

1. Introducció:

Aquest document és un recull de recomanacions d'autoprotecció online.

Sovint mantenir un nivell de seguretat alt i consistent pot arribar a dificultar l'ús. És per això que des de la comissió tècnica d'ANC Deutschland hem creat dos perfils d'usuari amb diferents recomanacions de seguretat.

Aquest document descriu les **recomanacions de seguretat per usuaris estàndard**. Aquest grup inclou membres d'ANC Deutschland o simpatitzants sense responsabilitats organitzatives.

El segon grup, amb unes recomanacions diferents, està orientat a persones amb responsabilitats organitzatives o persones amb projecció pública.

2. Gestió de dispositius:

- Mantenir els ordinadors, tauletes i telèfons sempre actualitzats.
- Establir una contrasenya, patró o empremta digital per desbloquejar els dispositius.
- No repetir mai contrasenyes. Emprar sempre contrasenyes diferents per a cada compte, programa o dispositiu, no repetint-les mai. Es recomana fer servir gestors de contrasenyes com Keepass (<https://keepass.info/>) o LastPass (<https://www.lastpass.com/>)^{*} o BitWarden (<https://bitwarden.com/>).

3. Encriptació:

Assegurar que els dispositius que fem servir tinguin les dades encriptades:

- **iPhone:** No cal fer res ja que encripta el telèfon per defecte.
- **Android:** Per certes versions cal fer-ho de forma manual:
 - Android > Security > Encrypt device
 - Android > Security > Encrypt SD-card

4. Comunicacions

- No fer servir trucades normals o SMS. Ni fent servir paraules clau.
- Evitar el correu electrònic per compartir informació sense xifrar.
- Per trucades de veu fer servir Signal.
- El problema de la missatgeria és sobretot els missatges oblidats al telèfon. És molt important mantenir la disciplina esborrant missatges antics de forma periòdica.
 - A Signal posar sempre un temps d'expiració dels missatges.
 - A Telegram esborrar els missatges de forma manual. En el cas de Grups l'Administrador ha d'anar esborrant els missatges de tot el grup de forma periòdica. Degut a aquesta limitació es recomana fer els grups a Signal.

5. Navegació:

És important emprar un navegador segur com Chrome, Firefox o Brave. Per poder accedir a web censurades en zones concretes fer servir TorBrowser (<https://www.torproject.org>) disponible per Windows, Mac, Android i iPhone entre d'altres. Assegurar-nos que els navegadors s'actualitzen de forma periòdica.

6. Connexions segures:

En llocs amb xarxes públiques d'internet (com per exemple aeroports o hotels) o si estem viatjant a països amb poques qualitats democràtiques, cal fer servir una VPN (Virtual Private Network). Això ens permetrà ocultar el tràfic i evitar que el manipulin.

Si encara no teniu accés a la VPN d'ANC-DE poseu-vos en contacte amb la comissió tècnica.

7. Avaluar riscos:

Una eina molt important per avaluar riscos en les nostres comunicacions és el nostre sentit comú. Hem de saber identificar quins llocs poden ser segurs i quins poden contenir riscos. Algunes recomanacions:

- Valorar i revisar els arxius adjunts d'un correu electrònic.
- Desconfiar dels enllaços rebuts per correu electrònic o SMS.
- Actualitzar aplicacions periòdicament per a evitar fallades en la seguretat.

En cas de dubte poseu-vos en contacte amb la comissió tècnica a tecnic@anc-deutschland.cat o al canal #seguretat de l'Ancora.