UNIVERSITAT
ROVIRA i VIRGILI

L'ús de "Capture The Flag" com a metodologia per a millorar l'assoliment de conceptes i els resultats acadèmics de ciberseguretat

Rubén Aldabó Labaila
Màster universitari en Formació del Professorat d'Educació Secundària Obligatòria i Batxillerat, Formació Professional i Ensenyaments d'Idiomes (Especialitat Tecnologia)
Curs 2024/2025
Marta Moya Arevalo

Resum

Aquest treball analitza l'efectivitat de la gamificació mitjançant reptes Capture The Flag (CTF) en l'aprenentatge de la seguretat informàtica en el marc del Cicle Formatiu de Grau Mitjà de Sistemes Microinformàtics i Xarxes. L'objectiu principal és avaluar si aquesta metodologia innovadora pot millorar la motivació, els coneixements i la satisfacció dels estudiants en comparació amb l'ensenyament tradicional. Per fer-ho, s'ha dissenyat un estudi quasi-experimental amb dos grups: un grup experimental, que ha realitzat activitats basades en reptes CTF; i un grup control, que ha seguit la metodologia tradicional.

Els resultats mostren que el grup experimental ha millorat significativament en motivació i coneixements de ciberseguretat respecte al grup control, mentre que no s'han trobat diferències significatives en la satisfacció. Aquests resultats avalen l'ús de la gamificació com a eina pedagògica eficaç per a potenciar l'aprenentatge actiu i la implicació de l'alumnat en assignatures tècniques. El treball també discuteix les limitacions de l'estudi, com la mida de la mostra i la manca de continuïtat en el temps, i proposa futures línies de recerca per explorar l'efectivitat de la gamificació en altres contextos educatius. Aquesta investigació ofereix evidència pràctica i teòrica que pot servir de guia per a docents interessats en aplicar metodologies actives a l'aula.

Paraules clau: gamificació, Capture The Flag, Ciberseguretat, Motivació, Ensenyament tècnic, Aprenentatge actiu.

Abstract

This study analyses the effectiveness of gamification through Capture The Flag (CTF) challenges in learning computer security within the Intermediate Vocational Training program in Microcomputer Systems and Networks. The main objective is to evaluate whether this innovative methodology can enhance students' motivation, knowledge, and satisfaction compared to traditional teaching. To achieve this, a quasi-experimental study was designed with two groups: an experimental group, which carried out activities based on CTF challenges, and a control group, which followed the traditional methodology.

The results show that the experimental group achieved significant improvements in motivation and cybersecurity knowledge compared to the control group, while no significant differences were found in satisfaction. These findings support the use of gamification as an effective pedagogical tool to enhance active learning and student engagement in technical subjects. The study also discusses its limitations, such as sample size and lack of longitudinal assessment, and proposes future research directions to explore the effectiveness of gamification in other educational contexts. This research provides practical and theoretical evidence that can guide educators interested in applying active learning methodologies in the classroom.

Keywords: gamification, Capture The Flag, cybersecurity, motivation, technical education, active learning.

Contingut

Índex de figures

Índex de taules

Agraïments

Al llarg del procés d'elaboració i redacció d'aquest treball de fi de màster, he comptat amb el suport de moltes persones que, d'una manera o altra, han contribuït a fer-lo possible.

Vull manifestar el meu agraïment, en primer lloc, a la Caparrella, que em va permetre realitzar les pràctiques a l'institut on em vaig començar a formar com a professional, on vaig compartir grans moments descobrint l'electrònica i la programació i on vaig conèixer al millor amic que vaig fer compartint la passió de la tecnologia i que l'any 2021 va ser el meu padrí de casament, JM. Bernat. I també als estudiants de l'assignatura de Seguretat Informàtica del CFGM de Sistemes Microinformàtics i Xarxes per la seva disponibilitat, per la participació, i per gaudir amb la gamificació dels reptes de ciberseguretat i amb les explicacions que van rebre. I, especialment, al meu tutor, Lluc Capacete, per les hores que hem passat com a companys de feina i per fer-me redescobrir el món de la seguretat informàtica. A més, amb les seves classes i amb les seves explicacions he descobert trucs sobre el hacking ètic, com funcionava el centre, i el món de la docència.

En segon lloc, a la Universitat Rovira i Virgili, pels continguts de qualitat que han servit per guiar-nos per aquest apassionant món de la recerca científica. La qualitat dels vídeos i la manera que han tractat la investigació ha sigut molt emocionant. A més, a la meva tutora, Marta Moya, gràcies als comentaris i a les observacions de la qual aquest treball no hagués sigut possible.

En tercer lloc, als directors del Centre de Formació Professional Santa Agatoclia, Rosina i Iñaki, que em van facilitar la conciliació acadèmica per a portar a terme aquest Màster. També els agraeixo l'interès per l'èxit d'aquests estudis.

En quart lloc, als meus companys de màster Anna, Quim, Pol i Christian, amb els quals hem compartit molts moments de molta feina i, tot i això, hem sigut un grup cohesionat i tots a una per a treure tots els treballs de manera satisfactòria.

Finalment, vull agrair als meus pares, els quals sempre m'han animat a estudiar, el fet de portar la carrera acadèmica que estic seguint i convertir-me en la persona que soc. I a Laura, la meva companya de vida, la paciència, els ànims i les hores que hem treballat junts en aquest despatx, el despatx que somiàvem. El simple fet que fos al meu costat escoltant els meus dubtes, acompanyant-me, m'ha ajudat a portar-lo endavant i fer front a la redacció d'aquest treball amb els seus consells. I, per acabar, a Tux, el meu amic pelut que no s'ho ha pensat gens a l'hora de demanar-me companyia en els moments de més concentració, però al mateix temps amb una mirada graciosa de "fes-me cas i juga amb mi...". A partir d'ara recuperarem tots els moments que no hem pogut compartir aquests últims mesos.

Mequinensa, 23 de maig del 2025

1. Introducció

La realització del present treball d'investigació s'ha vist impulsada per la necessitat de demostrar com les metodologies d'aprenentatge ajuden els estudiants a aprendre i veure els continguts des d'un altre punt de vista acadèmic. Concretament, amb la implementació de la gamificació en l'entorn educatiu, encara que no és una estratègia nova (el seu origen es troba en la dècada dels 70 amb la introducció d'elements lúdics en entorns educatius), aquesta tendència ha evolucionat amb l'adaptació a les tecnologies digitals i a les necessitats dels usuaris, i s'ha consolidat com una poderosa eina per a millorar la participació, la retenció d'informació i l'experiència d'usuari.

Aquesta metodologia trenca amb l'esquema tradicional en el qual el professor és el centre del coneixement i l'alumne és un simple receptor d'aquests coneixements, i sorgeix de la unió de la psicologia cognitiva, la tecnologia i el disseny d'interacció on el joc proporciona un feedback instantani als estudiants per saber si van pel bon camí o pel mal camí a l'hora de resoldre el joc. A més, la gamificació genera una sèrie d'emocions que, combinades amb els continguts, contribueix a crear una simbiosi gràcies a la qual finalment aconseguim facilitar el procés d'aprenentatge.

1.1. Detecció de necessitats

L'avaluació i l'estructura organitzativa de les Unitats Formatives (UF's) del 2n curs del Cicle Formatiu de Grau Mitjà de Sistemes Microinformàtics i Xarxes en l'assignatura del Mòdul Professional 6 "Seguretat Informàtica" del IES Caparrella, està ben definida a partir de les explicacions del tutor de pràctiques del centre. Però, a partir d'una conversa informal amb el tutor de pràctiques, es va plantejar la possibilitat d'implementar la gamificació com a metodologia educativa en aquesta assignatura utilitzant competicions CTF (Capture The

Flag)[1]. Aquestes competicions permeten posar a prova les habilitats i els coneixements sobre seguretat informàtica, com per exemple les lliçons que els alumnes han après durant el curs.

Dins del món de la ciberseguretat hi ha "jocs de hackers", anomenats CTF's (Capture The Flag), que el que fan és programar, xifrar i desxifrar codis, amagar missatges, etc., per a obtenir unes recompenses i per, finalment, "capturar la bandera". Sembla que els CTF's ja s'han utilitzat en entorns educatius CCTF's (Classroom CTF's) com una alternativa a l'aprenentatge tradicional (Karagiannis & Magkos, 2020).

Qualsevol innovació pedagògica ha de sorgir de l'observació a l'aula, d'una base de recerca científica i d'una innovació constant, per aquesta raó la present investigació pretén implementar aquesta metodologia basada en la gamificació (Blažič & Blažič, 2024). A continuació, es mostren les cinc fases que cal seguir per implementar-la:

1. **Detecció de necessitats**: observació de les mancances a l'aula, en aquest context s'ha detectat que la gamificació és interessant per a fer més eficient l'aprenentatge i l'assoliment dels conceptes de l'assignatura de seguretat informàtica a partir de jocs i reptes per aconseguir aquesta fita.
2. **Conèixer l'entorn**: analitzar el context educatiu i tecnològic disponible, incloent-hi els recursos materials i humans, el nivell de competències digitals de l'alumnat i del professorat, així com les condicions específiques del currículum que permetin o limitin la implementació de la metodologia gamificada.
3. **Disseny del pla d'acció**: plantejament de la investigació, definició de les variables, definició del temps d'intervenció, definició de la població i la mostra, etc.

[1] Els reptes CTF (Capture The Flag) de ciberseguretat són jocs pràctics on els participants han de resoldre proves tècniques per trobar "banderes" ocultes, simulant situacions reals d'atac o defensa informàtica. S'utilitzen per aprendre, practicar i avaluar habilitats en seguretat digital.

4. **Implementació del pla d'acció**: aplicació pràctica de la metodologia gamificada a l'aula. Això inclou l'execució de les activitats de gamificació, el seguiment del progrés dels alumnes i l'adaptació de les dinàmiques en temps real per maximitzar-ne l'efectivitat.
5. **Recerca**: tipus d'investigació quantitativa (quasi-experimental) per a establir relacions causals amb una assignació quasi-aleatòria dels usuaris del grup d'estudi.

Segons investigacions recents, la gamificació és una tècnica eficient per a empoderar als estudiants i per incrementar el compromís amb l'aprenentatge i la motivació en l'educació dels estudiants (Balon & Baggili, 2023; Boudadi & Gutiérrez-Colón, 2020; Kim et al., 2023).

1.2. Justificació de la proposta d'innovació

Aquesta proposta respon a la necessitat d'adaptar l'ensenyament a les demandes actuals de l'àmbit de la ciberseguretat i a les preferències d'un alumnat que està acostumat a entorns digitals i interactius.

La recerca està fonamentada en evidències científiques que avalen l'ús de la gamificació com a estratègia pedagògica per millorar la retenció de coneixements, fomentar el treball col·laboratiu i desenvolupar habilitats de resolució de problemes (Balon & Baggili, 2023; Blažič & Blažič, 2024). A més, permet aplicar els continguts curriculars de manera pràctica i significativa, apropant l'alumnat a contextos professionals reals. Aquesta recerca pretén demostrar que la gamificació no només incrementa la motivació, sinó que també contribueix a una millor assimilació dels conceptes clau de la seguretat informàtica, tot promovent un aprenentatge més competencial i adaptat a les necessitats del mercat laboral actual.

Aquesta metodologia fomenta un aprenentatge actiu, col·laboratiu i basat en la resolució de reptes reals de ciberseguretat, cosa que permet als alumnes posar en pràctica els coneixements adquirits i

desenvolupar competències clau com el pensament crític, la creativitat i la resiliència. A més, la gamificació proporciona un feedback immediat, afavoreix la motivació intrínseca i facilita una experiència immersiva que pot millorar la retenció de continguts. La seva aplicació es recolza en la recerca científica, que demostra la seva eficàcia en l'educació tècnica i digital. En definitiva, aquesta proposta respon a una demanda pedagògica actual i pretén enriquir el procés d'ensenyament-aprenentatge a través d'una estratègia innovadora, contextualitzada i alineada amb les necessitats reals de l'alumnat.

2. Marc teòric

2.1. Gamificació

La gamificació és l'aplicació d'elements relacionats amb el joc en contextos no lúdics. Va començar a generar molt d'interès en diversos dominis empresarials com els sistemes de puntuació basats en estrelles per a plataformes de venda (*Marketplaces*) on hi havia compradors i venedors, com eBay, Amazon, etc.; a banda de les barres de progrés per a completar els perfils d'usuari en la majoria d'aplicacions digitals. Aquesta va ser una manera de millorar la usabilitat de plataformes complexes (Basten, 2017).

En l'àmbit educatiu, la gamificació aprofita els avantatges dels videojocs pel fet que els usuaris poden veure el seu progrés i el seu èxit els quals poden augmentar la motivació i el compromís en l'experiència d'aprenentatge en incorporar elements com desafiaments i emocions (Khodabandelou et al., 2023). A diferència de l'Aprenentatge Basat en Jocs (ABJ), on s'utilitzen jocs per aconseguir objectius educatius, la gamificació no es compromet amb un joc en concret, cosa que resulta un efecte a llarg termini (Alsawaier, 2018; Boudadi & Gutiérrez-Colón, 2020).

2.2. Capture The Flag (CTF)

Els reptes CTF són competicions de seguretat informàtica en les quals els participants han de trobar i explotar vulnerabilitats[2] en sistemes informàtics per a descobrir "banderes" ocultes al darrere d'uns reptes (de vegades es fan competicions i juguen uns equips contra uns altres). Aquests reptes estan dissenyats per a ensenyar habilitats en ciberseguretat a través de desafiaments pràctics i realistes, i permeten als participants desenvolupar habilitats tècniques i estratègies en el camp de la seguretat de les tecnologies de la informació i comunicació

[2] Consisteix a aprofitar-se d'una debilitat o error en un sistema informàtic per a obtenir un accés no autoritzat, alterar el seu funcionament o obtenir informació confidencial.

(TIC) (Ortiz-Garces et al., 2023). A més, els reptes CTF poden abastar molts camps de la seguretat informàtica, com criptografia[3], esteganografia[4], explotació web, enginyeria inversa[5], entre d'altres (Karagiannis & Magkos, 2020).

Per a portar a terme aquests reptes CTF, s'utilitzen plataformes que faciliten la creació i la gestió d'aquests desafiaments, com: 1) CTFd està dissenyada per a què sigui fàcil d'utilitzar tant per als usuaris com per als administradors i és Open Source[6]; 2) PicoCTF és una plataforma educacional on la gent jove pot aprendre conceptes bàsics de la seguretat informàtica mitjançant reptes per a entrenar i competir; 3) HackTheBox permet la generació de models d'entrenament a gran escala per a tota classe d'organitzacions i millora les seves habilitats de hàcking ètic; 4) TryHackMe és una plataforma que ensenya seguretat informàtica mitjançant exercicis curts que són rèpliques del món real; i 5) FbCTF és una plataforma creada per desenvolupadors de Facebook i dissenyada per a què sigui flexible i adaptable amb diferents tipus de facilitats en funció del tipus d'usuari (Ortiz-Garces et al., 2023). A més, aquestes plataformes permeten la integració de tecnologies com el Blockchain[7] i la intel·ligència artificial, ja que ofereixen una experiència única i atractiva per als participants i organitzadors.

[3] És la tècnica que permet protegir la informació mitjançant codificació, de manera que només les persones autoritzades puguin accedir-hi o desxifrar-la.
[4] És l'art de dissimular informació dins d'un altre suport, com imatges, àudio o text, per ocultar-ne l'existència.
[5] És el procés per mitjà del qual s'analitza un sistema, programari o dispositiu per entendre el seu funcionament intern i reproduir-lo o millorar-lo.
[6] És un model de desenvolupament de programari en què el codi font és accessible al públic, cosa que en permet l'ús, la modificació i la distribució lliure.
[7] És una tecnologia de registre distribuït que emmagatzema dades en blocs enllaçats de forma segura i immutable, garantint la transparència i la traçabilitat de les transaccions sense la necessitat d'un intermediari central.

2.3. Vinculació de la gamificació amb les teories d'aprenentatge

La gamificació està connectada amb algunes teories d'aprenentatge: en primer lloc, es relaciona amb la teoria de l'aprenentatge social de Bandura, en la qual es destaca l'autoeficàcia i la manera com les creences sobre les capacitats poden impulsar la motivació intrínseca (Boudadi & Gutiérrez-Colón, 2020). En segon lloc, es connecta amb el conductisme, que utilitza recompenses i penalitzacions per a corregir el comportament semblant als elements de gamificació com punts o medalles (Alsawaier, 2018). A més, la teoria de flux de Csikszentmihalyi apareix en el context de la gamificació, on la motivació sostinguda sorgeix d'un equilibri entre els desafiaments i les habilitats (Boudadi & Gutiérrez-Colón, 2020). En tercer lloc, la gamificació es vincula amb teories com la teoria de l'autodeterminació i la teoria d'aprenentatge experiencial, que són les teories més populars per a la investigació sobre la gamificació (Khodabandelou et al., 2023). Finalment, també es fa referència a la teoria de l'aprenentatge constructivista en relació amb la gamificació, en la qual el paper de l'instructor és guiar i facilitar el procés d'aprenentatge ajudant els alumnes a aconseguir els seus objectius. També s'ha tingut en compte la teoria del constructivisme social i la zona del desenvolupament pròxim de Vygotsky com a fonaments per a l'enfocament pedagògic (Karagiannis & Magkos, 2020).

