La seguretat de l'espai

És important garantir la permanència i la seguretat de la informació que publiquem. Per norma general les aplicacions funcionen correctament, però cal poder preservar, com a mínim, la informació més essencial de la nostra activitat en cas que hi hagi un malfuncionament. Per aquest motiu es recomana fer una còpia de seguretat del contingut del l'espai digital de la biblioteca com a mínim un cop l'any, normalment en acabar el curs, sempre i quan hi hàgim introduït canvis.

En el cas de la biblioteca digital és recomanable tenir una carpeta amb el títol "Documentació BD" on es guardi una còpia de les imatges dels recursos, les descripcions i els enllaços (en un full de càlcul, per exemple) i l'última còpia de seguretat de l'espai digital. Aquesta carpeta es pot guardar en local a l'ordinador, a la xarxa del centre, en una memòria externa i al núvol del compte de la biblioteca.

Ciberseguretat: no guardeu mai els noms d'usuaris ni les contrasenyes de les aplicacions al núvol. Cal que les custodiï l'equip directiu del centre.

La copia de seguretat cal fer-la en el moment de posada en marxa i, després, un cop cada curs. El procediment de copia de seguretat dels blogs és força senzill i intuïtiu, tant per la plataforma blocs.xtec com la de blogger.

La custòdia de la carpeta de BD haurà de ser compartida entre la persona responsable de la biblioteca, la direcció del centre i les persones de la comissió de la biblioteca.

Una estratègia de centre per a un ús més segur de la xarxa que, amb seguretat, s'acordarà des de la Comissió d'estratègia digital del centre, hauria d'incloure, a més:

- Configuració: la correcta configuració dels elements de seguretat del sistema operatiu i dels navegadors que utilitzem.

- Antivirus: l'ús d'antivirus permanentment actualitzats per prevenir la constant proliferació i mutació de codis maliciosos. N'hi ha de gratuïts, per a executar des de l'escriptori del nostre ordinador –com AVG-Antivirus o BitDefender- i per a utilitzar directament en línia –com els que ofereix Panda Software o Trend- Micro-. És recomanable, en tot cas, utilitzar també un antivirus resident –instal·lat al nostre ordinador- i particular –de pagament- que ens asseguri una actualització permanent i garantida dels mitjans que protegeixen el nostre ordinador contra atacs provinents de l'exterior.
- Tallafocs: el reforç preventiu del nostre ordinador amb utilitats com tallafocs, que controlen i regulen l'accés a l'ordinador a través de la connexió, i programes detectors de codis maliciosos que poden provocar fuites incontrolades d'informació del nostre terminal.
- Fonts informatives: la consulta periòdica de fonts informatives sobre seguretat que alerten de noves amenaces i proporcionen instruments per fer-hi front.