UNIVERSIDAD A DISTANCIA DE MADRID

(UDIMA)

Facultad de Ciencias de la Salud y de la Educación
Departamento de Educación

Máster Universitario en Formación del Profesorado de Educación Secundaria, Bachillerato, Formación Profesional y Enseñanza de Idiomas

DISEÑO DE UN ESCAPE ROOM DIGITAL COMO RECURSO INNOVADOR PARA LA ENSEÑANZA DE CIBERSEGURIDAD EN 4º ESO

María Mogica Romero

TRABAJO DE FIN DE MÁSTER

Bajo la dirección de:

Carlos Andrés Martínez Casais

MADRID
Enero 2026

Resumen

La presencia constante de las tecnologías digitales en la vida cotidiana de las personas demanda una formación que vaya más allá del simple uso instrumental, desarrollando competencias relacionadas con la seguridad, la responsabilidad y el pensamiento crítico en entornos digitales. En este contexto, la ciberseguridad se configura como un contenido educativo fundamental en Educación Secundaria Obligatoria, especialmente en la materia Digitalización de 4º ESO, de acuerdo con el marco normativo vigente.

El presente Trabajo de Fin de Máster tiene como objetivo principal diseñar un escape room educativo digital como recurso didáctico innovador para la enseñanza de ciberseguridad en 4º ESO, favoreciendo el desarrollo de la competencia digital del alumnado. La propuesta está fundamentada en el uso de metodologías activas, en particular, de la gamificación y el Aprendizaje Basado en Retos, las cuales sitúan al alumnado en el centro de su proceso de aprendizaje y promueven la motivación, la participación activa y la resolución de problemas en contextos significativos.

La intervención didáctica se plantea de una forma adaptable a distintos entornos escolares y se alinea con los principios del Diseño Universal de Aprendizaje. El escape room se estructura en cinco retos prácticos, integrados en una narrativa gamificada, que abordan contenidos clave: gestión de contraseñas, detección de phishing, identificación de malware, huella digital y privacidad. Además, se lleva a cabo una evaluación formativa con el fin de acompañar el proceso de aprendizaje del alumnado.

Como conclusión, el trabajo pone de manifiesto el potencial del escape room digital como recurso pedagógico eficaz para la enseñanza de ciberseguridad, al combinar innovación metodológica, aprendizaje significativo y el desarrollo competencial necesario para formar una ciudadanía digital crítica, segura y responsable.

Palabras clave: *ciberseguridad, competencia digital, escape room educativo, gamificación, metodologías activas.*

Índice

Índice de figuras

Índice de tablas

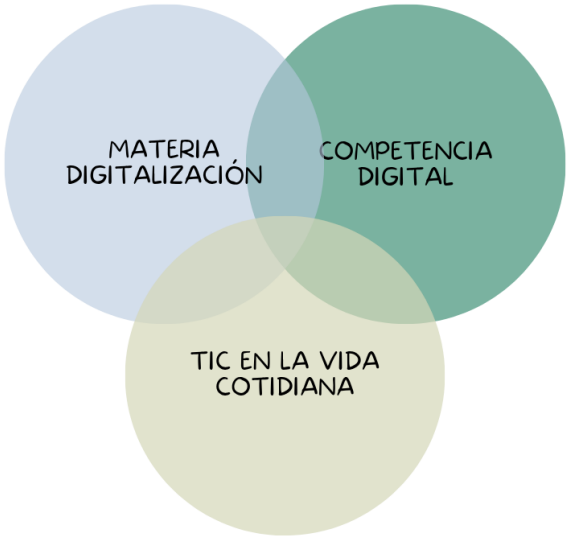
1. Introducción

La sociedad actual se caracteriza por la presencia constante de las TIC (tecnologías de la información y la comunicación), así como por el avance continuo hacia un mundo digital. Es por esto que el proceso de enseñanza-aprendizaje de los jóvenes no debe contemplar únicamente la adquisición de habilidades técnicas básicas, sino también de competencias críticas, seguras y responsables en el ámbito digital. En este contexto, la ciberseguridad adquiere gran relevancia como ámbito educativo, tanto desde la perspectiva de la prevención de riesgos como de la formación de una ciudadanía digital competente. El presente Trabajo de Fin de Máster, titulado "Diseño de un escape room digital como recurso innovador para la enseñanza de ciberseguridad en 4º ESO", se enmarca dentro de esta línea y propone una intervención didáctica que combina contenido disciplinar (ciberseguridad) con innovación metodológica (escape room digital) en la etapa de la Educación Secundaria Obligatoria.

El tema a tratar se encuentra en la convergencia de tres ámbitos clave (ver Figura 1): por una parte, el marco curricular de la materia Digitalización en 4º ESO. Según el Real Decreto 217/2022, de 29 de marzo, por el que se establece la ordenación y las enseñanzas mínimas de la Educación Secundaria Obligatoria, uno de los planteamientos de la asignatura Digitalización es que "la formación de la ciudadanía actual va más allá de la alfabetización digital, ya que requiere una atención específica a la adquisición de los conocimientos necesarios para usar los medios tecnológicos de manera ética, responsable, segura y crítica" (RD 217/2022, p. 42). En este sentido, la materia organiza sus saberes básicos en cuatro bloques: «Dispositivos digitales, sistemas operativos y de comunicación», «Digitalización del entorno personal de aprendizaje», «Seguridad y bienestar digital» y «Ciudadanía digital crítica» (RD 217/2022, p. 43). Por otra parte, en el Perfil de salida al término de la enseñanza básica se incluye la competencia digital como una de las competencias clave, definida como "el uso seguro, saludable, sostenible, crítico y responsable de las tecnologías digitales para el aprendizaje, para el trabajo y para la participación en la sociedad […]. Incluye […] la seguridad (incluido el bienestar digital y las competencias relacionadas con la ciberseguridad)" (RD 217/2022, p. 29). Finalmente, el interés (y la preocupación) por incluir la ciberseguridad en el ámbito educativo se fundamenta en la interacción sistemática y cada vez más temprana de los jóvenes con dispositivos, redes sociales y plataformas digitales, lo que plantea riesgos (como el ciberacoso, la suplantación de identidad, la vulneración de datos personales o la dependencia tecnológica) y exige el desarrollo de actitudes de prevención, responsabilidad y uso crítico.

Figura 1

Esquema de los ámbitos que convergen hacia la temática de la ciberseguridad



Nota. Elaboración propia.

Desde un punto de vista disciplinar, la ciberseguridad se trata de un contenido educativo emergente y que repercute en muchos aspectos de la vida cotidiana. El aumento de la exposición a los entornos digitales requiere que la formación del alumnado alcance una mayor profundidad, no solo conociendo el uso de las herramientas, sino entendiendo sus vulnerabilidades y riesgos, dando importancia a la identidad digital y fomentando la prevención y el actuar de una manera ética. En el currículo de la materia Digitalización se incluye explícitamente como competencia específica 3: "Desarrollar hábitos que fomenten el bienestar digital, aplicando medidas preventivas y correctivas, para proteger dispositivos, datos personales y la propia salud." (RD 217/2022, p. 44). Esto realza el hecho de que el aprendizaje de ciberseguridad tiene una vertiente meramente técnica, pero también contribuye a la formación de una ciudadanía digital crítica y con valores. Por otra parte, desde un punto de vista metodológico, llevar a cabo esta propuesta didáctica mediante un escape room digital representa una innovación educativa alineada con, según Negre y Carrión (2020), un aprendizaje activo, transversal y colaborativo, potenciando la resolución de problemas, la comunicación, el pensamiento deductivo y la resiliencia del alumnado. Además, sitúa al estudiante como protagonista de su aprendizaje en un entorno retador, motivador y lúdico. Este enfoque favorece el desarrollo de la competencia digital, el pensamiento computacional, la toma de decisiones y el trabajo colaborativo, todos ellos objetivos clave de la asignatura Digitalización. En cuanto a su relación con la ciberseguridad, el escape room aporta beneficios altamente relevantes: permite trabajar la

seguridad digital, la protección de datos personales, la privacidad y el uso responsable de la tecnología a través de retos prácticos y contextualizados. Además, situar al alumnado en escenarios simulados bajo cierta presión, facilita la concienciación sobre los posibles riesgos digitales, refuerza la capacidad de reacción ante amenazas y fomenta la actitud crítica y preventiva que desarrolla la competencia digital.

La justificación de este trabajo se puede plantear desde tres perspectivas. En primer lugar, incluir contenido de ciberseguridad en la educación secundaria pretende contribuir a dar respuesta a la demandas sociales y tecnológicas de la realidad actual. Se busca, por tanto, proporcionar un conocimiento integral del mundo digital, desde sus riesgos a las maneras de interactuar de una manera crítica, reflexiva y segura con él. En segundo lugar, la materia Digitalización en 4º ESO representa un escenario adecuado para acometer esta temática, ya que su estructura competencial y de saberes permite abordar de manera práctica, significativa y contextualizada temas relacionados con la identidad digital, la seguridad digital y los riesgos vinculados al uso de tecnologías. Por último, la elección de un escape room digital como recurso innovador atiende a la necesidad de hacer del proceso de enseñanza-aprendizaje un recorrido motivador, centrado en el alumnado y que favorezca la implicación y el descubrimiento del conocimiento. Este tipo de recurso educativo permite, además, combinar el aprendizaje colaborativo con la gamificación y la resolución de problemas.

