

Darrerament, n'hi ha hagut molts i de molt variats. Afecten empreses que operen a gran escala, però també a petites entitats, de caire més local. En un món eminentment globalitzat, ningú està lliure de patir aquests atacs cibernètics.

Com podem minimitzar els seus efectes? Primer de tot, cal **tenir actualitzats els equips**, perquè no quedin al descobert i s'aprofitin les vulnerabilitats presents en velles versions de certs programes i aplicacions del nostre sistema. És convenient, també, **realitzar còpies de seguretat** dels sistemes **amb freqüència**. Si els nostres equips queden bloquejats per un ciberatac, podrem recuperar l'última còpia de seguretat realitzada. Finalment, cal tenir present que **aquestes còpies han d'estar emmagatzemades fora de la xarxa** a la qual es connecten els treballadors d'una empresa i que, per tant, pot rebre moltes ingerències exteriors. **En** aquest sentit, és aconsellable utilitzar **discs durs externs** que només es connectin a l'equip quan fem les còpies de seguretat.

Tot i aquests consells, empreses públiques com SEPE o despatxos professionals de tot el món, no han pogut evitar problemes en la gestió de les seves dades per culpa de ciberatacs. En alguns casos, es demanen rescats econòmics per descriptar i restablir el bon funcionament. **És**, per tot això, **un bon moment per apostar per la ciberseguretat**.