täysin. Tästä prosessista saatava informaatio on hyödynnettävissä erinomaisesti mm. osana riskienarviointia ja turvasuunnittelua.

9.5. Pääsynhallinta

Pääsynhallinta on olennainen osa organisaation turvallisuutta, ja sen tavoitteena on varmistaa, että vain valtuutetut henkilöt pääsevät tiloihin, tietoihin ja järjestelmiin. Henkilöstölle pääsynhallinta toteutetaan usein henkilökohtaisilla kulkutunnisteilla, vahvoilla salasanoilla ja käyttöoikeuksien säännöllisellä tarkistuksella. Sidosryhmien, kuten alihankkijoiden ja yhteistyökumppaneiden, osalta on tärkeää määritellä selkeät pääsyoikeudet ja rajata ne vain tarpeellisiin resursseihin.

Vierailijoille pääsy järjestetään yleensä rekisteröinnin ja saattamisen kautta, jolloin heidän liikkumistaan organisaation tiloissa valvotaan. Näin organisaatio pystyy hallitsemaan riskejä, estämään luvattoman pääsyn ja tukemaan turvallisuusjohtamisen tavoitteita.

Vieraiden pääsynhallintaa toimii erinomaisena esimerkkinä sellaisesta hallinnollisesta prosessista, joka on valittavan helppo jättää huomioimatta, mutta puuttues-

saan heikentää merkittävästi kulunhallinta- ja valvontajärjestelmien sekä muiden tilaturvallisuusratkaisujen vaikuttavuutta.

9.6. Turvallisuusauditoinnit

Turvallisuusauditointeja voidaan pitää olennaisena osana turvallisuusjohtamista. Auditoinnin avulla pyritään selvittämään fyysisen turvallisuuden olemassaoloa, tehokkuutta ja toimivuutta. Auditoinnilla kerättävää tietoa verrataan asetettuihin turvallisuuskriteereihin ja vähimmäisvaatimuksiin. Kriteeristönä voi toimia lain vähimmäisvaatimusten lisäksi esimerkiksi kansallinen turvallisuusauditointikriteeristö (Katakri).

Auditointien tulokset tarjoavat organisaatiolla tärkeää informaatiota liittyen siihen, millaista organisaation turvallisuustoiminta nykyisellään on, auttaa löytämään kehityskohteita, tukee varautumista ja ennaltaehkäisee ongelmia. Lisäksi sisäinen auditointi on keskeinen työkalu organisaation vaatimustenmukaisuuden varmistamiseksi, eli sen varmistamiseksi, että organisaation toiminta on sitä velvoittavien lakien, regulaatioiden ja asetusten mukaista.

Vaikuttava auditointi:

1. Organisaatio tunnistaa tarpeen auditoinnille
2. Määritellään organisaation lähtökohdat ja auditoinnin tavoitteet
3. Määritetään auditointimenetelmät, jolla auditointikriteereihin peilaaminen tapahtuu
 - a. Näitä voi olla esimerkiksi ennalta laaditut tarkastuslistat, paikan päällä tehtävät testaukset tai tarkastukset
4. Selvitetään nykytilanne, tutustutaan olemassa olevaan turvallisuuskirjallisuuteen ja suoritetaan haastatteluja
5. Auditointitapahtuma, jossa todennetaan auditointikriteerien täyttyminen
 - a. Osallistujilla tulee olla riittävä asiantuntemuksen taso auditoitavaan kohteeseen tai asiaan
6. Auditointiraportin laadinta, josta ilmenee mm.:
 - a. Auditoinnin kohde
 - b. Miten tavoitteet saavutettiin
 - c. Havaitut poikkeamat
 - d. Havaitut hyvät käytänteet
 - e. Johtopäätökset
7. Mahdollisten poikkeamien korjaaminen ja uudelleen auditointi