Este documento se organiza en cinco apartados principales. En primer lugar, la Introducción pretende presentar el tema de estudio, así como su justificación y objetivos generales. A continuación, en el apartado de Objetivos, se enumeran tanto el objetivo general como los objetivos específicos que orientan el desarrollo del trabajo. El Marco teórico contextualiza la propuesta, basándose en los conceptos y antecedentes de la misma. En el apartado Procedimiento de la propuesta de innovación, se detalla la propuesta en sí, incluyendo el contexto, los destinatarios, la finalidad de la propuesta y su planificación. Por último, el apartado Conclusiones y valoración crítica recoge la consecución de los objetivos planteados, así como las principales reflexiones tras la realización del trabajo.

En resumen, este Trabajo de Fin de Máster plantea la propuesta de diseñar un escape room digital como recurso didáctico innovador para la enseñanza de la ciberseguridad en 4º ESO, dentro de la materia Digitalización, atendiendo al marco curricular de la Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación (LOMLOE) y del RD 217/2022, a la competencia digital del alumnado y a la necesidad social de formar ciudadanos digitales competentes, responsables y críticos.

2. Objetivos

Los objetivos del trabajo se articulan desde dos perspectivas. Por una parte, la investigación y desarrollo didáctico, dirigida al diseño y fundamentación del recurso educativo, y, por otra, la aplicación pedagógica, centrada en los aprendizajes que se espera promover en el alumnado.

2.1. Objetivo general

⇒ Diseñar un escape room digital educativo que integre contenidos de ciberseguridad, para la materia Digitalización de 4º ESO, con el fin de favorecer el desarrollo de la competencia digital, la concienciación en el uso responsable de la tecnología y la comprensión de los riesgos asociados al entorno digital.

2.2. Objetivos específicos

2.2.1. Objetivos relativos al diseño y fundamentación del recurso

⇒ Analizar el marco curricular de la materia Digitalización de 4º ESO.

- Resultados esperados:
  - Identificación de los elementos curriculares de la materia (competencias específicas, saberes básicos y criterios de evaluación), relevantes para el diseño del escape room.

⇒ Revisar literatura diversa sobre metodologías activas, gamificación y aprendizaje basado en retos, destacando su potencial motivador en la educación secundaria.

- Resultados esperados:
  - Fundamentación teórica del recurso didáctico, mediante una revisión crítica de estudios y experiencias educativas sobre metodologías activas, gamificación y aprendizaje basado en retos.

⇒ Seleccionar los contenidos de ciberseguridad, basados en los saberes básicos y competencias específicas de la materia Digitalización de 4º ESO.

- Resultados esperados:
  - Selección coherente y adecuada de contenidos relacionados con la ciberseguridad, ajustados al nivel educativo del alumnado y vinculados a los saberes básicos y competencias específicas de la materia.

⇒ Diseñar un escape room digital, estructurado en retos, desafíos y pruebas, que promueva la resolución de problemas en entornos digitales.

- Resultados esperados:
  - Diseño de un escape room digital que integre los contenidos seleccionados, así como todos los elementos analizados que favorezcan

el éxito de la propuesta, tanto desde un punto de vista didáctico como pedagógico.

⇒ Establecer los criterios de evaluación para valorar la adquisición de aprendizajes, la participación del alumnado y la eficacia del recurso como herramienta didáctica innovadora.

- Resultados esperados:
  - Establecimiento de criterios de evaluación claros y coherentes, que permitan medir los resultados de aprendizaje y la viabilidad de la propuesta innovadora.

2.2.2. Objetivos relativos al proceso de enseñanza-aprendizaje

⇒ Fomentar la adquisición de conocimientos sobre ciberseguridad, de manera que el alumnado comprenda y maneje de forma adecuada conceptos como la creación y gestión de contraseñas seguras, la protección de datos personales, la identificación de casos de suplantación de identidad y el reconocimiento de diferentes tipos de malware.

- Resultados esperados:
  - El alumnado define correctamente los conceptos básicos de ciberseguridad,
  - identifica situaciones de riesgo digital (phishing, malware y uso indebido de datos personales) en casos prácticos o simulaciones, y
  - diseña contraseñas seguras siguiendo los criterios establecidos.

⇒ Promover el desarrollo de hábitos seguros en el uso de tecnologías digitales, favoreciendo las competencias para detectar riesgos digitales y potenciando la autonomía y el pensamiento crítico para identificar vulnerabilidades y aplicar estrategias de protección digital en cualquier contexto.

- Resultados esperados:
  - El alumnado aplica buenas prácticas de seguridad digital en el uso cotidiano de dispositivos y servicios en línea,
  - analiza de forma crítica contenidos, enlaces y solicitudes de información antes de interaccionar con ellos,
  - propone y justifica medidas de protección digital adecuadas ante situaciones concretas, y
  - demuestra autonomía en la toma de decisiones relacionadas con la seguridad digital.

⇒ Motivar e interesar al alumnado hacia la materia Digitalización mediante el uso de una perspectiva lúdica y activa, mejorando su implicación y percepción de la utilidad de los contenidos.

- Resultados esperados:
  - Aumento de la participación activa del alumnado en las actividades propuestas,
  - actitud positiva y mayor grado de implicación durante las sesiones de trabajo,
  - valoración favorable de la materia y de los contenidos relacionados con la ciberseguridad, y
  - capacidad del alumnado para relacionar los contenidos aprendidos con situaciones reales de su entorno digital.

3. Marco teórico

3.1. Las metodologías activas en la educación

3.1.1. Concepto y principios de las metodologías activas

En la actualidad, las metodologías activas se han consolidado como enfoques pedagógicos centrados en el estudiante, con el objetivo de fomentar un aprendizaje significativo. Según la teoría del aprendizaje significativo de David Ausubel, "el estudiante aprende realmente cuando relaciona los nuevos conocimientos adquiridos con los conocimientos que ya posee." (BeChallenge, 2022). Esta teoría se engloba dentro de una corriente pedagógica denominada constructivismo, la cual determina que "el aprendizaje es un proceso continuo y en movimiento." (Universidad Europea, 2023). En línea con esto, las metodologías activas buscan que el alumnado sea el protagonista del proceso de enseñanza-aprendizaje, mediante la exploración, la reflexión y la resolución de problemas. El docente, en este caso, adopta un rol de guía o facilitador, lejos de ser un mero transmisor de información. En contraposición a modelos tradicionales, centrados en la figura del profesor, las metodologías activas pretenden reforzar la interacción, la colaboración y el desarrollo competencial, preparando al estudiantado para enfrentarse a entornos cambiantes.

El término metodologías activas engloba métodos, técnicas y estrategias con base en las teorías constructivistas del aprendizaje, las cuales defienden que el conocimiento se construye a través de la interacción con el entorno (Lejárraga et al., 2023).

3.1.2. Ventajas y desafíos de su implementación en la educación secundaria

La implementación de metodologías activas en la educación secundaria aporta múltiples beneficios al situar en el centro del proceso de enseñanza-aprendizaje al estudiante. En cualquier caso, también presenta desafíos considerables que deben tenerse en cuenta para sacar el máximo provecho de su uso.

Las principales ventajas que se obtienen están relacionadas con el incremento de la motivación, un mejor rendimiento académico y mayor participación activa por parte del alumnado (Gaitan & de la Cruz, 2024). Al conectar los contenidos con la realidad y los intereses de los estudiantes, estos se sienten más involucrados y motivados. Este aumento de la motivación se encuentra directamente relacionado con una mayor participación activa, puesto que el hecho de contextualizar los contenidos en situaciones reales o simuladas ayuda a la comprensión de los mismos y, por tanto, favorece la interacción y el debate. A su vez, estas dos variables se encuentran relacionadas con la mejora del rendimiento académico, dado que este enfoque favorece el aprendizaje significativo, caracterizado por construirse de una manera activa, por

lo que la comprensión resulta más profunda.

Por otra parte, el uso de metodologías activas favorece el desarrollo de habilidades y competencias transversales del alumnado, esenciales para el mundo laboral y la ciudadanía, como son el fomento de la autonomía, el pensamiento crítico, el trabajo en equipo y la resolución de conflictos, entre otras.

A pesar de sus numerosas ventajas, la aplicación de estas metodologías en el contexto de la educación secundaria enfrenta algunas dificultades que es necesario tener en cuenta. En primer lugar, es necesario tener en cuenta que, por lo general, se utilizan enfoques tradicionales, los cuales sitúan al estudiante como una figura pasiva en el proceso de enseñanza-aprendizaje. Este cambio de rol, en ocasiones, genera una resistencia al cambio, tanto por parte del alumnado, que debe adoptar una postura activa, como por parte del docente, que debe modificar también su rol. En esta línea, el profesorado requiere cierta formación específica, así como recursos para actualizar su enfoque. Por último, cabe destacar que las clases dinámicas e interactivas pueden resultar más difíciles de gestionar, sobre todo con ratios elevadas de alumnos, pudiendo surgir problemas de indisciplina.

3.1.3. Relación con la innovación educativa y el desarrollo competencial

Llegados a este punto, es necesario comprender qué se entiende por innovación educativa. Según Orrego (2022), la innovación educativa se caracteriza por introducir cambios en las prácticas actuales, manteniendo un carácter abierto y en pro del cambio constante. Además, considera que debe partir de una planificación deliberada, así como disponer de objetivos concretos. En definitiva, "la innovación educativa supone realizar un cambio significativo para mejorar el procedimiento de enseñanza-aprendizaje" (Universidad Internacional de La Rioja, 2022). En esta línea, uno de los caminos para aproximarse a la innovación educativa se enfoca en las metodologías que se utilizan en el proceso de enseñanza-aprendizaje. De esta manera, el uso de metodologías activas pretende cambiar el foco del proceso en sí, considerándose este hecho una innovación en sí misma. Además, la puesta en marcha de diferentes experiencias basadas en estas metodologías requiere la incorporación de herramientas innovadoras, ya sean tecnológicas o no, utilizadas de una manera crítica y con una finalidad específica.

