



Unitat de programació 2 - Estic segur/a al món digital?	
Competències específiques	
CE 2 Valorar i preveure els riscos per a la salut i la seguretat dels dispositius i les dades personals, identificant les principals amenaces per tal de saber fer-ne un ús segur, saludable i legal.	
Criteris d'avaluació	
CA 2.2 Configurar i actualitzar contrasenyes, sistemes operatius i antivirus de manera periòdica en els diferents dispositius digitals d'ús habitual. CA 2.3. Identificar i saber reaccionar davant situacions que representen una amenaça a la xarxa triant la millor solució entre diverses opcions i valorant el benestar personal i col·lectiu.	
Sabers bàsics	
D. Ciutadania digital crítica i seguretat ● Cerca i selecció d'informació fiable. Eines per detectar notícies falses i frauds. Ús crític de les xarxes. ● Seguretat i protecció de dades. Mesures preventives (gestió de contrasenyes, còpies de seguretat). Identitat, reputació i empremta digitals. ● Seguretat dels dispositius. Mesures preventives i correctives per fer front a riscos, amenaces i ciberatacs.	
Dinàmica de presa de consciència	
Joc inicial: Contrasenya més forta - Joc en grups petits. Cada alumne crea una contrasenya; després es passen a un generador/test de fortaleza (per exemple How Secure is My Password, o eines similars). - Repte: guanya qui crea la contrasenya més segura però fàcil de recordar (es poden puntuar la seguretat i la creativitat). - Mini-debat: Què fa que una contrasenya sigui segura? Per què costa recordar-les? - Tasca curta: fer una "frase-contrasenya" a partir d'una dita, cançó o llibre favorit.	
Seqüència d'activitats i/o situacions d'aprenentatge	
Sessió	Planificació activitats
1	- Dinàmica inicial
2	- Contrasenyes febles i errors habituals: anàlisi de llistes de contrasenyes més comunes (ex. 123456, qwerty, password...). - Exercici pràctic: els alumnes reben targetes amb contrasenyes fictícies i han de classificar-les (febles, mitjanes, fortes) i millorar-les.



	- Reflexió guiada: què passa si reutilitzes la mateixa contrasenya en moltes apps?
3	Els dispositius també es protegeixen • <i>Importància d'actualitzar sistemes operatius i apps.</i> • <i>Funció dels antivirus i dels escaneigs periòdics.</i>
4	Perills digitals: el costat fosc de la xarxa • Anàlisi de missatges fraudulents (phishing, SMS, emails) → distingir els reals dels falsos. • Exercici de "<i>Troba la trampa</i>": missatges editats amb errors típics (links sospitosos, ortografia, urgència...). • Debat sobre experiències pròpies o casos coneguts.
5	Tipus de ciberatacs i com reaccionar-hi • Explicació amb exemples visuals de malware, ransomware, phishing, doxxing, etc. • Activitat: cada grup rep un "cas" i ha de representar com reaccionaria (role play curt). • Conclusió: "<i>Què faig si em passa a mi?</i>".
6	Seguretat en xarxes Wi-Fi
7 - 10	Creació de presentació multimèdia sobre els tipus de ciberatacs i com protegir-nos
11 - 12	Presentació individual de la presentació a l'aula
Producte final	
Creació de presentació multimèdia sobre els tipus de ciberatacs i com protegir-nos.	
Mesures d'atenció a les necessitats individuals	



• Adaptació de tasques segons les habilitats de cada alumne. • Supervisió individualitzada durant les sessions.
Estratègies didàctiques i metodològiques
• Aprenentatge basat en projectes (ABP) amb producte final. • Metodologies actives • Treball cooperatiu. • Autoavaluació i coavaluació.
Materials i recursos
Materials: - Presentació contrasenyes segures. - Documents imprimibles contrasenyes segures: base i targetes. Recursos: - Ordinador amb connexió a internet. - Compte de Google Workspace for Education - Documents de Google
Avaluació i qualificació
S'avaluarà a l'alumne mitjançant la observació directa a classe i les qualificacions de les tasques i del producte final.