

Proposta d'hackatò educatiu en seguretat informàtica i ètica per a alumnes de 4t de l'ESO

Màster Universitari en Professorat d'Educació Secundària Obligatòria i Batxillerat, Formació Professional i Ensenyament d'Idiomes

Facultat d'Educació

Treball Fi de Màster

Autor:

Jose Luis Lucas Palaci

Tutor/es:

Maria Teresa Signes Pont

Juliol 2021



Universitat d'Alacant
Universidad de Alicante

Índex

1. Introducció	4
1.1. Definició de la problemàtica:	4
1.2. Conceptes clau:	6
1.3. Proposta	8
1.4. Objectius.....	8
2. Fonamentació teòrica	9
2.1. Motivació en els aules.....	9
2.2. La gamificació com a recurs didàctic motivador	10
3. Proposta d'hackatò	11
3.1. Per que un hackatò?.....	11
3.2. Contextualització.	13
3.3. Competències i continguts didàctics a desenvolupar	16
3.4. Objectius didàctics	17
3.5. Metodologia	17
3.6. Atenció a la diversitat de l'alumnat.....	18
3.7. Desenvolupament de la proposta de hackatò	18
3.7.1. Definició d'objectius i reptes.....	20
3.7.2. Recursos disponibles.....	20
3.7.3. Pla de continuïtat	21
3.7.4. Materials didàctics	21
3.8. Avaluació	21
3.8.1. Avaluació de l'alumnat	21
3.8.2. Avaluació del professorat.....	23
4. Conclusions i propostes de futur	24
5. Referències bibliogràfiques.....	26
6. ANNEX	27

Índex de taules i figures

Taula 1: Relació del currículum amb les activitats i competències	15
Taula 2 Planificació temporal de l'activitat.....	19
Taula 3: Test d'autoavaluació	22
Taula 4: Qüestionari de satisfacció	23
Fig. 1: Ús de les TIC en la població 16-74 anys. Dades de l'INE 2021	4

1. Introducció

1.1. Definició de la problemàtica:

A hores d'ara, cada dia és més freqüent l'ús de noves tecnologies; quasi tots els habitants del planeta tenen aparells electrònics que usen la connexió internet; la gran majoria dels usuaris són menors d'edat i, per tant, no saben el perill que comporta el mal ús d'aquests dispositius.

A Espanya, segons dades de l'Institut Nacional d'Estadística (INE), el 2021, d'una població d'entre 16 i 74 anys, el 93,2% ha utilitzat internet en els tres últims mesos, el 83,1% en fa ús diàriament i el 53,8% ha fet una compra per internet en els últims 3 mesos, com es mostra en la Figura 1.

Frecuencia de uso de Internet por las personas de 16 a 74 años. Año 2020

Porcentajes de población de 16 a 74 años

	Últimos 12 meses	Últimos tres meses	Semanalmente	A diario	Varias veces al día
Año 2020	93,5	93,2	91,3	83,1	81,0
Año 2019	91,0	90,7	87,7	77,6	74,9

Uso de TIC por las personas de 16 a 74 años

Porcentajes de población de 16 a 74 años

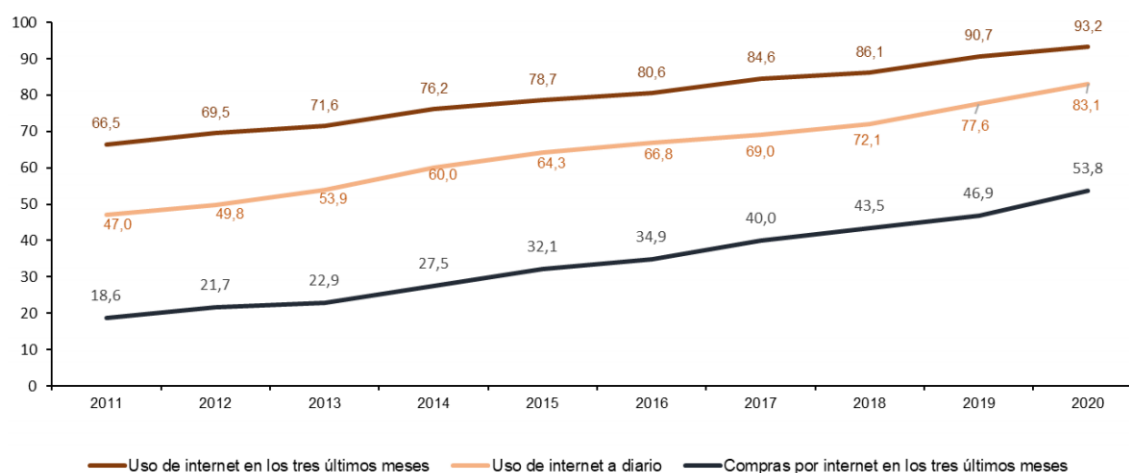


Fig. 1: Ús de les TIC en la població 16-74 anys. Dades de l'INE 2021

En un entorn on predominen les 'fake news', els phishing, els ransomwares i mil enganyifes que els "crackers" usen indiscriminadament, crec que és oportú la introducció de temes de ciberseguretat en el dia a dia de l'alumnat, familiars i docents, atés que un bon coneixement pot evitar molts dels problemes que hi ha avui en dia en aquesta qüestió.