Por otra parte, las metodologías activas favorecen el desarrollo competencial al dar al estudiante un papel central en el proceso de enseñanza-aprendizaje. Este enfoque promueve no solo la adquisición de conocimientos, sino también el desarrollo de habilidades, actitudes y valores (el "saber", el "saber hacer" y el "saber ser"). Al tratarse de una experiencia que busca una aplicación real o simulada de los conocimientos, el estudiante debe ser capaz de utilizar los contenidos de una forma significativa, desarrollando la competencia de resolución de

problemas. También las metodologías activas fomentan la autonomía, buscando que el alumnado gestione su propio proceso, favoreciendo el "aprender a aprender". Además, la mayoría de metodologías activas están basadas en el trabajo en equipo, exigiendo a los alumnos cooperar, negociar, argumentar y comunicar ideas, así como desarrollar el respeto y el sentido de la responsabilidad, promoviendo la mejora de competencias sociales y comunicativas.

3.2. La gamificación en el ámbito educativo

3.2.1. Concepto y fundamentos teóricos de la gamificación

La gamificación se basa en la aplicación de elementos y técnicas propias del juego en contextos no lúdicos con el objetivo de aumentar la motivación y la implicación y de favorecer la participación y el compromiso, entre otros. Para ponerla en práctica, se utilizan elementos de los juegos como puntos, niveles, insignias o logros, recompensas, clasificaciones y/o desafíos.
Existen ciertas similitudes y diferencias entre un enfoque lúdico y un enfoque gamificado. Según la Real Academia Española, el término lúdico se define como "Perteneciente o relativo al juego.", concibiendo el juego como una actividad libre, voluntaria y placentera que se realiza por diversión o entretenimiento. El enfoque gamificado, entonces, trata de ampliar el alcance del enfoque lúdico, dándole un propósito de motivación y aprendizaje significativo, haciéndose valer de todos aquellos componentes del juego que activan sistemas dopaminérgicos en las personas.
En cualquier caso, el docente asume el rol de facilitador o guía, en lugar de ser un mero transmisor de información. Su labor consiste en diseñar experiencias de aprendizaje significativas en ambientes enriquecedores. El papel del alumno se basa en construir su propio aprendizaje, adquiriendo protagonismo sobre su conocimiento. En consecuencia, su participación debe estar caracterizada por el dinamismo, la proactividad y la reflexión (Saldarriaga-Zambrano et al., 2016).
La gamificación se apoya en varias teorías que explican su eficacia para motivar. Según la teoría de la autodeterminación, las personas tienen tres necesidades psicológicas que, al cubrirse, fomentan la motivación intrínseca. La gamificación pretende satisfacer estas tres necesidades: autonomía, competencia y vinculación (García et al., 2024). También en las actividades gamificadas se utilizan elementos como puntos, insignias y recompensas, que actúan como refuerzos positivos. Esto se encontraría estrechamente relacionado con el con el conductismo.
En el ámbito educativo, la gamificación se vincula fuertemente con modelos de aprendizaje que ponen al estudiante en el centro. El constructivismo defiende que el conocimiento se construye de forma activa, mientras que el conectivismo describe la adquisición de conocimiento en la

era digital. Se basa en que el conocimiento está localizado en redes y no solo en las personas, y el aprendizaje implica la capacidad de acceder a esas redes y mantenerlas actualizadas (Gutiérrez, 2012).

En resumen, en la gamificación se utilizan dinámicas (lo que motiva el juego, como la recompensa o la competición), mecánicas (reglas, puntos o niveles) y componentes (avatares, insignias) para crear un entorno motivador, que fomente el compromiso y la consecución de objetivos.

3.2.2. Beneficios pedagógicos de la gamificación

La integración de propuestas gamificadas en el aula tiene como objetivo transformar la propia experiencia de aprendizaje. En este sentido, uno de los beneficios pedagógicos de la aplicación de esta metodología es el aumento de la motivación y el interés del alumnado sobre la temática a tratar. El uso de elementos del juego hace que el proceso de enseñanza-aprendizaje sea más emocionante, en comparación con modelos tradicionales. Por otra parte, su naturaleza lúdica incita al alumnado a querer superarse, ya sea a sí mismos o en equipo, consiguiendo un interés sostenido por el aprendizaje. Este aumento del interés está relacionado con otro de los beneficios pedagógicos, como es la mejora del compromiso y, por tanto, de la atención sostenida. Además, el hecho de conceptualizar y hacer más amenos los contenidos facilita su asimilación. En un tercer pilar encontraríamos el propio desarrollo de competencias transversales como el trabajo en equipo, el pensamiento crítico, la autonomía o la toma de decisiones. Muchos retos requieren de trabajo en equipo y colaboración, así como asunción de roles y comunicación, para alcanzar objetivos. Así, los retos requieren del uso de la lógica, la estrategia y el pensamiento crítico para dar soluciones efectivas. Por último, cabe mencionar que los entornos de juego se consideran entornos “seguros”, donde equivocarse forma parte del proceso, lo que favorece un avance sin miedo a fracasar. Además, la retroalimentación es, normalmente, inmediata, por lo que corregir errores se convierte en algo dinámico y rápido, lo que retroalimenta a la propia motivación (Pérez & Gértrudix-Barrio, 2021).

3.2.3. Limitaciones, riesgos y buenas prácticas

Cada vez más, la gamificación se ha consolidado como una de las metodologías más extendidas para aumentar la motivación, el compromiso y la participación en contextos educativos, organizacionales y sociales. Diversos estudios identifican resultados positivos en la mejora del rendimiento académico y la implicación del alumnado (Contreras-Espinosa & Eguia, 2017).

Sin embargo, a medida que la gamificación se va expandiendo, se detectan limitaciones y riesgos sobre su uso. Los efectos de la gamificación no son siempre sostenibles en el tiempo y

pueden depender de factores como el diseño, los usuarios o la tecnología disponible. Además, puede llegar a ser contraproducente si no se implementa de forma crítica y rigurosa. Las propuestas genéricas o mal contextualizadas pueden convertirse en una sobrecarga superficial, sin consecuencias pedagógicas.

Con todo esto, se hace imprescindible revisar no solo los beneficios, sino también aquellas limitaciones y riesgos que rodean su implementación.

Como señalan Contreras-Espinosa y Eguía (2017), no existen recetas mágicas, sino que existen diferentes variables que se deben alinear para que la práctica sea efectiva.

Una de las limitaciones más destacadas es el "efecto novedad", afectando a la pérdida progresiva de la motivación de los estudiantes. Esto, si la gamificación no se ha integrado de manera transversal con el currículo, podría comprometer su viabilidad en el tiempo.

Por otra parte, los sistemas de clasificación y las recompensas extrínsecas podrían reducir la motivación intrínseca, afectando el desarrollo de la autonomía y autorregulación. En este punto, se destaca la necesidad de diseñar experiencias que incrementen la reflexión crítica y el sentido de propósito, más allá del cumplimiento mecánico de tareas o de ganar un juego.

Existe una notable variabilidad en los efectos de unas u otras gamificaciones, lo que se traduce en que no todas las formas de gamificar tienen la misma repercusión ni son igual de válidas en todos los contextos educativos. Más allá del aumento de la implementación de prácticas gamificadas, su adopción a gran escala depende de la iniciativa individual del docente o de proyectos aislados. Esto remarca la necesidad de formar a docentes de una manera específica sobre el diseño de experiencias gamificadas, así como de establecer marcos normativos y curriculares que sustenten una integración efectiva en las aulas (López et al., 2025).

3.2.4. Integración en el diseño del escape room

En el diseño de un escape room educativo digital, la gamificación se integra como eje principal de la situación de aprendizaje. A través de una narrativa atractiva, los estudiantes se implican en una historia con finalidad didáctica que pone en contexto los retos relacionados con los contenidos curriculares de ciberseguridad. Esta narrativa organiza los objetivos de aprendizaje en forma de retos secuenciados, fomentando la participación activa en el proceso de enseñanza-aprendizaje. Según Navarro-Mateos et al. (2021), la narrativa gamificada contribuye a reforzar la motivación intrínseca del alumnado, al convertir el aprendizaje en una experiencia vivencial y orientada a objetivos claros.

Por otra parte, los diferentes elementos del juego se utilizan para estructurar la progresión de pruebas y desafíos dentro del escape room. Estas mecánicas no solo enriquecen el diseño, sino que permiten que el alumnado sea capaz de percibir su avance.

Por último, la retroalimentación inmediata es otro componente de la gamificación que se integra en el diseño del escape room. A través de mecanismos automáticos de confirmación de respuestas o de desbloqueo de retos, el alumnado recibe información sobre su desempeño. Esto favorece un aprendizaje autorregulado, ya que permite realizar ajustes sobre la marcha a los estudiantes, potenciando la reflexión metacognitiva (Navarro-Mateos et al., 2021).

El estudio de Pozo-Sánchez et al. (2022) sobre experiencias de escape room educativo indica que este tipo de actividad gamificada puede mejorar la motivación y el compromiso del alumnado con los contenidos académicos, superando a los modelos de enseñanza tradicionales que descentralizan la figura del estudiante. En contextos digitales, esta mejora se observa tanto en la implicación emocional como en la activación cognitiva, lo que sugiere que la gamificación no es un fin en sí mismo, sino un camino para facilitar aprendizajes significativos y duraderos.