2.4. La implementació dels CTFs en els resultats acadèmics

Les competències CTF poden millorar significativament els coneixements i les habilitats de ciberseguretat dels estudiants, de manera que a la literatura es recomana la utilització de plataformes de formació en aquest camp (Ortiz-Garces et al., 2023). A la literatura es destaca que els CTF poden augmentar la motivació i el rendiment dels estudiants en cursos de seguretat informàtica: en un estudi els

participants que van utilitzar CTFs van esmenar una satisfacció més gran en comparació amb els estudiants que no la van utilitzar (Ortiz-Garces et al., 2023), i en un altre estudi hi va haver un augment significatiu d'inscripcions i participació en el procés d'aprenentatge (Karagiannis & Magkos, 2020). A la literatura també es fa referència a la idea que els reptes CTF poden integrar-se al currículum acadèmic oficial per involucrar els estudiants en temes bàsics i complexos de ciberseguretat, per a superar obstacles del coneixement i per millorar l'adquisició d'habilitats (Karagiannis & Magkos, 2020). Els CTF i els laboratoris virtuals permeten simular escenaris realistes de ciberseguretat, la qual cosa pot involucrar estudiants i professionals en tàctiques ofensives i pot fomentar l'aprenentatge (Karagiannis et al., 2021).

2.5. Conclusió

El present marc teòric ha explorat els conceptes relacionats amb la gamificació i els reptes CTF, així com la relació amb diverses teories de l'aprenentatge i l'impacte que tenen en els resultats acadèmics. Es destaca com la gamificació pot fomentar la motivació, augmentar el compromís i millorar la seva experiència d'aprenentatge, i s'ha demostrat que els reptes CTF poden ser una eina pedagògica innovadora que estimula habilitats transversals com la resolució de problemes, la col·laboració i el pensament crític i les habilitats tècniques de ciberseguretat. En definitiva, aquest estudi pretén contribuir al coneixement existent i posar en pràctica aquesta metodologia d'aprenentatge per tal de validar-ne l'efectivitat en entorns reals educatius.

3. Proposta de recerca

3.1. Definició del problema

Segons les observacions i els comentaris del tutor de pràctiques del cicle formatiu de grau mitjà de Sistemes Microinformàtics i Xarxes, i professor de l'assignatura del Mòdul Professional 6 "Seguretat Informàtica" de l'IES Caparrella, hi ha una possibilitat de millora pel que fa a l'aprenentatge dels alumnes mitjançant la implementació de nous materials, recursos o metodologies.

El fet d'implementar una nova metodologia en aquesta assignatura es va veure impulsat pel plantejament d'utilitzar un sistema de gamificació, concretament, les competicions CTF (Capture The Flag), que són molt comunes en el món de la ciberseguretat.

3.2. La pregunta d'investigació

Els estudiants que utilitzen la gamificació mitjançant reptes CTF's assoleixen millor els coneixements que els estudiants que reben una explicació i els apliquen de manera pràctica dels mateixos continguts aplicats en els reptes CTF?

3.3. Hipòtesi

El fet d'utilitzar la metodologia de gamificació amb els reptes CTF (mitjançant les eines i els coneixements ensenyats prèviament en l'assignatura) fa que augmenti la motivació, que millorin els coneixements i les habilitats en ciberseguretat, i que es generi una major satisfacció en els estudiants en comparació amb les metodologies tradicionals.

3.4. Objectius

L'objectiu general i els objectius específics d'aquest treball tenen com a finalitat validar la hipòtesi que la implementació de la gamificació amb CTF's incrementa la motivació, l'adquisició dels coneixements i la satisfacció dels estudiants.

Objectiu general

- Avaluar la influència de la gamificació mitjançant reptes CTF en la motivació, l'assoliment de coneixements i habilitats en ciberseguretat, i la satisfacció dels estudiants.

Objectius específics

- **OE1**: Analitzar la influència de la gamificació en la motivació dels estudiants.
- **OE2**: Comparar els coneixements i habilitats en ciberseguretat dels estudiants que utilitzen reptes CTF amb els que no ho fan.
- **OE3**: Avaluar la satisfacció dels estudiants que han participat en els reptes CTF.

Variables

Pel que fa a la variable independent a manipular, és la implementació d'una metodologia d'aprenentatge, concretament, la gamificació amb reptes CTF, amb la qual teòricament tindrà un efecte causal directe sobre les variables dependents, que són: impulsar la motivació, millorar els coneixements i habilitats de ciberseguretat i la satisfacció dels estudiants incorporant desafiaments i emocions.

Per a intentar minimitzar algunes variables de confusió i el biaix pel que fa al temps d'estudi i les capacitats dels alumnes i augmentar la fiabilitat de l'estudi, s'utilitzarà la tècnica de mostreig no probabilística a criteri o intencional (Arrogante, 2022) per assegurar la comparabilitat dels grups control i intervenció. S'analitzaran les característiques clau de cada grup (edat, coneixements previs, etc.) per assegurar que

siguin el més similars possibles, i també s'intentaria controlar l'assignació equitativa dels dos grups en termes de mida i característiques.

Pel que fa a les variables estranyes, n'hi haurà algunes que no es podran controlar, però que ens donarien informació per a la representació dels resultats. Aquestes podrien ser: el temps d'estudi extra per a superar els següents reptes CTF, si estan fent pràctiques i estan cansats el dia següent, la presencialitat els dies de la intervenció, que es coneguin entre grups i que els grups que ja han fet algun repte el comentin amb un grup que no l'ha fet encara, etc.

3.5. Disseny de recerca

L'estudi es durà a terme mitjançant un disseny quasi-experimental amb grups no equivalents on no hi ha una assignació aleatòria dels usuaris de l'estudi. A diferència dels estudis vertaders, l'investigador no controla completament totes les variables. El tutor de pràctiques de l'IES Caparrella porta 4 dels 5 grups-classe de ciberseguretat ja existents i no aleatoris i per aquesta raó s'ha plantejat fer aquest tipus d'estudi amb dos grups de control i dos d'experimentals. A efectes d'anàlisi, els dos grups de control es consideraran com un sol grup (control), i els dos grups experimentals es consideraran també com un sol grup (experimental). A més, els continguts a explicar durant la intervenció per aquests dos grups estaran basats en els diferents camps de la seguretat informàtica, com ara: seguretat física/lògica, seguretat activa/passiva, criptografia, explotació web, etc.:

- Els dos grups experimentals, que realitzaran activitats d'aprenentatge basades en reptes CTF.
- Els dos grups de control, que estudiaran els continguts mitjançant una metodologia tradicional (exposicions teòriques i exercicis pràctics convencionals).

Els estudiants seran avaluats abans i després de la intervenció mitjançant proves de coneixement, nivells de motivació i satisfacció.

Aquest enfocament d'implementació metodològica: 1) permet dissenyar objectius d'aprenentatge progressius, des de nivells bàsics (memorització) fins a habilitats més avançades (creativitat i innovació); 2) ajuda a crear activitats didàctiques adaptades als diferents nivells cognitius dels alumnes; i 3) guia l'avaluació, pel fet d'assegurar que les preguntes i els exercicis estan alineats amb el nivell d'aprenentatge esperat.

A part de treballar els continguts prèviament vistos i utilitzar-los per als reptes CTF "grup experimental" o fer un repàs dels mateixos "grup control", si seguim els nivells d'aprenentatge segons la complexitat cognitiva de la taxonomia de Bloom (Krathwohl et al., 2005; Toala Ponce et al., 2022), es van explicar els conceptes que els tocaven (UF5: Monitoratge de xarxes) en funció d'aquests nivells: 1) recordar els conceptes del *Man in The Middle*; 2) comprendre la suplantació d'ARP's; 3) aplicar aquest mètode mitjançant un atac Man in The Middle; 4) analitzar les trameses de xarxa utilitzant WireShark; 5) avaluar les possibles defenses davant d'aquest tipus d'atac; i finalment 6) crear la solució per a prevenir-los.

L'elecció d'aquest disseny quasi-experimental està justificada per la naturalesa de la present investigació i per les condicions en les quals es desenvolupa. L'estudi, que busca avaluar l'impacte de la gamificació, implica comparar dos grups abans i després d'una intervenció educativa en comparació amb els mètodes tradicionals. Com que la definició dels grups ja està feta, aquest disseny ens permet utilitzar els grups no-aleatoritzats que hi ha en el mòdul d'informàtica del IES Caparrella. Així, el disseny quasi-experimental ofereix una solució metodològica consistent, adaptada a l'entorn educatiu real, que permet establir relacions causals parcials sobre l'eficàcia de la gamificació en l'aprenentatge de la ciberseguretat.

3.5.1. Instruments de recollida de dades

Per tal d'obtenir una visió global i rigorosa dels efectes de la intervenció, s'utilitzaran diversos instruments que permetran mesurar diferents ítems en el context real d'aprenentatge, com:

- Escala de coneixement *ad-hoc* abans i després de la intervenció per mesurar l'impacte en l'assoliment dels conceptes (veure annex I.III).
- Escala de Motivació Acadèmica (EMA) (Froment et al., 2021) (veure annex I.I) i l'Escala de Satisfacció Acadèmica (ESA) (González Casas et al., 2023) (veure annex I.II) per conèixer la percepció dels estudiants sobre l'experiència d'aprenentatge gamificat.
- Observació directa per analitzar la participació, la implicació i la dinàmica dels estudiants durant les sessions CTF.

3.5.2. Anàlisi de dades

L'objectiu de la recerca és analitzar l'efecte causal de la variable independent, que és la implementació de la metodologia d'aprenentatge basada en la gamificació "reptes CTF (Capture The Flag) de seguretat informàtica", sobre les variables dependents, que són la millora de la motivació dels estudiants, la millora dels coneixements i habilitats en ciberseguretat i l'increment del nivell de satisfacció en el procés d'aprenentatge.

La presa de dades es farà d'una manera pseudoanonimitzada, és a dir que els usuaris es codificaran en funció del grup classe al qual pertanyen (AA, BB, AB i CA) i se'ls assignarà un número aleatori, de manera que no es podran vincular a la persona directament a través de dades personals identificatives (nom, cognom, etc.) però sí que es podran vincular a la informació recollida durant l'estudi. Aquesta estratègia permet protegir la privacitat dels participants i complir amb els requisits ètics en la recollida de dades.

Abans de la intervenció es recolliran dades sociodemogràfiques, com ara l'edat i el sexe, que poden influir en els resultats, per tal d'analitzar patrons i relacions entre variables. A més, al principi de l'estudi es recolliran els resultats de les escales validades de motivació (EMA) i satisfacció (ESA) i els resultats d'una escala *ad-hoc* de coneixements de seguretat informàtica. Després de la intervenció, es tornaran a recollir aquestes mateixes dades en ambdós grups (control-intervenció), per tal d'analitzar els possibles canvis i determinar si la metodologia aplicada ha tingut un efecte significatiu en les variables independents (satisfacció, motivació i coneixements). Això permetrà observar no només l'impacte de la intervenció, sinó també possibles canvis espontanis que puguin haver-se donat en el grup control.

Pel que fa l'anàlisi de les dades, es realitzaran una sèrie de proves estadístiques per garantir la validesa dels resultats. D'una banda, s'aplicarà l'anàlisi de t-Student per a mostres independents per a comprovar si els dos grups (control i experimental) són comparables en el pretest (amb un valor de $p > 0.05$, que indica l'absència de diferències significatives entre ells). D'altra banda, es tornarà a fer la mateixa prova en el postest per determinar si hi ha diferències significatives entre el grup control i el grup experimental en el postest després de la intervenció (amb un valor de $p < 0.05$, que suggeriria que la metodologia basada amb gamificació ha tingut efecte).

Finalment, s'aplicarà l'anàlisi t-Student per a mostres relacionades dins de cada grup per separat (control i experimental). Aquesta prova permetrà analitzar si cada grup ha experimentat un canvi significatiu entre la mesura prèvia i posterior a la intervenció. Així, es podrà determinar no només si el grup experimental ha experimentat una millora significativa, sinó també si el grup control ha mantingut resultats estables o si ha presentat alguna variació inesperada.

4. Intervenció educativa

Actualment, al mòdul de seguretat informàtica s'està treballant la unitat formativa 5, "Tallafocs i monitoratge de xarxes", però la intervenció es farà sobre els continguts de les següents unitats formatives: UF 4 ("Seguretat activa") i UF 5 ("Tallafocs i monitoratge de xarxes").

Durant les tres setmanes que va durar la intervenció i per no interrompre el normal funcionament de les dinàmiques del tutor, es van utilitzar dues de les tres hores setmanals de l'assignatura per a portar a terme l'estudi. Tal com s'esmenta a les taules 26 i 27 de l'annex VI: Situació d'Aprenentatge, en primer lloc, durant la primera setmana es va fer la pressa de dades inicial i les explicacions teòriques pertinents. En segon lloc, la següent setmana es van portar a terme les proves gamificades amb el grup experimental i la resolució de dubtes i exercicis amb el grup control, amb els conseqüents resolucions de dubtes en ambdós casos. Finalment, la tercera setmana es van acabar de fer les proves, es va realitzar una reflexió grupal i es van prendre les dades de la post-intervenció.

5. Mètode

En aquesta secció es descriu l'enfocament metodològic utilitzat per a investigar l'impacte de la gamificació a través de la realització de reptes CTF en l'ensenyament de ciberseguretat dins del CFGM de Sistemes microinformàtics i xarxes.

L'objectiu principal d'aquest estudi és avaluar si l'ús d'aquesta estratègia didàctica contribueix a augmentar la motivació de l'alumnat, a millorar els seus coneixement i les seves habilitats en seguretat informàtica, i a generar una major satisfacció en comparació amb la metodologia tradicional d'ensenyament. Per aquet motiu, s'ha dissenyat un estudi que permetrà analitzar de manera estructurada i rigorosa les diferències entre aquests enfocaments pedagògics.

A continuació, s'esmenten els aspectes clau del disseny de la investigació, incloent-hi les característiques dels participants, les variables de l'estudi, els instrument utilitzats per a la recopilació de les dades, el procediment portat a terme i l'anàlisi de dades emprat per a interpretar-les.

5.1. Participants

Per una banda, la població són tots els estudiants els quals es podien incloure en aquest estudi que, en aquest cas, són tots els estudiants matriculats en mòdul de ciberseguretat dins del CFGM de Sistemes Microinformàtics i Xarxes. Per l'altra banda, la mostra és el subconjunt de la població que realment va participar en l'estudi que, en aquest cas, són els estudiants que formen part dels grups específics de l'assignatura de ciberseguretat en el centre educatiu IES Caparrella, de Lleida, que porta el tutor del TFM (LCG), segons els criteris d'inclusió esmentats en aquesta subsecció.

Per al reclutament dels estudiants, s'utilitzarà la tècnica de mostreig no probabilística a criteri o intencional (Arrogante, 2022) a fi de poder tenir grups equilibrats i permetre la comparabilitat entre el grup control

i el grup intervenció. Pel que fa als grups control, es va determinar que fossin els grups "CA" (12 nois i 0 noies) i "AB" (7 nois i 1 noia) i per als grups experimentals, "AA" (14 nois i 0 noies) i "BB" (4 nois i 2 noies). Pel que fa a l'edat i els coneixements previs, eren bastant similars. Les característiques de la mostra que s'han esmentat permeten que els participants s'ajustin als objectius de l'estudi, però no garanteixen la representativitat de la mostra en relació amb la població, de manera que es poden introduir biaixos en els resultats si tenen característiques molt diferents.

Pel que fa a les característiques sociodemogràfiques, els participants de l'estudi són majoritàriament homes d'entre 16 i 19 anys d'edat, que tenen un coneixement mitjà de la informàtica, ja que són al 2n curs del mòdul, i que poden tenir uns coneixements de la seguretat informàtica a diferents nivells. Els estudiants venen de la comarca del Segrià, això és, de la capital, Lleida, o dels pobles dels voltants de Lleida. També hi ha estudiants que venen de poblacions que pertanyen a la Franja de Ponent.

Pel que fa als criteris d'inclusió, són els següents: acceptar participar en l'estudi després de la respectiva explicació mitjançant el full d'informació; ser estudiants matriculats en el mòdul de ciberseguretat dins del mòdul de sistemes microinformàtics i xarxes; assistir regularment a classe i participar activament a l'aula. I, pel que fa als criteris d'exclusió, són els següents: no ser alumne dels grups que porta el tutor del centre educatiu.