"Un jove que tinga certes pautes i hàbits de ciberseguretat es convertirà en un adult que ja els té assimilats, i ho posarà més difícil als delinqüents" [1]

En aquest any tan difícil de pandèmia, l'ús de les noves tecnologies s'ha incrementat substancialment, i amb ell tot tipus d'atacs, segons l'informe 2021 Webroot BrightCloud® Threat Report, el 2020 els atacs de phishing han augmentat un 34,4% i els atacs de programari maliciós un 86,1%. Els atacs dedicats als telèfon intel·ligent Android presenten un increment del 92,2% respecte al 2020, i el 90% d'aquestes infeccions són per no tindre actualitzat el sistema operatiu. D'altra banda, el 53% de les empreses espanyoles han patit un atac de ransomware, ja no sols en l'àmbit privat sinó també en el públic. Només cal recordar que el Servei Públic d'Ocupació Estatal va estar 2 mesos sense donar servici [2] i l'ajuntament de Castelló de la Plana també ha tingut problemes d'aquest tipus. [3].

En la meua experiència en les pràctiques realitzades, he observat que la gran majoria de l'alumnat no tenia ni idea de cap tema relacionat en la seguretat informàtica, principalment per la desinformació que hi ha sobre aquest tema generalment, causada per els mitjans de comunicació, un clar exemple són:

- El concepte de hacker, l'alumnat té la concepció que és un concepte maligne en quant hi ha de bons.
- Les contrasenyes que usualment utilitzen són el seu nom, o el nom de la seva parella, del gos, etc...
- Cap d'ells utilitzen una verificació en dos passos.
- Habitualment es connecten a xarxes sense fils públiques sense cap tipus de protecció.
- No saben realment com tracten les principals companyies de xarxes socials les seves dades.
- No realitzen cap comprovació de si les webs són perilloses o il·legals.

- Descarreguen continguts multimèdia de xarxes p2p sense cap mena de seguretat.
- Parlen de la deepweb com a un concepte que és divertit.
- No coneixen els conceptes de malwares, phishing, correu brossa, entre altres.

Una causa possible d'aquesta desinformació és el caràcter abstracte del concepte que dificulta a la gran majoria de la població poder indagar en el tema. No obstant això, en parlar-ne en classe de pràctiques, l'alumnat es va mostrar interessat, atès que ells són els que més utilitzen el telèfon intel·ligent, el correu electrònic i els ordinadors en el seu dia a dia.

1.2. Conceptes clau:

Algunes de les preguntes més importants que ens podem plantejar en aquest tipus de tema es:

- Seguretat de la informació: Què és?
Dit de la forma més senzilla possible, són les mesures preventives per a protegir la informació.
- Seguretat informàtica: Què és?
Són les mesures que s'adopten per tal de protegir la integritat i la privacitat de la informació emmagatzemada en un sistema informàtic, que suposen un risc si aplega en mans d'altres persones.
- Ciberseguretat: Què és?
És la capacitat per a minimitzar el risc a què està exposat la informació davant d'amenaques o incidents de naturalesa cibernètica. La principal feina és la protecció de la informació digital.
- Phishing:
És un tipus d'estafa que consisteix a obtenir de forma fraudulenta les dades bancàries a través d'internet. L'estafador es fa passar per una persona o empresa de confiança en un aparent comunicat oficial.
- Malwares:
És un terme ampli que descriu qualsevol programa o codi que siga maliciós per als sistemes informàtics.

- Ransomwares:

És un tipus de programari maliciós que restringeix l'accés a les dades, xifrant el contingut i demanat un rescat per a l'alliberament.

- Hacker:

És una persona que és apassionada per la informàtica, té un gran coneixement de les xarxes i dels sistemes informàtics, es dedica a explotar les característiques i posa a prova els sistemes per a descobrir vulnerabilitats. Hi han diferents tipus de hackers:

- ❖ White Hat: Són els encarregats de protegir els sistemes, la seua principal funció és la de trobar diferents forats en els sistemes.
- ❖ Black Hat: És també conegut com a cracker, la seua habilitat és la de trencar sistemes de seguretat i tindre accés a zones restringides, ho fan per benefici personal o d'altres, el 99,99% dels casos són per a lucrarse.
- ❖ Grey hat: No tot pot ser o blanc o negre, està el gris, en aquest cas és una mescla dels dos anteriors. Són capaços de trencar un sistema de forma il·legal, però sempre amb bones intencions. També solen obtenir informació de forma il·legal, i fer-la pública.
- ❖ Red Hat: Són els hackers menys coneguts, són els que actuen desapiadadament cap als Black hat els intercepten i trenquen els sistemes dels intrusos.
- ❖ Blue Hat: Són aquells que realitzen consultories informàtiques, provant els errors d'un sistema abans que es publiqui.
- ❖ Hactivist: Són hackers novençans amb una posició social, ideologia o política determinada, que utilitzen la tecnologia per a ser activistes. Un exemple dels més famosos és Anonymous.
- ❖ Script-kiddie: Són els hackers. No solen tindre habilitats tècniques, i volen beneficiar-se d'un hackeig sense saber molt bé com fer-ho.