3.3. El Aprendizaje Basado en Retos (ABR)

3.3.1. Concepto y fundamentos teóricos del ABR

El Aprendizaje Basado en Retos (ABR) es una metodología activa en la que el alumnado intenta buscar soluciones a problemas de su entorno. El hecho de vincular el aprendizaje con estos problemas favorece el desarrollo de competencias como la resolución de problemas, el trabajo en equipo y el pensamiento crítico.

La investigación realizada por Guzmán et al. (2025) concluye que el ABR tiene un elevado potencial para transformar el proceso educativo, dado que promueve entornos de aprendizaje centrados en el estudiante, donde la resolución de problemas reales, el trabajo en equipo y la toma de decisiones se convierten en motores del aprendizaje significativo y del desarrollo competencial. Además, la implementación del ABR se vincula fuertemente al incremento de la motivación intrínseca, entendida como el interés genuino por el aprendizaje, la participación y la superación en el proceso educativo.

Apple (2011) propone la siguiente secuencia para su implantación:

- Idea general: es fundamental que sea relevante tanto para los estudiantes como para la sociedad
- Pregunta esencial: se deben plantear una serie de preguntas entorno a la idea general, con la finalidad de comprender el contexto
- Reto: de la pregunta esencial surge un reto que implica la creación de una solución por parte de los estudiantes
- Preguntas, actividades y recursos guía: el profesor actúa como guía del proceso de aprendizaje, proporcionando diferentes cuestiones, acciones y medios que sirvan de

ayuda para elaborar las posibles soluciones

- Solución e implementación: el alumnado deberá plantear soluciones al problema e implementarlas, de una manera real o simulada
- Evaluación y validación: se deberá evaluar la implementación de la solución, validando si se consiguen los objetivos
- Publicación de soluciones y reflexiones: se debe documentar el proceso, generando un debate y reflexión acerca del mismo y de los resultados obtenidos

3.3.2. Relación con la competencia digital

Podría decirse que existe una relación recíproca entre el Aprendizaje Basado en Retos y la competencia digital. El ABR actúa como marco metodológico para poner en práctica habilidades digitales, mientras que la competencia digital se desarrolla de una manera implícita durante el uso del ABR. En la sociedad actual, en la que las tecnologías de la información y la comunicación se encuentran plenamente introducidas en la vida cotidiana, la resolución de retos reales (núcleo del ABR) requiere, por lo general, el uso de herramientas y recursos digitales de una manera crítica (competencia digital).

En la Tabla 1 se puede ver cómo el Aprendizaje Basado en Retos contribuye al desarrollo de la competencia digital, tomando las áreas del DigComp 2.2 como hitos independientes que la conforman.

Tabla 1

Aportación del ABR al desarrollo de la competencia digital

Área (DigComp 2.2)	**Contribución del ABR**
Búsqueda y gestión de información y datos	El alumnado debe investigar para comprender el reto que se plantea y sus posibles soluciones. Esto implica la búsqueda de información y la evaluación crítica de las fuentes (fiabilidad, relevancia, etc.).
Comunicación y colaboración	El ABR es una metodología colaborativa, que requiere el uso de herramientas digitales tanto para la comunicación como para la colaboración en documentos.
Creación de contenidos digitales	Para presentar sus soluciones, el alumnado debe crear contenidos digitales (vídeos, presentaciones, podcasts, etc.). Esto implica tener un manejo adecuado de diferentes tipos de software de diseño, edición o publicación.

Seguridad	El hecho de poner solución a retos reales, basados en la sociedad digital en la que vivimos, crea conciencia acerca de la responsabilidad, la ética y el respeto en entornos digitales.
Resolución de problemas	Uno de los pilares del ABR es la resolución de problemas en sí. Los estudiantes deben dar solución a un reto utilizando las herramientas idóneas.

Nota. Elaboración propia.

3.3.3. Integración en el diseño del escape room

En el diseño de un escape room educativo digital, el reto se presenta como el hilo conductor de toda la actividad, que los estudiantes deben resolver a través de una serie de pruebas. El planteamiento de un reto relevante implica que los estudiantes no solo adquieren conocimientos, sino que también los aplican.

Desde una perspectiva pedagógica, el ABR en el escape room digital se articula en fases que guían el aprendizaje. Tomando como base la secuencia propuesta por Apple (2011), en el juego se parte de un planteamiento inicial del reto, que despierta interés y activa conocimientos previos, para, después, permitir que el alumnado explore e investigue el problema, favoreciendo el diseño y la prueba de soluciones. En último lugar, se realiza una evaluación y reflexión, mediante la cual el alumnado revisa sus procesos y resultados para consolidar lo aprendido y ser capaz de extrapolarlo a contextos reales.

Un aspecto destacable del ABR es su énfasis en el desarrollo competencial, más allá de lo meramente disciplinar (Universidad Europea, 2024). El escape room educativo no solo hace posible la adquisición de conceptos de ciberseguridad, sino que también promueve habilidades transversales como el pensamiento crítico, la colaboración y la comunicación.

En resumen, la integración del ABR en el diseño del escape room educativo digital configura una experiencia de aprendizaje activa, significativa y orientada al desarrollo integral de competencias.

3.4. El escape room educativo como estrategia de aprendizaje

3.4.1. Escape room y escape room educativo: origen y evolución

El origen del escape room resulta algo difuso. Según diversas fuentes (EscapeUp, 2022; González, 2021; Qualia, 2023), sus inicios podrían remontarse a los años 80, en Japón, pero no fue hasta principios del siglo XXI que aparecieron los primeros videojuegos cuyo objetivo era resolver un enigma en tiempo limitado. En 2008, surgió el primer juego de escape en vivo en Japón y, más tarde, en 2011, el húngaro Attila Gyurkovics creó la franquicia Parapark, usando

edificios en ruinas de Budapest como escenarios para sus juegos de escape.

Los escape room educativos se instalan como una herramienta innovadora de enseñanza-aprendizaje, los cuales pretenden aprovechar los beneficios del juego para favorecer dicho proceso. Los participantes, a la vez que operan en un entorno lúdico, desarrollan habilidades como el pensamiento crítico, la colaboración y la resolución de problemas. Esta herramienta utiliza la motivación para conectar al alumnado con los contenidos a tratar. Además, se trata de una herramienta versátil, la cual puede presentarse tanto en un entorno presencial como en remoto, mediante los escape room educativos digitales (ERED).

3.4.2. Características pedagógicas

Negre y Carrión (2020) sugieren 10 razones por las que utilizar un escape room educativo puede ser beneficioso:

1. Fomenta la actividad y el movimiento en el alumnado
2. Tiene cabida cualquier contenido, por lo que un escape room puede tener un carácter transversal y enlazar contenidos de diversas asignaturas
3. Promueve la colaboración y el trabajo en equipo, dado que se requiere la interacción entre los participantes para alcanzar los objetivos
4. Desarrolla habilidades de resolución de problemas, desde el planteamiento de hipótesis hasta su ejecución
5. Mejora la competencia verbal, favoreciendo el diálogo y el intercambio de ideas
6. Ofrece retos a superar, y esto incrementa la resiliencia
7. Construye el pensamiento deductivo, incrementando la creación de inferencias para dar soluciones a los retos
8. Se trabaja bajo presión, lo que sitúa al alumnado fuera de su zona de confort
9. El alumnado es líder de su propio aprendizaje y el error forma parte del camino
10. Es divertido, tanto para el alumnado como para el profesor

3.4.3. Diseño de un escape room educativo

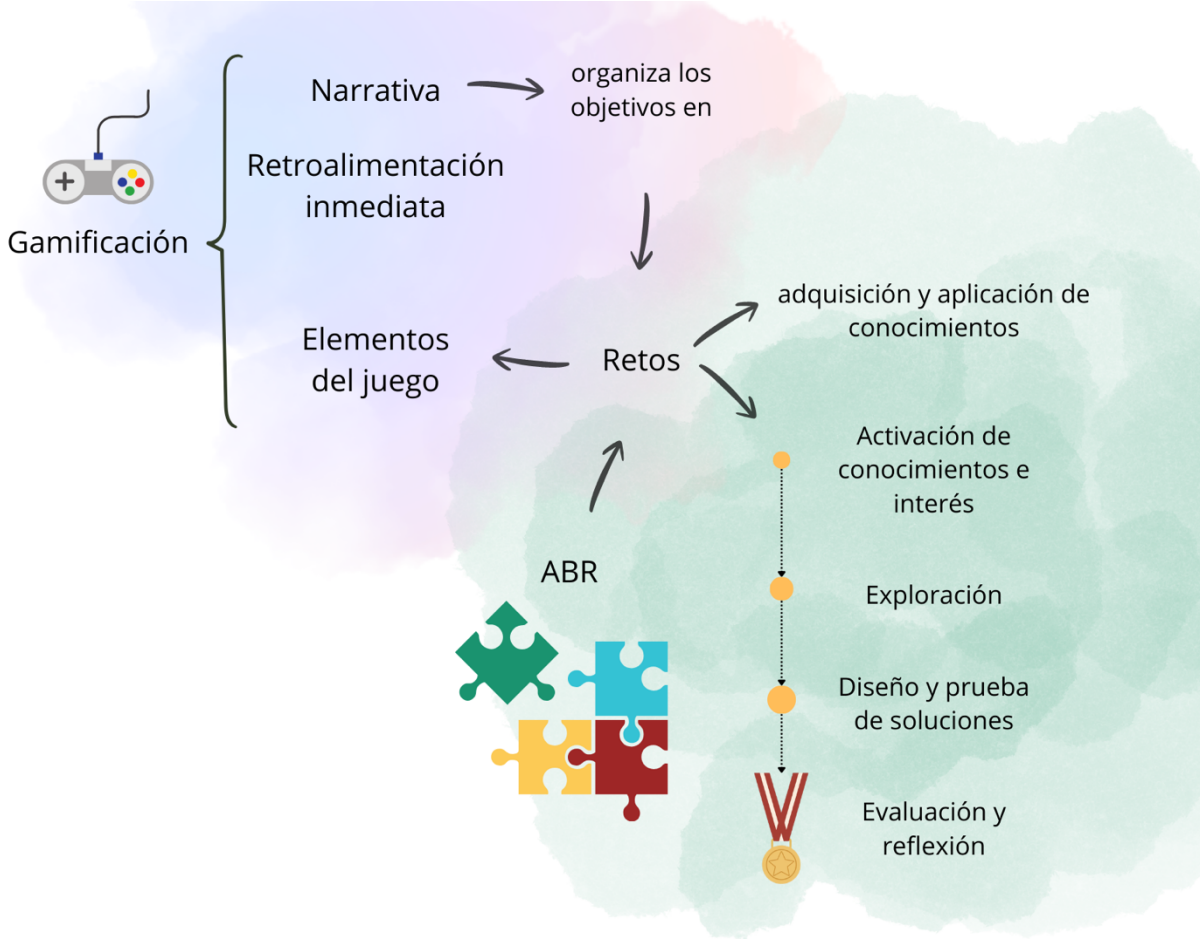
El Instituto de la Juventud de Extremadura (2018), en su *Manual de diseño de un juego de escape*, sugiere que, antes de empezar a diseñar un escape room, es importante tener experiencia personal, ya sea en aventuras gráficas o en escape room virtuales, de mesa o reales. Además, disponer de un portfolio de puzles amplio enriquece el diseño del juego.