9.7. Jatkuva parantaminen

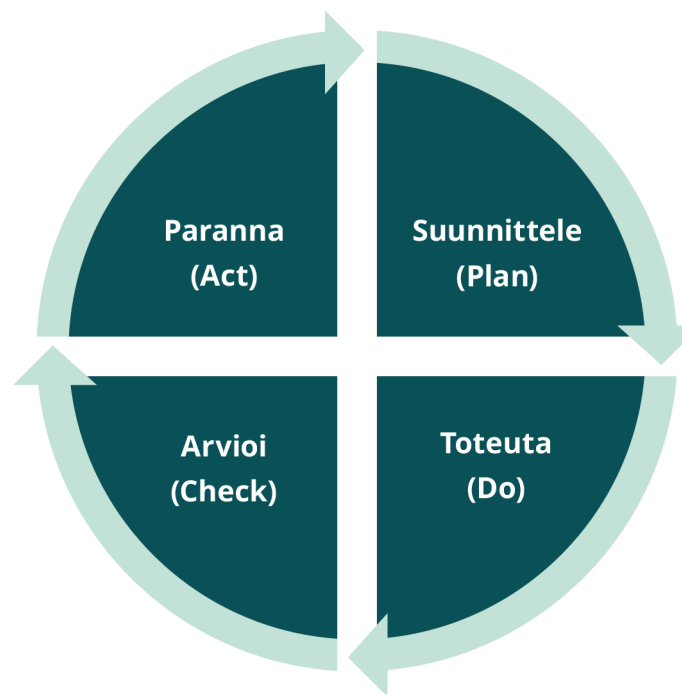
Organisaatioiden toiminnassa sekä sisäisessä ja ulkoisessa toimintaympäristössä tapahtuu jatkuvasti muutoksia, jotka edellyttävät organisaatiolta muutosta ja mukautumiskykyä. Esimerkkeinä tällaisista mukautumiskykyä vaativista muutoksista toimii muun muassa lainsäädännölliset muutokset sekä organisaatioiden toiminnalliset muutokset.

Turvallisuuteen liittyviin muutoksiin mukaudutaan usein reaktiivisesti esimerkiksi vuosittaisilla katselmoinneilla, joissa ei ehditä pureutua keskeisiin turvallisuusasioihin riittävässä laajuudessa. Tällöin muutostarpeiden tunnistaminen, arvioiminen sekä tarvittavien toimenpiteiden suunnittelu jää pintapuoleiseksi. Lisäksi katselmointiin mennessä organisaation turvallisuuteen liittyvät ohjeet ja toimintamallit ovat saattaneet muuttua jo useampaan otteeseen, kun muutoksiin mukautumiseksi muodostetaan epävirallisia käytänteitä, jotka poikkeavat toisistaan.

Jatkuvan parantamisen prosessilla puolestaan pyritään varmistamaan se, että organisaatio on ennalta tunnistanut ja määritellyt asiat, jotka edellyttävät siltä mukautumiskykyä, ja määritellyt mukautumiseen liittyvät käytänteet ja toimintamallit. Näin organisaatio kykenee mukautumaan muutoksiin luonnollisena osana jokapäiväistä toimintaa.

Tyypillinen prosessimalli jatkuvaan parantamiseen on niin sanottu PDCA tai Plan-Do-Check-Act malli, jossa jatkuva parantaminen nähdään ympyrämallisena päätymättömänä syklinä, jossa ensin suunnitellaan (Plan),

sitten tehdään (Do), jonka jälkeen arvioidaan tehdyn toimen vaikuttavuus (Check), ja tehdään tarvittavat muutokset ja korjaukset (Act) ja aloitetaan sykli alusta.



Kuva 13: Plan-Do-Check-Act (PDCA) malli jatkuvaan parantamiseen



10 Työkalut

Oppaan rinnalle on kehitetty neljä erilaista ongelmanratkaisupuuhun perustuvaa työkalua tukemaan tarvemäärittelyä. Ne ovat saatavilla HVO Extranetistä.

**Kameravalvontajärjestelmän
ongelmanratkaisupuu**

**Murtohälytysjärjestelmän
ongelmanratkaisupuu**

**Kulunhallinta- ja
kulunvalvontajärjestelmän sekä
lukitusratkaisujen
ongelmanratkaisupuu**

**Vartiointipalveluiden
ongelmanratkaisupuu**

11 Liite 1 – Lait, standardit ja oheismateriaalit

Vaatimustenmukaisuus

Fyysisen suojauksen kehittäminen aloitetaan tunnistamalla vaatimukset, joita organisaatioon ja toimintaan kohdistuu. Kuvassa 14 on esitetty vaatimustenmukaisuuden (Compliance) keskeiset kokonaisuudet, joilla fyysisen turvallisuuden tasoa voidaan määritellä.