- Correu brossa:

Denominat com correu brossa, és un missatge enviat per un mitjà electrònic de forma massiva i indiscriminada, sense el consentiment del receptor.

- Crackers:
És un terme per a denominar a algú que viola un sistema informàtic, de forma molt similar a un hacker amb la diferència que ho realitza per al benefici personal i en àmbits criminals.
- Robatori d'identitat
És la forma de robatori de dades personals d'algú del que el criminal pretén suplantar la identitat, normalment per a accedir a recursos.
- Fake news:
Consisteix en ocultar informació de manera deliberada i difondre falsedats a través dels mitjans de comunicació.
- Hackató:
És una marató o esdeveniment en la qual els programadors informàtics desenvolupen programari en un temps limitat, l'objectiu és crear un programari utilitzable a una solució plantejada.
- Gamificació:
Metodologia que es basa en els jocs com a mecàniques per a la formació i aprenentatge.

1.3. Proposta

La proposta que es desenvolupa en aquest projecte consisteix a programar una seqüència d'activitats taller al llarg d'un curs acadèmic, per a 4t de l'ESO principalment, atés que en aquesta edat l'alumnat ja té la maduresa suficient per comprendre els continguts i a més, aquest alumnat és usuari avançat de certes tecnologies (PC, Tauleta tàctil, Telèfon intel·ligent,...). L'estructuració de les activitats es farà a la manera d'un hackató amb una metodologia de gamificació per tal de motivar l'alumnat que podrà aprendre de manera entretinguda i divertida mitjançant un sistema de puntuació.

1.4. Objectius

- Els objectius generals d'aquest treball són:
 - Analitzar els beneficis que aporta l'aprenentatge del concepte de ciberseguretat.

- Proporcionar als docents de 4t de l'ESO les ferramentes per a educar i sensibilitzar el seu alumnat sobre la importància de la seguretat en línia, seguint el Bloc de l'assignatura d'Informàtica en el currículum de la Generalitat Valenciana (veure Annex)
- Ajudar els pares/tutors a conscienciar l'alumnat d'aquestes amenaces.
- Els objectius específics són:
 - Identificar els principals problemes existents en l'aprenentatge
 - Despertar l'interès per aprendre.
 - Dissenyar els diferents tallers o activitats per al context específic.
 - Desenvolupar activitats per a realitzar un hackató.
 - Analitzar els beneficis que aporten aquestes activitats com a estratègia d'aprenentatge

2. Fonamentació teòrica

2.1. Motivació en els aules

Dins el marc legislatiu vigent, tant el professorat com l'alumnat tenen dificultats en assolir la totalitat dels coneixements proposats en el currículum i això crea un desinterès per al tema, de per sí molt abstracte. En la meua experiència al centre de pràctiques, el tutor em va comentar que el tema de la seguretat el solen donar molt per damunt, donant més importància a altres qüestions com editors de text, programació orientada a objectes i altres, que consideren més importants. El tema seguretat només s'aborda superficialment quan es comenta algun tema de xarxes socials.

El principal objectiu d'aquest projecte és el que aquest tema siga més fàcil d'impartir mitjançant una sèrie d'activitats enfocades en la metodologia de la gamificació i fent un hackatons al final de curs on l'alumnat té a assolir les diferents competències.

Per a aconseguir que els estudiants estiguen motivats, sempre és necessari conèixer i orientar els seus objectius, necessitats i expectatives cap a conductes eficients. No s'aconseguirà que un alumne aprengui i interioritzi els conceptes si el treball del professorat es basa simplement en explicar bé la matèria i exigir el seu aprenentatge. És necessari i imprescindible captar la seua atenció, provocar un interès per el que s'està explicant. Incitar l'afany per aconseguir resultats favorables i generar en ells un gust per treballar i continuar aprenent [4]

Juan Vaello, professor i psicòleg, posa molt d'èmfasi en el que acabe de comentar i dona el secret per a estimular l'aprenentatge mitjançant el que denomina com "les vocals de l'educació" [5] Per damunt de tot, l'estudiantat té sobre les seves espatlles la A d'Atenció, del professor cap als estudiants i dels estudiants cap a la matèria i la tasca; la E d'Empatia, que significa tindre la capacitat de connectar amb l'alumnat de forma efectiva i emocional fent-los veure la disponibilitat com a professor/a; la I d'Interès, oferint una classe interessant per a l'alumnat, la O d'Obligatorietat, en la que cal fer front amb les altres vocals i, per últim, la U d'Utilitat, perquè quan no hi ha utilitat hi ha treballs forçats. Com a professors, tenim l'obligació de planificar la nostra intervenció en l'aula de tal manera que es complisquen les regles anteriors, assegurant així un ambient còmode i adequat per a què els estudiants aprenguen i es desenvolupen com a persones.

