

Que no t'enganin! Trivial de la Ciberseguretat

Competències específiques i criteris d'avaluació vinculats.

Competència específica 1 a desenvolupar

2. Configurar l'entorn personal d'aprenentatge interactuant i aprofitant els recursos de l'àmbit digital per optimitzar i gestionar l'aprenentatge permanent.

Aquesta competència específica es connecta amb els següents descriptors del perfil de sortida: CD1, CD2, CD3, CPSAA1, CPSAA4, CPSAA5, CE3.

Criteri d'avaluació

2.3. Crear, integrar i reelaborar continguts digitals de manera individual o col·lectiva, seleccionant les eines més apropiades per generar nou coneixement i continguts digitals de manera creativa, respectant drets d'autor i llicències d'ús.

Competència específica 2 a desenvolupar

3. Desenvolupar hàbits que fomentin el benestar digital, aplicant mesures preventives i correctives per protegir dispositius, dades personals i la pròpia salut.

Aquesta competència específica es connecta amb els següents descriptors del perfil de sortida: CCL3, STEM5, CD1, CD4, CPSAA2, CPSAA5, CC2 i CC3.

Criteri d'avaluació

3.3. Identificar i saber reaccionar davant situacions que representen una amenaça en la xarxa triant la millor solució entre diverses opcions i valorant el benestar físic i mental, tant personal com col·lectiu.

Competència específica 3 a desenvolupar

4. Exercir una ciutadania digital crítica coneixent les possibles accions que es poden realitzar a la xarxa, i identificar les seves repercussions per fer un ús actiu, responsable i ètic de la tecnologia.

Aquesta competència específica es connecta amb els següents descriptors del perfil de sortida:

CD3, CD4, CPSAA1, CC1, CC2, CC3, CC4, CE1.

Criteri d'avaluació

4.2. Reconèixer les aportacions de les tecnologies digitals en les gestions administratives i el comerç electrònic, sent conscient de la bretxa social d'accés, ús i aprofitament d'aquestes tecnologies per a diversos col·lectius.

Sabers bàsics

- Desenvolupament d'aplicacions senzilles per a dispositius mòbils.
- Seguretat de dispositius. Mesures preventives i correctives per fer front a riscos, amenaces i atacs a dispositius.
- Seguretat i protecció de dades. Identitat, reputació, privacitat i empremta digital. Mesures preventives. Configuració en xarxes socials. Gestió d'identitats virtuals.
- Seguretat en la salut física i mental. Riscos, amenaces al benestar personal. Opcions de resposta. Situacions de violència i de risc en la xarxa.
- Comerç electrònic: factures digitals, formes de pagament.

Context o contextos

Personal i escolar.

Dinàmiques de presa de consciència

Avui dia és tan quotidià l'ús d'internet en totes les seves dimensions que a vegades se'ns escapen certes precaucions que en la vida real prendríem. A cap de nosaltres se'ns passaria pel cap penjar a la porta de casa nostra que som de vacances o dur penjat pel carrer un rètol amb el nostre nom, la nostra data de naixement o la nostra professió. En canvi, aquestes mateixes dades sí que s'exposen amb certa imprudència en el context de les xarxes socials. Preservar la nostra privacitat així com prendre certes precaucions en compres online, contrasenyes i dispositius és important per evitar ser víctimes de delictes informàtics.

Instruccions i material

Per dur a terme aquesta activitat s'aconsella que es treballin en equips cooperatius formats per parelles. És necessari almenys un

ordinador per parella amb connexió a Internet i que algun dels dos disposi d'un dispositiu mòbil amb sistema operatiu Android on provar l'aplicació resultant. Si els alumnes tenen un dispositiu IOS poden fer proves a casa on probablement tendran a la mateixa xarxa wifi tant l'ordinador com el mòbil, però no en el centre educatiu ja que la xarxa wifi només permet un dispositiu per usuari.

Descripció i planificació de la tasca o tasques. Tipus i característiques del producte o productes obtinguts

El producte final és una aplicació feta amb [AppInventor](#). AppInventor pot ser usat per via web i és un entorn molt potent del MIT (Massachusetts Institute of Technology) per crear aplicacions mòbils mitjançant un llenguatge visual de blocs de programació. En aquest cas, l'aplicació en qüestió no és més que un joc de preguntes i respostes sobre la ciberseguretat. A la xarxa, hi ha implementats exemples semblants.

Pel que fa a l'elaboració de les preguntes, no seria estrictament necessari elaborar-ne cap, ja que el joc ja està preparat a la pàgina web de l'[OSI](#) (Oficina de Seguridad del Internauta) des d'on es pot descarregar. Amb tot, si es vol incidir o incloure algun aspecte concret, l'equip pot afegir les preguntes que consideri oportunes. La web de l'OSI ofereix informació fiable i actualitzada de quins són els principals fraus i riscos que es poden trobar a la xarxa. El nivell d'exigència en l'aplicació el podem graduar en funció del nivell de l'alumnat amb AppInventor. L'exigència mínima és que han de fer un aplicatiu que permeti jugar contestant les preguntes, sabent quan s'encerta i quan no i en dugui un recompte. L'alumnat, que pot implementar el joc en equips de dues persones, haurà d'introduir les diferents preguntes en l'aplicació. Quedarà a criteri seu però, si volen crear un dau que indiqui la puntuació a sumar, o un dau de colors que indiqui el tipus de pregunta que toca contestar o un tauler per on desplaçar-se... Si el volen fer multijugador o no. Evidentment a

més nivell de complexitat, millor valoració tendran en aquesta part.

Procediments de retroacció, revisió i supervisió per part del professorat durant la realització de la tasca o tasques

En aquesta situació el docent primer entra en un diàleg amb l'alumnat sobre quina ha estat la seva experiència a la xarxa en tema de ciberseguretat. Si han sofert en primera persona o de manera molt propera algun incident que vulguin compartir amb els companys. Després es mostren i comenten alguns dels continguts interessants que es poden trobar dins la web de l'oficina de seguretat de l'internauta. Una vegada familiaritzats amb la pàgina, es fa una ullada al trivial que hi apareix i se'ls explica el producte final i com s'avaluarà. Aleshores s'acompanya l'alumnat a entrar a la web d'AppInventor i conjuntament fan una petita demostració d'un aplicatiu molt senzill. Per exemple, fer un dau que mostri una cara diferent de manera aleatòria o fer clic a la foto d'un animal i que aquest faci el renou

propi de l'animal. Es prova de passar l'app al mòbil i si no hi ha dubtes, endavant!

Procediment d'avaluació final, qualificació i transferència del coneixement

L'avaluació final tindrà dues vessants. Per una banda un examen de tipus test amb les preguntes de l'aplicatiu amb les quals prèviament l'alumnat s'haurà «entrenat» jugant. Amb aquest test es valoren els criteris d'avaluació vinculats a les competències 2 i 3. I una segona vessant avaluada mitjançant una rúbrica en què es valora el funcionament, l'estètica i la jugabilitat de l'aplicatiu creat i que s'emprarà per avaluar la primera de les tres competències a treballar. Pel que fa a la transferència del coneixement, les preguntes del joc són, en aquest cas, relacionades amb ciberseguretat però podrien ser de qualsevol altre àmbit/matèria amb què es volgués col·laborar per treballar-ne els seus continguts.