



RUOKAVIRASTO

Livsmedelsverket • Finnish Food Authority



RUOKAVIRASTO
Livsmedelsverket • Finnish Food Authority

CER- ja kyberturvallisuuslaki elintarvikealalla

Keskustelutilaisuus toimijoille

22.9.2026



Keskustelutilaisuuden aiheita

1. CER-laki
2. Kriittinen toimija
3. CER-lain velvoitteet
4. NIS2-toimijasta myös CER-toimija - mikä muuttuu
5. Johdon vastuu
6. Tuki kriittiselle toimijalle
7. Poikkeusolot ja valmiuslaki
8. Ohjaus ja valvonta
9. Komission tiedonanto: Suuntaviivat CER-direktiivin 13 artiklan 5 kohdan soveltamisesta (C/2026/3712)

1. Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta 310/2025 (CER-laki) voimaan 1.7.2025



- Lain tarkoituksena on vahvistaa **yhteiskunnan kriisinkestävyyttä** ja **kansallista turvallisuutta**.
- Tavoitteena on varmistaa, että **yhteiskunnan toiminnan ja turvallisuuden kannalta keskeiset palvelut toimivat** mahdollisimman häiriöttömästi kaikissa olosuhteissa → kriittisten toimijoiden määrittäminen eri toimialoilla/ministeriöt.
- Suomen lainsäädännön taustalla on EU:n CER-direktiivi, (EU) 2022/2557, joka velvoittaa jäsenmaita tunnistamaan yhteiskunnan kannalta kriittiset toimijat ja vahvistamaan niiden kykyä kestää häiriöitä ja kriisejä.
- Sisäministeriö koordinoi ja yhteensovittaa valtakunnallisesti lain toimeenpanoa.
- Koskee elintarvikeyrityksiä, jotka toimivat yksinomaan logistiikan ja tukkukaupan sekä laajamittaisen teollisen tuotannon ja jalostuksen alalla.
- Ruokavirasto toimii CER-lain valvovana viranomaisena elintarvikealalla.



2. Kriittinen toimija

- Eri toimialoista vastaavat ministeriöt ovat määrittäneet toimialansa kriittiset toimijat (keskeiset palvelut) ja MMM:n päätös kriittisestä toimijasta on tullut voimaan 17.7.2026. Se on voimassa enintään neljä vuotta.
- Kriittisten toimijoiden määrittämisessä on huomioitu valtakunnallinen suunnitelma (CER-strategia) ja kansallinen CER-riskiarvio (ei julkinen).
- Toimija on määritetty kriittiseksi, jos se
 - tarjoaa CER-lain mukaista keskeistä palvelua
 - keskeisellä palvelulla tarkoitetaan palvelua, joka on olennainen välttämättömien yhteiskunnan toimintojen, taloudellisen toiminnan, kansanterveyden, yleisen turvallisuuden tai ympäristön ylläpitämiseksi
 - toimii Suomessa ja sen infrastruktuuri sijaitsee Suomessa ja
 - poikkeamalla olisi merkittäviä haitallisia vaikutuksia palvelun tarjontaan tai siihen tukeutuviin toimialoihin.



3. CER-lain velvoitteet

1. Tee CER-lain mukainen poikkeamailmoitus
2. Kun CER-toimijuus tuo yrityksesi kyberturvallisuuslain piiriin
 - a. Ilmoittaudu kyberturvallisuuslain mukaiseen Ruokaviraston toimijaluetteloon
 - b. Tee kyberturvallisuuslain mukainen poikkeamailmoitus
 - c. Tee kyberturvallisuuslain mukainen riskienhallintamalli
3. Tee kriittisen toimijan riskiarviointi
4. Laadi ja toteuta häiriönsietokyvyn suunnitelmaa
5. Nimeä ja ilmoita yhteyspiste/yhteyspisteen muutokset

CER-laki ja kyberturvallisuuslain muutos



Tapahtuma	Päivämäärä	Kuvaus	Vastuullinen tah
Lait voimaan	01.07.2025	Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja kyberturvallisuuslain muutos voimaan.	Valtioneuvosto
Valtakunnallinen suunnitelma ja kansallinen riskiarvio	17.01.2026	Valtioneuvosto hyväksyy kriittisten toimijoiden häiriönsietokykyä koskevan suunnitelman ja riskiarvion.	Valtioneuvosto
Kriittisen toimijan määrittäminen	17.07.2026	MMM tekee päätöksen kriittisen toimijan määrittämisestä elintarvikealalla.	MMM
CER-lain poikkeamailmoitusvelvoite	17.07.2026	Velvoitetta sovelletaan kriittiseen toimijaan päätöksen saamisesta.	Kriittinen toimija
Kyberturvallisuuslain ilmoittautumis- ja poikkeamailmoitusvelvoite	17.10.2026	Velvoitetta sovelletaan kriittiseen toimijaan 3 kk kuluttua päätöksen saamisesta.	Kriittinen toimija
Kyberturvallisuuslain riskienhallinnan toimintamallivelvoite	17.04.2027	Velvoitetta sovelletaan kriittiseen toimijaan 9 kk kuluttua päätöksen saamisesta.	Kriittinen toimija
Kriittisen toimijan riskiarviointi	17.04.2027	Riskiarviointi suoritetaan 9 kk kuluessa päätöksen saamisesta.	Kriittinen toimija
Häiriönsietokyvyn suunnitelma	17.04.2028	Häiriönsietokykyä koskeva suunnitelma laaditaan vuoden kuluessa riskiarvioinnista.	Kriittinen toimija



Poikkeamailmoitukset

Tee poikkeamailmoitus

- Kriittisellä toimijalla on **velvollisuus ilmoittaa merkittävästä poikkeamasta, joka häiritsee tai voi häiritä** keskeisten palvelujen tarjoamista.
 - Ensi-ilmoitus poikkeamasta viimeistään 24 tunnin kuluttua siitä, kun poikkeama on tullut toimijan tietoon.
 - Poikkeaman yksityiskohtainen raportti viimeistään kuukauden kuluttua siitä, kun poikkeama on tullut tietoon viranomaisille, mikäli poikkeama on häirinnyt keskeisen palvelun tarjoamista tai jos poikkeamalla on ollut rajat ylittäviä vaikutuksia.
 - Yksityiskohtaista raporttia ei tarvitse toimittaa, mikäli toimija katsoo, että poikkeama ei ole häirinnyt keskeisen palvelun tarjoamista tai jos poikkeamalla ei ole ollut rajat ylittäviä vaikutuksia.
- Poikkeamailmoitus voi olla tarpeen tehdä sekä kyberturvallisuuslain nojalla että CER-lain nojalla (kaksi eri ilmoitusta!).
 - Kun uusi Traficomien sovellusjärjestelmä tulee käyttöön, pyritään vain yhteen ilmoitukseen.