Pel que fa al mètode de reclutament, se'ls va donar informació prèvia sobre l'estudi a partir del full d'informació i els estudiants del centre van acceptar participar-hi amb la realització de les enquestes, la intervenció (gamificació vs. mètode tradicional) i la posterior realització d'enquestes.

5.2. Variables

Pel que fa a les variables a utilitzar, la variable independent és la implementació d'una metodologia d'aprenentatge basada en la gamificació, i les variables dependents són les següents: impulsar la motivació, millorar els coneixements i habilitats de seguretat informàtica i la satisfacció dels estudiants. Aquestes variables concorden amb els objectius d'aquest estudi. Hi haurà variables estranyes (no controlades), com poden ser les següents: el temps d'estudi, fer pràctiques, assistir a les classes, conèixer-se amb persones de l'altre grup experimental, etc.

5.3. Instruments de recollida de dades

Per a mesurar les variables dependents i comprovar la comparabilitat intergrup a posteriori, s'utilitzarà una combinació d'escales validades i escales *ad-hoc*. Per a mesurar la motivació dels estudiants abans i després de l'estudi, s'utilitzarà, d'una banda, l'escala EMA (Stover et al., 2012), que és una escala multidimensional autoadministrada de 27 ítems que avalua la motivació dels estudiants en diferents contextos educatius i amb Alfa's de Cronbach considerades acceptables (>.70). D'altra banda, s'utilitzarà l'escala ESA (González Casas et al., 2023), que és una escala unidimensional autoadministrada de 8 ítems que avalua la percepció subjectiva de l'estudiant amb el valor de l'Alfa de Cronbach de .932, on els coeficients de fiabilitat són més grans de .9 i suggereixen una excel·lent fiabilitat interna, els ítems estan relacionats i mesuren el mateix constructe. Pel que fa a l'escala *ad-hoc* per a mesurar els coneixements de seguretat informàtica, es realitzarà una escala amb preguntes sobre ciberseguretat quant a: comandes per a fer proves de *pentesting* de caixa negra[8], és a dir, l'ordre lògic de com fer aquest tipus d'atac i per a què serveixen.

[8] Són tests de penetració a sistemes que avaluen els possibles fallades de seguretat informàtica on el testejador no sap res sobre el sistema a avaluar. Pentesting és el resultat de d'unir dos conceptes: *penetration* i *testing*.

5.4. Procediment

Per a fer aquest estudi es determina quins grups classe aniran al grup control i quins grups classe aniran al grup experimental, es preparen les escales per a passar-les abans de la intervenció, i s'organitza la intervenció de manera que durant les tres setmanes es farà una intervenció de dues hores a la setmana amb un total de sis hores en ambdós grups. Per al grup experimental, es farà una introducció i pretest (1/2 h), una explicació de conceptes clau dels CTF (3/4 h), una demostració d'un CTF (1/2 h), el desenvolupament d'un CTF (3 h), una reflexió i una discussió grupal (1/2) i un posttest (3/4 h). Per al grup control, es farà una introducció i un pretest (1/2 h), una explicació de teoria i de continguts actuals (1 i 3/4 h), un treball de pràctica (2 i 1/2 h), una discussió grupal (1/2) i un posttest (3/4 h).

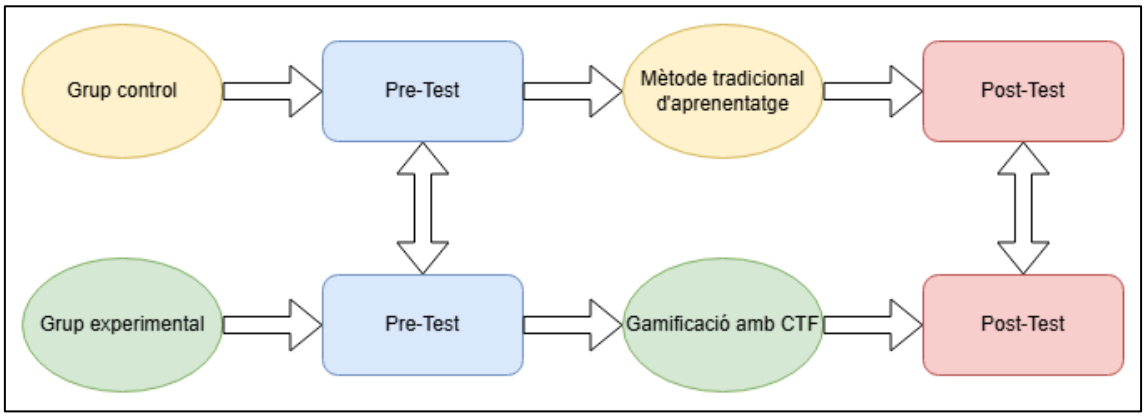

Figura 1: Diagrama de disseny quasi-experimental amb grup control no equivalent

5.5. Anàlisi de les dades

Es planteja l'ús de programaris lliures (JASP o R) per a realitzar aquesta anàlisi i l'aplicació de proves estadístiques per garantir la validesa dels resultats. En primer lloc, s'aplicarà l'anàlisi de t-Student per a mostres independents per comprovar si els dos grups (control i experimental) són comparables en el pretest (amb un valor de $p > 0.05$, que indica l'absència de diferències significatives entre ells). En segon lloc, es repetirà la mateixa prova en el posttest per determinar si hi ha diferències significatives entre el grup control i el grup experimental

després de la intervenció (amb un valor de $p < 0.05$, que suggeriria que la metodologia basada en gamificació ha tingut efecte). Finalment, s'aplicarà l'anàlisi t-Student per a mostres relacionades dins de cada grup per separat (control i experimental). Aquesta prova permetrà analitzar si cada grup ha experimentat un canvi significatiu entre la mesura prèvia i posterior a la intervenció. D'aquesta manera, es podrà determinar no només si el grup experimental ha experimentat una millora significativa, sinó també si el grup control ha mantingut resultats estables o si ha presentat alguna variació inesperada.

6. Resultats

Aquest estudi es va dissenyar per a donar resposta a la pregunta principal d'investigació següent: "Els estudiants que utilitzen la gamificació mitjançant reptes CTF's assoleixen millor els coneixements que els que fan una revisió dels mateixos continguts aplicats en els reptes CTF?". Els estudiants del CFGM de Sistemes Microinformàtics i Xarxes del Institut Caparrella de Lleida van participar en un estudi per a comprovar com la implementació de la gamificació a l'aula millora l'assoliment de continguts en comparació amb el mètode tradicional d'ensenyament.

L'estudi també va plantejar la següent hipòtesi: el fet d'utilitzar la metodologia de gamificació amb els reptes CTF (mitjançant les eines i els coneixements treballats prèviament a classe) fa que augmenti la motivació, que millorin els coneixements i les habilitats en ciberseguretat, i que es generi una major satisfacció en els estudiants en comparació amb les metodologies tradicionals.

Per a portar a terme els càlculs necessaris d'anàlisi i analitzar l'efecte de la intervenció basada amb gamificació mitjançant reptes CTF, es va aplicar la prova t de Student per a mostres independents per a comprovar si els dos grups eren comparables (es mira si les mitjanes aritmètiques difereixen significativament o no) segons la qual s'ha de complir el supòsit que les variàncies d'error del pretest i el posttest són iguals, si no, no es podria interpretar la t de Student. Si la p de la taula de Levenne tant del pretest com del posttest són superiors a 0.05 en ambdós casos (pretest i posttest), es compleix el supòsit d'igualtat de variàncies i podem interpretar la t de Student. Es van fer tres proves per a mostres independents (una per cada variable dependent) i, posteriorment, la t de Student per a mostres relacionades (dues per cada variable dependent: control vs. experimental). Aquesta prova va permetre comparar les dues mesures del mateix grup de participants en dos moments de la intervenció diferents (pretest i posttest) i també

va permetre veure si la diferència observada és estadísticament significativa.

Les anàlisis es van realitzar mitjançant el software estadístic JASP (versió 0.19.3.0), una eina d'anàlisi estadística de codi obert.

L'anàlisi estadística mostra diferències significatives en dues de les tres variable avaluades:

Satisfacció:

Pel que fa a la satisfacció acadèmica, els dos grups van mostrar increments lleus en les puntuacions mitjanes després de la intervenció, però cap d'aquestes diferencies va ser estadísticament significativa (*grup experimental*: $t(19) = -1.237$, $p = .231$; *grup control*: $t(19) = -0.872$, $p = .394$) (veure taules 1 i 3). Això indica que, en les condicions del present estudi, la metodologia basada amb reptes CTF no va generar un impacte significatiu en els nivells de satisfacció percebuda per l'alumnat.

Taula 1: Satisfacció, T de Student per a mostres relacionades del grup experimental

Mesura 1		Mesura 2	t	df	P
Pre	-	Post	-1.237	19	0.231

Taula 2: Satisfacció, dades descriptives del grup experimental

	N	Mitjana Aritmètica	SD	SE	Coeficient de variació
Pre	20	13.350	3.514	0.786	0.263
Post	20	14.500	3.035	0.679	0.209

Taula 3: Satisfacció, T de Student per a mostres relacionades del grup control

Mesura 1		Mesura 2	t	df	p
Pre	-	Post	-0.872	19	0.394

Taula 4: Satisfacció, dades descriptives del grup control

	N	Mitjana Aritmètica	SD	SE	Coeficient de variació
Pre	20	14.450	4.513	1.009	0.312
Post	20	15.600	5.576	1.247	0.357

En relació amb aquesta variable dependent, les diferencies entre les mesures pre i post no són tan significatives com les altres variables (motivació i coneixements). Totes dues mostren uns increments similars i lleus (veure figura 2), és possible que sigui a causa de la relació de la mitjana amb el grup experimental. Això podria indicar que la metodologia gamificada no ha tingut un impacte significatiu en la percepció general de satisfacció i aquesta ha estat influenciada per altres factors aliens a la intervenció, com la relació amb el professorat o el fet que un dels grups control era a la tarda.

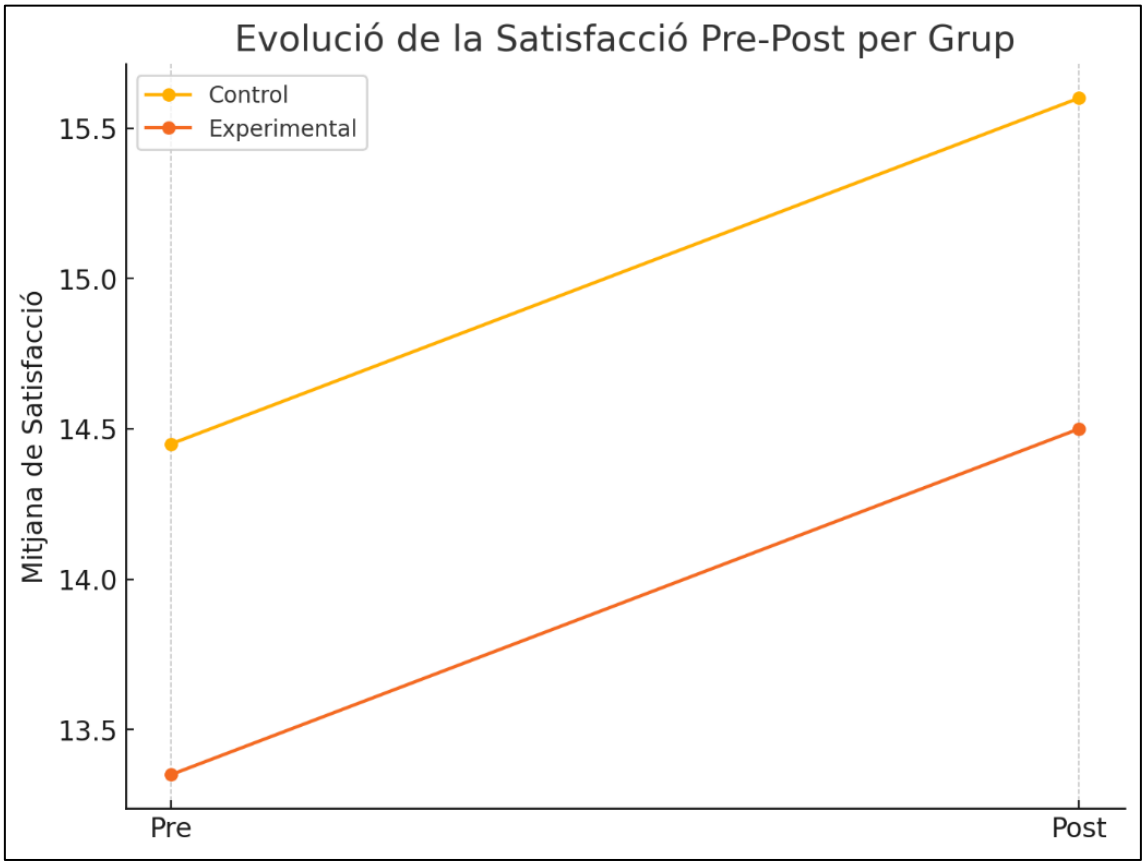

Figura 2: Evolució de la satisfacció Pre-Post en la satisfacció

Motivació:

Pel que fa a la motivació acadèmica, per una banda, el grup experimental va mostrar un augment significatiu després de la implementació de la metodologia basada amb reptes CTF ($t(19) = -4.788$, $p < .001$) (veure taula 5), gràcies a la qual va passar d'una mitjana de 2.798 (DE = 0.224) a 3.134 (DE = 0.284) (veure taula 6). Per l'altra banda, el grup control no va presentar diferències significatives entre les mesures pretest i posttest ($t(18) = 1.503$, $p = .150$) (veure taula 7), i a més es va observar una lleu disminució de la mitjana de motivació de 2.843 (DE = 0.387) a 2.726 (DE = 0.500) (veure taula 8). Aquests resultats permeten veure que la gamificació va tenir un efecte positiu en aquest aspecte (veure figura 3).

Taula 5: Motivació, T de Student per a mostres relacionades del grup experimental

Mesura 1		Mesura 2	t	df	p
Pre	-	Post	-4.788	19	< .001

Taula 6: Motivació, dades descriptives del grup experimental

	N	Mitjana Aritmètica	SD	SE	Coeficient de variació
Pre	20	2.798	0.224	0.050	0.080
Post	20	3.134	0.284	0.063	0.091

Taula 7: Motivació, T de Student per a mostres relacionades del grup control

Mesura 1		Mesura 2	t	df	p
Pre	-	Post	1.503	18	0.150

Taula 8: Motivació, dades descriptives del grup control

	N	Mitjana Aritmètica	SD	SE	Coeficient de variació
Pre	20	2.843	0.387	0.086	0.136
Post	19	2.726	0.500	0.115	0.184

Pel que fa a aquesta variable dependent, el diagrama mostra un augment significatiu en els resultats entre el grup experimental (pre i post), mentre que el grup control presenta una lleugera disminució o estabilitat. Aquestes dades suggereixen que la gamificació mitjançant reptes CTF no només millora l'aprenentatge, sinó que també incrementa la motivació de l'alumnat cap a l'assignatura, reforçant l'ús d'aquesta metodologia com a estratègia pedagògica per fomentar-ne la implicació.