En cuanto al diseño en sí, en primer lugar, se debe desarrollar una narrativa, una historia que haga de hilo conductor. En segundo lugar, será necesario crear los puzles, entendiendo como puzles los retos cuya resolución dependerá del uso de la lógica, el pensamiento analítico y los

procesos deductivos. Estos son los que mantienen la atención de los jugadores, por lo que deben ser variados y desafiantes, además de estar vinculados a la narrativa. Es fundamental que exista un equilibrio de dificultad para que la experiencia sea interesante ("muy fácil" puede resultar aburrido, mientras que "imposible" puede generar frustración y rechazo) y una temporalización adecuada para asegurar el éxito de la propuesta. Por último, en el diseño de la actividad se debe prestar atención a la retroalimentación que se ofrece, favoreciendo el aprendizaje y el mantenimiento de la motivación del alumnado.

Figura 2

Esquema de la integración de gamificación y ABR en el diseño del escape room educativo



Nota. Elaboración propia.

Diversas fuentes, como Lozano-Monterrubio et al. (2024), Macías-Guillén et al. (2023) o Úbeda (2025), exponen diferentes estudios sobre el uso de experiencias de escape room educativo, en diversas especialidades, así como el éxito que ha supuesto su aplicación como herramienta didáctica.

En concreto, Lozano-Monterrubio et al. (2024) plantean un análisis de la percepción que genera, entre el profesorado de seis centros educativos, la participación en el escape room *Learn*

to Escape, sobre Alfabetización Mediática e Informacional (AMI). Por otra parte, Macías-Guillén et al. (2023) comparan los resultados de aprendizaje obtenidos por estudiantes que asisten a una docencia presencial frente a otros que reciben una docencia híbrida, haciendo uso estos últimos de un Escape Room Educativo Digital (ERED) en la lección "La ratio precio valor". En ambos estudios, tanto la percepción docente como los resultados de aprendizaje son altamente positivos, lo que concluye la viabilidad del uso de este tipo de herramienta. Por último, el artículo de Úbeda (2025) presenta el escape room *L'última moneda*, cuyo objetivo es acercar conceptos financieros, como pueden ser el ahorro, el consumo responsable, la planificación de gastos o la inversión, mediante el trabajo en equipo, la toma de decisiones o la gestión estratégica.

3.5. La competencia digital en el ámbito educativo

3.5.1. Concepto y marcos de referencia

La competencia digital podría definirse como el conjunto de conocimientos, habilidades y actitudes necesarias para un uso crítico, responsable y seguro de las tecnologías de la información y la comunicación (TIC). En realidad, va más allá de saber usar herramientas tecnológicas. Implica un conocimiento profundo del funcionamiento del entorno digital para interactuar en la sociedad de una manera responsable y efectiva.

La competencia digital en el ámbito educativo se encuentra respaldada por marcos de referencia que buscan la coherencia en la capacitación de los ciudadanos.

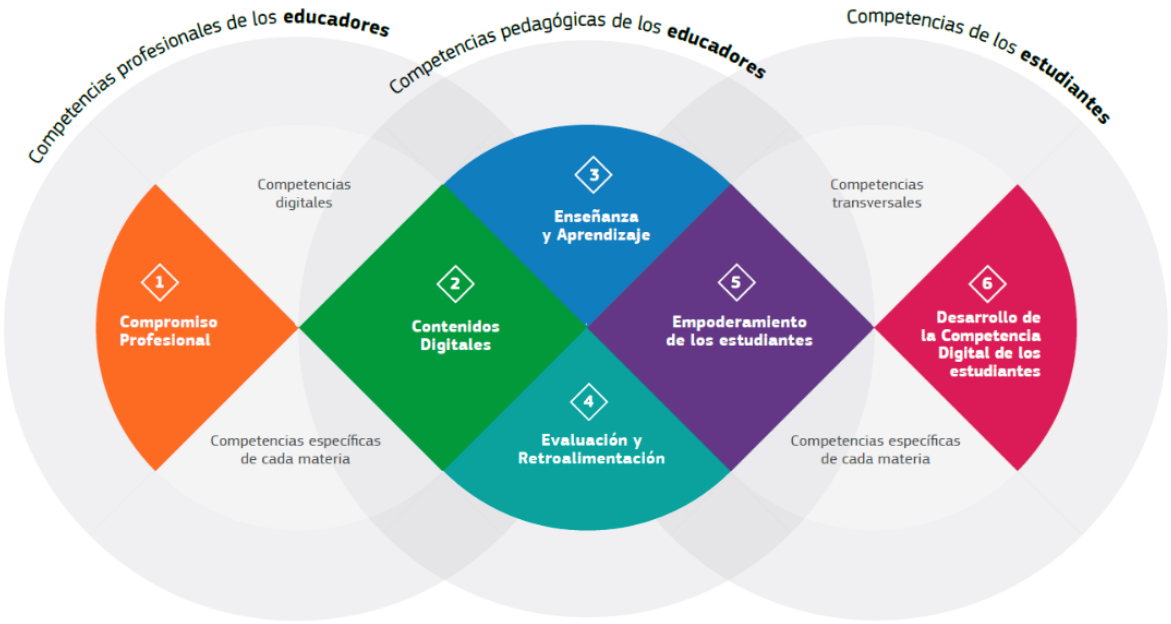
El DigComp 2.2 (Marco de Competencias Digitales para la Ciudadanía) proporciona un lenguaje común a nivel europeo para identificar y describir aquellas áreas clave de la competencia digital, la cual "implica el uso seguro, crítico y responsable de las tecnologías digitales para el aprendizaje, en el trabajo y para la participación en la sociedad, así como la interacción con estas." (Somos Digital, 2022). Este marco organiza la competencia digital en cinco áreas principales: búsqueda y gestión de información y datos, comunicación y colaboración, creación de contenidos digitales, seguridad y resolución de problemas. Estas áreas se desglosan en un total de 21 competencias específicas.

El Marco de Referencia de la Competencia Digital Docente (MRCDD) es la adaptación a las particularidades de España del Marco Europeo para la Competencia Digital de los Educadores (DigCompEdu). Su objetivo principal es describir aquellas competencias digitales que cualquier docente debe desarrollar a lo largo de su trayectoria profesional. El MRCDD mantiene la misma estructura del DigCompEdu (véase la Figura 3), con seis áreas de competencia: compromiso profesional, contenidos digitales, enseñanza y aprendizaje, evaluación y

retroalimentación, empoderamiento del alumnado y desarrollo de la competencia digital del alumnado. Estas áreas se agrupan en tres bloques: competencias profesionales (área 1), competencias pedagógicas (áreas 2-5) y competencias para el desarrollo de la competencia digital del alumnado (área 6).

Figura 3

Áreas y alcance del Marco DigCompEdu



Nota. Extraído de Redecker (2020).

El MRCDD integra un modelo de progresión, el cual se divide en tres etapas y, cada una de ellas, en dos niveles. En una primera etapa de Acceso (A), se encuentran los niveles de Conocimiento (A1) e Iniciación (A2). En una segunda etapa de Experiencia (B), se encuentran los niveles de Adopción (B1) y Adaptación (B2). Por último, en la etapa de Innovación (C), se encuentran los niveles de Liderazgo (C1) y Transformación (C2).

3.5.2. Competencia digital del alumnado en la Educación Secundaria Obligatoria

En el currículo que propone la LOMLOE (2020) se definen las competencias clave que se espera que adquiera el alumnado al finalizar la enseñanza básica. Entre ellas, se encuentra la competencia digital, la cual busca garantizar la plena inserción del alumnado en la sociedad digital, promoviendo un uso crítico, seguro y responsable de los medios digitales (RD 217/2022, p. 29).

Con el objetivo de trazar la consecución de dicha competencia, se establecen una serie de descriptores operativos, los cuales detallan aquellos aspectos que el alumnado debe comprender al finalizar cada una de las etapas de la enseñanza básica.

