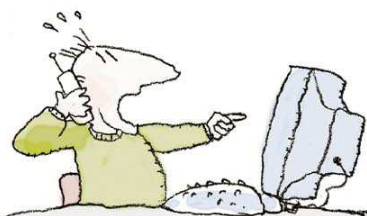
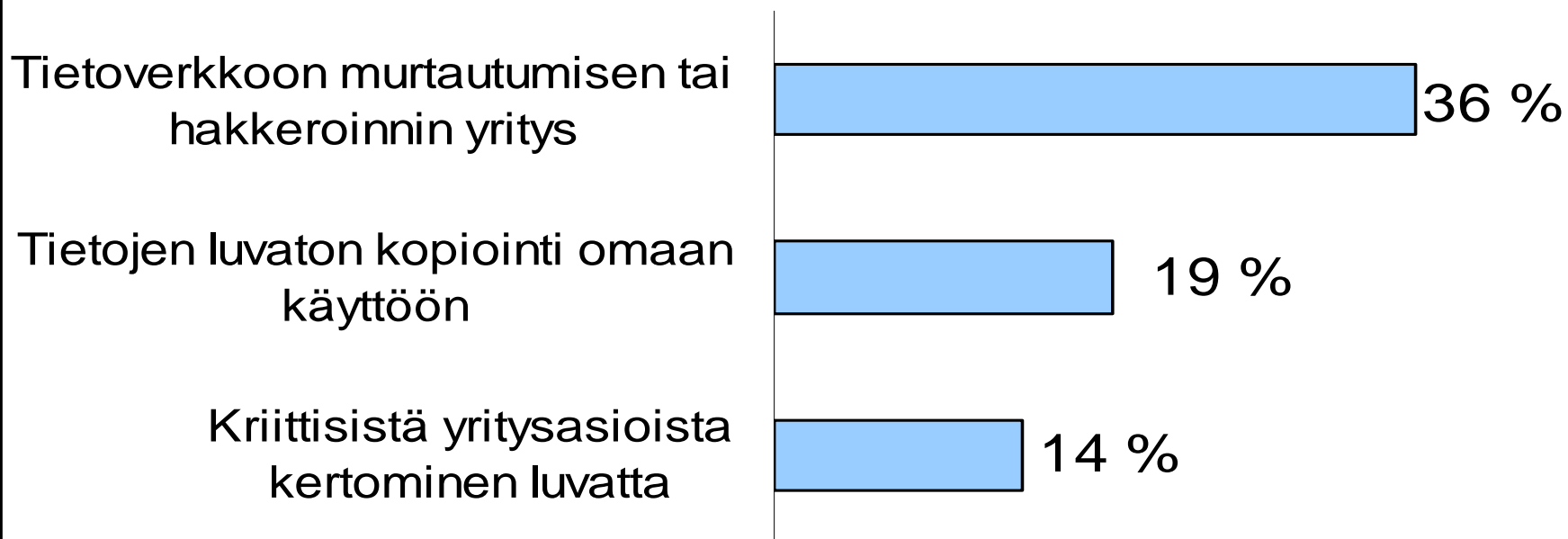


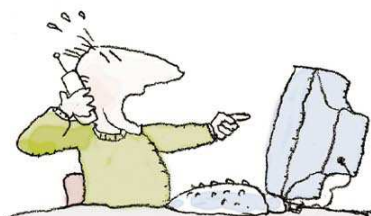


Tiedon turvaamisella menestykseen



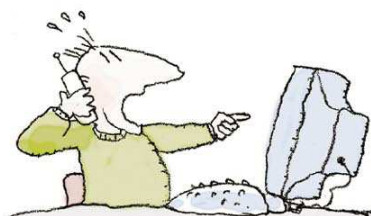
## Yleisimmät tietoriskit yrityksissä





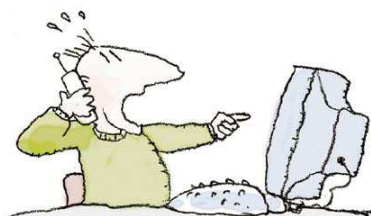
## Tutkittua pk-yritysten tietoturvasta

- Kauppa- ja teollisuusministeriön helmikuussa 2007 julkaiseman tutkimuksen mukaan:
  - 95 % pk-yrityksissä on käytössä palomuuuri
  - 94 %:ssa on automaattisesti päivittyvä haittaohjelmatorjunta
  - 21 %:ssa on tehty kirjallinen tietoturvaohjelma
  - 14 %:ssa on tehty tietoturvasuunnitelma
- Suunnitelmallisuutta tarvitaan!