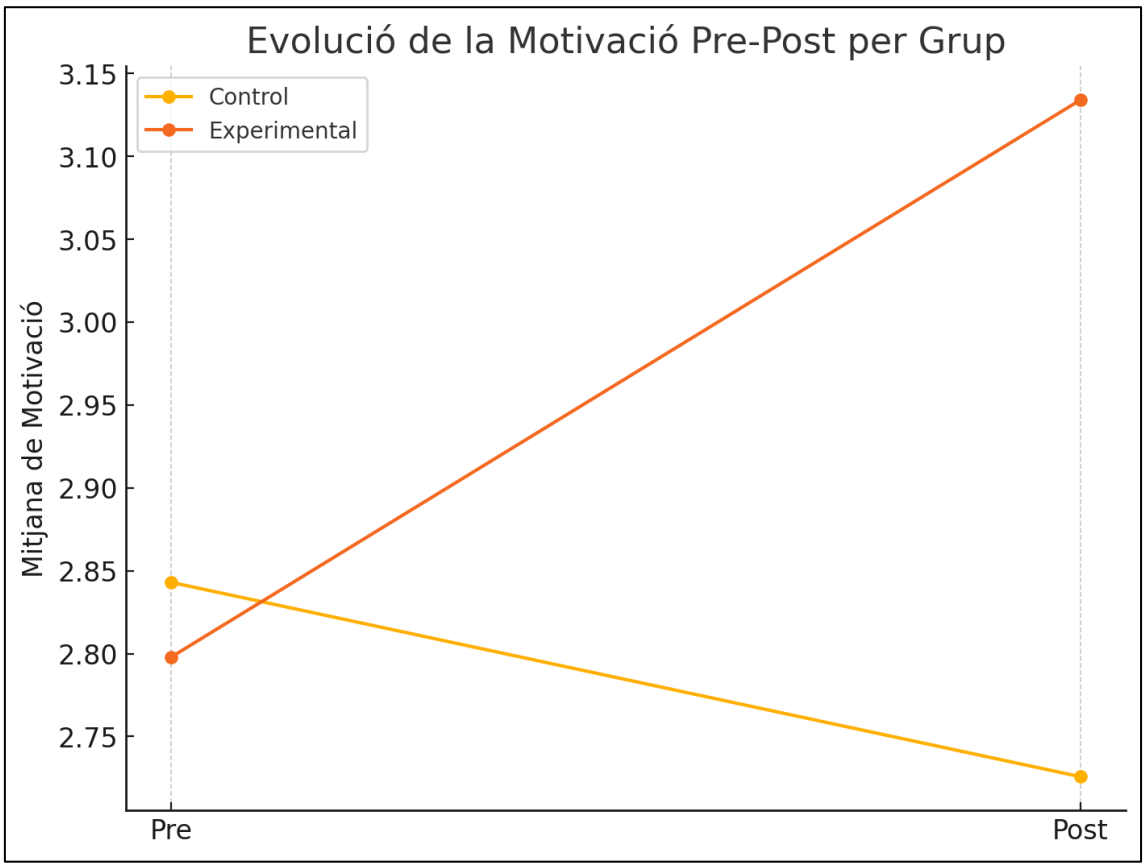

Figura 3: Evolució de la satisfacció Pre-Post en la motivació

Coneixements:

Pel que fa a la prova de coneixements de ciberseguretat, ambdós grups van mostrar millores significatives entre les mesures pretest i posttest. Per una banda, el grup experimental que va treballar amb reptes CTF va presentar una millora molt significativa ($t(19) = -11.706$, $p < .001$) (veure taula 9); va passar d'una mitjana de 4.900 (DE = 0.641) a 8.200 (DE = 1.361) (veure taula 10). Per l'altra banda, el grup control

també va millorar de forma significativa ($t(19) = -3.059$, $p = .006$) (veure taula 11), però amb un increment més lleuger, des de 4.600 (DE = 0.503) fins a 6.250 (DE = 2.245) (veure taula 12). Aquests resultats permeten veure que encara que els dos grups van millorar els seus coneixements, la metodologia és més eficaç quant a l'aprenentatge i l'assoliment de coneixements.

Els resultats en les mesures pre i post dels grups experimental i grup control mostren una millora notable en els coneixements de ciberseguretat. No obstant, l'increment és més pronunciat en el grup experimental, que obté una mitjana superior després de la intervenció respecte al grup control. Aquests resultats indiquen que la metodologia basada en reptes CTF ha tingut un impacte positiu més gran en l'assoliment dels coneixements en comparació amb la metodologia tradicional.

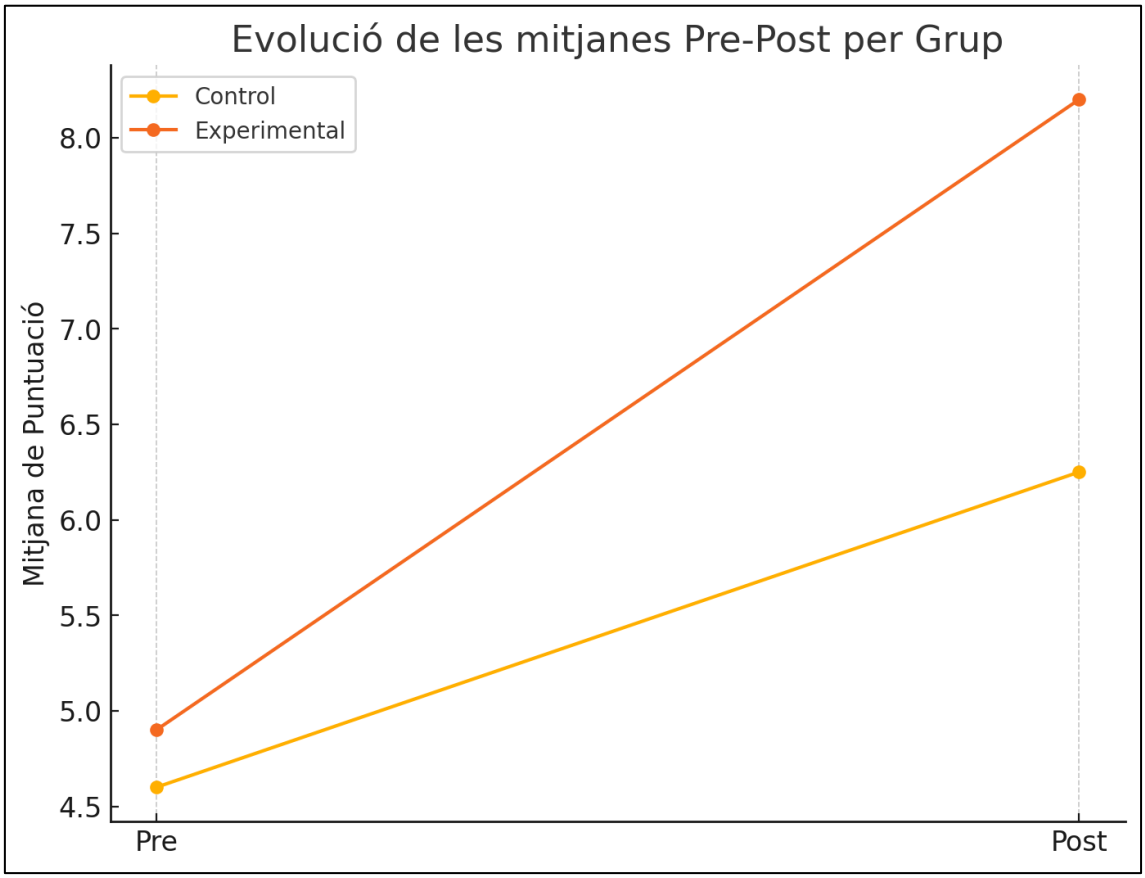

Figura 4: Evolució de la satisfacció Pre-Post en els coneixements

Taula 9: Coneixements, T de Student per a mostres relacionades del grup experimental

Mesura 1		Mesura 2	t	df	p
Pre	-	Post	-11.706	19	< .001

Taula 10: Coneixements, dades descriptives del grup experimental

	N	Mitjana Aritmètica	SD	SE	Coeficient de variació
Pre	20	4.900	0.641	0.143	0.131
Post	20	8.200	1.361	0.304	0.166

Taula 11: Coneixements, T de Student per a mostres relacionades del grup control

Mesura 1		Mesura 2	t	df	p
Pre	-	Post	-3.059	19	0.006

Taula 12: Coneixements, dades descriptives del grup control

	N	Mitjana Aritmètica	SD	SE	Coeficient de variació
Pre	20	4.600	0.503	0.112	0.109
Post	20	6.250	2.245	0.502	0.359

7. Discussió

El propòsit d'aquest estudi era analitzar l'efectivitat de la gamificació i avaluar-ne la influència com a metodologia innovadora d'aprenentatge en comparació amb la metodologia tradicional mitjançant reptes CTF en la motivació, assoliment de coneixements i habilitats en ciberseguretat, i satisfacció dels alumnes de l'assignatura de Seguretat Informàtica del CFGM de Sistemes Microinformàtics i Xarxes. Els resultats han mostrat que l'aplicació de la metodologia de gamificació ha tingut efectes favorables sobre l'aprenentatge i l'assoliment de conceptes (GC: $p = .006$; GE: $p < .001$), i la motivació dels estudiants (GC: $p = .150$; GE: $p < .001$), però no va tenir efectes favorables sobre la satisfacció dels estudiants (GC: $p = .394$; GE: $p = .231$) al final de la intervenció realitzada.

Els resultats obtinguts en aquesta recerca mostren que la implementació de reptes CTF com a metodologia d'aprenentatge és una bona eina per a assolir i posar a prova els coneixements adquirits, fomentar la cerca d'eines per a superar els reptes establerts en les proves. La gamificació mitjançant reptes CTF s'ha utilitzat en diversos casos per aprendre seguretat informàtica i millorar les aptituds en defensa d'atacs cibernètics a sistemes, identificació, explotació de vulnerabilitats (pentesting) i hacking ètic.

En aquest estudi la mitjana qualificativa de les respostes en el qüestionari post-intervenció de coneixements (ad-hoc) va ser més elevada que les del grup control (GC: 6.250; GE: 8.200). En un estudi publicat l'any 2023 es va trobar que la participació en CTF va millorar el rendiment dels estudiants en un curs de seguretat informàtica (Ortiz-Garces et al., 2023). A més, un altre article va destacar que la integració de desafiaments CTF en entorns d'aprenentatge virtual pot augmentar l'adquisició d'habilitats i coneixements en ciberseguretat i millorar la confiança dels estudiants (Karagiannis & Magkos, 2020).

Pel que fa a la satisfacció, l'Escala de Satisfacció Acadèmica (ESA) és un instrument dissenyat per avaluar la percepció objectiva dels estudiants sobre la seva satisfacció acadèmica. Aquesta escala va ser adaptada a l'espanyol (Medrano & Pérez, 2010) i consta de 8 ítems que responen a una escala Likert de 4 punts on 1 significa "mai" i 4 significa "sempre". Pel que fa a la temàtica d'aquests ítems, aquests aborden els temes d'interès per les classes, la motivació del curs, i si els agraden els professors i els continguts de l'assignatura. En el nostre cas, els resultats dels estudiants d'ambdós grups van mostrar una millora en la mitjana dels nivells de satisfacció (GC: 15.6; GE: 14.5). El grup experimental va presentar una menor dispersió en les respostes (DE = 3.035) (veure taula 13), la qual es pot interpretar com una percepció més uniforme en l'experiència d'aprenentatge. El grup control va tenir uns valor més allunyats de la mitjana (DE = 5.576) (veure taula 13), això suggereix que factors estranys poden haver influït significativament en aquesta variable depenent: podria ser que l'elecció d'aquesta escala per a mesurar la satisfacció no fos l'apropiada. Així, aquest resultat apunta que l'efecte en la satisfacció no és tan rellevant en l'aprenentatge o la motivació.

Pel que fa a la motivació, l'Escala de Motivació Acadèmica (EMA) és un instrument psicomètric basat en la Teoria de l'Autodeterminació de Deci i Ryan (Ryan & Deci, 2000b). Segons el document (Morales et al., n.d.), l'EMA ha sigut validada i consta de 27 ítems que responen a una escala Likert de 4 punts on 1 significa "Totalment en desacord" i 4, "Totalment d'acord". Aquesta té 4 subescales per avaluar la motivació intrínseca, la motivació extrínseca, la desmotivació, i la motivació general. En aquest estudi s'ha avaluat al motivació general. En aquest treball, els resultats dels estudiants del grup experimental va experimentar un increment mitjà de .336 punts, mentre que en el grup control va experimentar un increment de -.117 punts. Aquesta troballa reforça la hipòtesi que els entorns gamificats promouen una major

implicació de l'alumnat, probablement pel fet d'estimular un factor com el desafiament, la retroalimentació immediata i la sensació de progrés (Ryan & Deci, 2000a). Aquest és un factor clau per a la persistència i l'èxit en entorns educatius, i la seva millora utilitzant metodologies innovadores com són la implementació de dinàmiques i els CTF en assignatures tècniques.

Pel que fa al nivell pràctic, aquesta investigació pot ajudar a docents amb interès a aplicar metodologies basades en la gamificació a l'aula. Molts dels apartat d'aquest treball, com els resultats i la metodologia, poden guiar els professors en la planificació, la implementació i l'avaluació de l'execució d'aquest mètode.

Les anteriors afirmacions es poden veure a la figura següent:

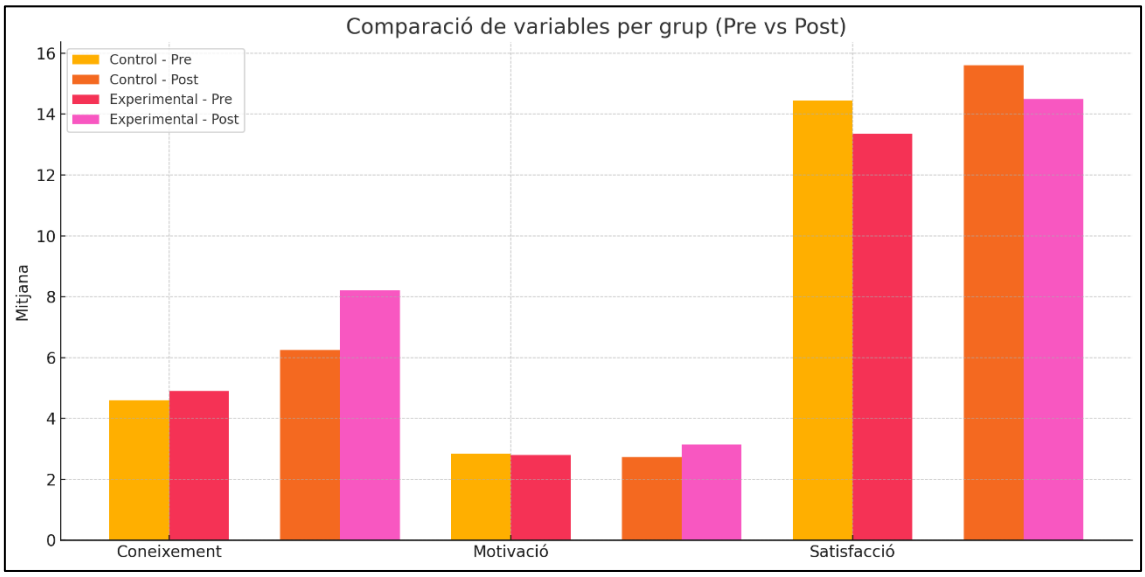

Figura 5: Comparació de les variables dependents

Pel que fa al nivell teòric, el present estudi contribueix a presentar l'evidència existent sobre l'eficàcia de la gamificació en entorns educatius, perquè aporta dades concretes en el context de la ciberseguretat i l'ensenyament tècnic. A més, obre les portes a futures investigacions que vulguin explorar l'impacte de altres tipus de gamificació, no només amb formació professional, sinó en altres etapes educatives com poden ser l'educació primària, secundaria o estudis

superiors. També pot ser d'interès per a altres investigadors d'altres àmbits com la psicologia educativa o la innovació pedagògica.

Pel que fa a les limitacions de l'estudi, tot i que els resultats obtinguts han estat positius i significatius en alguns aspectes, hi ha punts que es poden millorar quant al disseny i l'execució de l'estudi: 1) El desenvolupament d'una prova CTF no permet establir tendències clares al llarg del temps, però diversos conjunts de proves CTF en diferents àmbits (Jeopardy-style, Attack-Defense o Mixed CTF) i en diferents moments, incloent-hi enquestes de motivació abans i després de cada sessió, hauria aportat una visió més completa de l'evolució de la motivació i l'aprenentatge. 2) El lapse temporal de tres setmanes entre les dues passades dels qüestionaris pot haver introduït biaixos, ja que durant aquest període hi podrien haver influït altres factors externs (canvi d'assignatures, estat emocional, càrrega de treball, etc.) que no es van controlar. 3) La mostra d'estudi es va limitar a un únic centre i a un nombre reduït d'estudiants, la qual cosa limita l'extrapolació dels resultats a altres contextos o perfils d'estudiants.

Pel que fa a les futures línies d'investigació, a partir dels resultats i de les limitacions detectades, s'obren diverses possibilitats per a futures línies d'investigació: 1) Realitzar estudis longitudinals que analitzin l'impacte de la gamificació al llarg d'un període més extens. 2) Explorar l'efectivitat d'altres formes de gamificació (com ara sistemes de punts, narrativa, avatars, o competicions en grups) en diferents àrees de coneixement i nivells educatius. 3) Investigar de forma més específica les causes de la manca de diferència significativa en la satisfacció percebuda. 4) Aplicar la mateixa metodologia en altres àmbits, com la formació de docents o la capacitació en empreses, per comprovar-ne la transferibilitat fora del context escolar.

8. Conclusions

La hipòtesi principal d'aquesta recerca defensava que la implementació de la metodologia de gamificació amb el reptes CTF feia que augmentés la motivació, milloressin els coneixements i habilitats en ciberseguretat i que es generés major satisfacció en els estudiants en comparació amb les metodologies tradicionals d'aprenentatge.

Aquest estudi ha permès analitzar l'efectivitat de la gamificació mitjançant reptes CTF en l'àmbit de l'educació tècnica. Tal com s'esmenta en l'apartat de discussió d'aquest treball, les dades obtingudes permeten concloure que la gamificació mitjançant els reptes CTF és una metodologia eficaç per a potenciar l'aprenentatge i la motivació de l'alumnat en l'àmbit de la ciberseguretat i que hi té un impacte positiu i significatiu. Encara que la satisfacció percebuda no va mostrar diferències significatives marcades entre grups possiblement a causa de factors estranys, els beneficis observats en termes de coneixement i motivació avalen l'ús d'aquestes eines com a complement o fins i tot com a alternativa a la docència tradicional.

