

Varautuminen, yhteistyö ja muutokset toimintaympäristössä

Kirkkoneuvos Petri Määttä

KIRKKOHALLITUS⁺

Esityksen sisältö

1. Ajankohtaista varautumiseen ja valmiuteen liittyen
2. Ajatuksia kyberturvallisuudesta ja varautumisesta
3. Kriisiviestintä onnettomuuden sattuessa

1. Ajankohtaista varautumiseen ja valmiuteen liittyen



Varautumisella
turvataan

- 1) Perustehtävän toteuttaminen
- 2) Henkinen tuki ja huolto
- 3) Vainajien huolto ja
hautaustoimesta huolehtiminen

Yhteiskunnan häiriötilanteissa ja poikkeusoloissa teemme sitä, mitä teemme myös normaalioloissa.

Yhteiskunnan elintärkeät toiminnot

(Toiminnot, jotka on
turvattava kaikissa
olosuhteissa ja
muodostavat
varautumistyön
lähtökohdan)

ELINTÄRKEÄT TOIMINNOT



Seurakuntien valmiussuunnittelun ohjeistus

- Edellinen ohjeistus **vuodelta 2019**
- **Vuonna 2023:** uusi kansallinen riskiarvio ja uudistettu kirkkolaki
- **Syyskuussa 2023:** kirkkohallitukselta dokumentti uuden riskiarvion ja kirkkolain tuomista korjauksista ohjeistukseen.
- **Vuonna 2024** tulossa: Uusi yhteiskunnan turvallisuusstrategia ja valmiussuunnittelun ohjeistus kunnille
- **Vuoden 2024** aikana uudistettu seurakuntien valmiussuunnittelun ohjeistus, jonka valmistelussa huomioitu em. asiakirjat.

Kansallinen riskiarvio 2018 → 2023 painopisteiden muutokset



- **Uhat ja haasteet ovat monipuolistuneet:** informaatiovaikuttaminen, poliittinen ja taloudellinen painostus, sekä digitalisaatioon liittyvät riskit ovat korostuneet. Teknologinen kehitys ja globaalit muutokset lisäävät monimutkaisuutta turvallisuusympäristössä.
- **Digitalisaation haasteet:** 2023 riskiarviossa painottuu digitaalisen yhteiskunnan haavoittuvuudet, kuten kyberuhkat ja tieto- ja viestintäverkkojen häiriöt. Yhteiskunta on muuttunut entistä riippuvaisemmaksi sähköisistä järjestelmistä ja tietoverkoista.
- **Ilmastonmuutos ja ympäristötekijät:** 2023 riskiarvio kiinnittää enemmän huomiota ilmastonmuutoksen vaikutuksiin ja ympäristötekijöihin, kuten äärimmäisiin sääilmiöihin ja luonnonkatastrofeihin.
- [Kansallinen riskiarvio 2023 - Valto \(valtioneuvosto.fi\)](https://valtioneuvosto.fi/kansallinen-riskiarvio-2023)

Hehu-tilanteesta valtakunnallisesti

- Toukokuussa -23 kirkkohallituksessa aloittanut uusi sielunhoidon asiantuntija, joka vastaa HeHu-asioista.
- Kesäkuukausina yhteisiä kehittämistarpeita kartoitettiin hiippakuntien Hehu-vastaavien asiantuntijoiden sekä Sosiaali- ja kriisipäivystyksen (Sokri) valtakunnallisesta koordinaatiosta vastaavien työntekijöiden kanssa.
- Syyskuussa -23 alkavat yhteiset neuvottelut hiippakuntien asiantuntijoiden kanssa valtakunnallisista kehittämistarpeista.
- Yhteydenotot: petri.patronen@evl.fi, 040 484 2622.

2. Ajatuksia kyberturvallisuudesta ja varautumisesta

Kybersää heinäkuu 2023



Tietomurrot ja -vuodot

- ▶ Heinäkuussa ilmoitusmäärät laskivat alkuvuoden tasolle.
- ▶ Lasku oli tasaista niin SOME-tilimurtojen kuin yrityssähköposteihin kohdistuneiden murtojen osalta.



