01/2020

CIRCULAR TELETREBALL I PROTECCIÓ DE DADES: RECOMANACIONS BÀSIQUES

En una situació d'excepcionalitat com la que estem vivint, el teletreball pot ser una opció professional per seguir realitzant l'activitat professional en un entorn diferent de l'habitual i mitjançant dispositius que no són els que habitualment utilitzes.

Que la situació sigui excepcional, però, no implica que es relaxin les normes i criteris que estableix el Reglament General de Protecció de Dades, més enllà d'aquelles actuacions directament vinculades amb la emergència de salut pública.

Per tant hi ha recomanacions que s'han de seguir:

- No deixis desatesos als equips portàtils en llocs públics.
- Usa contrasenyes per accedir-hi o altres sistemes que l'equip t'ofereixi (empremtes digitals)
- Sempre que puguis, i especialment si trametes categories especials de dades, utilitza tècniques criptogràfiques per la transmissió de la informació, usa contrasenyes, firewall i antivirus.
- Adopta controls necessaris i apropiats en el domicili: evita l'accés no autoritzat a la informació o recursos per part de familiars o amics. Bloqueja la pantalla de l'ordinador quan no estiguis treballant.
- No usis xarxes WiFi públiques.
- Vigila amb les memòries USB, ja que son una possible porta a les infeccions de malware.
- Evitar la instal·lació d'aplicacions o la navegació per pàgines no segures en el dispositiu que usis pel teletreball.
- Tancar totes les connexions amb servidors i webs usant l'opció "tancar sessió" o "desconnectar".
- Eliminar:
    - la informació temporal en carpetes de descarrega
    - la informació esborrada a la paperera de reciclatge,
    - Esborra l'historial de navegació
    - Esborra les cookies i altres dades
    - Esborra les contrasenyes recordades.
- En els equips personals, crea un perfil professional (utilitzant els serveis més habituals, com Google i Microsoft) per mantenir separats els comptes i la navegació.

- Si uses **TAULETES** o **SMARTPHONES** per teletreballar:
    - Usa el sistema de bloqueig per accedir-hi que t'ofereix el dispositiu (contrasenya, patró, empremta digital, reconeixement facial o similar)
    - Activa les aplicacions o funcionalitats per localitzar el dispositiu o poder realitzar un esborrat remot en caso de pèrdua o robatori.
    - Realitzar o activa el sistema de copies de seguretat de la informació continguda al dispositiu.
    - Actualitza el sistema operatiu i el software a les versions més recents.
    - Instal·la un antivirus o mesures per prevenir i detectar el malware.
    - Inhabilita les connexions inhlàmbriques que no s'usin (Bluetooth, NFC o WiFi).

I en qualsevol cas recorda:

1. **Si treballes connectat a través del núvol o remotament, al sistema d'informació de la teva organització, no facis copies al teu dispositiu personal de les dades sobre les que treballes. No retiris del sistema la informació, ja que tota informació que treus del sistema la treus de la protecció del sistema.**

2. **La protecció de dades no s'ha d'utilitzar per obstaculitzar o limitar l'efectivitat de les mesures que adoptin les autoritats, especialment les sanitàries, en la lluita contra la pandèmia.**

Podeu tenir en compte, les normes que va publicar l'Agència de Ciberseguretat de Catalunya, en relació a les mesures de ciberseguretat per a la prestació de serveis en la modalitat de teletreball, adreçat als treballadors de la Generalitat de Catalunya i el seu Sector Públic DOCUMENT

Serveis de Protecció de Dades
Codi Tipus
Fundació Unió Catalana d'Hospitals
coditipus@uch.cat

Barcelona, 17 de març de 2020