Vaatimustason määrittämiseen vaikuttavat sekä sisäiset että ulkoiset tekijät. Ulkoisia tekijöitä ovat esimerkiksi organisaatiota koskevat lakisääteiset velvoitteet, asetukset, standardit sekä huoltovarmuuteen tai varautumiseen liittyvät viranomaismääräykset. Niitä, sekä eräitä fyysiseen turvallisuuteen liittyviä erityisohjeita ja muita aineistoja on koottu tarkemmin tähän liitteeseen. Kuvausten yhteydessä on myös verkkolinkit aineistoihin.



Kuva 14: Vaatimustenmukaisuuden keskeiset kokonaisuudet

11.1. Lait ja asetukset

Lait ja asetukset määrittelevät organisaatioille velvollisuuksia fyysiseen turvallisuuteen liittyen. Näitä velvollisuuksia esiintyy niin yleisesti yksityishenkilöitä sekä toiminnanharjoittajia koskevassa lainsäädännössä, mutta myös toimialakohtaisissa laeissa ja asetuksissa.

Lakien noudattamatta jättämisellä on aina negatiivisia seurauksia, joiden vaikutus riippuu noudattamatta jätetyn lain luonteesta, poikkeaman vakavuudesta, sekä muista mahdollisista tapauskohtaisista tekijöistä. Lain noudattamatta jättämisen seuraukset voivat vaihdella huomautuksista aina sakkorangaistuksiin, rikossyytteisiin tai jopa toimiluvan menetykseen.



Ohessa lista huoltovarmuuskeskuksen kannalta keskeisimmistä fyysiseen turvallisuuteen liittyen velvoittavista laeista ja asetuksista.

DORA-asetus asetus (EU) 2022/2554, perustuu EU:n asetukseen. Sen tarkoituksena on varmistaa, että finanssialan toimijat pystyvät sietämään, hallitsemaan ja palautumaan tieto- ja viestintätekniikkaan (TVT) liittyvistä häiriöistä ja kyberuhista.

[https://eur-lex.europa.eu/legal-content/fi/](https://eur-lex.europa.eu/legal-content/fi/TXT/?uri=CELEX:32022R2554)

[TXT/?uri=CELEX:32022R2554](https://eur-lex.europa.eu/legal-content/fi/TXT/?uri=CELEX:32022R2554)

<https://www.finlex.fi/fi/lainsaadanto/fi/saantely/saantelykokonaisuuDET/dora/>

Kyberturvallisuuslaki (124/2025), toimeenpanee EU:n **NIS2-direktiivin** vaatimukset. Lain tavoitteena on vahvistaa kyberturvallisuutta ja yhtenäistää turvallisuustaso koko EU:n alueella, erityisesti kriittisillä toimialoilla kuten energia-, liikenne-, terveydenhuolto-, finanssi- ja digitaalisen infrastruktuurin palveluissa.

<https://www.finlex.fi/fi/lainsaadanto/saaduskokoelma/2025/124>

Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (CER), toimeenpanee EU:n **CER-direktiivin** (Critical Entities Resilience Directive). Lain tavoitteena on vahvistaa yhteiskunnan kriisinkestävyyttä ja kansallista turvallisuutta varmistamalla, että elintärkeitä palveluja tuottavat toimijat pystyvät jatkamaan toimintaansa kaikissa olosuhteissa

<https://www.finlex.fi/fi/lainsaadanto/2025/310>

Laki yhteistoiminnasta yrityksissä (1333/2021)

säätää työnantajan ja henkilöstön välistä vuorovaikutusta ja osallistumista yrityksen päätöksentekoon. Sen tarkoituksena on luoda toimintakulttuuri, jossa työnantaja ja henkilöstö toimivat yhteistoiminnan hengessä, kunnioittaen toistensa oikeuksia ja velvollisuuksia.

<https://www.finlex.fi/fi/lainsaadanto/2021/1333>

Laki yksityisistä turvallisuuspalveluista (1085/2015)

on pääasiallinen laki, joka määrittelee vartijoiden oikeudet (esim. kiinniotto, poistaminen, turvallisuustarkastus), velvollisuudet (esim. asu, vartijakortti, voimakeinojen käyttö) ja toiminnan rajat (esim. tarpeellisuus, puolustettavuus)

<https://www.finlex.fi/fi/lainsaadanto/2015/1085>

Laki yksityisyyden suojasta työelämässä (759/2004)

on Suomen erityislaki, jonka tarkoituksena on turvata työntekijöiden ja työnhakijoiden yksityisyyden suoja työelämässä. Se täydentää EU:n tietosuojasetusta (GDPR) ja kansallista tietosuojalakia. Teknisten turvallisuusjärjestelmien osalta tulee kiinnittää erityistä huomiota lukuun 5, mikä määrittelee kameravalvonnan edellytykset – mihin tarkoituksiin työnantaja saa ja ei saa harjoittaa kameravalvontaa käytössään olevissa tiloissa – ja valvonnan avoimuuden.