Huijaukset ja kalastelut

- ▶ Huijausviestit kiertävät sähköpostisuodattimia piilottamalla kalastelusivulinkit QR-koodin taakse.
- ▶ Pankkitunnuksia kalasteltiin pitkin kesää pelottelemalla uhreja pankkien tai suomi.fi-viranomaispalvelun nimissä.



Haittaohjelmat ja haavoittuvuudet

- ▶ Heinäkuun aikana on julkaistu useita kriittisiä haavoittuvuuksia.
- ▶ Kyberturvallisuuskeskus on tehnyt heinäkuussa kriittisten ohjelmistohaavoittuvuuksien kartoitustyötä. Yksikään organisaatio Suomessa ei ole toistaiseksi ilmoittanut todetusta hyväksikäytöstä.



Automaatio ja IoT

- ▶ Yhdysvallat ottaa käyttöön uuden vapaaehtoisien äylaitteiden kyberturvallisuuden sertifiointi- ja merkintäohjelman "U.S. Cyber Trust Mark" vuonna 2024.^[3]
- ▶ Laitteiden päivitystarvetta on seurattava myös lomien aikana hyödyntäen riskiperustaista haavoittuvuuksien hallintaa.



Verkkojen toimivuus

- ▶ Heinäkuussa yleisissä viestintäpalveluissa oli kuusi merkittävää toimivuushäiriötä.
- ▶ Presidentti Bidenin vierailu ei aiheuttanut toimivuushäiriötä verkkosivuille.