La millora en els resultats comparatius entre el grup experimental i el grup control en els qüestionaris de coneixements i motivació reforça la idea que els entorns gamificats poden estimular la participació i el compromís dels alumnes, gràcies als reptes, a la retroalimentació immediata i a la sensació de progrés. Tot i aquests resultats, cal tenir en compte les limitacions d'aquest estudi, com ara l'ús d'una mostra reduïda i l'ús d'una sola experiència gamificada. Aquest estudi obre la porta a noves investigacions que explorin altres formes de gamificació, l'aplicació en altres contextos educatius i l'avaluació a llarg termini.

Per acabar, aquest treball proporciona dades concretes i aplicables per a docents que vulguin innovar a l'aula utilitzant metodologies actives. La gamificació, aplicada d'una manera adequada, es presenta com una

eina potent per a millorar l'aprenentatge i la implicació de l'alumnat en assignatures tècniques i complexes com la ciberseguretat.

A més, futurs estudis podrien explorar l'impacte d'aquesta metodologia en diferents perfils d'estudiants, analitzar l'efecte que té a llarg termini, o combinar-la amb altres estratègies actives d'aprenentatge.

9. Referències

Alsawaier, R. S. (2018). The effect of gamification on motivation and engagement. In *International Journal of Information and Learning Technology* (Vol. 35, Issue 1, pp. 56–79). Emerald Group Publishing Ltd. https://doi.org/10.1108/IJILT-02-2017-0009

Arrogante, O. (2022). Sampling techniques and sample size calculation: How and how many participants should I select for my research? In *Enfermeria Intensiva* (Vol. 33, Issue 1, pp. 44–47). Ediciones Doyma, S.L. https://doi.org/10.1016/j.enfi.2021.03.004

Balon, T., & Baggili, I. (Abe). (2023). Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education. *Education and Information Technologies*, *28*(9), 11759–11791. https://doi.org/10.1007/s10639-022-11451-4

Basten, D. (2017). *SOFTWARE TECHNOLOGY Gamification*. *34*(5), 76–81. https://doi.org/10.1109/MS.2017.3571581

Blažič, A. J., & Blažič, B. J. (2024). Toward effective learning of cybersecurity: new curriculum agenda and learning methods. *Journal of Cybersecurity*, *10*(1). https://doi.org/10.1093/cybsec/tyae018

Boudadi, N. A., & Gutiérrez-Colón, M. (2020). Effect of Gamification on students' motivation and learning achievement in Second Language Acquisition within higher education: a literature review 2011-2019. *The EUROCALL Review*, *28*(1). https://doi.org/10.4995/eurocall.2020.12974

Froment, F., González, A. J. G., Gómez-Millán, M. R. B., & Esquiva, Y. I. C. (2021). Adaptation and validation in spanish of the state motivation scale in university students. *Revista Iberoamericana de Diagnostico y Evaluacion Psicologica*, *58*(1), 117–126. https://doi.org/10.21865/RIDEP58.1.10

González Casas, D., Dorado Barbé, A., Gálvez Nieto, J. L., & Pérez Viejo, J. M. (2023). Psychometric Properties of the Academic Satisfaction Scale in a Sample of Spanish University Students. *Revista Iberoamericana de Diagnostico y Evaluacion Psicologica*, *69*(3), 89–100. https://doi.org/10.21865/RIDEP69.3.08

Karagiannis, S., & Magkos, E. (2020). Adapting CTF challenges into virtual cybersecurity learning environments. *Information and Computer Security*, *29*(1), 105–132. https://doi.org/10.1108/ICS-04-2019-0050

Karagiannis, S., Ntantogian, C., Magkos, E., Ribeiro, L. L., & Campos, L. (2021). PocketCTF: A fully featured approach for hosting portable attack and defense cybersecurity exercises. *Information (Switzerland)*, *12*(8). https://doi.org/10.3390/info12080318

Khodabandelou, R., Roghanian, P., Gheysari, H., & Amoozegar, A. (2023). A systematic review of gamification in organizational learning. In *Learning Organization* (Vol. 30, Issue 2, pp. 251–272). Emerald Publishing. https://doi.org/10.1108/TLO-05-2022-0057

Kim, S. K., Jang, E. T., Park, H., & Park, K. W. (2023). Pwnable-Sherpa: An interactive coaching system with a case study of pwnable challenges. *Computers and Security*, *125*. https://doi.org/10.1016/j.cose.2022.103009

Krathwohl, D., Airasian, P., Cruikshank, K. A., Mayer, R. E., Pintrich, P., Raths, J., & Wittrock, M. C. (2005). *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives* (Vol. 83, Issue 3).

Medrano, L. A., & Pérez, E. (2010). *Adaptación de la Escala de Satisfacción Académica a la Población Universitaria de Córdoba Adaptation of Academic Satisfaction Scale to University Population from Córdoba*. *7*(2), 5–14.

Morales, G. G., Del Rosario Cruz Cruz, M., Ramón, J., & Quezada, N. (n.d.). *Revista Española de Educación Médica*. https://orcid.org/0009-0007-6236-2647.3Vicerrectoríaacadémica,UniversidadHipócrates;jnieto@uhipocrates.edu.mx,https://orcid.org/0009-0007

Ortiz-Garces, I., Gutierrez, R., Guerra, D., Sanchez-Viteri, S., & Villegas-Ch, W. (2023). Development of a Platform for Learning Cybersecurity Using Capturing the Flag Competitions. *Electronics (Switzerland)*, *12*(7). https://doi.org/10.3390/electronics12071753

Ryan, R. M., & Deci, E. L. (2000a). Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemporary Educational Psychology*, *25*(1), 54–67. https://doi.org/10.1006/ceps.1999.1020

Ryan, R. M., & Deci, E. L. (2000b). *La Teoría de la Autodeterminación y la Facilitación de la Motivación Intrínseca, el Desarrollo Social, y el Bienestar Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being*. *55*(1), 68–78. https://doi.org/10.1037110003-066X.55.1.68

Stover, J. B., de la Iglesia, G., Boubeta, A. R., & Liporace, M. F. (2012). Academic motivation scale: Adaptation and psychometric analyses for high school and college students. *Psychology Research and Behavior Management*, *5*, 71–83. https://doi.org/10.2147/prbm.s33188

Toala Ponce, S. R., Gómez Pinillo, L. Y., Guevara Heredia, R. N., & Quiñonez Ortiz, E. C. (2022). Application of Bloom's taxonomy to improve teaching-learning. *Sapienza*, *3*(6), 176–189. https://doi.org/10.51798/sijis.v3i6.507

10. Annexos

I. Escales pre i post intervenció

I.I. Escala de Motivació Acadèmica

Classe: _____	Identificació d'estudiant: _____

Escala de Motivació Acadèmica (EMA)

		Totalmente en desacuerdo	Un poco de acuerdo	Bastante de acuerdo	Totalmente de acuerdo
1	Porque disfruto debatiendo/comunicando/escribiendo mis ideas a otros.				
2	Por la satisfacción que experimento mientras me supero a mí misma/o en mis estudios.				
3	Porque disfruto aprendiendo cosas nuevas.				
4	Porque pienso que la educación secundaria me ayudará a estar mejor preparada/o para el proyecto de vida que decida.				
5	Porque cuando tengo éxito en el colegio me siento importante.				
6	Porque se necesita por lo menos un título secundario para encontrar un trabajo bien pago en el futuro.				
7	Honestamente, no lo sé; realmente siento que estoy perdiendo el tiempo en el colegio.				
8	Por el placer que experimento cuando participo en debates interesante con algunos profesores.				
9	Por la satisfacción que experimento mientras me supero a mí misma/o en mis metas personales.				
10	Porque me gusta descubrir nuevos temas que nunca antes había visto.				
11	Porque es posible que me permita entrar en el mercado laboral en el campo que me gusta.				
12	Porque me gusta tener buenas notas y que me feliciten por eso.				
13	Para obtener un trabajo más prestigioso en el futuro.				
14	Hace un tiempo tenía razones para ir al colegio; sin embargo, ahora me pregunto si continuar o no.				
15	Por el placer de leer sobre temas que me interesan.				
16	Por la satisfacción que siento cuando logro llevar a cabo actividades académicas difíciles.				
17	Porque disfruto cuando aumento mi conocimiento sobre temas que me atraen.				
18	Porque, en nuestra sociedad, es importante ir al colegio.				

19	Porque no quiero ser un/a fracasado/a.				
20	Para tener un mejor sueldo en el futuro.				
21	No puedo entender por qué voy al colegio y, francamente, me importa muy poco.				
22	Por la satisfacción de hacer algo que me gusta, como por ejemplo, escribir un cuento en Castellano, o hacer un experimento en Biología, o preparar un proyecto o monografía, etc.				
23	Porque la escuela secundaria me permite experimentar un logro personal en mi búsqueda de la excelencia en mis estudios.				
24	Porque mis estudios me permiten continuar aprendiendo muchas cosas que me interesan.				
25	Porque creo que mi educación secundaria mejorará mis capacidades como trabajador/a.				
26	Porque no quiero decepcionar a mi familia.				
27	No lo sé; no puedo entender qué hago en el colegio.				

I.II. Escala de Satisfacció Acadèmica

Classe: _____	Identificació d'estudiant: _____

Escala de Satisfacció Acadèmica (ESA)

		Nunca	Raramente	Frecuentemente	Siempre
1	Las clases me interesan				
2	Me siento motivado con el curso				
3	Me gustan mi profesorado				
4	Me gustan las clases que recibo				
5	El curso responde a mis expectativas				
6	Me siento a gusto con el curso				
7	El profesorado es abierto al diálogo				
8	Siento que los contenidos de las clases se corresponden con los de mi profesión				

I.III. Escala de coneixements

Classe: _____	Estudiant ID: _____
Edat: _____	Sexe: _____

Sección 1: Pentesting en SSH (5 puntos)

1. ¿Cuál de los siguientes comandos de nmap te permite identificar la versión del servicio SSH en una máquina?

a) nmap -sV -p 22 <IP>
b) nmap -O <IP>
c) nmap -A -p 80 <IP>
d) nmap -Pn -p 22 <IP>

2. ¿Qué herramienta se utiliza para realizar ataques de fuerza bruta en SSH?

a) gobuster
b) sqlmap
c) hydra
d) crunch

3. ¿Qué comando de hydra permite realizar un ataque de fuerza bruta a SSH contra el usuario admin en el host 192.168.1.10 con una lista de contraseñas passwords.txt?

a) hydra -L admin -P passwords.txt ssh://192.168.1.10
b) hydra -l admin -P passwords.txt 192.168.1.10 ssh
c) hydra -U admin -W passwords.txt 192.168.1.10 ssh
d) hydra -U admin -L passwords.txt ssh://192.168.1.10

4. ¿Qué estrategia ayuda a mitigar ataques de fuerza bruta en SSH?

a) Permitir acceso solo con autenticación de clave pública
b) Usar contraseñas cortas y fáciles de recordar
c) Habilitar el acceso root por SSH
d) Desactivar el firewall en el servidor

5. Si el administrador cambió el puerto de SSH, ¿qué escaneo de nmap permite encontrar el nuevo puerto?

a) nmap -p- <IP>
b) nmap -sU <IP>
c) nmap -sC -p 22 <IP>
d) nmap -A -p 445 <IP>

Sección 2: Pentesting en SQL Inyección (5 puntos)

6. ¿Qué herramienta permite detectar y explotar vulnerabilidades de inyección SQL automáticamente?

a) hydra
b) sqlmap
c) nmap
d) crunch

7. ¿Qué opción de sqlmap permite enumerar las bases de datos disponibles en un sistema vulnerable?

a) --dump
b) --dbs
c) --tables
d) --users

8. Has encontrado un formulario de login en http://victima.com/login.php. ¿Cuál de los siguientes parámetros podrías probar para detectar SQLi con sqlmap?

a) sqlmap -u "http://victima.com/login.php" --forms --dbs
b) sqlmap -u "http://victima.com/login.php" --passwords
c) sqlmap -u "http://victima.com/login.php" --ftp
d) sqlmap -u "http://victima.com/login.php" --tcp

9. ¿Para qué se usa gobuster en un test de seguridad?

a) Descubrir directorios y archivos ocultos en un servidor web
b) Realizar ataques de fuerza bruta en bases de datos
c) Extraer información de contraseñas almacenadas
d) Escanear puertos abiertos en una red

10. ¿Cuál de las siguientes medidas reduce la probabilidad de una inyección SQL?

a) Usar consultas preparadas y validación de entradas
b) Permitir cualquier entrada sin filtrado en las consultas SQL
c) Usar nombres de usuario y contraseñas débiles en la base de datos
d) Exponer la base de datos directamente a internet sin restricciones