CER-lain poikkeamailmoitusmenettely

- Sekä ensi-ilmoitus että yksityiskohtainen raportti toimitetaan sisäministeriön verkkopohjaisella lomakkeella.
 - Ensi-ilmoitus: tieto poikkeaman havaitsemisesta ja sen luonteesta, **arvio** mahdollisesta syystä, mahdollisista seurauksista ja rajat ylittävistä vaikutuksista ja arvio palvelun käyttäjien lukumäärästä, johon häiriö vaikuttaa.
 - Yksityiskohtainen raportti: **tarkempi kuvaus** poikkeamasta ja sen vaikutuksista, laajuudesta sekä toimenpiteistä poikkeaman vaikutusten lieventämiseksi.
- Ensi-ilmoitus ohjautuu järjestelmästä CER-lain mukaiselle valvovalle viranomaiselle ja valtioneuvoston tilannekeskukselle (VNTIKE).
- Yksityiskohtainen raportti ohjautuu sisäministeriölle, toimijan kriittiseksi määrittäneelle ministeriölle, sekä asianomaiselle valvovalle viranomaiselle. Ruokavirasto toimittaa tarvittaessa raportin Huoltovarmuuskeskukselle tiedoksi (huoltovarmuuskriittinen poikkeama).

Merkittävä poikkeama CER ja NIS2 - toimija arvioi poikkeaman merkittävyyden



- CER-lain merkittävä poikkeama
 - Merkittävästi häiritsee tai **voi häiritä** keskeisten palvelujen tarjoamista
 - Häiriön merkittävyyden arvioinnissa huomioitava erityisesti
 - palvelujen käyttäjien lukumäärä ja osuus, joihin häiriö vaikuttaa
 - häiriön kesto
 - maantieteellinen alue, johon häiriö vaikuttaa ja maantieteellisen alueen eristyneisyys.
- Kyberturvallisuuslain merkittävä poikkeama
 - Merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka
 - on aiheuttanut tai **voi aiheuttaa** vakavan palvelujen toimintahäiriön tai huomattavia taloudellisia tappioita asianomaiselle toimijalle, sekä
 - on vaikuttanut tai **voi vaikuttaa** muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.



Riskien arviointi ja hallinta

Arvioi riskit ja määrittele tarvittavat riskienhallintatoimenpiteet

- Arvioi sekä fyysiset että kyberuhat.
- Riskien arvioinnin tulee kattaa **keskeiset palvelut, toimitusketjut ja riippuvuudet**, ja sen perusteella toimijan on toteutettava teknisiä ja organisatorisia toimenpiteitä, joilla vähennetään häiriöiden vaikutuksia.
- Riskien arviointi on päivitettävä säännöllisesti vähintään neljän vuoden välein.
- Arvioinnin perustana CER-strategia ja kriittisten toimijoiden käyttöön annettu kansallinen CER-riskiarvio.
- Riskien arvioinnissa kannattaa hyödyntää myös organisaation olemassa olevia riskien arviointeja.
- Riskejä voidaan pienentää ja hallita esim. teknisillä ratkaisulla (varajärjestelmät, kyberturva), organisatorisilla toimilla (koulutus, ohjeistus) ja sopimuksellisilla järjestelyillä (varatoimittajat).



Toimitusketjujen hallinnasta

- Tunnista, mistä yrityksen kriittiset palvelut ovat riippuvaisia.
- Aseta toimittajille selkeät vaatimukset, seuraa käyttöoikeuksia yms. ja harjoittele.
- Vastuuta ei voi siirtää kokonaan toimittajan vastuulle, vaikka itse palvelu olisi ulkoistettu.
- ”Toimitusketjujen häiriönsietokyky on olennainen tekijä häiriöistä toipumisessa. Kriittisten toimijoiden tulisi riskinarviointinsa perusteella kartoittaa keskeisten palvelujensa tarjoamiseen liittyvät toimitusketjut, laatia pitkän aikavälin strategioita toimitusketjujen häiriönsietokyvyn vahvistamiseksi sekä tarkistaa ja päivittää säännöllisesti toimitusketjuja koskevaa varautumissuunnitelmaa. Toimijoiden tulisi myös määrittää vaihtoehtoisia toimitusketjuja siltä varalta, että niiden tärkeimpiin toimittajiin kohdistuu häiriöitä.” (Komission tiedonanto)



Häiriönsietokykysuunnitelma

Laadi ja toteuta häiriönsietokyvyn suunnitelmaa

- Kriittisen toimijan on laadittava **asianmukaisia ja oikeasuhtaisia** teknisiä, turvallisuuteen liittyviä ja organisatorisia toimenpiteitä sisältävä suunnitelma häiriönsietokyvyn varmistamiseksi.
- Suunnitelman tarkoituksena on kuvata, miten organisaatio varmistaa toimintansa jatkuvuuden ja kestävyys erilaissa häiriötilanteissa.
- Suunnitelma häiriönsietokyvyn varmistamisesta perustuu toimijan tekemään riskien arviointiin.
- Suunnitelman tarkoituksena on lisäksi **määrittää toimenpiteet** ja luoda rakenteet, joilla häiriöiden vaikutuksia voidaan ehkäistä tai lieventää.
- Suunnitelmaan liitetään aikataulu toimenpiteiden määrääjoille ja toteuttamiselle. Aikataulun tulee olla realistinen ja perustua riskiarvioinnin tuloksiin.
- Voidaan laatia osana muuta organisaation suunnitelmaa (esim. valmiussuunnitelma, varautumissuunnitelma, jatkuvuudenhallinnan suunnitelma). Käytettävässä dokumentissa on tällöin mainittava, että se kattaa myös CER-lain vaatimuksen.
- Yrityksen määrittelemä ja käytössä oleva turvallisuusselvitysmenettely kuvataan suunnitelmaan.



