Criteris específics de seguretat TIC i protecció de dades personals en el teletreball

La persona teletreballadora ha de garantir la confidencialitat i la seguretat de les dades i de la informació que utilitzi i a les quals pugui accedir, i evitar-ne per tots els mitjans possibles l'alteració, la pèrdua, el tractament, l'accés no autoritzat o l'ús inadequat.

La persona teletreballadora ha de complir amb la política de seguretat de la informació de la UPC i el Manual UPC de protecció de dades.

Pel que fa a la **seguretat informàtica i el teletreball**, cal seguir les indicacions establertes, que es poden trobar en aquest enllaç: https://serveistic.upc.edu/ca/eines-teletreball/documentacio/guia-teletreball.

Pel que fa a la **protecció de dades personals i el teletreball**, cal respectar les següents indicacions addicionals a les establertes al Manual UPC de protecció de dades:

- El tractament de dades personals s'ha de fer mitjançant els sistemes i serveis que la Universitat posa a disposició de les persones teletreballadores: https://serveistic.upc.edu/ca/treballa-en-remot. No s'han de tractar dades personals en serveis al núvol amb què la UPC no tingui un contracte establert, ja que es perd la traçabilitat d'aquestes dades, no hi ha garanties de com es tractaran i es posen en perill.

- No es poden compartir documents amb dades de caràcter personal amb les eines de teletreball (p. ex. Drive de G Suite) amb usuaris de fora del domini upc.edu sense una autorització expressa.

- No s'han de fer servir adreces de correu electrònic que no siguin de la UPC per enviar dades personals.

- En cas de fer servir adreces de correu electrònic genèriques de la UPC, per enviar dades personals, cal que el correu electrònic indiqui la identitat de la persona que ho envia.

- Tothom és responsable del seu lloc de teletreball i, per tant, ha d'adoptar les mesures necessàries per impedir l'accés de persones no autoritzades a la informació confidencial. La persona teletreballadora n'ha de mantenir la màxima reserva per un temps indefinit i no pot divulgar ni utilitzar dades, documents, metodologies, claus, anàlisis, programes, estudis o altres informacions pertanyents a la UPC, tant en suport paper com electrònic, ni directament ni mitjançant terceres persones o entitats. No s'ha de permetre l'accés a les dades personals o a informació confidencial a persones no autoritzades, i per això cal evitar tenir-les a l'abast d'altres persones.

- La persona teletreballadora té una contrasenya personal i intransferible per accedir als fitxers que continguin dades de caràcter personal. Aquesta contrasenya té caràcter confidencial, de manera que:

    - No és permès de revelar-la a ningú sense l'autorització expressa del cap o la cap.
    - Es recomana memoritzar-la i no anotar-la enlloc.
    - En cas que sigui coneguda per persones no autoritzades, s'ha de canviar.
    - En cas que la persona no recordi la contrasenya, s'ha de posar en contacte amb els serveis informàtics de la Universitat. (És important tenir cura de no emmagatzemar les contrasenyes al navegador.)

- L'usuari ha d'utilitzar les dades personals a les quals tingui accés únicament i exclusivament per a les finalitats previstes corresponents al lloc de treball i no barrejar-les amb dades o fitxers privats.

- Cal eliminar la informació temporal de les carpetes de baixades i la paperera de reciclatge o altres carpetes similars que hi pugui haver en directoris de l'ordinador (p. ex., a Documents) en el cas que excepcionalment s'hagi baixat documentació en local.

- Cal tancar les connexions als servidors i llocs web o intranets amb l'opció Desconnecta o Tanca la sessió.

- Quan la persona s'absenti del lloc de teletreball, haurà d'impedir l'accés d'altres persones no autoritzades a documents a la pantalla i en paper que continguin dades de caràcter personal. Pel que fa als equips informàtics, se'n pot impedir la visualització mitjançant protectors de pantalla. Pel que fa a la documentació en paper, s'ha d'emmagatzemar en un lloc segur mentre no s'utilitzi.

- No s'ha de destruir fora de la Universitat la informació en paper amb dades personals o confidencials. És molt important que no es llenci en contenidors de reciclatge i que no es reutilitzi com a paper reciclat a casa. La documentació amb dades personals i confidencials s'ha de destruir d'acord amb les indicacions de l'Arxiu UPC.

El personal notificarà qualsevol incident de seguretat informàtica o de protecció de dades personals al servei d'atenció a l'usuari ATIC – atic@upc.edu -- i seguirà les seves instruccions, entre les que es podrien contemplar el bloqueig o desconnexió de la xarxa del dispositiu.

Versió 24 de març de 2021