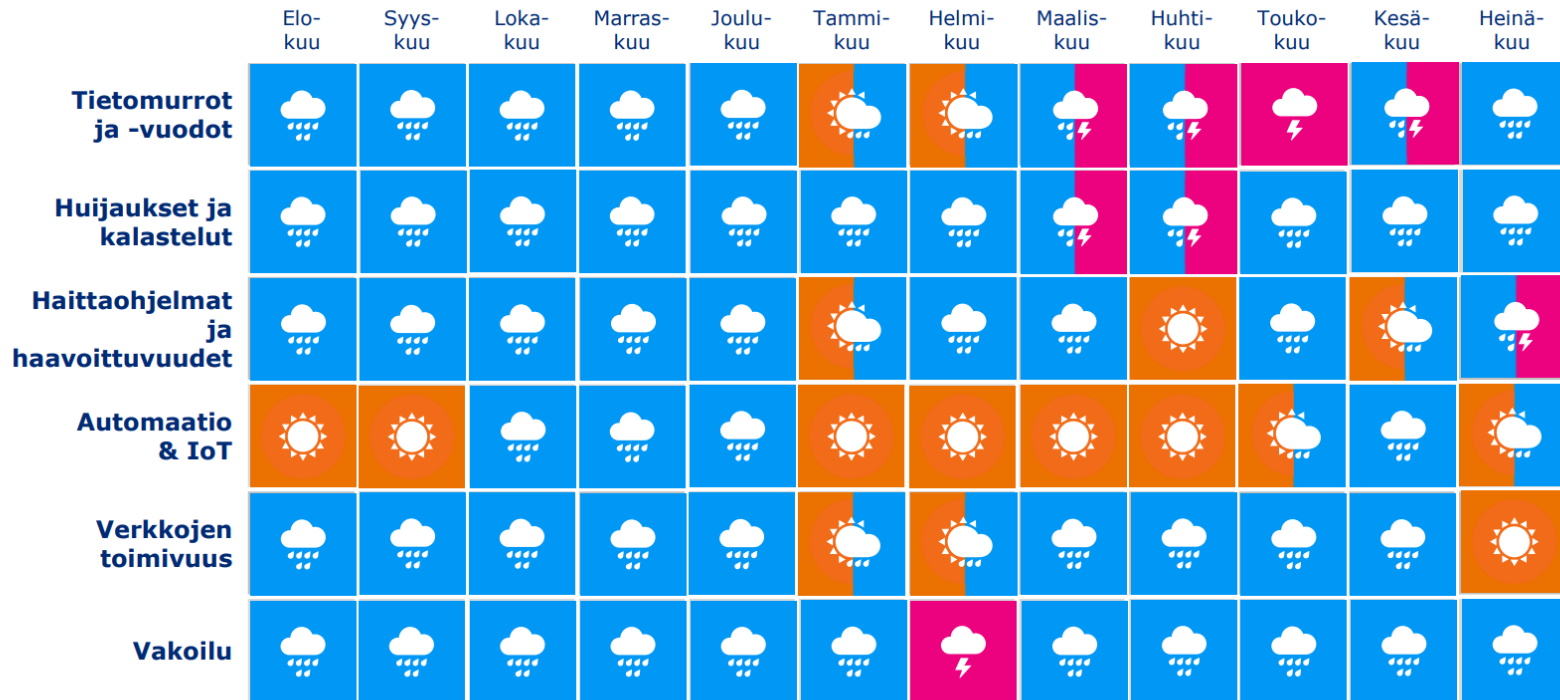


Vakoilu

- ▶ Kiinaan yhdistetty Storm-0558-toimija tunkeutui länsimaissa valtionhallinnon organisaatioiden sähköpostitileille saatuaan käyttöönsä salausavaimen, jolla se pystyi luomaan väärennettyjä Microsoft-tilien kirjautumistietoja. Hyökkäyksessä hyödynnettiin lisäksi näiden tietojen vahvistamisessa ollutta puutetta.^[4]



Kyberturvallisuuden trendit kulunut 12 kk



Top 5 uhat lähitulevaisuudessa (6kk–2v)

1.

Suomeen kohdistunut kyberympäristön uhkataso on pysynyt kohonneena.

Kohdistettujen hyökkäysten määrä on noussut. Kohonneen uhkatason vuoksi organisaatioiden varautumisen merkitys korostuu.

2.

Politiikan ja talouden ilmiöt heijastuvat myös kyberturvallisuuteen.

Ilmiöt voivat näkyä digitaalisessa toimintaympäristössä nopeasti ja aiheuttaa vaikeasti ennakoitavia tapahtumia kyberturvallisuudessa.

3. 

Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa.

Organisaatioiden olisi hyvä tunnistaa tekoälytuomia haasteita, ja varautua niihin esimerkiksi kouluttamalla henkilöstöään.



Uusi



Päivitetty

Symbolit

4.

Toimitus- ja palveluketjujen tietoturva ja jatkuvuus ovat yhä kriittisempiä.

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista.

5. 

Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

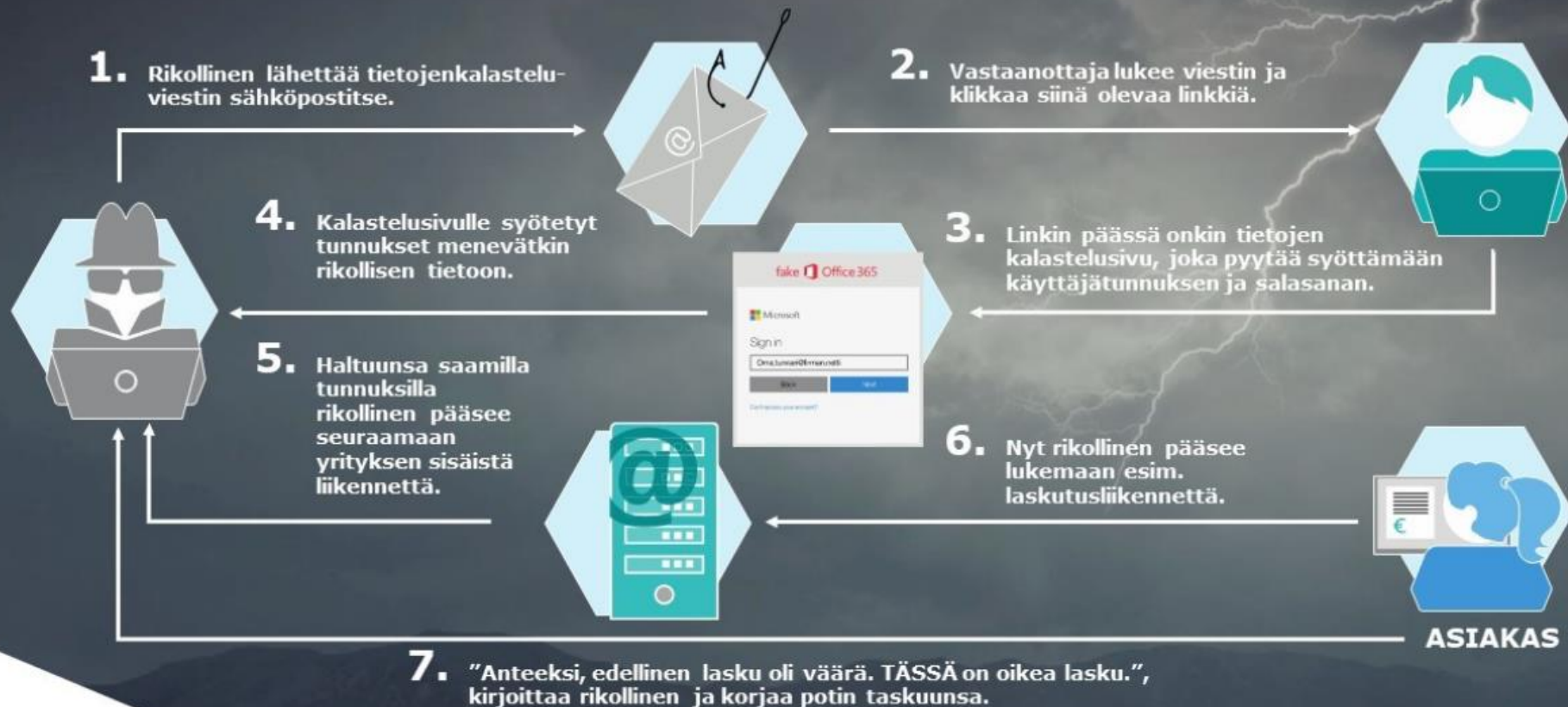
Uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää entisestään tarvetta erilaisille osaajille. Myös riskienhallinnan ja jatkuvuuden näkökulmasta riittävän osaamisen varmistaminen kaikkina vuodenaikoina on organisaatioille tärkeää.

Miten varautua tietomurtoihin

- 1) Pidä ohjelmistot ja järjestelmät päivitettyinä
- 2) Käytä monivaiheista tunnistautumista
- 3) Älä käytä samoja salasanoja useammassa eri palvelussa
- 4) Muista varmuuskopiot
- 5) Varaa riittävät resurssit tietoturvaa parantaviin ratkaisuihin (tekniikat ja käytännöt)

<https://www.kyberturvallisuuskeskus.fi/>

Office 365-huijauksen vaiheet



ASIAKAS

Kyberturvallisuuden johtaminen

1. Huomioi muutokset kyberturvallisuuden uhkakuvassa
2. Määrittele toiminnan kannalta kriittiset tekijät
3. Suojaa toiminnan kannalta kriittiset ympäristöt (monivaiheinen tunnistautuminen, tietoturvapäivitykset, tietoliikenteen turvallisuus, suojautuminen haittaohjelmilta, varautuminen palvelunestohyökkäyksiin, pilvipalveluiden suojaaminen, etäyhteyksien turvallisuus, varmuuskopiot, julkisen verkon palvelut, langattomat teknologiat)
4. Havainnoi tapahtumia ja reagoi niihin
5. Varmistakaa toiminnan jatkuvuus
6. Informoikaa henkilöstöä
7. Ilmoittakaa tietoturvaloukkauksista ja niiden epäilyistä

