RECOMANACIONS TELETREBALL

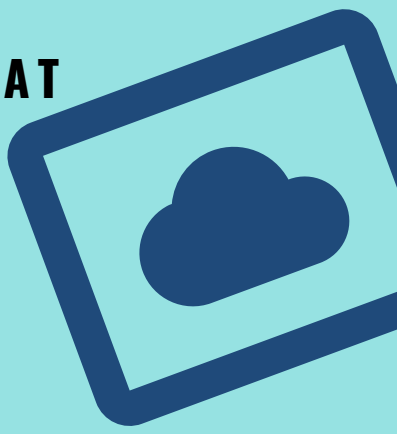
Agència Andorrana de Protecció de Dades

És recomanable prendre certes mesures per a assegurar-nos de **mantenir la seguretat i protecció dels equips informàtics fora del centre** de treball i, conseqüentment, de les dades que puguin tractar.

Aquestes **recomanacions** són tant perquè les tinguin en compte els **treballadors** a distància, com perquè els **empresaris** controlin que es compleixen, de manera que es respecti el que s'estableix en lleis i normatives vigents sobre protecció de dades i dades digitals.

1 AVALUAR ELS RISCS

Abans d'instaurar una mesura com el teletreball, el responsable de les dades haurà d'**avaluar el risc i adoptar els procediments i les mesures dee trol necessàries per a permetre el tractament de les dades des dels domicilis** particulars i per protegir la intimitat dels treballadors.



2 DEURE DE SECRET I CONFIDENCIALITAT

En els contractes laborals s'acostuma a incloure una clàusula mitjançant la qual el **treballador es compromet a no divulgar dades a que tingui accés arran de la seva feina**. Si aquesta no està inclosa al contracte, és recomanable que **el treballador signi un annex al seu contracte de treball o un acord específic sobre teletreball** abans de procedir al teletreball.
Aquest acord haurà de contenir, entre d'altres, les **instruccions dictades pel responsable de les dades en matèria de protecció de dades** personals, especialment aplicables al teletreball.
Els responsables de **recursos humans o representants dels treballadors hauran de ser informats** dels signants i del contingut d'aquests acords i annexos, sempre preservant la **intimitat** i el dret a la protecció de dades del treballador.
Els treballadors, en el desenvolupament del teletreball hauran de complir amb les **instruccions del responsable** tant a nivell de protecció de dades personals com a especificitats tècniques de seguretat de la informació.

3 DISPOSITIUS DE TREBALL

Obligacions treballadors:

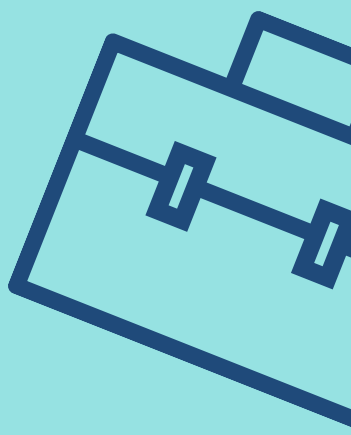
- No deixar **desatesos** els equips portàtils en **llocs públics**.
- **Restringir l'accés no autoritzat** a la informació o recursos per part d'altres persones que utilitzin el dispositiu personal (familiars o amics) i restringir l'ús de tercers a dispositius de l'empresa.
- Evitar la **instal·lació d'aplicacions o la navegació** per pàgines no segures.
- **Bloquejar la pantalla** de l'ordinador quan no estiguem treballant.
- Si s'usa un **equip personal** per al teletreball, a part de seguir totes aquestes recomanacions, és bona idea:
  - Crear un *perfil professional* per a mantenir separats comptes i navegació.
  - *No descarregar* fitxers amb dades de caràcter personal si es poden utilitzar en línia.
  - *Evitar distraccions amb tasques domèstiques* o amb altres membres de la família

Obligacions responsable:

- El responsable **no pot obligar a la instal·lació de programari en dispositius personals del treballador ni l'ús d'aquests** dispositius en el teletreball. Es recomana sempre que el responsable proporcioni els dispositius de treball per tal de minimitzar riscs de filtracions de dades.
- L'acord de teletreball haurà d'especificar quins **termes d'ús podrà fer el treballador de dispositius de l'empresa** durant el teletreball.

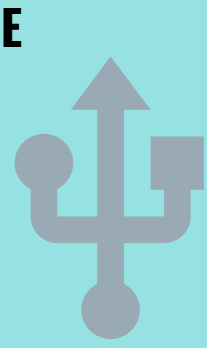
4 XARXES I NAVEGACIÓ

- Crear una **xarxa privada o VPN** (Virtual Private Network) per a connectar entre si als treballadors i amb l'oficina, on l'accés a la xarxa estigui protegit per un xifrat que doni una capa extra de protecció. Així evitarem l'accés de tercers no autoritzats a la informació que es comparteix a través d'aquesta xarxa.
- **No** emprar ***Wifi* públiques**.
- **Tancar totes les connexions amb servidors i webs** recorrent a "tancar sessió" o "desconnectar".
- **Esborrar l'historial** de navegació, les *cookies* i altres dades, així com les contrasenyes recordades.



5 CESSIÓ, DESCÀRREGA I EMMAGATZEMATGE

- Utilitzar tècniques de xifrat de dades **per a la transmissió** de la informació, ús de contrasenyes, *firewall* i antivirus.
- Cura amb l'ús de **memòries USB**, ja que són una possible porta a les infeccions de *malware*.
- **Eliminar la informació temporal** en carpetes de descàrrega, paperera de reciclatge, etc.



6 TAULETES I SMARTPHONES

- **Limitar l'accés al dispositiu** mitjançant un bloqueig amb contrasenya, patró o similar.
- Disposar de mesures per a **localització** del dispositiu o poder realitzar un esborrat remot en cas de pèrdua o robatori.
- Realitzar **còpies de seguretat periòdiques** (preferiblement diàries) de la informació continguda en el dispositiu. Aquestes còpies hauran de fer-se en un dispositiu diferent i a poder ser alocat en servidors de l'empresa o a la pròpia oficina.
- **Actualitzar el sistema operatiu i el programari** a les versions més recents abans de tractar dades personals.

Reforça la ciberseguretat: En una situació d'emergència social, la urgència i manca de temps poden fer-nos descurats, sobretot en el que a seguretat digital es refereix. Per això cal **prestar especial atenció i seguir les recomanacions en ciberseguretat** establertes per organismes oficials o per la mateixa empresa per tal d'assegurar-nos que no es filtrin dades personals o que siguem víctimes de ciberatacs. Alhora, recorda que **qualsevol escletxa de seguretat ha de notificar-se immediatament a l'empresa i a l'Agència andorrana de protecció de dades.**