Lisäksi **21 §**, joka velvoittaa työnantajan käsittelemään yhteistoimintamenettelyissä työntekijöihin kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutettavan valvonnan tarkoitus ja käyttöönotto sekä niissä käytettävät menetelmät.

https://www.finlex.fi/fi/lainsaadanto/2004/759#chp_5

Pelastuslaki (379/2011)

on Suomen keskeinen pelastustoimea koskeva laki, jonka tavoitteena on parantaa ihmisten turvallisuutta ja vähentää onnettomuuksia. Laki velvoittaa sekä yksityisiä henkilöitä, yrityksiä että yhteisöjä ehkäisemään tulipaloja ja muita onnettomuuksia, varautumaan vaaratilanteisiin ja rajoittamaan vahinkoja. Lisäksi se määrittää pelastusviranomaisten tehtävät ja toimivallan.

<https://www.finlex.fi/fi/laki/ajantasa/2011/20110379>

Rikoslaki (39/1889) on Suomen keskeinen rikosoikeudellinen laki, joka määrittelee mitkä teot ovat rikoksia ja millaiset seuraamukset niistä seuraavat. Teknisten turvajärjestelmien osalta tulee kiinnittää erityisesti huomiota **lukuun 24** - Yksityisyyden, rauhan ja kunnian loukkaamisesta.

https://www.finlex.fi/fi/lainsaadanto/1889/39-001#chp_24

Tietosuojalaki (1050/2018) on kansallinen laki, joka täydentää ja täsmentää EU:n yleistä tietosuojasetusta (GDPR). Sen keskeinen tarkoitus on varmistaa luonnollisten henkilöiden henkilötietojen suoja sekä näiden tietojen vapaa liikkuvuus EU:n sisällä.

<https://www.finlex.fi/fi/laki/ajantasa/2018/20181050>

Työturvallisuuslaki (738/2002) on Suomen keskeinen työturvallisuutta koskeva laki, jonka tarkoituksena on turvata työntekijöiden terveys- ja turvallisuustyössä sekä ehkäistä tapaturmia ja työperäisiä sairauksia. Teknisten turvallisuusjärjestelmien osalta tulee kiinnittää erityisesti huomiota **27 §** - Väkivallan uhka, joka velvoittaa työnantajaa turvallisuusjärjestelyihin työssä,

johon liittyy ilmeinen väkivallan uhka. Tällöin työpäällä on oltava väkivallan torjumiseen tai rajoittamiseen tarvittavat asianmukaiset turvallisuusjärjestelyt tai -laitteet sekä mahdollisuus avun hälyttämiseen.
<https://www.finlex.fi/fi/laki/ajantasa/2002/20020738>

Valmiuslaki (1552/2011) on Suomen poikkeusolojen varautumista koskeva laki, jonka tarkoituksena on turvata väestön toimeentulo, maan talouselämä, oikeusjärjestys, perusoikeudet ja valtakunnan alueellinen koskemattomuus sekä itsenäisyys kriisitilanteissa.
<https://www.finlex.fi/fi/laki/ajantasa/2011/20111552>

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta (1101/2019) määrittää, miten viranomaiset ja julkisen hallinnon organisaatiot luokittelevat asiakirjat niiden sisältämän tiedon salassapitotarpeen perusteella. Asetus täydentää tiedonhallintalakia (906/2019) ja tukee kansallista sekä kansainvälistä tietoturvallisuutta.
<https://www.finlex.fi/fi/lainsaadanto/2019/1101>

Yleinen tietosuoja-asetus (GDPR) joka sääntelee henkilötietojen käsittelyä, asettaa organisaatioille velvollisuuden osoittaa, että ne käsittelevät henkilötietoja lainmukaisesti, läpinäkyvästi ja turvallisesti
<https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32016R0679>

11.2. Standardit

Standardit eroavat lainsäädännöstä siten, ettei standardeilla lähtökohtaisesti ole oikeudellista asemaa. Standardit voivat kuitenkin saada tämän aseman, mikäli ne julkaistaan lakien ja asetusten kautta erikseen määritettyinä. Tyypillisesti standardeilla viitataan niin sanottuihin virallisiin standardeihin (esim. SFS, EN ja ISO), mutta myös yrityksillä ja eri organisaatioilla voi olla omia, joko sisäisesti tai ulkoisesti julkaistuja standardeja. Näiden noudattamista voidaan vaatia vain sopimuksellisin keinoin.