Yhteyspiste

Nimeä ja ilmoita yhteyspiste (yhteyshenkilö) Ruokavirastolle

- Yhteyspiste toimii ensisijaisena kanavana viranomaisten ja kriittisen toimijan välillä.
- Yhteyspisteen tehtävänä on varmistaa, että tiedonkulku on nopeaa ja luotettavaa erityisesti häiriötilanteissa ja poikkeamien ilmoittamisessa.
- Yhteyspiste voi olla henkilö tai yksikkö, jonka yhteystiedot toimitetaan valvovalle viranomaiselle. Yhteyspiste vastaa muun muassa seuraavista asioista:
 - vastaanottaa viranomaisilta tulevat ohjeet ja tiedotteet
 - välittää poikkeamailmoitukset ja muut velvoitteisiin liittyvät tiedot viranomaisille
 - koordinoi sisäistä ja ulkoista viestintää häiriötilanteissa.
- Pidä yhteyspisteen yhteystiedot ajan tasalla.
- Ilmoita myös toiminnan olennaisesta muutoksesta Ruokavirastoon.



4. NIS2-toimijasta myös CER-toimija - mikä muuttuu

- CER ja NIS2 muodostavat kokonaisuuden, jossa
 - CER-laki kattaa fyysisen turvallisuuden, henkilöstöturvallisuuden ja häiriönhallinnan ja
 - kyberturvallisuuslaki (NIS2) kattaa digitaalisen turvallisuuden ja kyberresilienssin.
- Kyberturvallisuuslain muutos: kaikki CER-lain nojalla kriittisiksi toimijoiksi määritellyt toimijat ovat automaattisesti myös NIS2-säätelyn alaisia riippumatta niiden koosta.
- Mikäli NIS2-toimija nimetty myös CER-toimijaksi → toimija muuttuu tärkeästä toimijasta keskeiseksi toimijaksi. Ruokavirasto tekee tarvittavat muutokset ja ilmoituksen päivittämistä ei tarvita.
- CER-toimijat tulevat kyberturvallisuuslain mukaiseen ennakkovalvonnan piiriin.



5. Johdon vastuu

- **Kyberturvallisuuslaki:** Toimijan johto vastaa kyberturvallisuutta koskevan riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy kyberturvallisuutta koskevan riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Toimijan johdolla tulee olla riittävä perehtyneisyys kyberturvallisuutta koskevaan riskienhallintaan.
- **CER-direktiivi/komission tiedonanto:** Riittävä häiriönsietokykyä koskeva osaaminen olisi varmistettava johtoryhmän tasolla sekä häiriönsietokykyyn tai riskinhallintaan liittyvissä toiminnoissa, jotta voidaan varmistaa asianmukaiset strategiat, käytännöt ja operatiivinen suunnittelu häiriönsietokykyyn liittyvien tavoitteiden varmistamiseksi. Koordinointitehtävien ja -vastuiden selkeä määrittely on tarpeen häiriönsietokykyä koskevien tavoitteiden saavuttamiseksi.



6. Tuki kriittiselle toimijalle

- CER-käsikirja - opas kriittisille toimijoille
- Tuki yhteistyössä Huoltovarmuuskeskuksen kanssa
 - Huoltovarmuuskeskus osallistuu yhdessä sisäministeriön, muiden ministeriöiden ja valvovien viranomaisten kanssa kriittisten toimijoiden häiriönsietokyvyn parantamiseen liittyvään työhön sekä toimijoille annettavaan tukeen.
 - Annettava tuki voi pitää sisällään esimerkiksi ohjemateriaaleja ja menetelmiä, häiriönsietokykytestien järjestämistä sekä neuvontaa ja koulutusta.
 - Tuen yhteistyön toimintamalli tarkentuu vielä.
- Kyberturvallisuuskeskuksen palvelut, mm. tilannekuvatuotteet ja ISAC-tiedonvaihtoryhmät



7. Poikkeusolot ja valmiuslaki

- CER-lainsäädännöllä pyritään varmistamaan toiminnan jatkuvuus ja tuotteiden markkinoille saattaminen erilaisissa häiriötilanteissa niin normaalioloissa kuin mahdollisissa poikkeusoloissa. Yritys määrittää itse riskienhallintansa mekanismit, esimerkiksi toimiiko varastointi yhtenä toimenpiteenä jatkuvuudenhallinnan varmistamisessa.
- **Poikkeusoloissa voidaan soveltaa valmiuslakia**, jolla voidaan tarvittaessa valtiojohtoisesti puuttua esimerkiksi tuotannon ja jakelun ohjaamiseen, tuotantopanosten käytön priorisointiin tai säännöstelyyn ja kulutuksen ohjaukseen. On huomioitava, että valmiuslakia voidaan soveltaa ainoastaan tietyin kriteerein todetuissa poikkeusoloissa ja niissäkin vain ja ainoastaan ehdottomasti vaadituilta osin. CER-lainsäädännön mukainen riskienarviointi ja -hallinta vahvistavat yrityksen toiminnan jatkuvuudenhallintaa myös mahdollisissa poikkeusoloissa.
- Lähtökohtaisesti erilaisten **elintarviketurvallisuuden kriteerien tulee täytyä myös häiriötilanteissa**, CER-lainsäädäntö ei anna tähän poikkeuksia. Viranomaiset voivat kuitenkin tilannekohtaisesti arvioida, onko välttämätöntä tarvetta esimerkiksi tilapäisille joustoille, tarvittaessa tietyin ehdoin. Kaikki mahdolliset joustot arvioidaan kuitenkin aina tilannekohtaisesti.



8. Ohjaus ja valvonta

- Tehtävänä ohjata ja valvoa kriittisten toimijoiden velvoitteiden noudattamista varmistaen, että kyberturvallisuuslain ja CER-lain velvoitteiden vaatimukset täytetään.
- Kriittiset toimijat ovat saaneet meiltä ohjausviestin heinäkuussa.
- Tarkastuksen pohjana lainsäädäntöjen vaatimukset.
 - Hyödynnetään Traficomien suositusta (kyberturvallisuus) ja komission tiedonantoa (CER).
 - Tarkastetaan mm. toimijaluetteloon ilmoittautuminen (NIS2), riskienhallinnan velvoitteet ja -toimintamallit (NIS2/CER), häiriönsietokyvyn suunnitelma ja toteutus (CER), poikkeamailmoitusmenettely (NIS2/CER), yhteyspisteen nimeäminen (CER) sekä tietojen ajantasaisuus (NIS2/CER).
 - Tarkastus voi sisältää dokumenttien tarkastamista, haastatteluja, ulkopuolisen tekemiä auditointeja sekä tarvittaessa myös ohjausta tai korjauskehotuksia.
 - Vaatimustenmukaisuus on pystyttävä todentamaan dokumentein (suunnitelma ja toteutus), ei erityisvaatimuksia muotoon, käsikirjaan tai standardiin liittyen → voidaan yhdistää jo olemassa oleviin hallintamalleihin.
 - Tarkastus voidaan tehdä joko pelkkänä asiakirjatarkastuksena, etäyhteydellä tai läsnä. Asiakirjat toimitetaan valvovalle viranomaiselle pyydettäessä ja tarkastuksen yhteydessä.
 - Tarkastuksista sovitaan etukäteen toimijan kanssa (ajankohta, menettelyt, haastateltavat henkilöt).
- Teemme yhteistyötä MMM:n, sisäministeriön, Huoltovarmuuskeskuksen, Traficomien ja muiden NIS2- ja CER-valvovien viranomaisten kanssa.