És per tot açò que sorgeix la necessitat de recolzar-se en diferents metodologies actives d'ensenyament i aprenentatge. De totes les existents, destaquen aquelles en les que el treball col·lectiu, el desenvolupament de les habilitats i el pensament crític adopten una gran importància. Parlem de l'aprenentatge basat en jocs. Per tant, basarem la proposta en la gamificació com a metodologia per a assolir les diferents competències.

2.2. La gamificació com a recurs didàctic motivador

Trobem diverses i variades definicions de gamificació. Per aquest treball, ens basarem en la de Deterding, S., Dixon, D., Khaled, R. i Nacke, L., que defineixen la gamificació com a "l'ús d'elements de videojocs en entorns aliens al joc per millorar l'experiència i el compromís de l'usuari" [6].) És un fet que els jocs i les tecnologies

transcendeixen cada vegada més els límits del seu entorn, sent utilitzats en diferents contextos amb diferents propòsits, com per exemple per a promoure un canvi en la conducta de l'usuari través de la conscienciació [7], .), o per a facilitar la formació en l'àmbit empresarial [8] En tots aquests àmbits on s'utilitza aquesta tècnica, es transforma als usuaris en jugadors, introduint-los completament en un entorn lúdic on han d'afrontar reptes i missions, augmentat així el seu nivell de compromís, la seua concentració i esforç per a aconseguir la màxima puntuació.

El fet que molts ambients estiguen introduint el joc, dins les seues pràctiques quotidianes, deriva de l'èxit que tenen en la societat actual. Segons un estudi realitzat per l'Associació Espanyola del Videojoc (AEVI) en 2017, el sector del videojoc va generar una producció de 1.177 milions d'euros en el nostre país, incloent-hi la venda de videojocs, tant físics com digitals, hardware, aplicacions mòbils, subscripcions, entre altres [9].

És un fet que els videojocs agraden, entretenen i generen diversió a qualsevol adolescent que s'introdueix en ells. Aconsegueixen captar completament la seua atenció, fent que perden la noció del temps quan se submergeixen, passant-se hores i hores davant de la pantalla sense estranyar la vida real. Així doncs, queda al descobert un clar exemple de la concentració profunda a la qual poden dur els jocs. De totes aquestes observacions i dades, sorgeix la idea de traslladar les tècniques i dinàmiques pròpies dels jocs al camp de l'educació, amb l'objectiu de captivar i implicar l'alumnat, construint així un ensenyament més estimulant i divertit.

3. Proposta d'hackató

3.1. Per que un hackató?

L'hackató integra els conceptes marató i hacker, i, per tant, proporciona una experiència col·laborativa que pretén desenvolupar aplicacions en un període de temps mínim. Un hackató suposa una magnífica experiència per a què els alumnes posen en pràctica totes les competències i habilitats del segle XXI amb l'objectiu de resoldre problemes en un context real.

Durant aquesta activitat els participants han d'organitzar-se en equips segons les seues diferents actituds disciplinàries, així l'alumnat és capaç d'idear, desenvolupar, prototipar i iterar solucions d'una forma creativa.

Si ho trasllem a un entorn escolar, les possibilitats d'aquesta metodologia són ràpidament apreciables: més enllà de l'aprenentatge i la posada en pràctica d'habilitats per resoldre problemes en context reals, l'alumnat no soles té una magnífica oportunitat per aprendre, sinó també per desenvolupar les següents competències:

- Habilitats de comunicació.
- Capacitat d'organització i planificació.
- Perseverança.
- Capacitat per a prendre decisions.
- Capacitat d'aprenentatge, d'adaptació i de lideratge.
- Creativitat.
- Sensibilitat artística.

Des del punt de vista de l'aprenentatge, amb l'hackatò el professor introdueix d'una manera fàcil i explicativa el concepte a desenvolupar, amb tots els reptes a abordar i una planificació de la jornada. De la mateixa forma, l'alumnat té que estar atent a tots els conceptes i reptes que haurà d'abordar i així aconseguir la màxima puntuació en el seu treball.

Es pot senyalar el benefici que aporta aquest joc sobre el treball grupal, ja que permet que els estudiants interactuen entre sí, reflexionant, construint junts les possibles solucions als reptes, mitjançant la comunicació i el pensament crític. També cal ser conscients de que aquesta metodologia d'aprenentatge exigirà un gran treball de coordinació i formació per part del professorat; sense això no es pot aconseguir formular tots els reptes propis d'un hackatò ni que l'alumnat siga capaç de desenvolupar les seues habilitats i competències. És a dir, no es podria assegurar una bona experiència.

