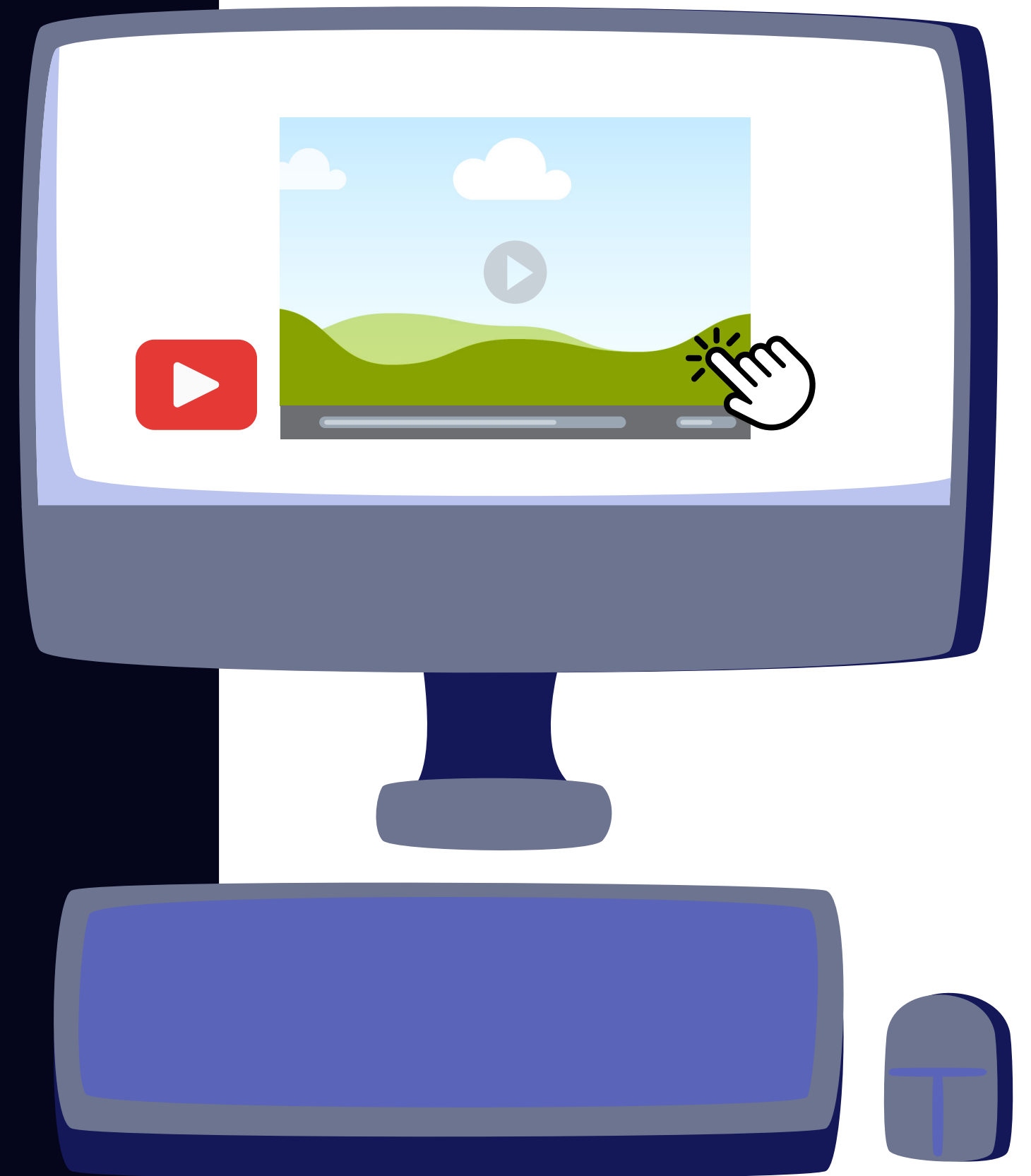
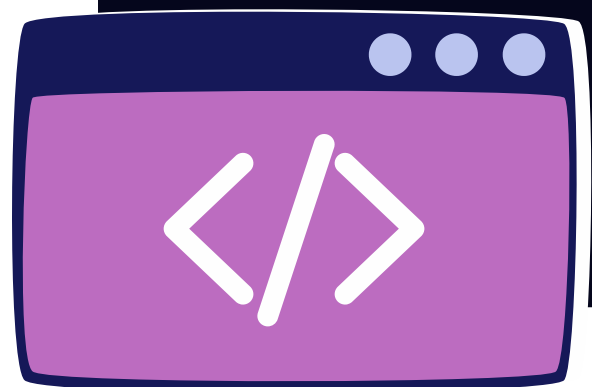