<https://www.kyberturvallisuuskeskus.fi/>

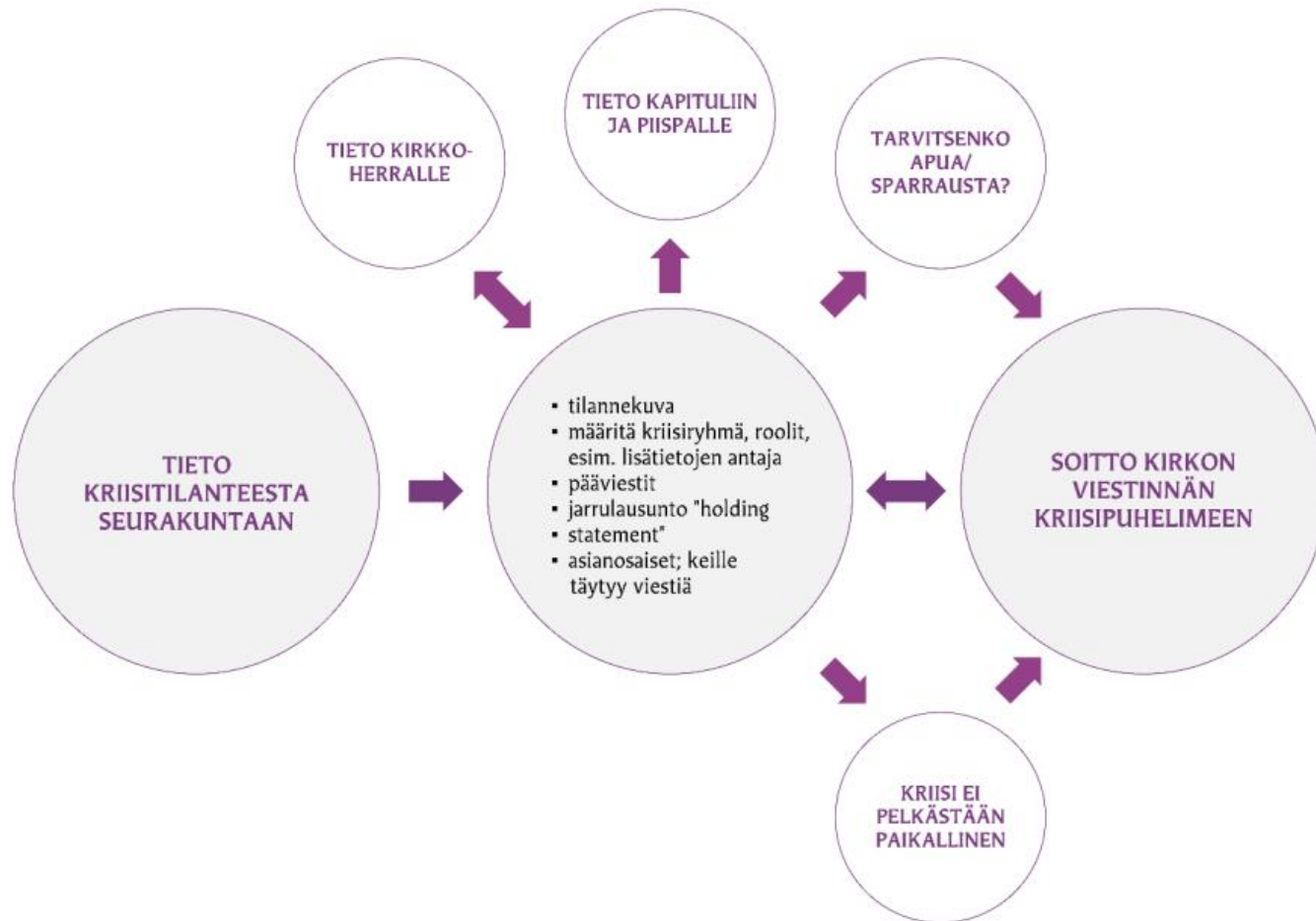
3. Kriisiviestintä

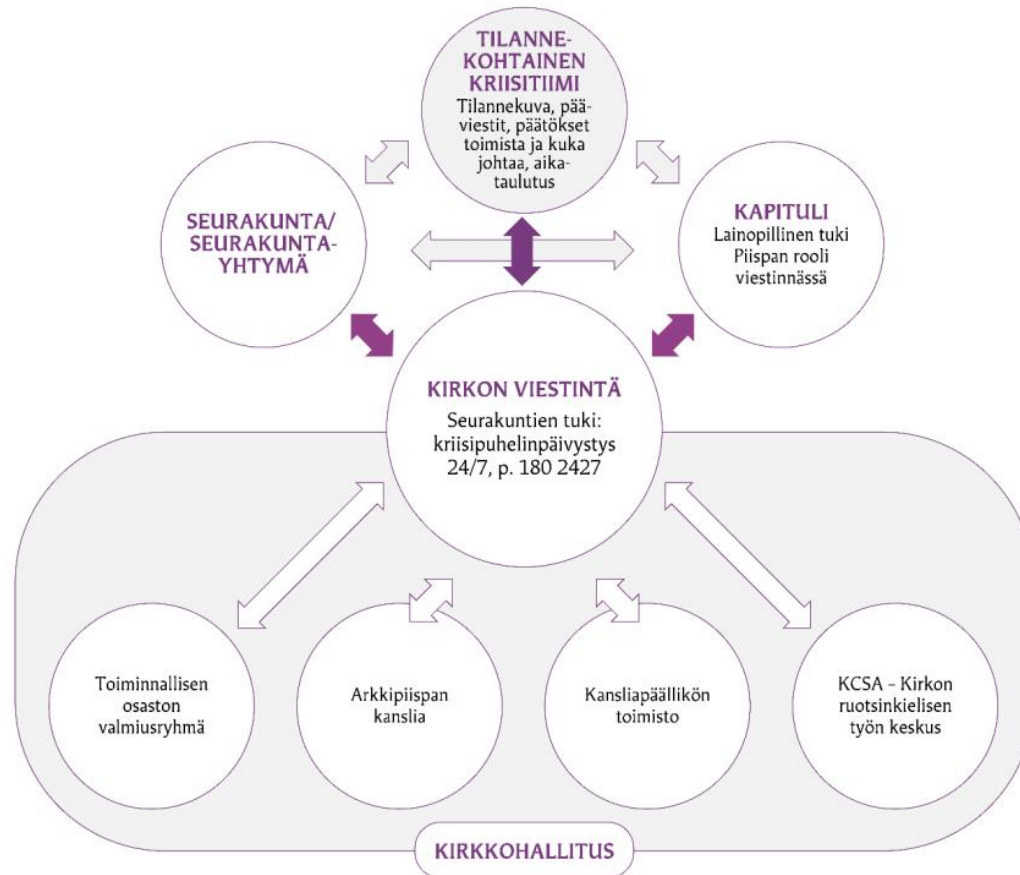
Kriisiviestintä

- EI OLE
 - asian painamisesta villaisella tai asian piilottelua
 - asian tutkimista
 - kaverin puolelle asettumista
 - tuomion tekemistä asiasta.
- VAAN
 - on avointa
 - on vastuullista
 - pyrkii minimoimaan kriisin keston sekä vahingot
 - tukee asianosaisia kriisissä.

Kriisiviestinnän tavoitteet

- luoda faktoihin perustuva tilannekuva
- tukea asianosaisia ja organisaatiota kriisissä
- turvata kirkon toimintaedellytykset ja toiminnan jatkuvuus paikallisesti tai laajemmalla alueella
- tarjota luotettavaa ja ajantasaista tietoa kriisin osallisille, työntekijöille, luottamushenkilöille, medialle ja suurelle yleisölle
- leikata vääriltä huhuilta ja disinformaatiolta siivet
- tuoda esille kirkon näkökulma ja sanoma - kertoa että kirkko on ihmisten tukena arkena, häiriötilanteissa ja poikkeusoloissa
- viestiä armosta ja toivosta; lisätä myötätuntoa, lohduttaa.







Kriisi- viestintä- numero

Kirkon viestinnän
kriisiviestintänumero
äkillisiin kriiseihin

09 180 2247

- Sparrausta, ohjeita
- Konkreettista tukea
- Valtakunnallinen viestintä

Kriisiviestintäohjeistot Sakastissa

<https://sakasti.fi/kriisit-ja-varautuminen/nain-varaudut/nain-valmistaudut-kriisiviestintaan/>

Ole yhteydessä:

- Tuula Putkinen, p. 046 9220232,
tuula.putkinen@evl.fi
- Eevu Heikura, p. 040 688 1421,
eeva-kaisa.heikura@evl.fi