Com en qualsevol situació, existeixen avantatges i inconvenients en la pràctica d'aquesta metodologia.

- Avantatges:

- Es fomenta el treball en equip i col·laboratiu, millorant les relacions entre l'alumnat i fent que tots formen part i tinguen la mateixa experiència.
- Es desenvolupen habilitats com el pensament crític o l'enginy
- Millora la competència verbal, pel fet que els estudiants han de dialogar i intercanviar idees per a poder avançar.
- És una activitat divertida que motiva l'alumnat.

- Inconvenients:

- Es necessita molt de treball i esforç per part del docent per al disseny i implementació.
- Es pot generar frustració en l'alumnat.

Llevat del gran esforç que suposa per al docent, aquesta activitat, destaca per la quantitat d'habilitats que els estudiants poden desenvolupar: pensament lògic, comunicació, cooperació, esforç, iniciativa, confiança i autoestima, entre moltes altres. És per totes aquestes habilitats, que queda demostrat com aquesta activitat pot ser beneficiosa per l'alumnat.

3.2. Contextualització.

Aquest projecte s'ubica en 4º curs d'Educació Secundària Obligatòria (ESO), a l'institut IES Pare Arques de Cocentaina. És cert que es pot realitzar l'hackatò en qualsevol any d'escolarització, sempre adaptant les activitats al nivell de cada estudiant, en aquest cas, es pren com a referència l'estudiant de 4º d'ESO.

En aquest institut el plantejament de les classes és diferent del convencional, ja que no només és el professor el que es mou per les aules, si no que també són els estudiants els que van a les aules en el seu horari. Així, hi a una organització en aules temàtiques repartides per tot el centre on els departaments de l'institut tenen les seues zones i classes. Dins de cada aula trobem un ordinador, un

projector i una xicoteta biblioteca amb diversos llibres de l'especialitat corresponent a cada aula.

L'hackató es planteja en el context específic de l'àrea d'informàtica, amb el propòsit de què l'activitat siga motivadora per a aprendre sobre aquest tema, i siguen capaços d'identificar les diferents problemàtiques. Per tal de què les activitats realitzades en aquest projecte tinguen una base en el Currículum de la Generalitat Valenciana, he agrupat els diferents temes per blocs, i cada bloc està relacionat amb els conceptes clau amb els quals l'alumnat ha de generar els coneixements:

Taula 1: Relació del currículum amb les activitats i competències

Bloc	Tema	Activitat	Competències
1	Ferramentes de seguretat: L'antivirus. El tallafocs. El programari antiespia.	Principals ferramentes de seguretat.	CD CAA
2	La protecció de les dades de caràcter personal: Informació i consentiment. Principis de qualitat, seguretat i secret. Drets d'accés, rectificació, cancel·lació i oposició. Riscos de seguretat en les comunicacions. El frau a internet. Hàbits per a detectar el frau a internet. Hàbits adequats en la interacció en la xarxa.	Protecció en una era digital.	CD CSC
3	Polítiques preventives per a la protecció de la informació personal. La identitat digital. L'empremta digital. Hàbits adequats en la interacció en la xarxa.	Protecció personal.	CD
4	La netiqueta. La suplantació de la identitat. Sistemes d'identificació en la xarxa. El certificat i la firma digital. El DNI electrònic. Generació de contrasenyes segures.	Perills a la red.	CD
5	Mètodes de protecció passius de les dades i en l'intercanvi d'informació.	Hacking ètic	CD CSD

CD: Competències digitals
CAA: Competències de aprendre a aprendre

CSD: Competències socials i cíviques

3.3. Competències i continguts didàctics a desenvolupar

Per tal d'assolir els conceptes anteriorment citats, és important que l'alumnat desenvolupi les competències següents:

1. Competències digitals: Aquest grup d'activitats inicia l'alumne a l'ús de telèfon intel·ligent, tauletes i ordinadors. A més, necessitaran coneixements bàsics de hardware per a utilitzar els diferents dispositius.
2. Competències de aprendre a aprendre: En aquesta activitat s'impulsa l'autonomia de l'alumnat a l'hora de treballar. L'alumnat ha de ser capaç de comprendre l'activitat per a després posar en pràctica el que ha après en la presentació final.
3. Competències socials i cíviques: Els estudiants han de cooperar entre ells, en els diferents mitjans de comunicació, ja siga en la classe, per correu electrònic o mitjançant els fòrums.
4. Sentit de la iniciativa i esperit emprenedor: L'alumnat, ha d'estar preparat per a poder fer una presentació final el més interessant possible.
5. Consciència i expressions culturals: Els grups estan formats per diversos estudiants, tots ells diferents entre si. En les diferents activitats tenen l'oportunitat de conèixer-se millor entre ells.
6. Competències de comunicació lingüística: En les diferents activitats es necessita d'una comunicació continuada entre els membres del grup.