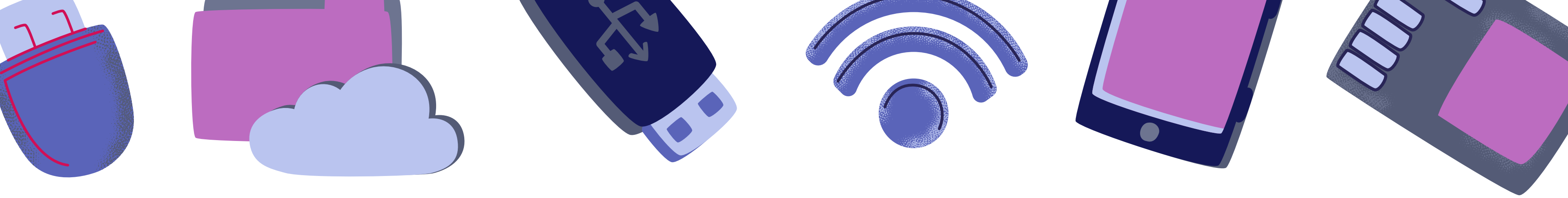
UT5. LA CIBERSEGURETAT



Introducció

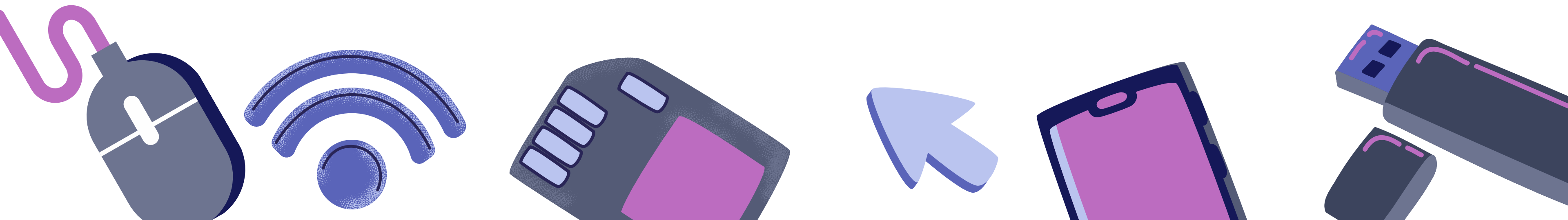
En l'era de la digitalització, on gran part de la nostra informació es transllada a l'espai digital, és crucial que s'apliquin mesures de protecció als sistemes informàtics.
És del que s'ocupa la *ciberseguretat*





CIBERSEGURETAT

La **ciberseguretat** es defineix com el conjunt de tècniques i pràctiques que protegeixen els sistemes de computació, les xarxes i les dades digitals.





Per què és important la ciberseguretat?

01. PROTECCIÓ DE DADES PERSONALS

En un món cada vegada més digital, moltes persones tenen informació personal, financera i metgessa emmagatzemada en sistemes en línia. Un atac a la seguretat pot donar accés a aquesta informació sensible, la qual cosa pot portar a robatoris d'identitat, frau o violacions de privacitat.

02. PROTECCIÓ DE CIBERDELICTES

Els ciberdelinqüents utilitzen diverses tàctiques, com phishing, per a robar dades, segrestar sistemes o extorquir a les persones o organitzacions. La ciberseguretat protegeix contra aquests atacs, que poden tenir conseqüències devastadores tant per a individus com per a empreses.



Per què és important la ciberseguretat?

03. PROTECCIÓ DE LA INFRAESTRUCTURA CRÍTICA

Les infraestructures com a xarxes elèctriques, sistemes de transport, hospitals i serveis financers depenen de sistemes tecnològics. Un atac reeixit a aquests sistemes pot paraitzar serveis essencials i posar en risc la seguretat pública.

04. GARANTIR LA CONTINUÏTAT DEL NEGOCI

Per a les empreses, les bretxes de seguretat poden afectar greument la seva operativitat, danyant la reputació, interrompent operacions i fins i tot resultant en pèrdues econòmiques. Tenir mesures de ciberseguretat efectives ajuda a prevenir aquests riscos i a assegurar que els negocis puguin continuar funcionant fins i tot en cas d'un atac.