Seuraamukset CER

- Jos kriittinen toimija ei noudata lain velvoitteita, valvova viranomainen voi antaa sille huomautuksen tai varoituksen.
 - Varoitus annetaan silloin, kun pelkkä huomautus ei riitä tilanteen vakavuuden vuoksi. Varoitus annetaan aina kirjallisesti, ja siinä kerrotaan, mikä puute tai laiminlyönti on kyseessä.
- Valvova viranomainen voi valvontapäätöksellä velvoittaa toimijan korjaamaan havaitut puutteet tai laiminlyönnit kohtuullisessa ajassa.
 - Viranomainen voi liittää päätöksen tehosteeksi uhkasakon tai teettämisuhan.
- Valvova viranomainen voi määrätä päätöksellään kriittisen toimijan maksamaan laiminlyöntimaksun, jos velvoitteiden laiminlyönti johtuu tahallisuudesta tai törkeästä huolimattomuudesta.
 - Laiminlyöntimaksun määrä on vähintään 2 000 euroa ja enintään 20 000 euroa.



Seuraamukset NIS2

- Seuraamukset, mikäli lain velvoitteita ei noudateta
 - Varoitus
 - Uhkasakko
 - Teettämisuhka
 - Keskeyttämisuhka
- Hallinnollinen seuraamusmaksu
 - Keskeiselle toimijalle voidaan määrätä hallinnollinen seuraamusmaksu max. 10 000 000 euroa tai 2 prosenttia toimijan edellisen tilikauden maailmanlaajuisesta vuotuisesta liikevaihdosta, kumpi on suurempi, jos se tahallaan tai törkeästä huolimattomuudesta laiminlyö velvollisuudet.
 - Seuraamusmaksulautakunta määrää hallinnollisen seuraamusmaksun valvovan viranomaisen esityksestä (jäsenet jokaisesta valvovasta viranomaisesta).

9. Komission tiedonanto: Suuntaviivat kriittisten toimijoiden häiriönsietokyvystä annetun direktiivin (EU) 2022/2557 13 artiklan 5 kohdan soveltamisesta



- Komission heinäkuussa 2026 julkaisema tiedonanto antaa **ei-sitovia suuntaviivoja** siitä, millaisia teknisiä, turvallisuuteen liittyviä ja organisatorisia toimenpiteitä kriittiset toimijat voivat toteuttaa täyttääkseen CER-direktiivin (EU) 2022/2557 artiklan 13 velvoitteet.
- Tarkoituksena on auttaa toimijoita vahvistamaan häiriönsietokykyään **kaikkiin uhkiin varautumisessa**.
- Komissio jäsentää ohjeet seuraaviin toimenpidekokonaisuuksiin:
 - A. Yleiset periaatteet (hallinto ja riskienhallinta)
 - B. Ennaltaehkäisy
 - C. Fyysinen suojaus
 - D. Poikkeamien hallinta: reagointi, kestävyys ja vaikutusten lieventäminen
 - E. Palautuminen
 - F. Henkilöstöturvallisuus
 - G. Tiedottaminen, koulutus ja harjoitukset.

Seuraaville dioille on poimittu muutamia käytännön esimerkkejä komission tiedonannossa esitetyistä suuntaviivoista toimenpidemuotoon. Esimerkit eivät ole tyhjentävä lista toimenpiteistä.



Toimijan toteuttamat toimenpiteet

Kriittisten toimijoiden toteuttamien toimenpiteiden on oltava **asianmukaisia ja oikeasuhteisia**. Toimenpiteiden asianmukaisuutta ja oikeasuhteisuutta olisi arvioitava suhteessa edellä mainittujen riskinarviointien tuloksiin.

- a) **"Asianmukaisilla"** toimenpiteillä tarkoitetaan riskeihin tai vaikutuksiin perustuvia, tehokkaita ja tarkoituksenmukaisia toimenpiteitä, joilla kriittinen toimija voi varmistaa keskeisten palvelujen vankan häiriönsietokyvyn. **Toimenpiteiden asianmukaisuus voi vaihdella kriittisen toimijan ja sen erityispiirteiden mukaan.**
- b) **"Oikeasuhteisilla"** toimenpiteillä tarkoitetaan välttämättömiä ja riittäviä toimenpiteitä, jotka eivät ole kohtuuttomia suhteessa riskin tasoon ja häiriön vakavuuteen. **Toimenpiteet olisi räätälöitävä kunkin kriittisen toimijan erityispiirteiden mukaan**, ja niissä tulisi ottaa huomioon muun muassa tarjottujen keskeisten palvelujen luonne, toimitusketjut ja keskinäiset riippuvuudet, toimenpiteiden kustannustehokkuus, toimijan koko sekä tarjottujen palvelujen maantieteellinen kattavuus.



A. Yleiset periaatteet (hallinto ja riskienhallinta)

Tunnista palvelut, resurssit, riskit ja riippuvuudet.