3.4. Objectius didàctics

Els principals objectius didàctics que aquesta activitat proposada son:

- Cooperar i treballar en equip
- Fomentar la participació activa i presa de decisions.
- Cultivar el diàleg entre iguals, amb el fi d'aplegar a una idea en comú.
- Aprendre de l'error per a poder avançar.
- Revisar i consolidar els coneixements impartits al curs

3.5. Metodologia

La metodologia que segueix aquesta proposta és que els estudiants aprenguen jugant. El que es persegueix és que cadascun d'ells exercite diferents processos mentals en la resolució de reptes i desenvolupe diferents competències. Mitjançant els jocs, farem que l'alumnat estimule la seua intel·ligència i les seues relacions socials d'una forma divertida i al mateix temps es fomenta la comunicació i el treball en equip.

Com que està plantejat com un hackathó, cada equip haurà de desenvolupar una solució per a una sèrie de reptes. Totes les solucions són vàlides i correctes si en equip és capaç de solucionar la problemàtica principal. Cada repte serà puntuat i al final de l'activitat, cada equip serà valorat per al professorat i els mateixos alumnes, amb una puntuació. L'equip que més puntuació aconseguixin, serà el guanyador.

Aquesta activitat és una forma de canviar la dinàmica de classe, i això motiva l'alumnat, que moltes vegades necessita un canvi d'aires i trencar la rutina de classe. Mitjançant la gamificació i l'hackató, l'alumnat experimenta i enforteix la imaginació i la creativitat de forma divertida. A més, es converteix en amo del seu propi aprenentatge, demostrant-se a sí mateix els seus límits i capacitats per a superar obstacles.

Al professorat se l'encarrega principalment de dissenyar l'hackató, adaptant les diferents activitats a l'alumnat dins del context i tenint en tot moment com

a objectiu que l'estudiant tinga una experiència bona i enriquidora en el seu aprenentatge.

També serà el “mentor” dels reptes, que ajuda l'alumnat en temes tècnics per a resoldre dubtes sobre el tema exposat.

Una volta acabada l'activitat, serà responsabilitat del professor avaluar l'alumnat, reflexionar al voltant de l'activitat i fer un intercanvi d'opinions amb ells. També és necessari l'autoavaluació i l'autocrítica, analitzar els errors o les faltes que han sorgit durant l'activitat, i fer una proposta de millora.

3.6. Atenció a la diversitat de l'alumnat

Com ja he comentat anteriorment, el hackató és una manera de treballar conjuntament amb diferents components del grup que aporten les seues destreses més importants. aquest fet permet integració d'estudiants amb diferents habilitats o necessitats específiques en el grup.

Per a triomfar en una hackató, l'alumnat ha de desenvolupar diferents valors i habilitats en grup, com són la companyonia, l'organització i l'enteniment. Els grups més exitosos són els més heterogenis, ja que al ser els més diversos, són capaços d'interpretar diferents punts de vista de la mateixa problemàtica. Per tant la combinació d'estudiants amb capacitats i habilitats diferents fa que cada participant de l'activitat aporte la seua experiència, fent que les possibles barreres que un puga tindre s'alliberen. Inclús es poden crear diferents rols dins dels grups per a incentivar la participació d'aquells estudiants més vulnerables i adaptar l'activitat per a la seua participació.

3.7. Desenvolupament de la proposta de hackató

L'activitat es realitzarà a final de curs, durarà 14 hores i s'impartirà en els dies que hi han activitats als instituts. Podrà ser en 2 jornades completes, de 8 a 15, com mostra la Taula 1. Hem d'aclarir que els alumnes ja tenen uns coneixements previs de diferents camps relacionats amb les tecnologies de la informació perquè han cursat l'assignatura d'Informàtica.

Hora	Activitat	
Dia 1		
1	Realitzar els equips Elecció del problema plantejat.	Es realitzen els grups, es seleccionen els rols al grup i es selecciona un problema plantejat per el professor.
2	Entendre el problema.	S'analitza la problemàtica seleccionada buscant Que es va a realitzar: <ul style="list-style-type: none"> ● Programa informàtic ● Document explicatiu ● Innovació tecnològica ● Innovació social. ● Entre altres.
3	Realitzar una tempesta de idees i identificar les millors	Posta en comú de les idees de tots els integrants del grup.
4	Crear un prototip del projecte	Crear un xicotet prototip de el que es va a realitzar.
5		
6	Posta en comú	Cridar al teu "mentor" per a que revise el prototip, i faci una primera valoració del que s'està realitzant
7		
Dia 2		
8	Treball	Treballar en el projecte.
9		
10		
11	Exposició	Cada grup, exposa el projecte que ha realitzat. Fent una exposició del mateix.
12		
13	Avaluació	El professor evalua els projectes i realitza una xicoteta valoració de cada un d'ells.