II. Fotos de la intervenció

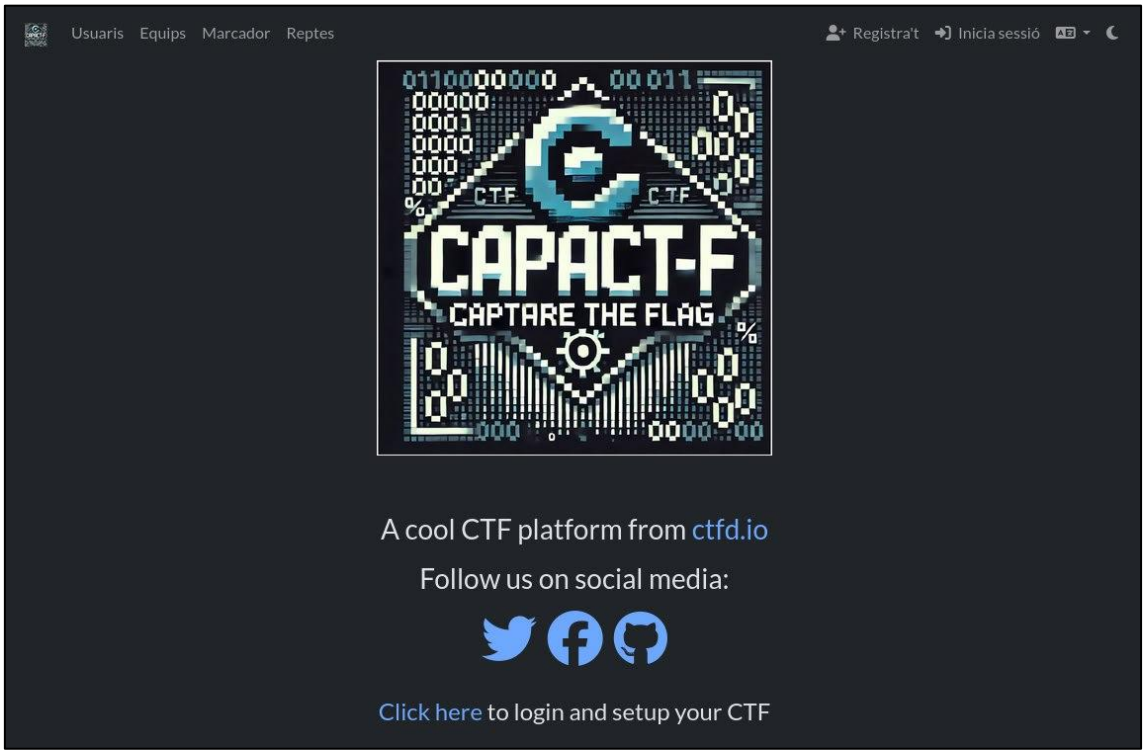

Figura 6: Portada de la plataforma CTF

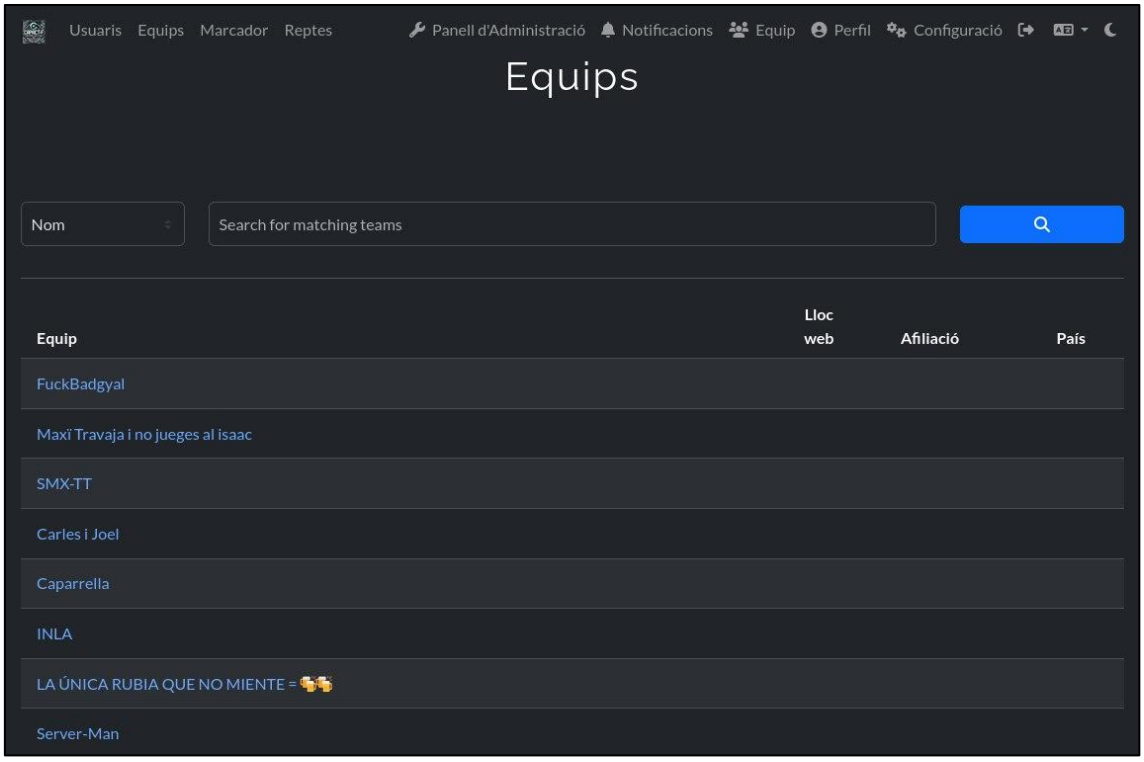

Figura 7: Formació dels equips

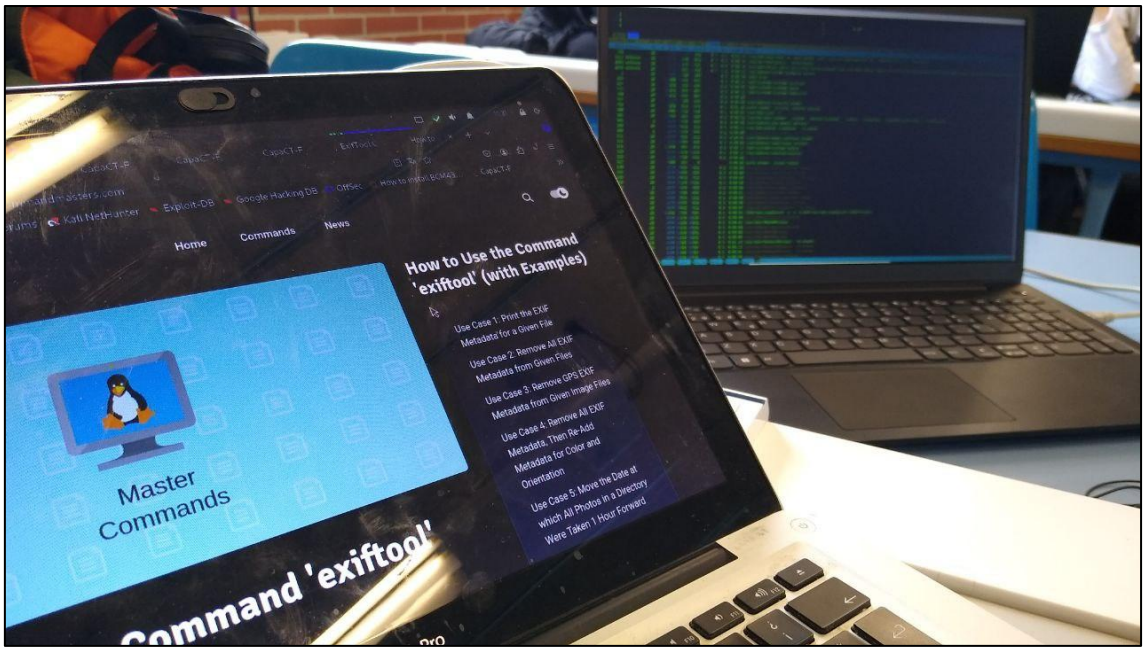

Figura 8: Anàlisi de xarxes i consulta d'informació

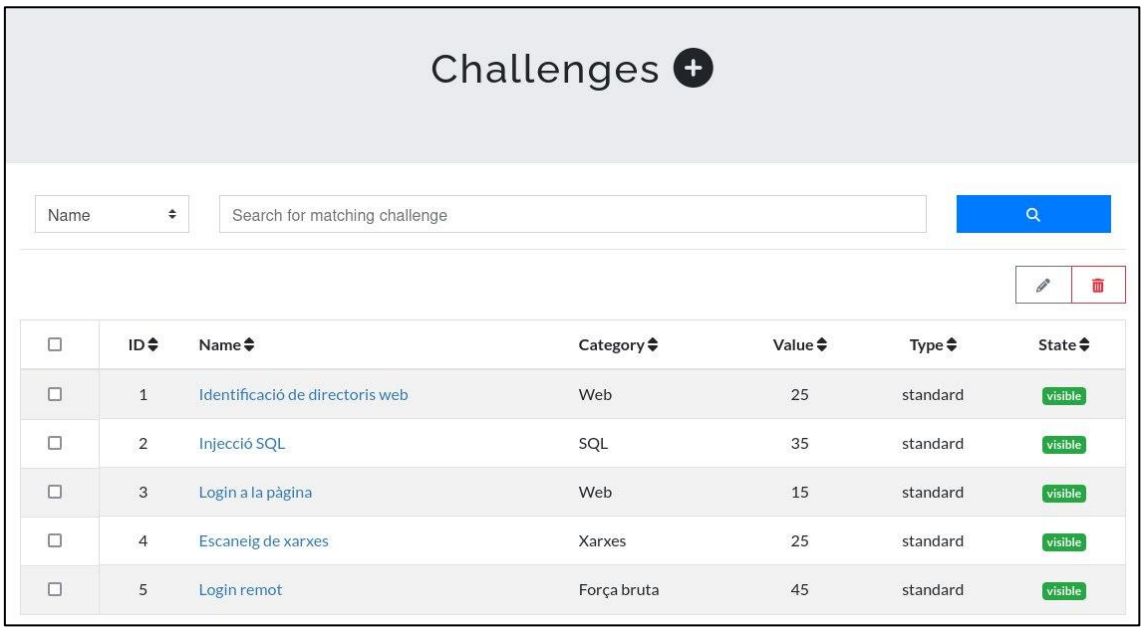

Figura 9: Reptes a assolir pels alumnes

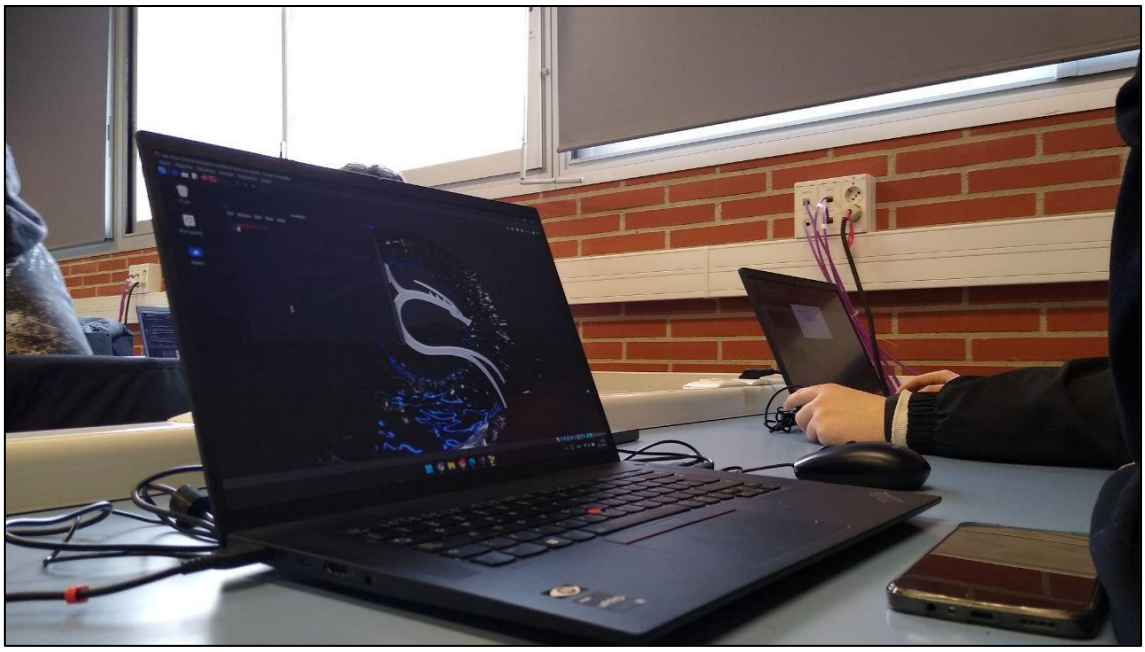

Figura 10: Sistema Operatiu per a fer auditories informàtiques "Kali Linux"

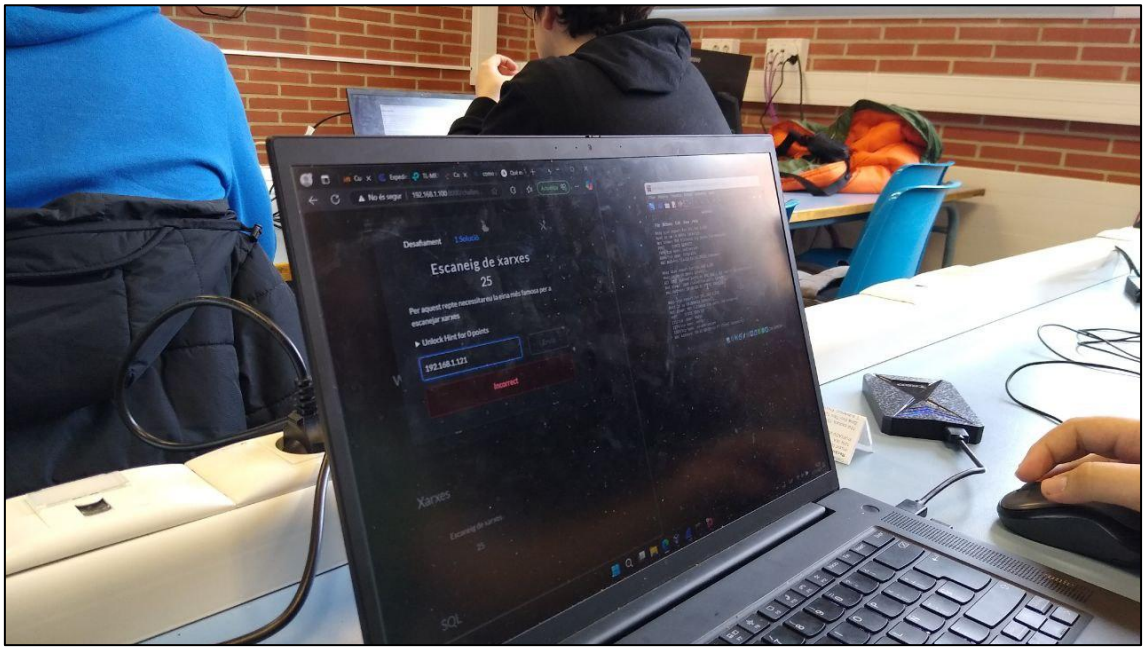

Figura 11: Anàlisi de xarxes 1

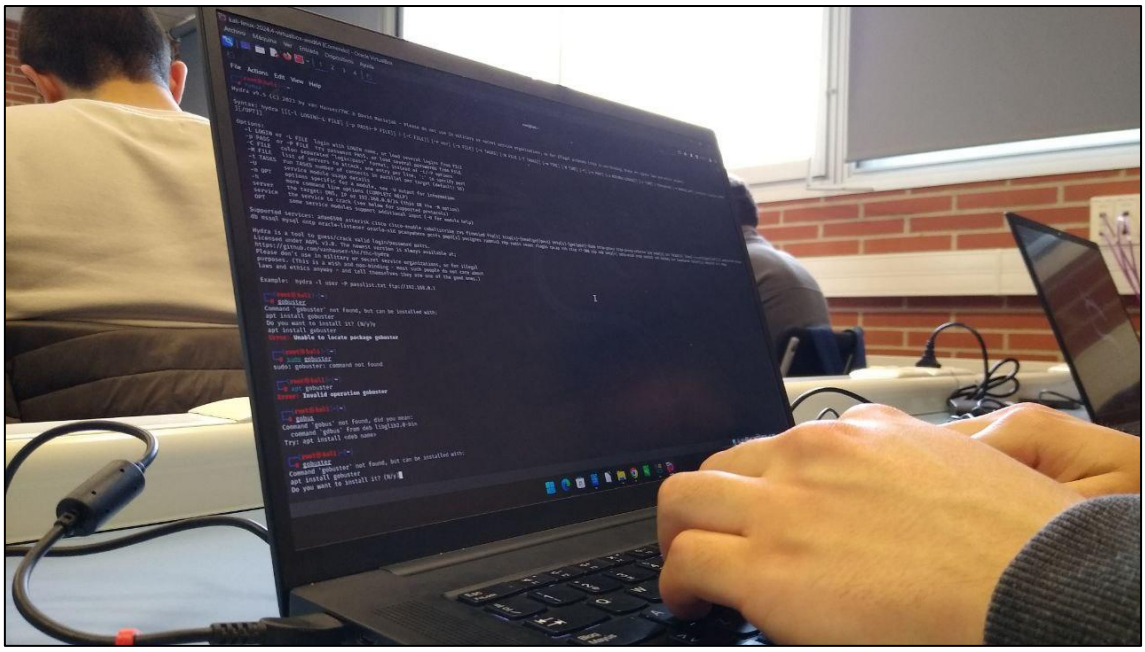

Figura 12: Anàlisi de xarxes 2

```
ruben@kaliBook: ~
Archivo  Acciones  Editar  Vista  Ayuda
ruben@kaliBook: ~   ruben@kaliBook: ~
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "secret" - 42 of 14344400 [child 12] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "andrea" - 43 of 14344400 [child 9] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "carlos" - 44 of 14344400 [child 8] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "jennifer" - 45 of 14344400 [child 10] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "joshua" - 46 of 14344400 [child 11] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "bubbles" - 47 of 14344400 [child 8] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "1234567890" - 48 of 14344400 [child 2] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "superman" - 49 of 14344400 [child 5] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "hannah" - 50 of 14344400 [child 6] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "amanda" - 51 of 14344400 [child 0] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "loveyou" - 52 of 14344400 [child 3] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "pretty" - 53 of 14344400 [child 4] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "basketball" - 54 of 14344400 [child 7] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "andrew" - 55 of 14344400 [child 14] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "angels" - 56 of 14344400 [child 12] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "tweety" - 57 of 14344400 [child 15] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "flower" - 58 of 14344400 [child 9] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "playboy" - 59 of 14344400 [child 10] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "hello" - 60 of 14344400 [child 11] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "elizabeth" - 61 of 14344400 [child 1] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "hottie" - 62 of 14344400 [child 8] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "tinkerbell" - 63 of 14344400 [child 0] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "charlie" - 64 of 14344400 [child 2] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "samantha" - 65 of 14344400 [child 3] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "barbie" - 66 of 14344400 [child 4] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "chelsea" - 67 of 14344400 [child 5] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "lovers" - 68 of 14344400 [child 6] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "teamo" - 69 of 14344400 [child 7] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "jasmine" - 70 of 14344400 [child 12] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "brandon" - 71 of 14344400 [child 14] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "666666" - 72 of 14344400 [child 9] (0/1)
[ATTEMPT] target 192.168.1.167 - login "osboxes" - pass "shadow" - 73 of 14344400 [child 15] (0/1)
[2522][ssh] host: 192.168.1.167   login: osboxes   password: charlie
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-07 17:25:08
```