## Hyvät kysymykset

- Mikä on yritykselle kriittistä tai luottamuksellista tietoa?
- Voiko työntekijä tuhota kriittistä tietoja tai hyötyä siitä väärässä yhteydessä?
- Tieto joutuu väärin käsiin – mikä on yrityksen vastuu ja korvausvelvollisuus?

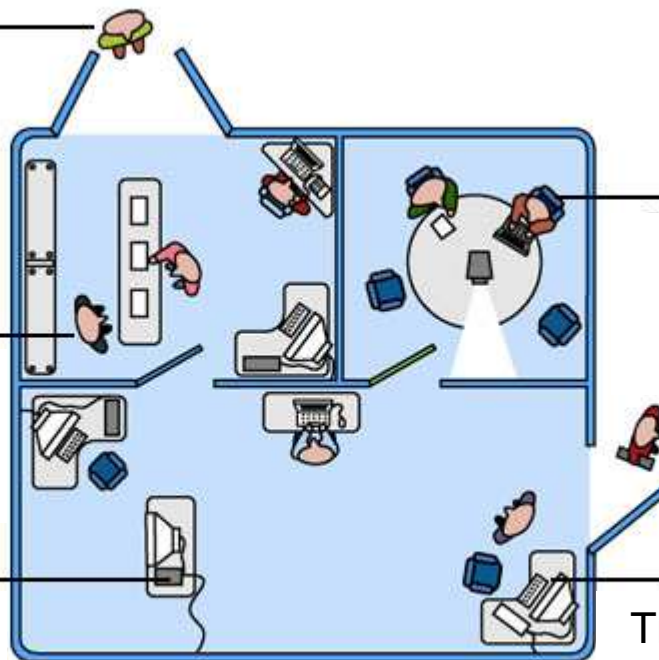


## Toimivan tietoturvan avainkysymyksiä

Tiedetäänkö, missä tietoa säilytetään ja ketkä tiloihin pääsevät?

Tietääkö henkilöstö, miten toimitaan eri tilanteissa ja mitkä ovat tietoturvan pelisäännöt?

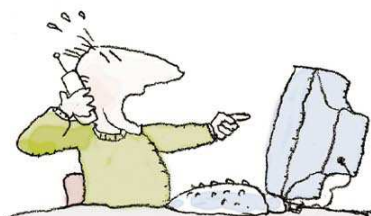
Ovatko tietokoneiden ja verkon suojaukset ajan tasalla?



Noudatetaanko ohjeita?

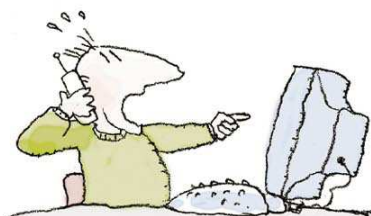
Onko johto määritellyt yrityksen tietoturvan periaatteet ja tehnyt siihen liittyvät päätökset?

Tiedetäänkö, mikä tieto on suojattava?



## Toimiva tietoturva säästää aikaa ja rahaa

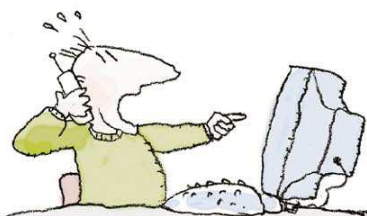
- Luottamukselliset tiedot eivät joudu väärin käsiin.
- Tiedot eivät vahingoitu.
- Tiedot ovat käytettävissä silloin, kun niitä tarvitaan.
- Yritys pystyy hallitsemaan tietojensa liikkumista yrityksen sisällä ja ulkopuolella.
- Ei turhia huolto- ja korjauskustannuksia.
- Maine ja uskottavuus säilyvät.
- Yritys voi keskittyä olennaiseen - ydinliiketoimintaansa.



## Kriittisiä ja turvattavia tietoja ovat

- Yrityksen järjestelmiä koskevat tiedot
- Liiketoimintatiedot
- Tuotekehitystiedot
- Tuotantotiedot
- Taloushallinnon tiedot
- Asiakastiedot
- Myyntitiedot
- Henkilöstötiedot
- Markkinointitiedot jne.





## Toimivan tietoturvan rakentaminen

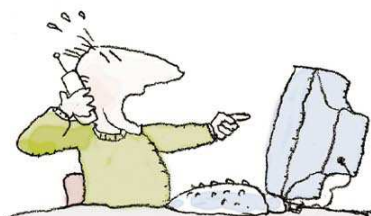
Tietoturvan rakentaminen alkaa suojattavien kohteiden kartoituksesta, riskianalyysistä ja tiedon luokittelusta. Ne luovat pohjan johdon päätöksille, joilla linjataan yrityksen tahto.