Taula 2 Planificació temporal de l'activitat

3.7.1. Definició d'objectius i reptes

Els objectius principals a desenvolupar responen a certes preguntes que l'alumnat s'ha de fer:

- Estic segur utilitzant internet?
 - Ferramentes de seguretat
 - Tallafoc
 - Antiespia
- Les meues dades personals, estan protegides?
 - Utilitzar diferents cercadors web
 - Cercar els principals problemes als correus electrònics
 - Conèixer i generar una política preventiva per a la informació personal.
- Quins són els principals perills que existeixen en la xarxa?
 - Analitzar principals perills
 - Cercar informació
 - Implementació de programa o activitat per a identificar-los
- Sé utilitzar correctament Internet i els seus servicis?
 - Generació de contrasenyes segures
 - Autenticació doble factor
- Com puc ser un hacker ètic?
 - Conèixer els diferents malwares
 - Implementar algun taller o laboratori com a demostració.

L'alumnat ha de pillar qualsevol dels objectius anteriors amb els seus reptes, i realitzar un joc de forma creativa. Basant-se principalment en les recomanacions que dóna l' Institut Nacional de Ciberseguretat (INCIBE) [12] i ajudant-se d'internet i les diferents ferramentes que es proporcionaran en classe.

3.7.2. Recursos disponibles

L'activitat es desenvoluparà a la classe d'informàtica. Principalment el que fa falta és l'ordinador del professor, un projector per a projectar les diferents activitats, un ordinador per alumne.

A l'aula, les taules i cadires han d'estar disposades en grups de 4, encarades cara a cara perquè els alumnes puguin relacionar-se entre ells.

Com a complement, es poden posar una sèrie de pissarres perquè l'alumnat pugui generar en elles les diferents idees i estructurar-les.

3.7.3. Pla de continuïtat

Quan acaba l'hackathó, l'alumnat decideix si els projectes plantejats formen part d'un projecte més gran, ja que l'hackathó servix per a fer prototips i per a què l'alumnat aprengui jugant i treballant conjuntament.

3.7.4. Materials didàctics

Per a les diferents activitats necessitarem:

Ordinadors.

Raspberrypi.

Router Wifi

Laboratori de xarxa controlat

Connexió a internet

Pissares

Sckartch als ordinadors

Python

3.8. Avaluació

Com ja s'ha dit anteriorment, l'activitat té que ser avaluada per a comprovar el funcionament, per realitzar una autocrítica per part de l'alumnat i per valorar el treball realitzat pel docent.

3.8.1. Avaluació de l'alumnat

Les competències adquirides per l'alumnat, aniran avaluant-se a mesura que transcorregui l'activitat, i es deixarà de segon part els coneixements propis de la

matèria, com que aquesta activitat està plantejada com a repàs de tots els conceptes donats a classe i d'investigació pròpia de cada projecte triat per al grup d'alumnes.

Al finalitzar l'activitat, cada estudiant realitza una autoavaluació, on haurà de tindre consciència crítica sobre el seu treball, esforç, compromís i conducta durant l'activitat. Cada estudiant, de forma individual, omplirà el qüestionari que es presenta en la Taula 3, on s'avalua el grau d'actuació en cada situació:

	Res	Poc	Algo	bastant	molt
Control de la frustració.					
Compromís en el grup.					
Esforç.					
Interacció amb el grup.					
Inspiració.					
Direcció del grup.					
Adaptació d'idees contràries.					
Treball en grup.					
Capacitat de diàleg.					
Aportació d'idees.					
Observacions:					

Taula 3: Test d'autoavaluació

Després es dialogarà i debatrà sobre el conjunt del grup. Cada un dels membres del grup exposarà els problemes que ha tingut i com els ha solucionat, així com el comportament i el rol que ha tingut durant tota l'activitat.

Després es tornarà a omplir el qüestionari però aquesta vegada no s'avaluarà els alumnes, sinò al grup en el seu conjunt, de manera que el docent tinga una visió del grup i del treball en equip.

3.8.2. Avaluació del professorat

És molt important tindre una valoració de l'activitat per a poder millorar-la i fer-la més efectiva en un futur. Aquesta avaluació la farà tant el docent com a l'alumnat, valorant l'activitat des de la pròpia experiència. L'avaluació per par dels estudiants serà anònima i es realitzarà mitjançant el qüestionari presentat a la Taula 4.

	Res	Poc	Algo	Bastant	Molt
T'ha agradat l'activitat?					
Has après?					
Repetiries la experiència?					
T'ha paregut una bona metodologia per aprendre?					
Els objectius han sigut útils?					
Els reptes han sigut divertits?					
El nombre d'alumnes per grup era l'adequat?					
El paper del professor ha sigut el correcte?					
Observacions:					

Taula 4: Qüestionari de satisfacció

Per la seua part, el docent, ha de fer una avaluació personal de tot el procés, analitzant els aspectes següents:

- Quin ha sigut el resultat general.
- Quins han sigut els projectes entregats.
- Si els objectius i reptes ha estat adequats.

- Si l'ambient i l'activitat han fet que l'alumnat desenvolupi les competències fixades.
- Quina ha estat la motivació de l'alumnat.
- Si la distribució dels estudiants en els equips ha sigut correcta, i ha afavorit la inclusió.
- Si la metodologia ha millorat la relació entre els estudiants i ha incrementat la participació i la confiança en ells mateixos.