Viralliset standardit jakaantuvat kansallisiin, eurooppalaisiin sekä kansainvälisiin eli maailmanlaajuisiin standardeihin. Standardien käyttö lisää turvallisuutta sekä eri toimijoiden välisten toimintatapa menettelyiden yhteensopivuutta. Turvallisuutta ohjaavia standardeja ovat esimerkiksi:

ISO 31000 Riskienhallinta on kansainvälinen standardi, joka tarjoaa periaatteet, viitekehyksen ja prosessin organisaatioiden riskienhallintaan.
<https://sfs.fi/standardeista/tutustu-standardeihin/suosittut-standardit/iso-31000-riskienhallinta/>

ISO 22301 Turvallisuus ja kriisinkestävyys on kansainvälinen standardi, joka käsittelee liiketoiminnan jatkuvuuden hallintajärjestelmää (BCMS). Tavoitteena on varmistaa häiriötilanteilta suojautuminen, niiden esiintymisen todennäköisyyden pienentäminen, niihin varautuminen ja reagoiminen sekä niistä palautuminen.
<https://sfs.fi/standardeista/tutustu-standardeihin/suosittut-standardit/iso-22301-turvallisuus-ja-kriisinkestavyys/>

ISO 27001 Tietoturvallisuus on kansainvälinen standardi, joka määrittelee vaatimukset tietoturvallisuuden hallintajärjestelmälle (ISMS) joka kattaa riskienhallinnan, turvatoimet ja vaatimustenmukaisuuden varmistamisen, ja sitä voidaan soveltaa kaikenkokoisissa ja -tyyppisissä organisaatioissa.
<https://sales.sfs.fi/fi/index/tuotteet/ISO/ISO/ID9998/2/1154751.html.stx#>

SFS-EN 50131 Hälytysjärjestelmät on kansainvälinen standardi, joka määrittää vaatimukset rakennuksiin asennetuille murto- ja ryöstöhälytysjärjestelmille.
<https://sales.sfs.fi/fi/index/tuotteet/SFSSahko/CENELEC/ID2/5/137177.html.stx#>

SFS-EN 60839-11-1 Sähköiset kulunvalvontajärjestelmät. Järjestelmävaatimukset ja komponenttiväätimukset on kulunvalvontajärjestelmän standardi, joka määrittelee sähköisten kulunvalvontajärjestelmien vähimmäistoiminnallisuuden, suorituskäyväatimukset ja testimenetelmät. Standardi koskee järjestelmiä ja komponentteja, joita käytetään rakennusten ja suojattujen alueiden sisään- ja uloskäyntien hallintaan.
<https://sales.sfs.fi/fi/index/tuotteet/sfssahko/cenelec/id2/6/240870.html.stx#>

SFS 6000-sarja Pienjännitesähkön asennus on Suomen kansallinen standardikokoelma, joka määrittelee pienjännitesähköasennusten turvallisuus- ja toteutusvaatimukset. Se on keskeinen työkalu sähköasennusten suunnittelijoille, asentajille ja tarkastajille, ja sen noudattaminen täyttää sähköturvallisuuslain ja viranomaismääräysten vaatimukset.
<https://sfs.fi/standardeista/tutustu-standardeihin/suosittut-standardit/sfs-6000-pienjannitesahkoasennusten-standardisarja/>



11.3. Ministeriöiden julkaisemat suositukset ja ohjeet

Kansallinen turvallisuusauditointikriteeristö (Katakri 2020) on Suomen viranomaisten kehittämä auditointityökalu, jonka avulla arvioidaan organisaation kykyä suojata turvallisuusluokiteltua tietoa – sekä kansallista että kansainvälistä.
https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) on Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen kehittämä kansallinen viitekehys, jonka tarkoituksena on varmistaa salassa pidettävän ja kriittisen tiedon turvallinen käsittely pilvipalveluissa. Viitekehys on suunnattu erityisesti viranomaisille, mutta soveltuu myös yrityksille, jotka käsittelevät liiketoimintakriittistä dataa.
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) on Valtiovarainministeriön ja Tiedonhallintalautakunnan kehittämä kansallinen viitekehys, jonka tarkoituksena on arvioida ja kehittää julkisen hallinnon tietoturvallisuutta.
<https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/e5a47b31-d1d4-46c3-a1fa-cde2dcff0180/content>

Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä on Valtiovarainministeriön julkaisema ohje, jonka tarkoituksena on varmistaa, että salassa pidettävät ja turvallisuusluokiteltavat asiakirjat käsitellään asianmukaisesti julkisessa hallinnossa. Suositus perustuu tiedonhallintalakiin (906/2019) ja valtioneuvoston asetukseen asiakirjojen turvallisuusluokittelusta (1101/2019).
<https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/8d9a8c52-b9a8-4935-92a3-21c313b89611/content>

Kansainvälisen turvallisuusluokittelun tietoineiston käsittelyohje 2024 on Ulkoministeriön ja Kansallisen turvallisuusviranomaisen (NSA) julkaisema ohje, joka määrittelee EU:n ja Naton turvallisuusluokiteltujen asiakirjojen käsittelyvaatimukset Suomessa.
<https://um.fi/documents/35732/0/Kansainv%C3%A4lisen%20turvallisuusluokittelun%20tietoineiston%20k%C3%A4sittelyohje%20-%202024.pdf/1c620d81-cdbd-c20b-1cf3-7d03147260b2?t=1709276822483>

11.4. Muut oppaat ja ohjeet

Kameravalvontaopas 2.0 (2020) on Turva-alan yrittäjät ry:n julkaisema yleishyödyllinen opas, joka tarjoaa ohjeistusta kameravalvonnan suunnitteluun, toteutukseen ja käyttöön Suomessa. Oppaan toinen versio perustuu kesällä 2020 voimassa olleeseen lainsäädäntöön ja alan käytäntöihin.
<https://www.finanssiala.fi/wp-content/uploads/2020/10/Kameravalvontaopas.pdf>

Turvaa oikein opas 2.0 (2019) on Turva-alan yrittäjät ry:n julkaisema ohje, joka tarjoaa hyvät käytännöt turvallisuusjärjestelmien hankintaan, suunnitteluun ja urakointiin. Oppaan tarkoituksena on parantaa alan laatua ja varmistaa, että turvasuojaustyöt toteutetaan lainsäädännön ja tietosuojavaatimusten mukaisesti.
https://www.turva-alanyrittajat.fi/doc/2019/Turvaa-oikein--opas_v2_0.pdf

Finanssialan turvallisuusohjeet ovat Finanssiala ry:n ja alan toimijoiden laatimia ohjeita, joiden tarkoituksena on ehkäistä vahinkoja, torjua rikoksia ja varmistaa toiminnan jatkuvuus. Ne kattavat sekä fyysisen että digitaalisen turvallisuuden ja tukevat riskienhallintaa koko finanssialalla.
<https://www.finanssiala.fi/aiheet/turvallisuusohjeet/>, joista fyysisen turvallisuuden osalta tärkeimpinä:

Rakenteellinen murtosuojaus I:
<https://www.finanssiala.fi/wp-content/uploads/2024/01/rakenteellinen-murtosuojaus-i.pdf>

Rakenteellinen murtosuojaus II:
<https://www.finanssiala.fi/wp-content/uploads/2024/01/rakenteellinen-murtosuojaus-ii.pdf>

Rakenteellinen murtosuojaus III:
<https://www.finanssiala.fi/wp-content/uploads/2024/01/rakenteellinen-murtosuojaus-iii.pdf>

Murtohälytysjärjestelmät ja palvelut ohje:
https://www.finanssiala.fi/wp-content/uploads/2017/08/Murtohalytysjarjestelmat_ja_palvelut_ohje.pdf

**Kassakaappiohje:**

<https://www.finanssiala.fi/wp-content/uploads/2017/08/Kassakaappiohje.pdf>

Avainturvallisuusohje:

https://www.finanssiala.fi/wp-content/uploads/2021/04/FA_Avainturvallisuus_2021.pdf

Finanssialan testattuja ja luotettavia turvallisuustuotteita yrityksille ja kuluttajille

-sivulta löydät eurooppalaisten ja kansallisten standardien mukaisia palo-, murto- ja vuotovahinkojen torjuntaan liittyviä tuotteita sekä näitä suunnittelevia tai asentavia liikkeitä. Luetteloiden tarkoituksena on ohjata yrityksiä ja kuluttajia testattujen ja luotettavien turvallisuustuotteiden ja -järjestelmien valintaan.