- Perusta toimenpiteet riskinarviointeihin (kansallinen riskinarviointi (tulossa), CER-riskinarviointi, oma riskinarviointi).
- Varmista kokonaisvaltainen toimintamalli siirtymällä pelkästä kriittisen infrastruktuurin suojaamisesta tarjoamiesi keskeisten palvelujen jatkuvuuden varmistamiseen.
- Arvioi riippuvuuksia laajasti (riippuvuudet muista toimialoista, rajat ylittävät riippuvuudet, toimitusketjut, fyysiset ja ympäristöön liittyvät riippuvuudet, kyberturvallisuuteen liittyvät riippuvuudet)
- Valitse asianmukaiset toimenpiteet (perustuvat riskeihin ja vaikutuksiin, ovat tehokkaita ja tarkoituksenmukaisia).
- Huolehdi toimenpiteiden oikeasuhteisuudesta (välttämättömiä ja riittäviä, mutta ei kohtuuttomia suhteessa riskitasoon ja mahdolliseen häiriön vakavuuteen).
- Räätlöi toimenpiteet toiminnan erityispiirteisiin nähden ja **sovita yhteen muun lainsäädännön (mm. kyberturvallisuus, elintarvike, tietosuoja, tekoäly, logistiikka) kanssa.**
- Laadi häiriönsietokykyä koskeva suunnitelma tai vastaavat asiakirjat ja sovelta suunnitelmaa käytännössä.
- Hyödynnä olemassa olevia suunnitelmia ja asiakirjoja, jos ne täyttävät samalla direktiivin mukaiset vaatimukset.
- Nimeä yhteyshenkilö, joka huolehtii tehokkaasta viestinnästä ja koordinoinnista toimijan ja toimivaltaisten viranomaisten välillä.



B. Ehkäisevät toimenpiteet

Ehkäise häiriöitä ja suojaa fyysiset sekä digitaaliset resurssit.

- Kokoa ehkäisevät toimenpiteet yhdeksi kokonaisuudeksi osaksi häiriönsietokykysuunnitelmaa. Fyysistä suojausta, poikkeamiin vastaamista, vaikutusten lieventämistä ja henkilöstöturvallisuutta ei tule käsitellä toisistaan irrallisina.
- Varaudu sekä akuutteihin että pitkäaikaisiin ilmastomuutoksiin (äärimmäinen kuumuus, tulvat, merenpinnan nousu ja veden niukkuus).
- Tee stressitestejä, joilla varmistetaan toiminnan jatkuminen tavanomaista lämpimämmissä, kylmemmissä, kosteammissa, kuivemmissä tai epävakaimmissa olosuhteissa.
- Vältä kriittisen infrastruktuurin sijoittamista korkean riskin alueille.
- Vahvista infrastruktuuria rakenteellisesti (tulipalot, tulvat, kuivuus, räjähdykset, vuodot, säteily).
- Toteuta muita kuin rakenteellisia ehkäisytöitä, kuten koulutus- ja turvallisuuskäytäntöjä.
- Ota käyttöön järjestelmällinen poikkeamaraportointi ja tapahtumahistorian ylläpito.
- Tunnista inhimillisille virheille alttiit tehtävät ja ehkäise virheitä (automatisointi, jatkuva koulutus, valvonta, selkeä vastuunjako, dokumentointi, auditoinnit ja tarkastukset).
- Edistä häiriönsietokykyä ja vastuullisuutta tukevaa organisaatiokulttuuria.
- Yhdenmukaista verkko- ja tietojärjestelmien turvallisuustoimet NIS2 -vaatimusten kanssa.



C. Fyysinen suojaus

Varmista varavoima, varajärjestelmät, kunnossapito, materiaalit ja vaihtoehtoiset toimitusketjut.

- **Uhka-arviointi ja yhteistyö**
 - Varaudu luonnonuhkien lisäksi ihmisen aiheuttamiin uhkiin (hybridiuhka, sabotaasi, terrorismi, rikollisuus, vakoilu, sisäpiiriuhka ja sotilaallinen tai sodanaikainen operaatio).
 - Arvioi konkreettisten uhkaskenaarioiden todennäköisyys.
 - Luo käytännöt julkisen ja yksityisen sektorin yhteistyölle, viranomaisyhteistyölle sekä uhka- ja poikkeamatietojen vastavuoroiselle vaihtamiselle.
 - Huomio valtiollisten toimijoiden koordinoitua ja monikanavaisia hyökkäyksiä ml. välikäsien kautta toiminta.
- **Alueen ja rakenteiden suojaaminen**
 - Vahvista alueen ulkorajoja (turvallisuusaidat, muurit, portit, ajoneuvoesteet, varoituskyltit ja turvavalaistus).
 - Keskitä ajoneuvojen, henkilöiden ja tavaroiden kulku valvottuihin tarkastuspisteisiin.
 - Suojaa lähestymisreitit kiinteillä tai sisään vedettävillä törmäyssuojilla, luonnollisilla esteillä ja nopeutta rajoittavilla ratkaisuilla.
 - Vahvista ovet, portit, ikkunat, kattoikkunat ja muut kulkureitit (lukitukset, turvasaranat, kalterit, iskunkestävät lasit jne.)
 - Suojaa myös epätavanomaiset pääsyreitit (kattoluukut, kulkuaukot ja tuuletusaukot).



C. Fyysinen suojaus

- **Valvonta, havainnointi ja valaistus**

- Kata koko alue tunkeutumisen havaitsemisratkaisuilla ja liitä niihin yhdenmukaiset seuranta- ja reagointikäytännöt.
- Testaa havainnointijärjestelmät säännöllisesti sekä analysoi todelliset havainnot, väärät hälytykset ja järjestelmäviat.
- Varmista videovalvonnan riittävä laatu, reaaliaikaisuus, aikasynkronointi, tallennus ja säilytysajat sekä testaa tallenteiden käyttökelpoisuus myöhempää tutkintaa varten.
- Varaa valvontajärjestelmien kriittisille osille varalaitteita ja varavoimaa.
- Huolehdi tasaisesta valaistuksesta sisäänkäynneillä, kulkuväylillä, pysäköintialueilla ja kameroiden kuvausalueilla.
- Testaa hätä- ja varavalaistus sekä huolla valaistus ja näkyvyyteen vaikuttava ympäristö säännöllisesti.
- Käytä selkeitä opasteita, joissa ilmoitetaan turvallisuusrajoitukset, valvonta, tietosuoja sekä henkilöstön, vierailijoiden ja kuljetusten reitit.



C. Fyysinen suojaus

- **Kulunvalvonta ja vierailijat**

- Jaa tilat turvavyöhykkeisiin ja käytä monitasoista kulunhallintaa.
- Hyödynnä kulkukortteja, biometrisiä ratkaisuja, turva-auvoja, turvalukittuja ovia ja tarvittaessa paikan päällä olevaa turvahenkilöstöä.
- Pidä teknistä ja herkkää infrastruktuuria sisältävät tilat lukittuina ja kulunvalvonnan piirissä.
- Perusta yksi virallinen avain- ja tunnisterekisteri, johon kirjataan tunnisteidien myöntäminen, peruuttaminen ja palauttaminen.
- Peruuta kadonneet tai varastetut avaimet ja tunnistheet välittömästi sekä tarvittaessa sarjoita lukot uudelleen tai vaihda ne.
- Noudata pienimmän valtuuden periaatetta ja tarkista kulkuoikeudet säännöllisesti sekä aina tehtävän vaihtuessa.
- Kirjaa kulkutapahtumat lokeihin.
- Rekisteröi vierailijat, anna heille näkyvä tunniste ja huolehdi saattamisesta sekä mitätöi tunniste vierailun päätyttyä.