4. Conclusions i propostes de futur

Aquest treball ha tingut com a objectiu principal desenvolupar una sèrie d'activitats mitjançant el plantejament d'una hackató, com a proposta de millora de la metodologia actual que l'equip docent utilitza habitualment en el centre on vaig fer les pràctiques.

L'activitat plantejada afavoreix que l'alumnat pugui ser més creatiu en buscar una solució possible per resoldre problemes quotidians. Aquesta manera de treballar motiva moltíssim l'alumnat, ja que és diferent de com es fa tot en el dia a dia: particularment perquè es treballa amb el mateix grup durant un temps determinat, perquè ells són els encarregats de posar-se les metes, els objectius i la metodologia. A més a més, afavoreix l'aprenentatge digital i proporciona recursos a l'alumnat.

Un dels principals avantatges que suposa, és que l'alumnat potencia molt la creativitat, i el professorat pot observar diferents solucions a un mateix problema plantejat a classe.

El projecte, a més d'oferir una proposta d'activitats per una hackató per a l'assignatura d'informàtica de 4t de l'ESO, és també una xicoteta guia amb els punts clau que són la pauta que qualsevol docent que vulgui fer aquesta activitat pot seguir.

La gran limitació d'aquesta proposta de treball ha sigut no tindre la possibilitat de posar-la en pràctica, degut, especialment a les circumstàncies que estem vivint. Haguera sigut interessant poder realitzar l'activitat amb l'alumnat i així

recórrer tot el procés d'avaluació, l'estudi de detecció d'errors i propostes de millora, que ens permetria reportar informació molt interessant i una retroalimentació molt útil.

Finalment i per concloure, he de dir que aquest treball en l'àmbit educatiu fa veure que el professorat no sols ha de transmetre els coneixements a les futures generacions sinó que també ha de potenciar la capacitat de l'alumnat de crear projectes, activitats, jocs, etc... amb la originalitat i les característiques diverses de cadascú (una). És una mena "d'empoderament" de l'alumnat que ha de ser protagonista del seu aprenentatge.

5. Referències bibliogràfiques

[1] Rafael García, CTO de Hack By security

[2] <https://www.elmundo.es/economia/2021/03/09/6047578dfc6c83411b8b4795.html>

[3] <https://www.elperiodicomediterraneo.com/castello/2021/03/31/hackers-toman-ayuntamiento-castello-46003318.html>

[4] Farias,D.,Pérez,J.(2010). Motivacion en la enseñanza de las Matematicas y la Administracion. Venezuela: Universidad Simón Bolívar

[5]]Vaello Orts, J.(2007). Como dar clase a los que no quieren. Madrid:Santillana.

[6] Deterding, S., Dixon, D., Khaled, R., Nacke, L. (2011). From Game Design Elements to Gamefulness: Defining Gamification.

[7] Quintana, M. H. (2014). Sistema interactivo desarrollado bajo el concepto de gamificación: Una experiencia de juego para promover el cuidado del medio ambiente. Colombia: Universidad Autònoma de Occidente.

[8] Valera, J. F. (2013). Gamificación en la Empresa: Lo que los videojuegos nos enseñan sobre gestionar personas.

[9] ASOCIACION ESPAÑOLA DE VIDEOJUEGOS. El sector de los videojuegos en España: impacto económico y escenarios fiscales. <http://www.aevi.org.es/documentacion/estudios-y-analisis/>.

[10] Hackató. <https://ca.wikipedia.org/wiki/Hackat%C3%B3>

[12] Institut Nacional de Ciberseguretad. <https://www.incibe.es/>

6. ANNEX

Al currículum de l'assignatura d'Informàtica de 4rt de la ESO, al Bloc 3, determina els següents continguts:

Bloc 3: Seguretat informàtica i ètica Curs 4t ESO		
Continguts	Criteris d'avaluació	CC
Ferramentes de seguretat: L'antivirus. El tallafocs. El programari antiespia. La protecció de les dades de caràcter personal: Informació i consentiment. Principis de qualitat, seguretat i secret. Drets d'accés, rectificació, cancel·lació i oposició. Riscos de seguretat en les comunicacions. El frau a internet. Hàbits per a detectar el frau a internet. Polítiques preventives per a la protecció de la informació personal. La identitat digital. L'empremta digital. Hàbits adequats en la interacció en la xarxa. La netiqueta. La suplantació de la identitat. Sistemes d'identificació en la xarxa. El certificat i la firma digital. El DNI electrònic. Generació de contrasenyes segures. Mètodes de protecció passius de les dades i en l'intercanvi d'informació.	BL3.1. Adoptar hàbits i conductes de seguretat activa i passiva i d'ús responsable en la protecció dels sistemes informàtics, en la protecció de dades, en la interacció en la xarxa i en l'intercanvi d'informació.	CD CSD