Per què és important la ciberseguretat?

05. COMPLIMENT NORMATIVES LEGALS

Moltes indústries estan subjectes a lleis i regulacions estrictes sobre la protecció de dades (com el GDPR a Europa). L'incompliment d'aquestes normatives pot implicar moltes severes i sancions.

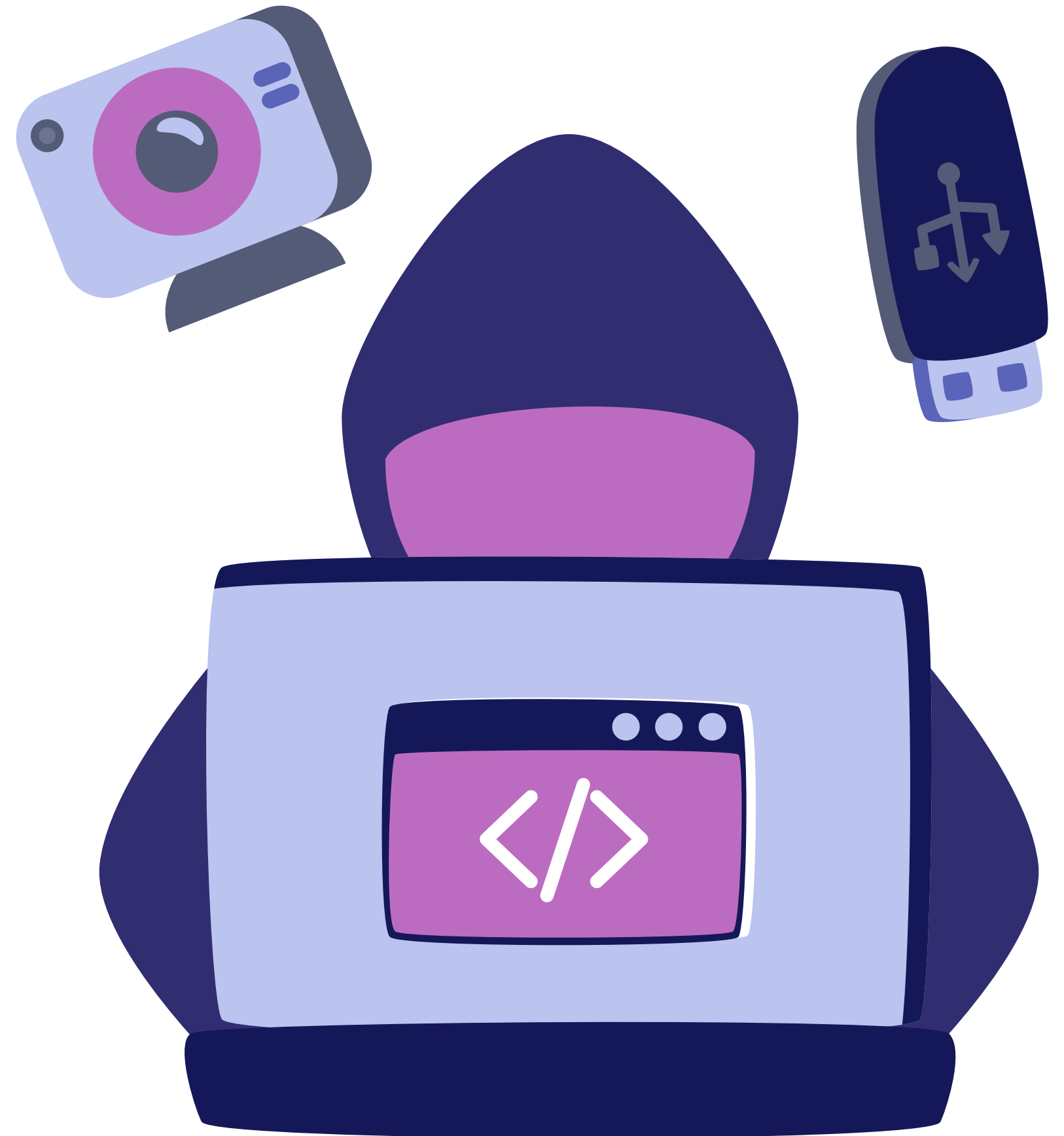
06. CONFIANÇA DELS USUARIS

Els consumidors, clients i usuaris de serveis esperen que les seves dades estiguin segures. La ciberseguretat adequada contribueix a guanyar la confiança dels usuaris, la qual cosa és fonamental per a la fidelitat a llarg termini i l'èxit de qualsevol empresa que manegi informació personal o financera.