- **Drooniuhat**

- Hanki kyky havaita, seurata ja tunnistaa drooneja esimerkiksi tutkien, radiotaajuusskannereiden, kameroiden ja akustisten antureiden avulla.
- Heikennä kriittisten resurssien näkyvyyttä peittämällä tai siirtämällä niitä ja sijoittamalla niitä mahdollisuuksien mukaan suljettuihin tiloihin.



C. Fyysinen suojaus

- **Lähetykset ja ulkoiset kohteet**

- Sijoita postihuoneet ja jakelukeskukset erilleen kriittisistä resursseista ja vilkkaista alueista.
- Mahdollista epäilyttävien lähetysten turvallinen erottelu ja tarkastus.
- Ohjeista henkilöstö epäilyttävien lähetysten eristämiseen ja ilmoittamiseen sekä varaa tarvittavat työkalut ja henkilönsuojaimet.
- Dokumentoi arvokkaiden tai valvottujen lähetysten hallintaketju ja tee pistokokeita.
- Suojaa, tarkasta ja huolla myös ulkoiset resurssit, laitokset ja laitteet.

- **Arkaluonteiset tiedot**

- Laadi arkaluonteisten tietojen luettelo ja luokittelujärjestelmä.
- Rajoita pääsy tietoihin tiedonsaantitarpeen perusteella ja valvo ja arvioi käyttöoikeuksia säännöllisesti.
- Suojaa tiedot luvattomalta katselulta, peukaloinnilta, varkauksilta ja ympäristövahingoilta.
- Nimeä arkistot, palvelinhuoneet ja muut vastaavat tilat turva-alueiksi.
- Määritä tietojen säilytysajat sekä turvallisen puhdistamisen ja tuhoamisen menettelyt.
- Sovi ulkopuolisten sidosryhmien tietojen käsittelystä esimerkiksi käyttäjäohjeilla ja salassapitosopimuksilla.
- Huomioi kansalliset turvallisuusluokiteltujen tietojen suojaamista koskevat säännöt.



D. Poikkeamien hallinta (reagointi, kestävyys ja vaikutusten lieventäminen)

Valmistaudu poikkeamiin selkeillä vastuu-, viestintä- ja päätöksentekorakenteilla.

- **Poikkeamien hallinta ja infrastruktuurin turvallisuus**
 - Sovita laitoksen sisäiset ja ulkopuoliset kriisi-, katastrofi- ja avustustoimet yhteen.
 - Perusta toimivat viestintäkanavat viranomaisiin ja järjestä säännöllisiä kriisi- ja katastrofinhallintaharjoituksia.
 - Suunnittele infrastruktuuri vikaturvalliseksi, jotta häiriö ei vaaranna ihmisiä ja jotta kriittiset toiminnot voidaan pitää käynnissä tai ajaa hallitusti alas.
 - Mitoita riittävä varastointi, varasähkö, lämpötilanhallinta ja vaarallisten aineiden suojaaminen kriittisten toimintojen säilyttämiseksi mahdollisen vikaantumisskenaarion perusteella.
 - Varmista huolto- ja korjausvalmius sekä määrittele varajärjestelmien toimintaa, kestoja ja palauttamisen järjestystä koskevat vaatimukset.
 - Varmista tietoteknisten verkkojen, järjestelmien ja ohjelmistojen eheys, erityisesti silloin, kun toiminta riippuu korkean riskin toimittajista.
 - Suojaudu radiotaajuushäiriöiltä ja kyberhyökkäyksiltä.



D. Poikkeamien hallinta (reagointi, kestävyys ja vaikutusten lieventäminen)

- **Energia-, vesi- ja materiaalivarautuminen**
 - Monipuolista energianlähteitä, palveluntarjoajia ja toimitusreittejä.
 - Ota käyttöön esimerkiksi generaattoreita, UPS-akkuja ja muita varajärjestelmiä sekä testaa niitä säännöllisesti.
 - Varastoi polttoainetta vähintään 72 tunniksi ja sisällytä toimittajasopimukseen hätäapulausekkeet.
 - Rajoita vesihuollon häiriöissä vedenkäyttö kriittisiin toimintoihin ja käytä tarvittaessa varakaivoja, vesisäiliöitä, siirrettäviä vedenkäsittelylaitteita ja joustavia varastoja.
 - Määritä juomaveden ensisijaiset toimituskohteet ja varmista veden laatuvaatimusten täyttyminen.
 - Harkitse tarvittaessa just in time -mallista siirtymistä just in case -varautumismalliin kriittisten hyödykkeiden, kemikaalien, raaka-aineiden ja varaosien osalta.
 - Ylläpidä puskurivarastoja ja ennakolta hankittuja vararesursseja.



D. Poikkeamien hallinta (reagointi, kestävyys ja vaikutusten lieventäminen)

- **Kunnossapito**

- Laadi kattava kunnossapito-ohjelma, joka perustuu valmistajien suosituksiin, toiminnasta saatuihin kokemuksiin ja riskinarviointeihin.
- Hyödynnä ennakoivaa ja suorituskykyyn perustuvaa kunnossapitoa: anturiverkostoja, data-analytiikkaa ja tekoälytyökaluja.
- Määrittele muun muassa hälytysten todentamis-, kiireellisyys-, käynnistämisen- ja eskalointimenettelyt.
- Täydennä automaattista valvontaa säännöllisillä fyysisillä tarkastuksilla.

- **Johtaminen**

- Sisällytä häiriönsietokyky hallintorakenteen kaikille tasoille ylhäältä alas.
- Aseta tavoitteet ja laadi häiriönsietokykystrategia, -politiikka ja -suunnitelma.
- Varmista häiriönsietokykyä koskeva riittävä osaaminen johtoryhmässä.
- Nimeä tarvittaessa häiriönsietokyvystä vastaava henkilö ja määrittele päätöksentekohierarkiat, koordinoitavat ja -vastuut selkeästi.