Tabla 2

Descriptores operativos de la competencia digital al finalizar la enseñanza básica

Información	CD1. Realiza búsquedas en internet atendiendo a criterios de validez, calidad, actualidad y fiabilidad, seleccionando los resultados de manera crítica y archivándolos, para recuperarlos, referenciarlos y reutilizarlos, respetando la propiedad intelectual.
Creación de contenidos	CD2. Gestiona y utiliza su entorno personal digital de aprendizaje para construir conocimiento y crear contenidos digitales, mediante estrategias de tratamiento de la información y el uso de diferentes herramientas digitales, seleccionando y configurando la más adecuada en función de la tarea y de sus necesidades de aprendizaje permanente.
Comunicación y colaboración	CD3. Se comunica, participa, colabora e interactúa compartiendo contenidos, datos e información mediante herramientas o plataformas virtuales, y gestiona de manera responsable sus acciones, presencia y visibilidad en la red, para ejercer una ciudadanía digital activa, cívica y reflexiva.
Seguridad	CD4. Identifica riesgos y adopta medidas preventivas al usar las tecnologías digitales para proteger los dispositivos, los datos personales, la salud y el medioambiente, y para tomar conciencia de la importancia y necesidad de hacer un uso crítico, legal, seguro, saludable y sostenible de dichas tecnologías.
Resolución de problemas	CD5. Desarrolla aplicaciones informáticas sencillas y soluciones tecnológicas creativas y sostenibles para resolver problemas concretos o responder a retos propuestos, mostrando interés y curiosidad por la evolución de las tecnologías digitales y por su desarrollo sostenible y uso ético.

Nota. Adaptado de RD 217/2022, p. 29

La competencia digital debe desarrollarse de una manera transversal. Lo que se pretende es, a efectos prácticos, que el alumnado sea capaz de identificar la calidad de la información (incluso detectar noticias falsas), utilizar herramientas necesarias tanto en el ámbito académico como en el personal o el futuro laboral y participar en la sociedad de una forma activa, respetuosa y crítica.

3.5.3. Importancia de la competencia digital en el profesorado

A lo largo de este apartado, se ha puesto de manifiesto la importancia del desarrollo de la competencia digital en el alumnado de ESO, pero este desarrollo no sería posible sin un profesorado competente digitalmente. Un profesorado competente en el ámbito digital usa la innovación metodológica, diseñando actividades interactivas y adaptadas a las diferentes formas de aprender de los estudiantes, favorece el desarrollo de la competencia digital del alumnado, puesto que sirve de guía en dicho proceso, y contribuye a que se haga un uso seguro, ético y responsable de las TIC. Por otra parte, esta característica permite al profesorado ser más eficiente en la propia gestión de contenidos, así como en la comunicación y la participación con la comunidad educativa.

No se debe olvidar que, pese a que se considere a los estudiantes "nativos digitales", la competencia digital va mucho más allá del saber usar cierta tecnología, y es en ese desarrollo donde el profesorado adquiere gran relevancia.

3.6. La ciberseguridad en la educación secundaria

3.6.1. Ciberseguridad y bienestar digital

Según Microsoft (2024), la ciberseguridad o seguridad digital hace referencia a la práctica de proteger la información digital, los dispositivos y los activos, como información personal, cuentas, archivos, fotos e incluso el dinero. El acrónimo CID (en inglés, CIA) representa los tres pilares de la ciberseguridad:

- Confidencialidad, la cual garantiza que solo los usuarios autorizados puedan tener acceso
- Integridad, la cual asegura que nadie inserte, modifique o elimine información sin consentimiento
- Acceso, el cual garantiza que se puede tener acceso a la información y sistemas cuando se necesite.

Por otra parte, "el bienestar digital se refiere al estado de equilibrio saludable en la vida digital de una persona" (Cuesta, 2024). En una etapa como la adolescencia, el uso intensivo de la tecnología y las redes sociales impacta de una manera negativa en la salud mental, favoreciendo la comparación y la autoexigencia, incluso abriendo la puerta al ciberacoso o la vulneración de la privacidad, y en la salud física, afectando a la calidad y cantidad del sueño y a los hábitos saludables, dado que resta tiempo de otras actividades como el ejercicio físico y otras actividades de ocio. Además, también existe una afectación en las relaciones sociales e incluso generar problemas de adicción.

3.6.2. La ciberseguridad como contenido educativo

La ciberseguridad se trata de una temática con una presencia transversal en el currículo de la ESO. Entre los saberes básicos de la materia Digitalización se incluyen los bloques «Digitalización del entorno personal de aprendizaje» y «Seguridad y bienestar digital», los cuales, en Educación Secundaria Obligatoria, abarcan contenidos como el uso de contraseñas seguras y métodos de autenticación, la gestión y protección de la información personal y la huella digital, la configuración de la privacidad en redes sociales y otras plataformas, la netiqueta y el comportamiento respetuoso en entornos virtuales, lo que incluye la prevención y actuación ante el ciberacoso, la evaluación crítica de la información, la protección de dispositivos contra malware o los riesgos derivados del mundo digital.

En resumen, lo que se pretende en esta etapa es una alfabetización digital del alumnado, creando ciudadanos digitales conscientes.

3.6.3. Relación entre el escape room digital y la enseñanza de ciberseguridad

Un escape room digital es una de las formas más eficaces para trabajar la seguridad digital en la ESO, dado que combina narrativa, reto, colaboración y aplicación práctica de contenidos.

Como se ha comentado a lo largo del presente trabajo, la gamificación activa mecanismos de motivación extrínseca, lo que hace que el alumnado quiera avanzar de manera autónoma. Este hecho favorece la retención de conceptos sobre ciberseguridad. Además, se facilita el aprendizaje activo, ya que los estudiantes aplican la teoría para resolver las pruebas, por ejemplo, al descifrar mensajes encriptados o elegir contraseñas robustas para desbloquear pistas, lo que promueve un aprendizaje por descubrimiento. Al reproducir situaciones reales de riesgo, se desarrolla una conciencia crítica de los riesgos que se pueden producir en el día a día. Por último, es fundamental la retroalimentación inmediata que ofrece este tipo de gamificación, lo que ayuda a detectar lo que no se comprende para hacer los ajustes necesarios. En este caso, la evaluación es una parte del juego, por lo que pierde su connotación negativa.

4. Procedimiento de la propuesta de innovación

4.1. Contexto

El diseño de este escape room digital se plantea como un recurso adaptable, abordando la diversidad del sistema educativo español de la ESO. Poniendo el foco en la dotación tecnológica del centro, se podrían plantear lo siguientes contextos:

Tabla 3

Contextos en función de la dotación tecnológica del centro

Contexto del centro	**Repercusión en el escape room**
Dotación tecnológica alta (disponibilidad de tabletas/portátiles 1:1 y red Wi-Fi estable)	Se puede hacer un mayor uso de recursos digitales avanzados (vídeos, programación básica, etc.) y plantear pruebas que requieran trabajo individual.
Dotación tecnológica media (aula de informática de capacidad limitada y/o red Wi-Fi inestable)	Se deben incluir versiones offline, imprimibles y/o ser compatible con teléfonos móviles. Las pruebas deberán resolverse en grupo o de manera individual offline.
Dotación tecnológica baja (recursos tecnológicos escasos o nulos)	La mayor parte del juego se deberá realizar sin recursos tecnológicos. Se puede hacer uso de pizarras digitales o sistemas de audio para plantear escenarios generales.

Nota. Elaboración propia.

Prensky (2001) acuñó el término "nativos digitales" para referirse a aquellas personas que han crecido rodeadas de tecnología digital, diferenciándolas de las "inmigrantes digitales", que serían aquellas personas nacidas antes de la era digital y que han adoptado la tecnología posteriormente. El juego de escape que se diseña en el presente TFM está contextualizado en la materia Digitalización de 4º ESO, por lo que el alumnado que se pretende alcanzar está incluido dentro de dichos nativos digitales. Lejos de los beneficios que esta denominación pueda conllevar, este alumnado se caracteriza por un uso intensivo de Internet, redes sociales y videojuegos y un déficit de competencias digitales (Cabrera, 2017). Por otra parte, con la gamificación que se plantea se pretende abarcar la diversidad del aula, tratando de conectar con el alumnado por diferentes vías. De esta manera, la actividad se podría implementar independientemente de que en el centro/aula exista diversidad cultural, socioeconómica, de capacidades, de identidad, etc.

La propuesta que se plantea se integra con los tres principios del Diseño Universal de Aprendizaje (DUA): proporcionar múltiples medios de representación (el qué), múltiples medios de acción y expresión (el cómo) y múltiples medios de implicación y motivación (el por qué) (educaDUA, 2016). En la Tabla 4 se resume a aplicación de estos principios al escape room, así como las barreras que se pretenden superar.

Tabla 4

Principios del DUA aplicados al escape room

Principio del DUA	**Aplicación al escape room**	**Barreras que supera**
Múltiples medios de representación	Presentación de conceptos mediante texto, vídeos, audios, ejemplos visuales.	Barreras lingüísticas, dislexia o dificultades de lectura. Diferencias en el procesamiento de información.
Múltiples medios de acción y expresión	Respuestas a los retos de diversas maneras: escribir códigos, seleccionar opciones, arrastrar/soltar elementos, respuesta oral.	Diferentes capacidades para demostrar el conocimiento.
Múltiples medios de implicación y motivación	Uso de elementos propios de la gamificación. Trabajo cooperativo. Ofrecer pistas flexibles.	Desinterés, desmotivación, evaluación tradicional. Vinculación con un tema relevante para el día a día.

Nota. Elaboración propia.