Tietoturvasuunnitelma luo pohjan jatkuvalle kehitystyölle.

Perehdytyksellä ja yhteisillä pelisäännöillä tietoturvasta tulee jokaisen yrityksessä työskentelevän asia.

Jatkuvuus on varmistettava. Tietoturvan on toimittava myös muuttuneissa olosuhteissa.

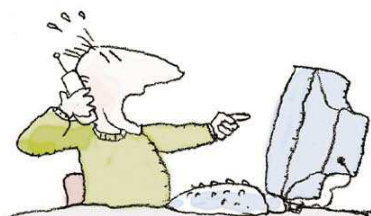




## Suojattavien tietojen kartoitus

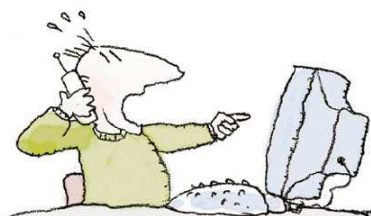
- Tietoturvan kohentaminen alkaa yrityksen tietoturvariskien kartoittamisesta.
- Riskianalyysi tehdään yrityksen tarpeiden mukaan.
- Aluksi on tärkeää erotella kriittinen tieto.
- Myös laki asettaa yritykselle velvoitteita pitää salassa esimerkiksi henkilötiedot.

Kuka on päättänyt laittaa kaikkien nähtäväksi tiedon siitä, että Pirjo on sairauslomalla auto-onnettomuuden vuoksi?



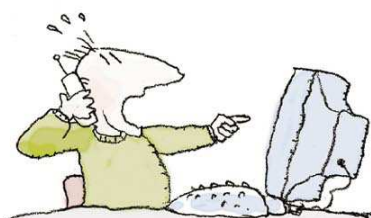
## Tiedon luokittelu

1. Tiedon omistaja luokittelee tiedon.
2. Miten tieto luokitellaan ja merkitään?
  - Julkinen – hyötyä yritykselle
  - Sisäinen – ei hyötyä eikä haittaa yritykselle
  - Luottamuksellinen – vahinkoa tai haittaa yritykselle tai työntekijälle
  - Salainen – vakavaa vahinkoa tai haittaa yritykselle tai työntekijälle
3. Tiedon käyttäjä käsittelee tietoa valitun luokan mukaisesti.