D. Poikkeamien hallinta (reagointi, kestävyys ja vaikutusten lieventäminen)



- **Yhteistyö, viestintä ja hätätilanteet**

- Käynnistä ja virallista yhteistyö asiaankuuluvien viranomaisten kanssa, mukaan lukien päättäjät, lainvalvontaviranomaiset, pelastuspalvelut ja puolustusalan toimijat.
- Määritä roolit ja menettelyt tiedonvaihtoon, poikkeamailmoituksiin ja koordinointiin.
- Harkitse yhteistyötä oman ja muiden toimialojen toimijoiden sekä muiden jäsenvaltioiden toimijoiden kanssa.
- Laadi kriisiviestintäkäytännöt varmistaen tiedonkulun sisäisille ja ulkoisille sidosryhmille, asiakkaille ja suurelle yleisölle poikkeamien aikana.
- Ylläpidä ennalta hyväksytyjä viestintämalleja ja monikanavaisia viestintävalmiuksia, mukaan lukien varajärjestelmät.
- Huomioi viestinnässä eri kielet, kohderyhmät ja esteettömyysvaatimukset.
- Perusta monikanavainen ja tarvittaessa maantieteellisesti kohdennettava hälytysjärjestelmä.
- Nimeä tiedottajat ja kriisiryhmät, pidä hätälaitteisto toimintakunnossa ja kouluta kriisiryhmät.
- Varmista evakuointireittien esteettömyys ja harjoittele evakuointia säännöllisesti.



E. Palautuminen

Suunnittele palvelujen jatkuvuus ja hallittu palautuminen.

- Määritä keskeisten palvelujen kriittisimmät osat ja niiden palautusjärjestys.
- Varaudu laitteiden manuaaliseen ohjaukseen, jos automaattiset tai tekoälyyn perustuvat järjestelmät pettävät tai niitä peukaloidaan.
- Suunnittele henkilöstökapasiteetti häiriöiden varalta.
- Perusta käyttövalmiudeltaan tarkoituksenmukaiset varajärjestelmät tai -toimipaikat.
- Sijoita varajärjestelmät riittävän kauas ensisijaisista tiloista, mutta silti saavutettavasti.
- Harkitse siirrettäviä tiloja, kuten siirrettävää komentokeskusta.
- Säilytä varmuuskopiot fyysisesti erillisissä tai logistisesti eristetyissä sijainneissa.
- Kehitä ja ylläpidä toimintaan kohdistuvien vaikutusten arviointiin perustuvia kattavia toiminnan jatkuvuussuunnitelmia.
- Testaa, tarkista ja päivitä käytännöt säännöllisesti ja aina merkittävien poikkeamien tai toiminnan muutosten jälkeen.
- Määritä kriisinhallinnan komentorakenne, päätöksentekovaltuudet ja poikkeamien hallintasuunnitelmat.
- Harkitse kriisiryhmiä ja määritä niiden roolit, eskalointikäytännöt, koulutus ja ensisijaiset sekä vaihtoehtoiset viestintäkanavat.



E. Palautuminen

- Ylläpidä luetteloa kriisitilanteessa käytettävästä lisähenkilöstöstä.
- Tee kumppaniorganisaatioiden kanssa keskinäisen avunannon sopimuksia.
- Varmista kriittisten roolien osaaminen ja riittävä varahenkilöstö pitkittyneiden häiriöiden tai henkilöstöpulan varalta.
- Ota käyttöön vaiheittaiset uudelleenkäynnistysmenettelyt etusijalla kriittisten toimintojen palauttaminen.
- Sisällytä menettelyihin kriittisten järjestelmien järjestelmällinen validointi, tietojen eheyden ja toimintojen kattava testaus, laadunvalvontatoimenpiteet ja hallittu siirtyminen hätätilanteesta normaaliin toimintaan lisäämällä asteittain kapasiteettia ja seuraamalla suorituskykyä.
- Tee poikkeamien jälkeen perussyyanalyysi ja toiminnan jälkeinen arviointi.
- Dokumentoi havainnot ja sisällytä ne menettelyihin, koulutuksiin ja riskinarviointeihin.
- Kartoita keskeisten palvelujen tarjoamiseen liittyvät toimitusketjut ja laadi pitkän aikavälin strategia niiden häiriönsietokyvyn vahvistamiseksi.
- Määritä vaihtoehtoisia toimitusketjuja ja toimittajia.
- Harkitse puskurivarastoja, varastojen nopean täydentämisen mekanismeja ja suojattuja laitoksen ulkopuolisia varastoja.
- Harkitse resurssien, laitteiden ja henkilöstön jakamista koskevia sopimuksia muiden saman alan toimijoiden kanssa laajamittaisten palautumisoperaatioiden aikana.



F. Henkilöstöturvallisuus

Hallitse henkilöstöriskit, käyttöoikeudet, osaaminen ja varahenkilöstö.

- Arvioi henkilöstöön liittyvät uhat, mukaan lukien inhimilliset virheet, sabotaasi, sisäpiiriuhat sekä sairaudesta, hätätilanteesta tai ulkoisista uhkista johtuvat poissaolot.
- Tunnista kriittisiä tehtäviä hoitavat henkilöstöryhmät, mukaan lukien urakoitsijoiden ja alihankkijoiden henkilöstö.
- Ylläpidä ajantasaista luetteloa ja dokumentaatiota kriittisestä henkilöstöstä sekä kytke henkilöstöryhmät niihin keskeisiin palveluihin, joiden tuottamiseen ne osallistuvat.
- Määrittele, kenelle ja millä ehdoilla annetaan pääsy tiloihin, kriittiseen infrastruktuuriin, järjestelmiin ja arkaluonteisiin tietoihin.
- Ota käyttöön tehokkaat menettelyt käyttö- ja kulkuoikeuksien myöntämiseksi ja välittömäksi peruuttamiseksi ja valvo oikeuksia.
- Myönnä oikeudet vain tarpeen perusteella ja vähimmäislaajuisina tehtävien hoitamiseksi.
- Käytä rooliperusteista pääsynhallintaa, vahvaa todentamista ja identiteetinhallintaa, tehtävien eriyttämistä, aikarajoituksia ja määräaikaista käyttöoikeuksia.
- Tarkasta ja arvioi käyttöoikeudet säännöllisesti.
- Määrittele taustatarkastuksia koskevat sisäiset käytännöt.
- Yhdenmukaista henkilöstöturvallisuustoimet NIS2-vaatimusten ja soveltuvien EU-säätöjen kanssa.
- Määrittele tehtäväkohtaiset pätevyys- ja koulutusvaatimukset ja järjestä riittävä koulutus.
- Kouluta henkilöstöä sen roolin mukaan häiriönsietokykyyn liittyvistä toimenpiteistä.
- Kirjaa vaadittavat pätevyydet organisaation henkilöstö- ja häiriönsietokykyä koskeviin käytäntöihin.