CIBERSEGURETAT

És fonamental que totes les empreses comptin amb un pla director de seguretat que detalli les estratègies per protegir els recursos digitals.

Cada persona té la responsabilitat d'adoptar pràctiques segures. A continuació es detallen les més rellevants.



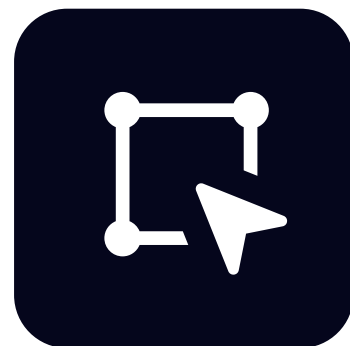


PRÀCTIQUES SEGURES



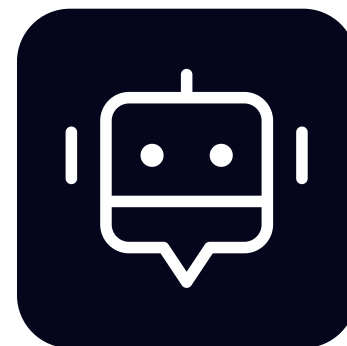
Fer servir constrasenyes fortes i úniques

Optar per combinacions de lletres, números i símbols, i canviar-les regularment.



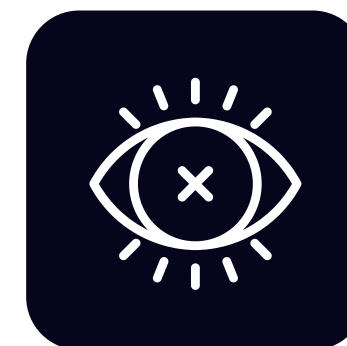
Actualitzar el programari

Instal·lar actualitzacions de seguretat tan aviat com estiguin disponibles.



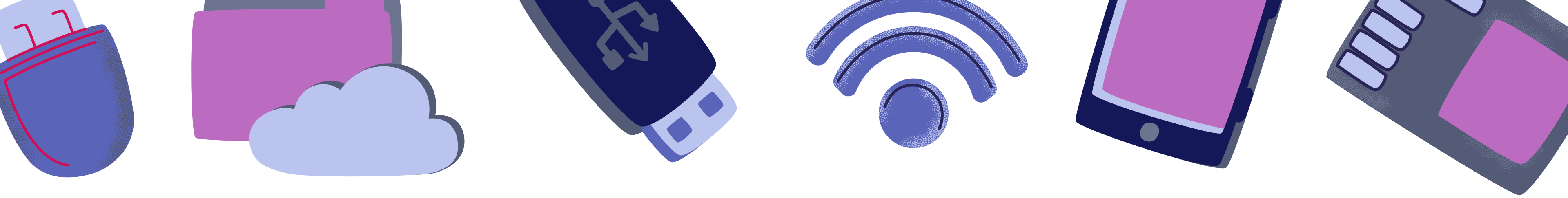
Evitar l'ús de xarxes wifi públiques

Fer servir connexions segures quan s'accedeix a informació confidencial des de fora l'oficina.



Vigilar els correus sospitosos

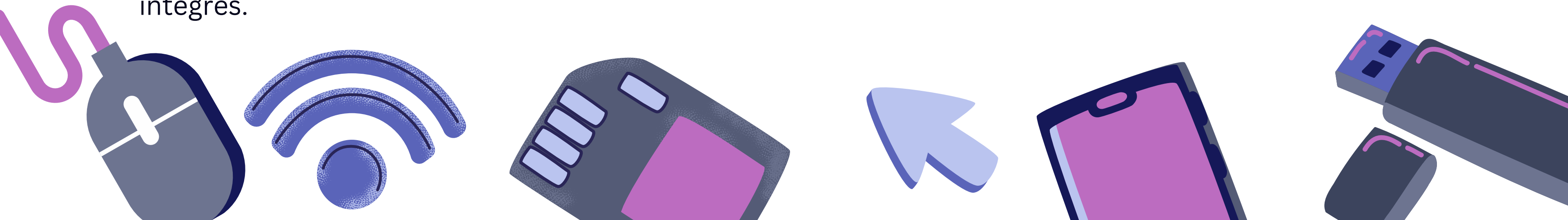
Evitar obrir correus no sol·licitats o descarregar fitxers de fons desconegudes.