Figura 13: Atac contra sistema SSH

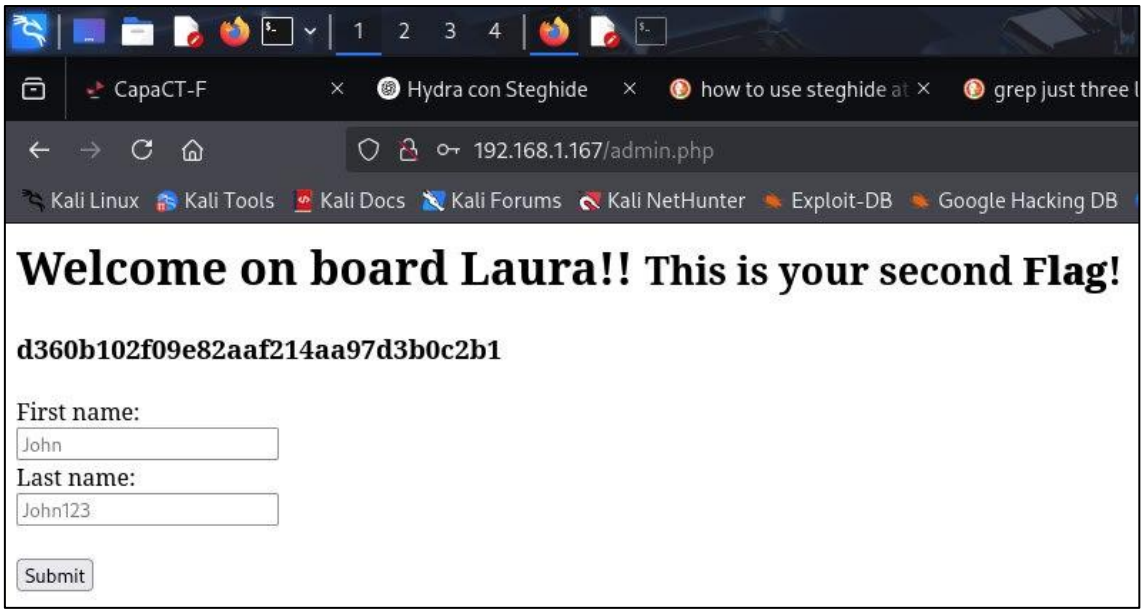

Figura 14: Obtenció de la 2a flag

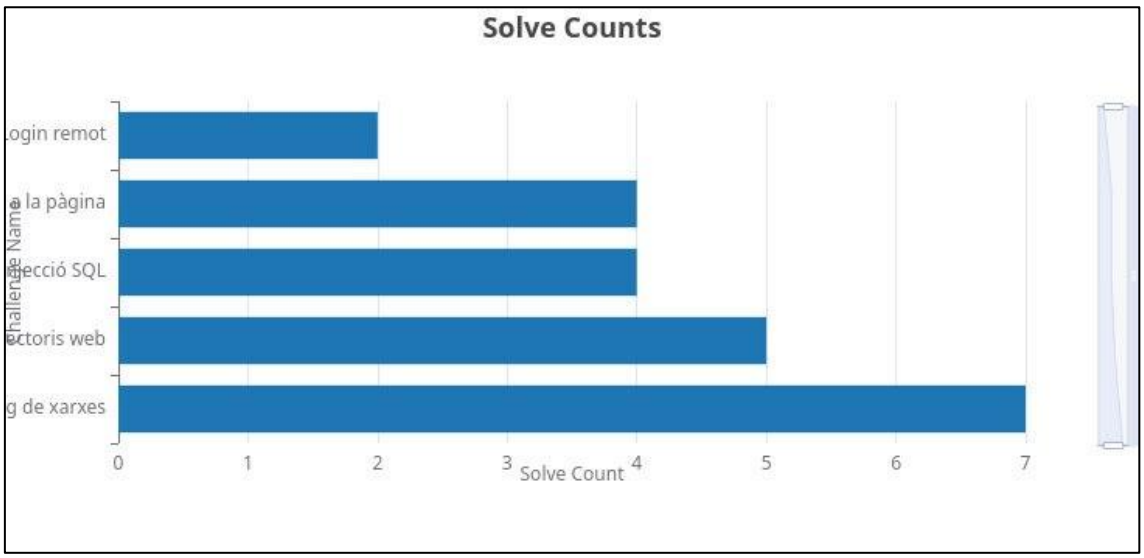

Figura 15: Quantitat de reptes assolits pels estudiants

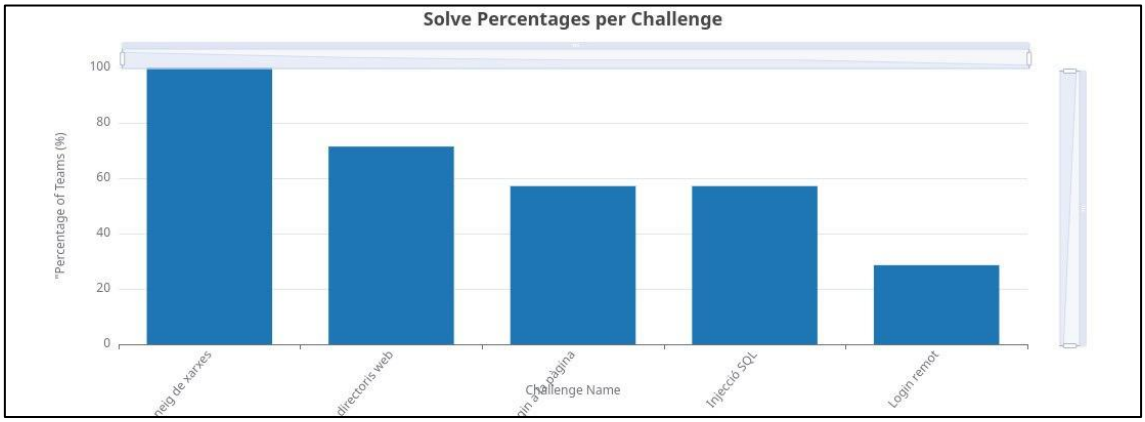

Figura 16: Puntuació per repte

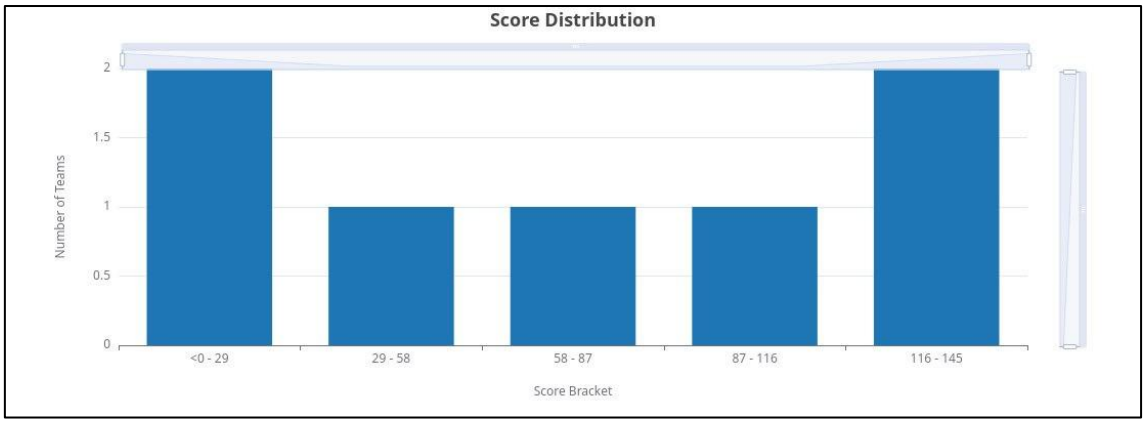

Figura 17: Distribució de puntuacions per equips

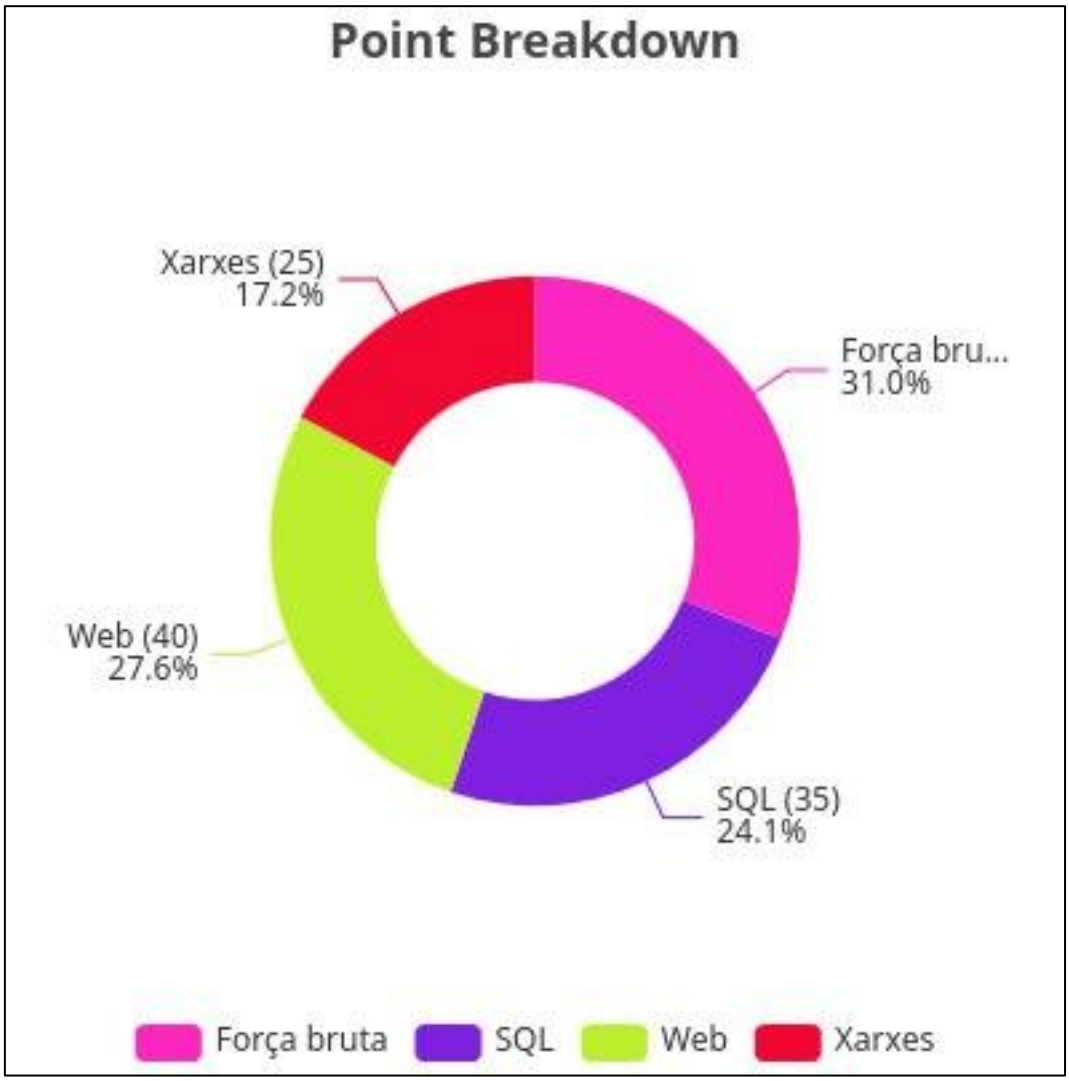

Figura 18: Quantitat de respostes dels equips per repte

III. Taules estadística

Satisfacció

Taula 13: Estadístiques descriptives satisfacció

	Pre		Post	
	0	1	0	1
Valid	20	20	20	20
Missing	0	0	0	0
Mean	14.450	13.350	15.600	14.500
Std. Deviation	4.513	3.514	5.576	3.035
Minimum	6.000	4.000	0.000	9.000
Maximum	24.000	19.000	24.000	18.000

Taula 14: T de Student per mostres independents (satisfacció)

	t	df	p
Pre	0.860	38	0.395
Post	0.775	38	0.443

Taula 15: Test de Levenne (satisfacció)

	F	df_1	df_2	p
Pre	1.284	1	38	0.264
Post	0.929	1	38	0.341

Motivació

Taula 16: Estadístiques descriptives motivació

	Pre		Post	
	0	1	0	1
Valid	20	20	19	20
Missing	0	0	1	0
Mean	2.843	2.798	2.726	3.134
Std. Deviation	0.387	0.224	0.500	0.284
Minimum	2.150	2.330	2.190	2.520
Maximum	3.780	3.070	4.000	3.540

Taula 17: T de Student per mostres independents (motivació)

	t	df	p
Pre	0.450	38	0.655
Post	-3.154	37	0.003

Note. Student's t-test.

Taula 18: Test de Levenne (motivació)

	F	df_1	df_2	p
Pre	2.149	1	38	0.151
Post	2.221	1	37	0.145

Coneixement

Taula 19: Estadístiques descriptives coneixement

	Pre		Post	
	0	1	0	1
Valid	20	20	20	20
Missing	0	0	0	0
Mean	4.600	4.900	6.250	8.200
Std. Deviation	0.503	0.641	2.245	1.361
Minimum	4.000	4.000	0.000	6.000
Maximum	5.000	6.000	10.000	10.000

Taula 20: T de Student per mostres independents (coneixements)

	t	df	p
Pre	-1.648	38	0.108
Post	-3.322	38	0.002

Note. Student's t-test.

Taula 21: Test de Levenne (coneixements)

	F	df_1	df_2	p
Pre	0.087	1	38	0.770
Post	0.964	1	38	0.332

Estadística descriptiva

Taula 22: Estadístiques descriptives

	Sexe		Edat	
	0	1	0	1
Valid	20	20	20	20
Missing	0	0	0	0
Mean			18.500	17.550
Std. Deviation			1.960	0.605
Minimum			17.000	17.000
Maximum			26.000	19.000

Taula 23: Freqüències per sexe

G. Experimental	Sexe	Frequency	Percent	Valid Percent	Cumulative Percent
0	Dona	1	5.000	5.000	5.000
	Home	19	95.000	95.000	100.000
	Missing	0	0.000		
	Total	20	100.000		
1	Dona	1	5.000	5.000	5.000
	Home	19	95.000	95.000	100.000
	Missing	0	0.000		
	Total	20	100.000		

Taula 24: Freqüències per edat

G. Experimental	Edat	Frequency	Percent	Valid Percent	Cumulative Percent
0	17	5	25.000	25.000	25.000
	18	8	40.000	40.000	65.000
	19	5	25.000	25.000	90.000
	20	1	5.000	5.000	95.000
	26	1	5.000	5.000	100.000
	Missing	0	0.000		
	Total	20	100.000		
1	17	10	50.000	50.000	50.000
	18	9	45.000	45.000	95.000
	19	1	5.000	5.000	100.000
	Missing	0	0.000		
	Total	20	100.000		

Sexe

0

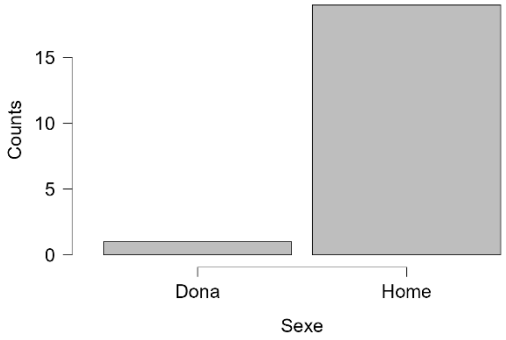

Figura 19: Diagrama sexe grup control

1

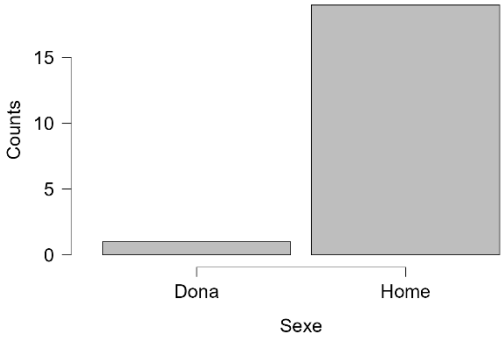

Figura 20: Diagrama sexe grup experimental

Edat

0

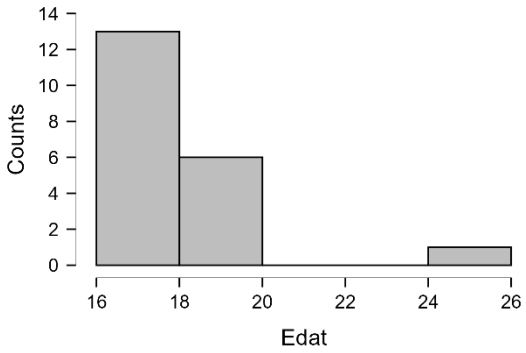

Figura 21: Diagrama edat grup control

1

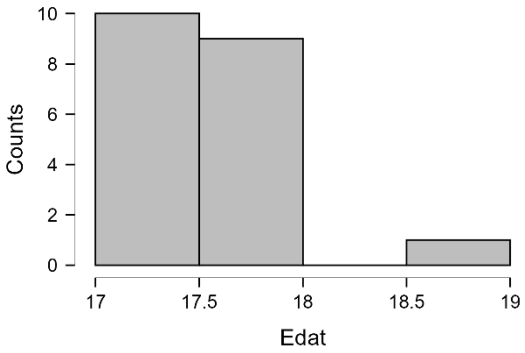

Figura 22: Diagrama edat grup experimental

VI. Situació d'Aprenentatge

Taula 25: MP6 (Seguretat Informàtica)

MP 6: Seguretat informàtica	UF 1: seguretat passiva	RA1: Aplica mesures de seguretat passiva en sistemes informàtics descrivint característiques d'entorns i relacionant-les amb les seves necessitats.	24 h
	UF 2: còpies de seguretat	RA1: Gestiona dispositius d'emmagatzematge descrivint els procediments efectuats i aplicant tècniques per assegurar la integritat de la informació.	26 h
	UF 3: legislació de seguretat i protecció de dades	RA1: Reconeix la legislació i la normativa sobre seguretat i protecció de dades analitzant-ne les repercussions de l'incompliment.	20 h
	UF 4: seguretat activa	**RA1**: Aplica mecanismes de seguretat activa descrivint-ne les característiques i relacionant-les amb les necessitats d'ús del sistema informàtic.	24 h
	UF 5: tallafocs i monitoratge de xarxes	**RA1**: Assegura la privadesa de la informació transmesa en xarxes informàtiques descrivint vulnerabilitats i instal·lant programari específic.	38 h

UF 1: seguretat passiva

Resultats d'aprenentatge i criteris d'avaluació (RA):

1. Aplica mesures de seguretat passiva en sistemes informàtics descrivint característiques d'entorns i relacionant-les amb les seves necessitats.