G. Tiedottaminen, koulutus ja harjoitukset

Ylläpidä turvallisuuskulttuuria tiedottamisella, koulutuksella ja säännöllisillä harjoituksilla.

- Laadi henkilöstölle suunnattu jatkuva tiedottamis- ja koulutusohjelma, joka tukee turvallisuuskulttuuria.
- Varmista, että henkilöstö ymmärtää oman roolinsa häiriöiden ehkäisyssä, sisäpiiriuhkien vähentämisessä, poikkeamiin reagoinnissa, ilmoittamisessa, toiminnan jatkuvuudessa ja palautumisessa.
- Sovita tiedottaminen tiedonsaantitarpeeseen ja tietojen arkaluonteisuuteen.
- Rakenna organisaatiokulttuuria, jossa häiriönsietokyvyn turvaaminen on henkilöstön yhteinen arvo.
- Yhdistä tiedottaminen NIS2-direktiivin mukaisiin perustason kyberhygieniakäytäntöihin ja kyberturvallisuuskoulutuksiin.
- Kouluta henkilöstöä koko häiriönsietokykyprosessista.
- Tarjoa kriittisiä tehtäviä hoitaville tehtäväkohtaista koulutusta.
- Perusta tiedotusmateriaali toimijan riskinarviointiin ja toteuttamiin toimenpiteisiin.
- Laadi materiaalit selkeiksi ja helppotajuisiksi sekä esittele niissä toimijan kriittinen rooli, häiriöiden yhteiskunnallisia ja taloudellisia vaikutuksia, kaikki uhkatekijät ja tärkeimmät turvallisuusperiaatteet.
- Tarjoa materiaalit useassa muodossa, kuten digitaalisina ja fyysisinä versioina.
- Järjestä säännöllisiä keskustelupohjaisia simulaatioita ja toiminnallisia harjoituksia.
- Kohdenna harjoitukset riskinarvioinnin tuloksiin ja testaa koko häiriönsietokykyprosessi.
- Ota lainvalvontaviranomaiset, palokunta, pelastuspalvelut ja muut asiaankuuluvat viranomaiset mukaan harjoituksiin.



Ennakkoon tulleista kysymyksistä

- Turvallisuusselvityksistä, riskiarvioista ja dokumentaatiosta, tarkastusprosessista, merkittävästä häiriöstä ja keskeisestä palvelusta, yhteyspisteestä ja -henkilöstä, tärkeästä toimijasta keskeiseksi, poikkeamailmoituksista ja valvonnasta, toiminnan muuttumisen ilmoittamisesta, tuotanto- ja varastointivelvoitteista, häiriötilanteiden raaka-aineiden laatuvaatimuksista, hallintamallista, fyysisestä turvallisuudesta, valvonnasta, toimitusketjuista, CER-NIS2 suhteesta, osaamisesta ja koulutuksesta
 - Esityksessä
- Kustannuksista
 - Hallituksen esitys eduskunnalle korkovähennysrajoitusta koskevan sääntelyn muuttamisesta
 - Esityksessä ehdotetaan muutettavaksi elinkeinotulon verottamisesta annetun lain korkovähennysrajoitussäännöstä siten, että yhteisö saisi eräin edellytyksin vähentää muutoin vähennyskelvottomia nettokorkomenoja, mikäli ne kertyvät lainoista, joilla rahoitetaan huoltovarmuuskriittisiä pitkän aikavälin infrastruktuurihankkeita.
 - Mahdolliset investoinnit perustuvat toimijan itsensä tekemään riskiarvioon ja häiriönsietokykysuunnitelmaan. Investointien kustannuksista vastaa toimija. Tällä hetkellä ei ole tiedossa tukia.



Ennakkoon tulleista kysymyksistä

- Salaisten tietojen turvallisuudesta
 - Ruokavirasto noudattaa henkilötietojen käsittelyssä EU:n tietosuoja-asetusta (679/2016), tietosuojalakia (1050/2018) sekä muita soveltuvia henkilötietojen käsittelyyn ja tietosuojaan liittyviä säännöksiä. Lisätietoa tietosuojasta Ruokaviraston sivulta.
 - Tiedonhallintalakiin 906/2019 on lisätty vuonna 2025 uusi 4 a luku Kyberturvallisuutta koskevat velvollisuudet ja niiden noudattamisen valvonta. Traficom valvoo Ruokavirastoa kyberturvallisuuden osalta.
 - Lista kriittisistä toimijoista on salassa pidettävä. Poikkeamailmoitukset, riskiarviot, häiriönsietokykysuunnitelmat ja tarkastusmateriaali sisältänevät julkisuuslain nojalla salassa pidettävää tietoa.
 - Palaamme ohjeistukseen CER-tietojen käsittelystä kriittisille toimijoille mahdollisimman pian.



Lisätietoa

[Ruokaviraston NIS2-sivut](#) ja [Ruokaviraston CER-sivut](#)

- NIS2.kyberturvallisuus@ruokavirasto.fi
- CER@ruokavirasto.fi

[Elintarvikelaki 297/2021](#) ja [Yleinen elintarvikeasetus \(EY\) N:o 178/2002](#)

[Elintarvikealan toimijoiden omavalvontajärjestelmät ja niiden valvonta –ohje](#)

[Lisätietoa Ruokaviraston tietosuojasta](#)

[Sisäministeriön sivut](#)

[Kriittisten toimijoiden häiriönsietokykyä koskeva valtakunnallinen suunnitelma](#)

[CER-käsikirja](#) | [Sisäministeriö](#)

[Sisäministeriön sivut: CER- ja NIS2-poikkeamalomakkeet](#)

[Suositus kyberturvallisuuden riskienhallinnan toimenpiteistä](#)

[NIS2-direktiivi \(EU\) 2022/2555](#)

[Kyberturvallisuuslaki 124/2025](#) ja [Laki kyberturvallisuuslain muuttamisesta 369/2025](#)

[CER-direktiivi \(EU\) 2022/2557](#)

[CER-laki 310/2025](#)

[Komission tiedonanto - suuntaviivat C/2026/3712](#)



Kiitos!

RUOKAVIRASTO

Livsmedelsverket • Finnish Food Authority