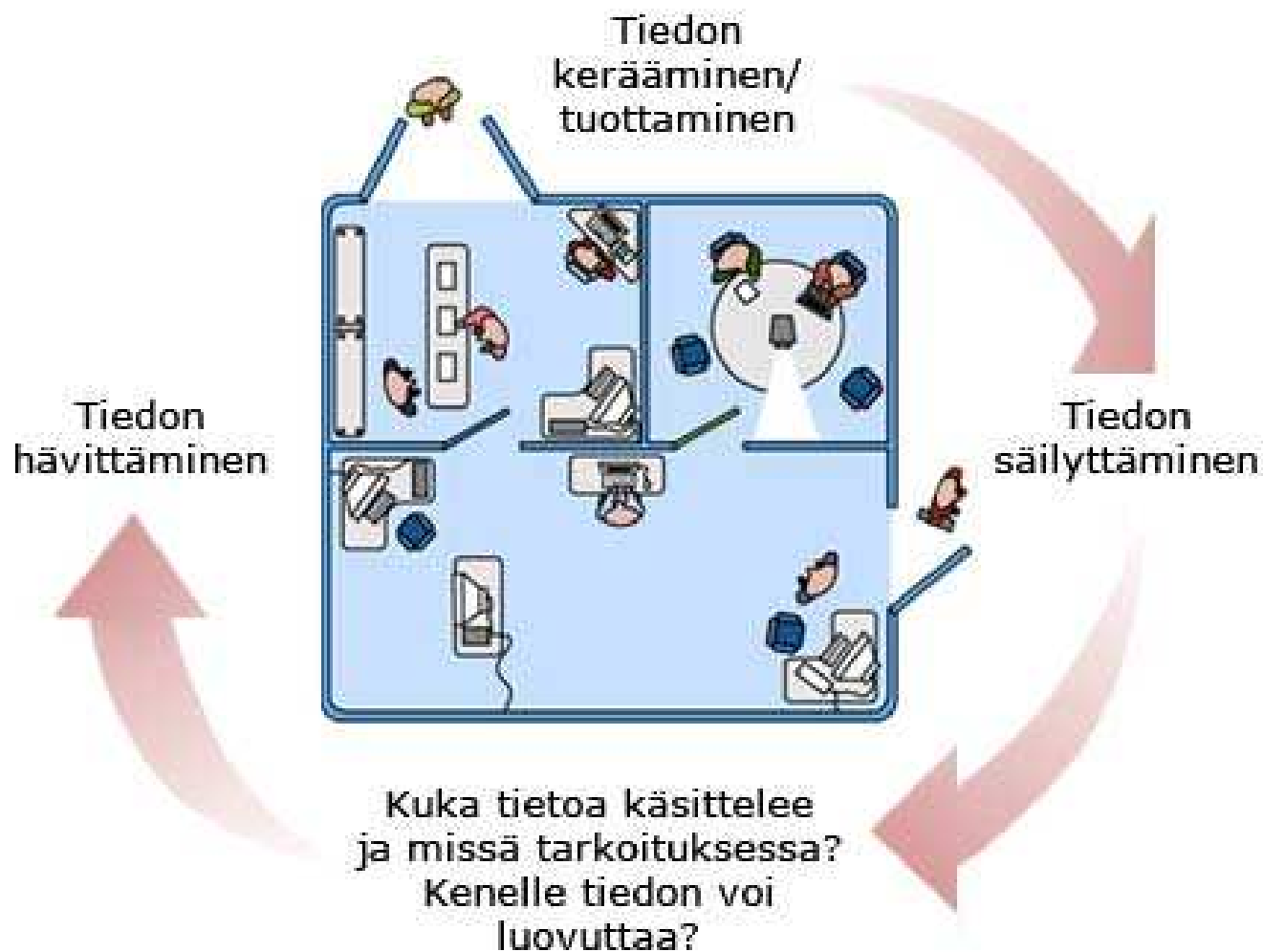


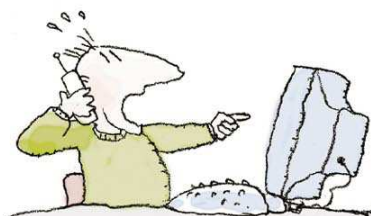
## Tiedon kartoitus: käytännön työkaluja

- Riskianalyysi
  - materiaalikansiossa: Tietoturvakartoitus – kysymyslista
- Tiedon luokittelu
  - materiaalikansiossa: Esimerkki tietojen luokittelumallista
- Tiedon käsittelyohjeet
  - materiaalikansiossa: Esimerkki tiedon käsittelyohjeista
- Tiedon elinkaaren määrittely
  - katso esimerkki seuraavalla sivulla



## Esimerkki tiedon elinkaaresta

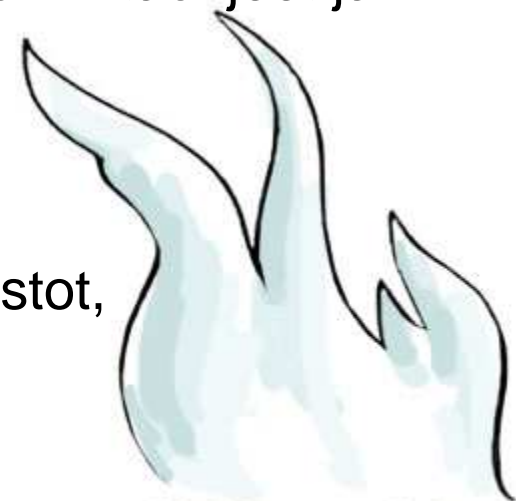




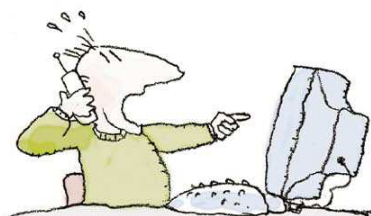
## Tietoturvasuunnitelma

Tietoturvasuunnitelma pitää sisällään seuraavat osa-alueet:

- Hallinnollinen tietoturva (tietoturvaperiaatteet, toimintaohjeet ja seuranta)
- Henkilöstön turvallisuus
- Tietoaineiston turvallisuus
- Tietotekninen turvallisuus, mukaan lukien laitteistot, ohjelmistot, tietoliikenne ja käyttö
- Fyysinen turvallisuus (toimitilat)