Criteris d'avaluació (CA):

1.1 Descriu les diferències entre seguretat física i lògica.
1.2 Defineix les característiques de la ubicació física i condicions ambientals dels equips i servidors.
1.3 Identifica la necessitat de protegir físicament els sistemes informàtics.
1.4 Verifica el funcionament dels sistemes d'alimentació ininterrompuda.
1.5 Selecciona els punts d'aplicació dels sistemes d'alimentació ininterrompuda.
1.6 Esquematitza les característiques d'una política de seguretat basada en llistes de control d'accés detallant-hi l'organització d'usuaris i grups per garantir la seguretat de la informació i funcionalitats suportades per l'equip informàtic, segons les especificacions tècniques.
1.7 Valora els avantatges que suposa la utilització de sistemes biomètrics i la importància d'establir una política de contrasenyes.
1.8 Identifica els tipus d'accés al sistema així com els mecanismes de seguretat descrivint-ne les característiques principals i eines associades més comunes per garantir l'ús dels recursos del sistema.
1.9 Explica els procediments dels sistemes per establir permisos i drets d'usuaris, detallant-ne l'organització i les eines administratives associades per organitzar polítiques de seguretat, segons els procediments establerts en el programari base.
1.10 Comprova el registre dels usuaris i grups a l'inventari, registrant-hi els canvis detectats.

Continguts (C):

1. Seguretat física i seguretat lògica:
1.1 Ubicació física i condicions ambientals dels equips i servidors.
1.2 Protecció física dels sistemes informàtics.
1.3 Els sistemes d'alimentació ininterrompuda.
1.4 Aplicació dels sistemes d'alimentació ininterrompuda.
1.5 Polítiques de seguretat basades en llistes de control d'accés.
1.6 Polítiques de contrasenyes; sistemes biomètrics.
1.7 Mecanismes de seguretat d'accés al sistema.
1.8 Permisos i drets d'usuaris.
1.9 Gestió de l'inventari dels registres d'usuaris, incidències i alarmes.

UF 2: còpies de seguretat

Resultats d'aprenentatge i criteris d'avaluació (RA):

1. Gestiona dispositius d'emmagatzematge descrivint els procediments efectuats i aplicant tècniques per assegurar la integritat de la informació.

Criteris d'avaluació (CA):

1.1 Interpreta la documentació tècnica relativa a la política d'emmagatzematge, fins i tot en cas d'estar editada en la llengua estrangera d'ús més freqüent en el sector, utilitzant-la d'ajuda.
1.2 Té en compte factors inherents a l'emmagatzematge de la informació (rendiment, disponibilitat, accessibilitat, entre d'altres), identificant els paràmetres de configuració i els components crítics del sistema.
1.3 Classifica i enumera els principals mètodes d'emmagatzematge, inclosos els sistemes d'emmagatzematge en xarxa.
1.4 Descriu les tecnologies d'emmagatzematge redundant i distribuït.
1.5 Programa còpies de seguretat tenint en compte la freqüència i l'esquema de rotació.
1.6 Realitza còpies de seguretat amb diferents estratègies.
1.7 Utilitza suports d'emmagatzematge remots i extraïbles.
1.8 Crea i restaura imatges de còpia de seguretat de sistemes en funcionament.
1.9 Identifica la necessitat de custòdia dels suports d'emmagatzematge.
1.10 Aplica i documenta procediments de mesura de rendiment, de verificació i de detecció d'anomalies seleccionant les eines adequades i utilitzant les mètriques de rendiment adequades indicades segons especificacions tècniques rebudes.

Continguts (C):

1. Polítiques d'emmagatzematge:
1.1 Emmagatzematge de la informació: paràmetres de configuració, rendiment, disponibilitat, accessibilitat.
1.2 Mètodes d'emmagatzematge locals i en xarxa.
1.3 Tecnologies d'emmagatzematge redundant i distribuït.
1.4 Programació temporal de còpies de seguretat seguint esquemes de rotació.
1.5 Realització de còpies de seguretat seguint diverses estratègies.
1.6 Utilització de suports d'emmagatzematge remots i extraïbles.
1.7 Creació i restauració de còpies de seguretat.
1.8 Aplicació de procediments de mesura de rendiment, de verificació i de detecció d'anomalies.
1.9 Custòdia de suports d'emmagatzematge.

UF 3: legislació de seguretat i protecció de dades

Resultats d'aprenentatge i criteris d'avaluació (RA):

1. Reconeix la legislació i normativa sobre seguretat i protecció de dades analitzant-ne les repercussions de l'incompliment.

Criteris d'avaluació (CA):

1.1 Descriu la legislació sobre protecció de dades de caràcter personal.
1.2 Determina la necessitat de controlar l'accés a la informació personal emmagatzemada.
1.3 Identifica les figures legals que intervenen en el tractament i manteniment dels fitxers de dades.
1.4 Contrasta l'obligació de posar a disposició de les persones les dades personals que els concerneixen.
1.5 Descriu la legislació actual sobre els serveis de la societat de la informació i comerç electrònic.
1.6 Contrasta les normes sobre gestió de seguretat de la informació, en especial les referents al correu electrònic.
1.7 Realitza actualitzacions periòdiques dels sistemes per corregir possibles vulnerabilitats.
1.8 Verifica que les llicències d'ús dels components de programari compleixen la legislació vigent.
1.9 Descriu els plans de manteniment i d'administració de seguretat.

Continguts (C):

1. Protecció de dades:
1.1 Legislació sobre protecció de dades.
1.2 Mecanismes de control d'accés a informació personal emmagatzemada.
1.3 Tractament i manteniment de fitxers de dades.
1.4 Dades personals.
1.5 Legislació sobre els serveis de la societat de la informació, comerç i correu electrònic.
1.6 Configuració de programes clients de correu electrònic per al compliment de normes sobre gestió de seguretat de la informació.
1.7 Actualitzacions de seguretat del sistema.
1.8 Legislació sobre llicències d'ús de programari.
1.9 Plans de manteniment i d'administració de seguretat.

UF 4: seguretat activa

Resultats d'aprenentatge i criteris d'avaluació (RA4):

1. Aplica mecanismes de seguretat activa descrivint-ne les característiques i relacionant-les amb les necessitats d'ús del sistema informàtic.

Criteris d'avaluació (CA4):

1.1 Segueix plans de contingència per actuar davant de fallades de seguretat.
1.2 Identifica els mecanismes de protecció del sistema contra virus i programes maliciosos per assegurar-ne i verificar-ne l'actualització.
1.3 Verifica l'origen i l'autenticitat de les aplicacions que s'instal·len en els sistemes.
1.4 Instal·la, prova i actualitza aplicacions específiques per a la detecció i eliminació de programari maliciós, automatitzant tasques de protecció i de desinfecció.
1.5 Aplica tècniques de recuperació de dades.
1.6 Descriu sistemes d'identificació com la signatura electrònica, certificat digital, entre d'altres.
1.7 Obté i utilitza sistemes d'identificació com la signatura electrònica, el certificat digital, entre d'altres, amb la finalitat bàsica de la signatura de documents i de missatgeria electrònica, seguint la documentació que descriu els procediments.
1.8 Interpreta la documentació tècnica associada, fins i tot en cas d'estar editada en la llengua estrangera d'ús més freqüent en el sector, i utilitzant-la d'ajuda.
1.9 Detecta i resol les alarmes i les incidències de seguretat seguint les instruccions pertinents.
1.10 Realitza la documentació adient sobre les incidències de seguretat, segons indicacions de l'administrador.

Continguts (C4):

1. Alarmes i incidències de seguretat. Protecció contra programari maliciós:
1.1 Fallades de seguretat: plans de contingència.
1.2 Virus i programes maliciosos.
1.3 Utilització de mecanismes per a la verificació de l'origen i l'autenticitat d'aplicacions.
1.4 Instal·lació, prova, utilització, actualització i automatització d'eines per a la protecció i desinfecció contra programari maliciós.
1.5 Utilització de tècniques de recuperació de dades.
1.6 Sistemes d'identificació: signatura electrònica, certificat digital.

1.7 Obtenció d'identificacions digitals; utilització de signatura electrònica, especialment en documents i de missatgeria electrònica, seguint la documentació que descriu els procediments.
1.8 Interpretació i utilització com a ajuda de documentació tècnica.
1.9 Detecció i resolució d'incidències seguint les instruccions pertinents.
1.10 Documentació de les incidències de seguretat.

UF 5: tallafocs i monitoratge de xarxes

Resultats d'aprenentatge i criteris d'avaluació (RA5):

1. Assegura la privadesa de la informació transmesa en xarxes informàtiques descrivint vulnerabilitats i instal·lant programari específic.

Criteris d'avaluació (CA5):

1.1 Identifica la necessitat d'inventariar i controlar els serveis de xarxa.
1.2 Contrasta la incidència de les tècniques d'enginyeria social en els fraus informàtics i robatoris d'informació.
1.3 Dedueix la importància de minimitzar el volum de trànsit generat per la publicitat i el correu brossa.
1.4 Aplica mesures per evitar el monitoratge de xarxes cablejades.
1.5 Classifica i valora les propietats de seguretat dels protocols usats en xarxes sense fil.
1.6 Utilitza eines de control del monitoratge de xarxes.
1.7 Instal·la i configura un tallafocs en un equip o servidor, seguint la documentació tècnica associada.
1.8 Interpreta la documentació tècnica associada, fins i tot en cas d'estar editada en la llengua estrangera d'ús més freqüent en el sector, utilitzant-la d'ajuda.
1.9 Realitza informes d'incidències de seguretat detallant les activitats realitzades.

Continguts (C5):

1. Assegura la privadesa de la informació:
1.1 Inventari i control dels serveis de xarxa.
1.2 Fraus informàtics i robatoris d'informació; enginyeria social.
1.3 Publicitat i correu brossa.
1.4 Seguretat en xarxes cablejades i control del monitoratge.
1.5 Seguretat en les xarxes sense fil i en els seus protocols.
1.6 Utilització d'eines de control del monitoratge en xarxes.
1.7 Tallafocs en equips i servidors: instal·lació, configuració i utilització.
1.8 Interpretació i utilització com a ajuda de documentació tècnica.
1.9 Realització d'informes d'incidències de seguretat.

Taula 26: Programació de la intervenció (grup experimental)

MP 6: Seguretat informàtica					**Hores: 6 h (experimental)**	
Activitats d'Ensenyament-Aprenentatge			**RA**	**Continguts**	**Avaluació**	
					CA	**Instruments d'Avaluació**
A1: Introducció i pretest		**1/2 h**	**RA1 RA2**	**C4.1 C4.5 C4.8 C4.9 C4.10**	**CA4.1 CA4.5 CA4.8 CA4.9 CA4.10**	- Registre de resultats acadèmics - Avaluació inicial de coneixements
Descripció	Explicació dels objectius, enquestes de motivació i prova inicial de coneixements.					
A2: Explicació de teoria breu		**3/4 h**	**RA1 RA2**	**C4.1 C4.5 C4.8 C4.9 C4.10**	**CA4.1 CA4.5 CA4.8 CA4.9 CA4.10**	- Observació directa de l'alumnat - Registre d'anotacions qualitatives sobre el comportament i reaccions
Descripció	Introducció als conceptes clau de seguretat informàtica rellevants per als reptes CTF.					
A3: Demostració d'un CTF		**1/2 h**	**RA1 RA2**	**C4.1 C4.5 C4.8 C4.9 C4.10**	**CA4.1 CA4.5 CA4.8 CA4.9 CA4.10**	- Observació directa de l'alumnat - Registre d'anotacions qualitatives sobre el comportament i reaccions
Descripció	Mostrar un repte CTF bàsic, com resoldre'l i les eines disponibles.					
A4: Desenvolupament d'un CTF		**3 h**	**RA1 RA2**	**C4.1 C4.5 C4.8 C4.9 C4.10**	**CA4.1 CA4.5 CA4.8 CA4.9 CA4.10**	- Observació directa de l'alumnat - Registre d'anotacions qualitatives sobre el comportament i reaccions
Descripció	Els participants resolen reptes amb dificultat progressiva. - G1: Amb guia i ajuda de l'instructor. - G2: Resolució autònoma amb feedback posterior.					
A5: Reflexió i discussió grupal		**1/2 h**	**RA1 RA2**	**C4.1 C4.5 C4.8 C4.9 C4.10**	**CA4.1 CA4.5 CA4.8 CA4.9 CA4.10**	- Observació directa de l'alumnat - Registre d'anotacions qualitatives sobre el comportament i reaccions
Descripció	Compartir estratègies, dificultats i aprenentatges.					
A6: Posttest i enquestes de satisfacció		**3/4 h**		**C4.1 C4.5 C4.8**	**CA4.1 CA4.5 CA4.8**	- Registre de resultats acadèmics

MP 6: Seguretat informàtica				**Hores: 6 h (experimental)**	
Descripció	Avaluació de coneixements, motivació i satisfacció final.		**C4.9** **C4.10**	**CA4.9** **CA4.10**	- Avaluació final de coneixements

Taula 27: Programació de la intervenció (grup control)

<table>
<tr><td colspan="3">MP 6: Seguretat informàtica</td><td colspan="3">Hores: 12 h (control)</td></tr>
<tr><td colspan="3" rowspan="2">Activitats d'Ensenyament-Aprenentatge</td><td rowspan="2">RA</td><td rowspan="2">Continguts</td><td colspan="2">Avaluació</td></tr>
<tr><td>CA</td><td>Instruments d’Avaluació</td></tr>
<tr><td colspan="2">A1: Introducció i pretest</td><td>1/2 h</td><td rowspan="2">RA1
RA2</td><td rowspan="2">C4.1
C4.5
C4.8
C4.9
C4.10</td><td rowspan="2">CA4.1
CA4.5
CA4.8
CA4.9
CA4.10</td><td rowspan="2">- Registre de resultats acadèmics
- Avaluació inicial de coneixements</td></tr>
<tr><td>Descripció</td><td colspan="2">Explicació dels objectius, enquestes de motivació i prova inicial de coneixements.</td></tr>
<tr><td colspan="2">A2: Explicació teòrica extensa</td><td>1 i 1/2 h</td><td rowspan="2">RA1
RA2</td><td rowspan="2">C4.1
C4.5
C4.8
C4.9
C4.10</td><td rowspan="2">CA4.1
CA4.5
CA4.8
CA4.9
CA4.10</td><td rowspan="2">- Observació directa de l’alumnat
- Registre d’anotacions qualitatives sobre el comportament i reaccions</td></tr>
<tr><td>Descripció</td><td colspan="2">Classe tradicional sobre seguretat informàtica.</td></tr>
<tr><td colspan="2">A3: Resolució d’exercicis</td><td>2 i 2/4 h</td><td rowspan="2">RA1
RA2</td><td rowspan="2">C4.1
C4.5
C4.8
C4.9
C4.10</td><td rowspan="2">CA4.1
CA4.5
CA4.8
CA4.9
CA4.10</td><td rowspan="2">- Observació directa de l’alumnat
- Registre d’anotacions qualitatives sobre el comportament i reaccions</td></tr>
<tr><td>Descripció</td><td colspan="2">- G3: Exercicis teòrics.
- G4: Problemes pràctics tradicionals.</td></tr>
<tr><td colspan="2">A4: Discussió grupal</td><td>1/2 h</td><td rowspan="2">RA1
RA2</td><td rowspan="2">C4.1
C4.5
C4.8
C4.9
C4.10</td><td rowspan="2">CA4.1
CA4.5
CA4.8
CA4.9
CA4.10</td><td rowspan="2">- Observació directa de l’alumnat
- Registre d’anotacions qualitatives sobre el comportament i reaccions</td></tr>
<tr><td>Descripció</td><td colspan="2">Reflexió sobre el que s’ha après.</td></tr>
<tr><td colspan="2">A5: Posttest i enquestes de satisfacció</td><td>3/4 h</td><td rowspan="2">RA1
RA2</td><td rowspan="2">C4.1
C4.5
C4.8
C4.9
C4.10</td><td rowspan="2">CA4.1
CA4.5
CA4.8
CA4.9
CA4.10</td><td rowspan="2">- Registre de resultats acadèmics
- Avaluació final de coneixements</td></tr>
<tr><td>Descripció</td><td colspan="2">Avaluació de coneixements i enquestes.</td></tr>
</table>