<https://www.finanssiala.fi/aiheet/laitteet-ja-liikkeet/>

Vakuutusyhtiöiden suojeleohjeet ovat vakuutus sopimukseen liitettyjä velvoittavia määräyksiä, joiden tarkoituksena on ehkäistä vahinkoja ja rajoittaa niiden laajuutta. Ne voivat koskea esimerkiksi laitteiden huoltoa, paloturvallisuutta, lukitusta, tietoturvaa tai kemikaalien käsittelyä.

11.5. Periaatepäätökset ja muut lähteet

Yhteiskunnan turvallisuusstrategia 2025 on Valtioneuvoston periaatepäätös yhteiskunnan turvallisuusstrategiasta. Se määrittelee Suomen varautumiseen liittyvät yleiset periaatteet. Toiminta perustuu suomalaiseen kokonaisturvallisuuden yhteistoimintamalliin, jossa valtionhallinto, viranomaiset, elinkeino-elämä, maakunnat ja kunnat sekä yliopistot ja tutkimuslaitokset, järjestöt ja yhteisöt sekä yksilöt muodostavat yhteistyöverkoston.

Varautuminen toteutetaan kokonaisturvallisuuden periaatteella, ja sen suunnittelussa lähtökohtana toimii yhteiskunnan elintärkeiden toimintojen turvaaminen. Suomen yhteiskunnan elintärkeät toiminnot ovat johtaminen, kansainvälinen ja EU-toiminta, puolustuskyky, sisäinen turvallisuus, talous, infrastruktuuri, huoltovarmuus, väestön toimintakyky ja palvelut sekä henkinen kriisinkestävyys.

<https://julkaisut.valtioneuvosto.fi/handle/10024/166024>

Suomen kyberturvallisuusstrategia 2024–2035 on uudistettu 2025 hallitusohjelman mukaisesti vastaamaan muuttunutta toimintaympäristöä. Kyberturvallisuusstrategian uudistamisessa on otettu huomioon kyberturvallisuudirektiivin (NIS2) vaatimukset sekä muu aiheeseen liittyvä keskeinen strategia- ja selontekotyö.

<https://julkaisut.valtioneuvosto.fi/handle/10024/165860>

Valtioneuvoston päätös huoltovarmuuden tavoitteista (568/2024) on strateginen päätös, joka ohjaa Suomen huoltovarmuuden kehittämistä. Päätöksen tarkoituksena on varmistaa, että yhteiskunnan kriittiset toiminnot ja väestön toimeentulo turvataan kaikissa olosuhteissa – normaalioloista poikkeusoloihin. <https://www.finlex.fi/fi/laki/alkup/2018/20181048>

Kansallinen ja alueellinen riskiarvio koostuu niin kansallisesta kuin alueellisista riskiarvioista. Suomen kansallinen riskiarvio perustuu EU-maita velvoittavaan pelastuspalvelumekanismiin. EU-maiden on kartoitettava säännöllisesti ihmisiä, ympäristöä, omaisuutta ja yhteiskunnan kriittisiä järjestelmiä uhkaavia riskejä, jotka edellyttävät viranomaistoimenpiteitä ja konkreettisuudessaan voivat johtaa avun pyyntöön muilta jäsenmailta. Alueellisissa riskiarvioissa kartoitetaan alueille ominaisia uhkia ja häiriöitä. Kansallinen ja alueelliset riskiarviot ovat saatavilla sisäministeriön Internetsivuilta.

<https://intermin.fi/pelastustoimi/varautuminen/kansallinen-riskiarvio>

Alueelliset rikos- ja pakkokeinotilastot, josta toimijat saavat lisätietoja alueensa turvallisuudesta esimerkiksi Tilastokeskuksen maksuttomista rikos- ja pakkokeinotilastoista kunnittain. Tilastokeskus kokoaa poliisien tietoon tulleet rikokset. Kuntakohtaisia rikoksia pystyy tarkastelemaan kuukausikohtaisesti rikosnimikkeittäin. <https://stat.fi/tilasto/rpk>



Huoltovarmuuskeskus