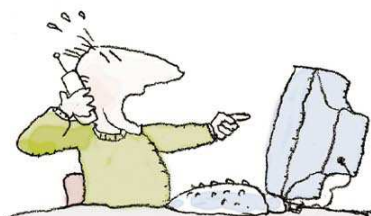


**Ohjeiden on toimittava  
myös poikkeus-  
olosuhteissa**



## Suunnittelu: tekninen tietoturva

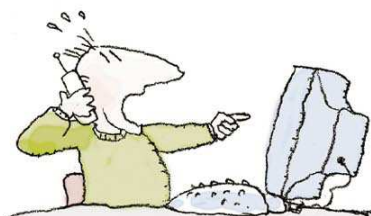
- Työasemien ja verkon monitasoinen tekninen suojaus on välttämätöntä liiketoiminnan jatkuvuuden varmistamiseksi.
- Roskaposti ja huijausviestit eivät saa kuormittaa normaalia päivittäistä työskentelyä ja tietojärjestelmiä.
- Älypuhelimiin pitää suhtautua kuten tietokoneisiin - käyttöönotto pitää olla hallittua ja säädeltyä.
- (Liike)toimintaa uhkaavat hyökkäykset pitää pystyä selkeästi raportoimaan – nopea reagointi ja toipuminen ovat avainasioita.
- Tietoturvan hankkiminen palveluna on mielekäs vaihtoehto, jos oma osaaminen puuttuu.



## Suunnittelu: käytännön työkaluja

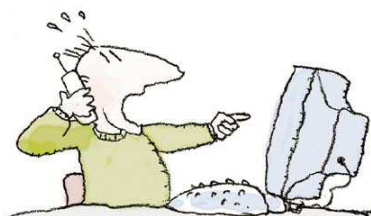
- Tietoturvaohjelman avainkohdat
- Tietoturvaohjeet (malli)
- Salassapitosopimuksen avainkohdat
- Vinkkejä henkilötietojen ulkoistamiseen

=> *löytyvät materiaalikansioista*



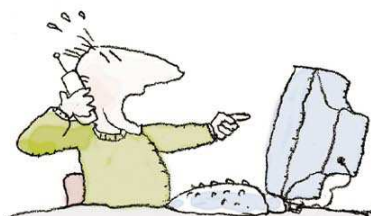
## Tietoturvan käyttöönotto

- Turvallisten toimintatapojen ja yrityskulttuurin luominen
- Johdon ja henkilöstön sitoutuminen
- Vastuuttaminen
- Valvonta ja ylläpito
- Tietoturvakoulutus
- Selkeiden toiminta-ohjeiden ja mallien toteutus
- Seuranta ja kehittäminen



## Yhteenveto

- Tiedon turvaaminen on osa liiketoimintaa ja kilpailuetu.
- Tietoturva on muutakin kuin tekninen ratkaisu – se on inhimillisten tekijöiden summa.
- Tietoturva on kaikkien asia.
- Tiedon turvaaminen on suunnitelmallista ja jatkuvaa työtä.



## Yrityksen tietoturvaopas

- Tarjoaa arjen liiketoimintaa hyödyttävää tietoturvatietoa.
- Käytännönläheisiä neuvoja ja työkaluja tiiviissä paketissa.
- Malleja pk-yrityksen tietoturvakartoituksen,-suunnitelman ja -ohjeistuksen toteuttamiseen sekä ylläpitoon.

[www.tietoturvaopas.fi](http://www.tietoturvaopas.fi)



# Tietoturvapäivä 2007 -hankkeen järjestävät

Asianajotoimisto Legistum Oy, D-Fence Oy, Digita Oy, Elisa Oyj, FiCom ry, fiMUG ry, Finanssialan Keskusliitto, Finnet, F-Secure Oyj, Hewlett-Packard Oy, Huoltovarmuuskeskus, Kauppa- ja teollisuusministeriö, Keskuskauppakamari, Kuluttajavirasto, Liikenne- ja viestintäministeriö, Mannerheimin Lastensuojeluliitto, Microsoft Oy, Opetushallitus, Opetusministeriö, Pelastakaa Lapset ry, TeliaSonera Finland Oyj, Suomen Kuntaliitto, Suomen Yrittäjät, TIEKE Tietoyhteiskunnan kehittämiskeskus, Tietosuojavaltuutetun toimisto, Tietoturva ry, Valtiovarainministeriö, Viestintävirasto, VTT, Väestörekisterikeskus

[www.tietoturvakoulu.fi](http://www.tietoturvakoulu.fi)

[www.tietoturvaopas.fi](http://www.tietoturvaopas.fi)