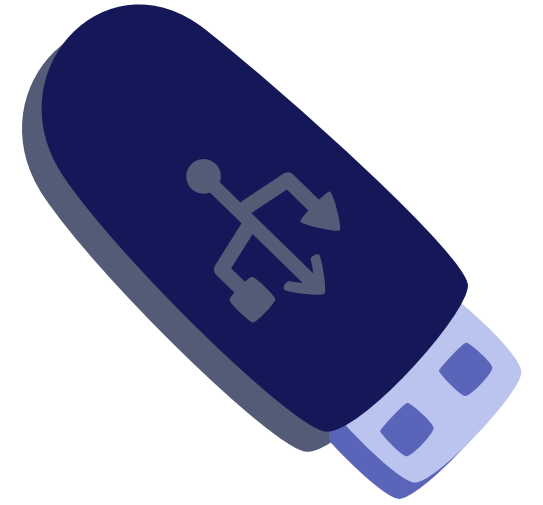
CIBERSEGURETAT VS. CIBERDEFENSA

La **ciberseguretat** és un enfocament **preventiu** que s'enfoca a protegir sistemes informàtics, xarxes, dispositius i dades contra accessos no autoritzats, atacs o danys. El seu objectiu principal és protegir la infraestructura digital d'amenaques i assegurar que la informació i els serveis estiguin disponibles, siguin confidencials i íntegres.

La **ciberdefensa** va un pas més enllà de la ciberseguretat i té un enfocament més reactiu i militaritzat. En lloc de centrar-se només en la protecció de la infraestructura digital, la ciberdefensa s'involucra a respondre als atacs cibernètics de manera activa i en alguns casos fins i tot a contraatacar.

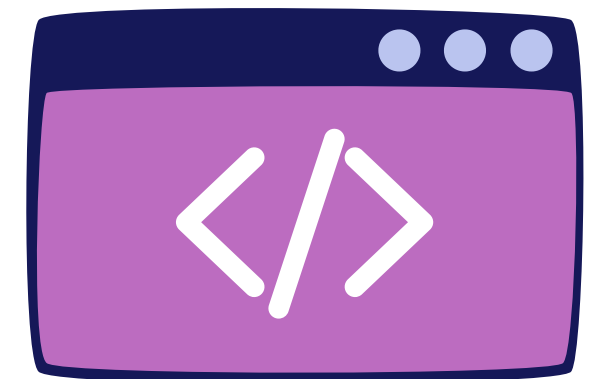


AMENACES CIBERNÈTIQUES



Les **amenaces cibernétiques** són qualsevol tipus de perill que pot afectar la seguretat d'un sistema informàtic, xarxa o dades. A mesura que la tecnologia avança, també ho fan les tècniques dels atacants. Algunes de les amenaces cibernètiques més comunes inclouen:

- **MALWARE**
- **RANSOMWARE**
- **PHISHING**



AMENACES CIBERNÈTIQUES

- **MALWARE:** és un terme general que inclou qualsevol tipus de programari dissenyat per danyar o obtenir accés no autoritzat a un sistema informàtic (**virus**).
- **RANSOMWARE:** és un tipus de malware dissenyat per encriptar fitxers o bloquejar l'accés a un sistema, i els atacants exigeixen un rescat (normalment en criptomonedes com el Bitcoin) per desbloquejar-los.
- **PHISHING:** és una tècnica d'engany on els atacants intenten obtenir informació sensible (com contrasenyes, números de targeta de crèdit o dades bancàries) a través de comunicacions falses, sovint correus electrònics, que semblen provenir de fonts legítimes.



ACT1. PÒSTER

En grups, elaboreu un pòster per conscienciarde la importància de la ciberseguretat per infants de 5è i 6è EP.

- Fer un pòster és una tasca creativa que ha de ser visualment atractiva, clara i efectiva en la transmissió d'un missatge.
 - Determina el missatge principal que vols comunicar.
 - Considera a qui va dirigit el pòster. Això t'ajudarà a triar l'estil visual, el to i la complexitat del missatge.
- 