Como se ha destacado a lo largo del presente trabajo, existe una creciente preocupación entorno a la seguridad digital, dado que, en la actualidad, el uso intensivo de la tecnología por parte de los jóvenes no se encuentra alineada con su conocimiento sobre ciberseguridad. En esta línea, la LOMLOE (2020) hace hincapié en una formación en el uso seguro y responsable de la tecnología, alejándose de una enseñanza meramente instrumental. Es por esta razón por la que se propone, de una manera dinámica y atractiva, que el alumnado conozca y comprenda los conceptos asociados a la ciberseguridad. De este modo, se pretende traspasar la línea de la adquisición de un conocimiento meramente teórico, buscando la aplicación de lo aprendido en el día a día.

A la hora de llevar a cabo la experiencia, nos podemos encontrar con desafíos diversos a los que habrá que dar solución. En cuanto a barreras de infraestructura, cabe la posibilidad de que

no haya tabletas/portátiles para cada estudiante o grupo o que los dispositivos tengan bajo rendimiento y la ejecución sea lenta. También podríamos enfrentarnos a conectividad a Internet limitada. Por otra parte, existen barreras pedagógicas, como la selección de contenidos o la adecuación del nivel de dificultad. En este sentido, el uso de pruebas demasiado fáciles podría llevar al aburrimiento, mientras que aquellas demasiado difíciles podrían causar frustración. Por otra parte, la temporalización de este tipo de actividades suele ser extensa, por lo que también puede suponer una limitación el hecho de encajarla en la programación. Por último, la diversidad en el aula es algo inevitable. Desde este punto de vista, cabe la posibilidad de que la competencia digital de los estudiantes presente diferencias significativas o que se produzcan conflictos en la gestión del estrés o de comportamiento. Todas estas casuísticas se deben tener en cuenta en el ajuste de la propuesta al grupo en el que se llevará a cabo para favorecer el éxito de la misma.

En oposición, se presentan diversos puntos positivos que potencian el éxito de la propuesta. El aprendizaje gamificado se encuentra altamente relacionado con una mayor motivación y compromiso, mientras que, a su vez, se produce un desarrollo de competencias como el pensamiento crítico, el trabajo en equipo y la resolución de problemas. Por otra parte, este tipo de propuestas están relacionadas con la adquisición de un aprendizaje significativo, lo que favorece que el conocimiento sea más duradero y extrapolable a otros ámbitos. Además, se trata de una actividad flexible y adaptable a las diferentes casuísticas que se puedan presentar.

En la Tabla 5 se presenta un esquema de las barreras y potencialidades mencionadas.

Tabla 5

Análisis DAFO de la propuesta

<table>
<tr><th colspan="2">Análisis interno</th><th colspan="2">Análisis externo</th></tr>
<tr><td colspan="2">Debilidades</td><td colspan="2">Amenazas</td></tr>
<tr><td colspan="2" rowspan="2">- Selección de contenidos y adecuación del nivel de dificultad
- Temporalización extensa</td><td>Alumnado</td><td>- Brecha digital
- Gestión del estrés/Comportamiento</td></tr>
<tr><td>Infraestructura</td><td>- Dispositivos insuficientes y/o con bajo rendimiento
- Conectividad a Internet limitada</td></tr>
<tr><td colspan="2">Fortalezas</td><td colspan="2">Oportunidades</td></tr>
<tr><td colspan="2">- Diseño flexible y adaptable (DUA)</td><td colspan="2">- Motivación
- Aprendizaje significativo y desarrollo competencial</td></tr>
</table>

Nota. Elaboración propia.

4.2. Destinatarios e implicados

La actividad que se plantea en el presente Trabajo de Fin de Máster está dirigida a alumnos de 4º ESO, curso en el que la edad media se encuentra entre los 15 y los 16 años, por lo que tienen un elevado contacto con el mundo digital. El grupo es, previsiblemente, heterogéneo, tanto en rendimiento, intereses o estilos de aprendizaje. Este curso se encuentra en un punto de inflexión entre la continuidad de los estudios, bien sea hacia Bachillerato o hacia Formación Profesional, o la incorporación al mundo laboral, por lo que los niveles de motivación son muy variables. En este sentido, ofrecer una actividad acerca de una temática de gran importancia, como lo es la ciberseguridad y el bienestar digital, alejándonos de una forma de enseñanza tradicional, posibilita conectar con aquellas personas que no se encuentran vinculadas con el sistema educativo. También el grupo ofrece características importantes a la hora de llevar a cabo la experiencia, como es la autonomía, la reflexión crítica o el trabajo en grupos eficaz. Por último, como se ha mencionado con anterioridad, se trata de un alumnado considerado como "nativos digitales", lo cual favorece el desarrollo de la propuesta.

Para llevar a cabo una actividad de estas características, la labor del docente es esencial. En este sentido, los profesores de la materia se encargan de diseñar, planificar, ejecutar y evaluar la actividad en el aula, siendo los responsables de la gestión del tiempo y de la adaptación de los contenidos a las características de cada grupo. Puesto que se trata de una experiencia que se va a llevar a cabo en una única materia, no se requiere la colaboración del resto del equipo docente de otras asignaturas, pero sí es importante contar con la jefatura de estudios y/o la dirección, de manera que puedan facilitar los recursos necesarios (espacios, materiales, etc.), así como validar la alineación con el proyecto del centro.

4.3. Finalidad

Con la propuesta de enseñanza-aprendizaje de ciberseguridad mediante el uso de un escape room digital se pretenden alcanzar múltiples objetivos, los cuales resultan altamente beneficiosos para el alumnado, dado que promueve el desarrollo de la competencia digital, que resulta de enorme importancia en la actualidad.

El objetivo final de esta actividad es la capacitación de los estudiantes para desenvolverse de manera segura, responsable y crítica en entornos digitales, mediante la adquisición de nociones sobre ciberseguridad, adaptados al nivel educativo en el que nos encontramos, comprendiendo conceptos como contraseñas seguras, protección de datos personales, suplantación de identidad o malware.

El alumnado que cursa 4º ESO es un tipo de ciudadano digitalmente activo, lo que implica el

manejo de información personal en el mundo digital, la interacción en redes sociales o la realización de transacciones en línea. Estas implicaciones los hace vulnerables a diversas amenazas. En este sentido, se pretende que desarrollen hábitos seguros en el uso de las TIC, siendo capaces de detectar riesgos y aumentando la autonomía y el pensamiento crítico a la hora de detectar vulnerabilidades y aplicar estrategias de protección en cualquier contexto. De la responsabilidad digital y la prevención de riesgos surge la necesidad formativa en este ámbito.

Puesto que se trata de un tema de gran importancia, y aprovechando la posibilidad de su aprendizaje desde un punto de vista práctico, se pretende motivar e interesar al alumnado mediante el uso de una perspectiva lúdica y activa, lo que mejorará su implicación y la percepción de la utilidad de los contenidos.

4.4. Planificación

4.4.1. Contexto general de la actividad

La actividad que se plantea se titula *¡Que no te pesquen!* y pretende, mediante el uso de metodologías activas como la gamificación y el Aprendizaje Basado en Retos (ABR), mostrar de una manera lúdica e interesante los contenidos de ciberseguridad de la materia Digitalización al alumnado de 4º ESO.

Se trata de una actividad cuya duración es de 2 sesiones de 60 minutos. En ella, se utilizarán diversos recursos, que pueden ser o no digitales, en función del contexto en el que nos encontremos. Cada reto puede adaptarse según los recursos disponibles. En la Tabla 6 se muestra un resumen de los aspectos generales que ponen en contexto a la actividad.

Tabla 6

Aspectos generales que contextualizan la actividad

Nombre de la actividad	¡Que no te pesquen!
Metodología	Gamificación y Aprendizaje Basado en Retos
Materia	Digitalización
Curso	4º ESO
Duración estimada	2 sesiones de 60 minutos
Recursos[1]	Aula de informática, proyector, material audiovisual.

Nota. Elaboración propia.

[1] En la Tabla 6 se indican los recursos necesarios atendiendo a un contexto genérico, en el que se presupone una disponibilidad adecuada de medios digitales. En cada apartado, se detallan alternativas para que la actividad se pueda llevar a cabo en cualquier contexto.

Con la realización de esta actividad, el alumnado avanza hacia varios de los objetivos planteados en el Real Decreto 217/2022, de 29 de marzo, por el que se establece la ordenación y las enseñanzas mínimas de la Educación Secundaria Obligatoria. Además, se trata de un recurso altamente competencial, ya que favorece el desarrollo de diversas competencias clave. En la Tabla 7 se detallan tanto los objetivos como las competencias clave, junto con los descriptores operativos, que el escape room planteado contribuye a desarrollar.

Tabla 7

Contribución de la actividad al desarrollo de objetivos y competencias clave de la ESO

Objetivos	
- Desarrollar y consolidar hábitos de disciplina, estudio y trabajo individual y en equipo como condición necesaria para una realización eficaz de las tareas del aprendizaje y como medio de desarrollo personal. - Desarrollar destrezas básicas en la utilización de las fuentes de información para, con sentido crítico, adquirir nuevos conocimientos. Desarrollar las competencias tecnológicas básicas y avanzar en una reflexión ética sobre su funcionamiento y utilización.	
Competencias clave	Descriptores operativos
Competencia en comunicación lingüística	CCL1, CCL2, CCL3
Competencia digital	CD1, CD2, CD3, CD4
Competencia personal, social y de aprender a aprender	CPSAA1, CPSAA2, CPSAA3, CPSAA4, CPSAA5
Competencia matemática y en ciencia, tecnología e ingeniería	STEM1, STEM2, STEM3, STEM5
Competencia ciudadana	CC1, CC2, CC3, CC4

Nota. Adaptado de RD 217/2022, pp. 8-9, 26-31.

