ÍNDEX

1. Recomanacions generals sobre seguretat

La política de seguretat de la informació del Departament de Justícia es recull al Document de seguretat, que pots consultar al següent enllaç:

https://espai.justicia.gencat.cat/Que-em-cal-saber/Proteccio-dades-personals/Serveis-informacions-relacionades-proteccio-dades-Departament/Documents/doc_28834698_1.pdf

2. Bones pràctiques per accedir a l'entorn de justícia des de dispositius personals

A més de les mesures de seguretat que es traslladen en les Normes de Seguretat per al Teletreball, es reiteren un conjunt de pràctiques de ciberseguretat a aplicar en el treball a través de dispositius personals que tractin dades corporatives:

- Tenir **actualitzats els dispositius** en els que s'executin les aplicacions corporatives, tant pel que fa a versions de sistema operatiu, com per les seves actualitzacions de seguretat periòdiques
- És molt recomanable **disposar d'un sistema antivirus** per a la detecció i eliminació de virus informàtics (per exemple, del ransomware), i procurant que aquest **sempre** estigui **actualitzat**
- Si descarregueu **aplicacions als vostres dispositius personals**, procureu que aquestes es facin **només** des de la pàgina web del fabricant o botigues **oficials** per a minimitzar l'entrada de softwares maliciosos
- En el cas d'utilitzar **contrasenyes en l'entorn virtualitzat**, cal vetllar per a què aquestes siguin **el més robustes possible**: majors a 8 caràcters, alfanumèriques, símbols i, a poder ser, que no tinguin paraules de diccionari. Considereu també la **revisió** de les vostres **contrasenyes** i la seguretat en l'accés a la xarxa **WIFI**
- Cal tenir cura de qui pot accedir la informació en la ubicació del dispositiu personal, pel que és recomanable disposar d'un **control d'accés al dispositiu** en el que s'executi l'aplicació (contrasenya, empremta, etc.)

També s'ha de tenir en compte que, a banda del nivell de seguretat de la infraestructura domèstica, cal extremar les precaucions en els possibles fraus als que estem exposades com a persones usuàries:

- **Casos de frau** per correu, SMS, apps de missatgeria o trucada telefònica, o el concepte conegut per **phishing**. En el phishing, els atacants intenten enganyar als usuaris per a què introdueixin les seves credencials en pàgines suplantades o que instal·lin programari, de manera que obtenen les credencials o el control de l'equip. Cal ser **escèptics i desconfiar de qualsevol emissor o contingut** que pugui semblar **sospitós**
- **El frau ha augmentat amb** la situació de la **pandèmia** a través de diferents mitjans (correus electrònics, mapes de seguiment fraudulents, SMS de falses campanyes, etc.)

Penseu en el vostre dispositiu personal **com una nova finestra de casa que permetrà l'accés** d'una forma més o menys senzilla a persones no autoritzades **segons com el tinguem protegit.**