El juego se enmarca en la materia de Digitalización de 4º ESO, por lo que abarca algunos de sus saberes básicos y fomenta el desarrollo de algunas de las competencias específicas vinculadas a la misma. En la Tabla 8 se detalla la vinculación de la actividad a las competencias específicas, criterios de evaluación y saberes básicos de la materia Digitalización.

Tabla 8

Competencias específicas, criterios de evaluación y saberes básicos de la actividad

Competencias específicas	Criterios de evaluación
Competencia específica 3: Desarrollar hábitos que fomenten el bienestar digital, aplicando medidas preventivas y correctivas, para proteger dispositivos, datos personales y la propia salud.	3.1. Proteger los datos personales y la huella digital generada en internet, configurando las condiciones de privacidad de las redes sociales y espacios virtuales de trabajo. 3.2. Configurar y actualizar contraseñas, sistemas operativos y antivirus de forma periódica en los distintos dispositivos digitales de uso habitual 3.3. Identificar y saber reaccionar ante situaciones que representan una amenaza en la red, escogiendo la mejor solución entre diversas opciones, desarrollando prácticas saludables y seguras, y valorando el bienestar físico y mental, tanto personal como colectivo.
Competencia específica 4: Ejercer una ciudadanía digital crítica, conociendo las posibles acciones que realizar en la red, e identificando sus repercusiones, para hacer un uso activo, responsable y ético de la tecnología.	4.1. Hacer un uso ético de los datos y las herramientas digitales, aplicando las normas de etiqueta digital y respetando la privacidad y las licencias de uso y propiedad intelectual en la comunicación, colaboración y participación activa en la red.
Saberes básicos	
C. Seguridad y bienestar digital D. Ciudadanía digital crítica	

Nota. Adaptado de RD 217/2022, pp. 8-9, 42-47.

Como se detalla en los siguientes apartados, el contenido que abarcará la actividad propuesta se vincula con la seguridad y el bienestar digital, tratando conceptos como contraseñas seguras, autenticación, phishing, malware, huella digital y privacidad.

4.4.2. Fase 1: activación

Los objetivos de la primera fase, de activación, se basan en introducir la actividad al alumnado, analizar los conocimientos previos y formar los grupos de trabajo.

En la Tabla 9 se detallan cada una de estas tareas, especificando su temporalización y su vinculación con los principios del DUA.

Tabla 9

Relación de tareas que componen la primera fase

Tarea	Principio DUA[2]	Temporalización	Descripción general
Introducción a la narrativa	Principios 1 y 3	5’	El docente presenta la narrativa: se ha detectado un intento de phishing masivo en el centro y debe ser detenido. Se utiliza un video *teaser* para captar la atención.
Activación de conocimientos previos	Principio 2	15’	El docente lanza dos preguntas abiertas: “¿Qué es la seguridad digital?” y “¿Qué es el bienestar digital?”. Las respuestas de los estudiantes se recogen y comentan, para orientarlos hacia una correcta definición.
Formación de grupos	Principio 3	5’	El docente forma los grupos de manera heterogénea, asegurando un equilibrio de habilidades. Se asignan roles para diversificar responsabilidades e involucrar a cada uno de los participantes (líder, evaluador, secretario, etc.).

Nota. Elaboración propia.

La temporalización total de la primera fase es de 25 minutos. A continuación, se detallan cada una de las tareas de la fase 1.

En primer lugar, la introducción a la narrativa se basa en presentar al alumnado la actividad.

[2] Los principios del DUA son: principio 1, múltiples medios de representación; principio 2, múltiples medios de acción y expresión; y principio 3, múltiples medios de implicación y motivación.

Una sesión lúdica lleva implícito un aumento de la motivación en el aula, por lo que se aprovecha este aspecto para conectar con el alumnado, incluso con aquellos estudiantes que tengan una vinculación más débil hacia la materia o los estudios. Además, la temática que se propone está relacionada con los retos que se plantean en el día a día de las personas, y de esta manera se da respuesta al porqué del aprendizaje. En relación al aspecto motivacional, y con la intención de aplicar el principio 3 del DUA, cada docente podrá incluir aquellos aspectos que considere necesarios para incrementar la vinculación del estudiantado con el ejercicio.

En la introducción a la narrativa, se usa un vídeo *teaser* (ver Tabla 10), caracterizado por ser un recurso audiovisual de corta duración, de unos 20" o 30", cuyo objetivo es captar la atención e impactar. Con el objetivo de aplicar el principio 1 del DUA, se puede entregar al alumnado la tabla descriptiva del vídeo o una presentación, en formato digital o en papel, con las diferentes escenas y su descripción de audio (ver Anexo I).

Tabla 10

Detalle del vídeo: temporalización, narración y escenas

Temporalización	**Narración (voz en off)**	**Escenas**
0:00–0:03	En la red…	- Pantalla negra → animación rápida de ondas azules de red conectándose - Texto: "En la red…" - Efecto de sonido: "ping" digital
0:03–0:06	nada es lo que parece.	- Iconos de correos, contraseñas y candados flotando, uno se rompe en *glitch* - Texto: "nada es lo que parece."
0:06–0:10	Cada clic puede abrir una puerta… o una trampa.	- Zoom a un móvil que recibe un mensaje sospechoso: "Tu cuenta ha sido bloqueada. Haz clic aquí." - Efecto: luz roja intermitente
0:10–0:14	Un mensaje sospechoso ha activado una alarma en el instituto…	- Fondo oscuro → aparecen palabras en *glitch*: "phishing", "fraude", "estafa", "robo de datos", …

0:14–0:20	Y solo tú puedes descubrir quién intenta pescar tus datos.	- Un candado digital se cierra de golpe - Transición rápida a un temporizador tipo escape room bajando de 30 segundos - Texto: "Descubre quién está detrás…"
0:20–0:24	¿Estás listo para poner a prueba tus habilidades digitales?	- Siluetas misteriosas, pistas digitales, fragmentos de páginas web rotas
0:24–0:30	Bienvenido a… ¡Que no te pesquen!	- Logo del proyecto: ¡QUE NO TE PESQUEN! - Efecto: animación tipo "red de pescar" que desaparece

Nota. Elaboración propia.

En la activación de conocimientos previos, el profesor lanza dos preguntas abiertas: "¿Qué es la seguridad digital?" y "¿Qué es el bienestar digital?". Para dar forma a lo que sugiere cada uno de estos ámbitos, se utiliza la plataforma online Mentimeter, generando una nube de palabras con las aportaciones del alumnado. En este punto, para aplicar el principio 2 del DUA, se plantea una versión en la que las aportaciones se digan en voz alta, y sea el profesor el que las traslade a Mentimeter, o bien una versión offline mediante pósits.

Figura 4

Mentimeter con la pregunta "¿Qué es el bienestar digital?"

Nota. Elaboración propia.

En cuanto a la formación de grupos, es el docente el que, basándose en el conocimiento del alumnado, plantea unos grupos con una distribución de habilidades equilibrada. En el caso de que el profesor no conociera lo suficiente al alumnado, puede realizar un cuestionario corto, en formato digital, como un Formulario de Google, o en papel, para distribuir a los estudiantes en función de la puntuación obtenida, de manera que los grupos queden balanceados. Una vez se han formado los grupos, es importante que se realice una asignación de roles, de manera que las responsabilidades queden distribuidas y la involucración en el juego sea mayor. En este sentido, en grupos de 4-5 estudiantes, los roles pueden ser: coordinador/a, secretario/a, portavoz, supervisor/a e investigador/a. Este punto está alineado con el principio 3 del DUA, dado que el hecho de que los equipos se encuentren equilibrados genera una percepción de igualdad de oportunidades, lo que repercute en la motivación del alumnado. Además, que cada estudiante tenga un rol dentro del grupo facilita el trabajo en equipo e incrementa la cohesión.

4.4.3. Fase 2: desarrollo del juego

El objetivo de la segunda fase, de desarrollo del juego, es resolver retos prácticos de ciberseguridad, de una forma lúdica, por parte del estudiantado, aplicando conocimientos de forma colaborativa.

La temporalización total de la segunda fase es de 60 minutos. En la Tabla 11 se listan cada uno de los retos, especificando su temporalización y su vinculación con los principios del DUA. En el Anexo II se puede ver un croquis de los retos que componen esta segunda fase.

Tabla 11

Relación de retos que componen la segunda fase

Reto	Principio DUA	Temporalización	Descripción general
Reto 1	Principios 1 y 2	12-15’	El primer reto consiste en resolver un cuestionario con contenidos de contraseñas y autenticación. El resultado es la contraseña maestra, de cuatro dígitos, con la que se abre un documento con las instrucciones del siguiente reto.

Reto 2	Principios 1 y 2	12-15’	El segundo reto consiste en detectar los indicadores de peligro de tres intentos simulados de phishing para obtener las partes de la clave final, la cual se tiene que resolver mediante un acertijo. Con ella, se busca el documento con las instrucciones del siguiente reto.
Reto 3	Principios 1 y 2	12-15’	El tercer reto consiste en resolver tres pruebas sobre malware y buenas prácticas de seguridad. El resultado de las dos primeras pruebas es el código de desbloqueo para acceder al documento que se descubre en la tercera prueba, que contiene las instrucciones del siguiente reto.
Reto 4	Principios 1 y 2	12-15’	El cuarto reto consiste en responder un cuestionario de diez preguntas sobre la huella digital y la privacidad, con el objetivo de obtener tiempo extra que se sumará a un tiempo base de 30” para hacer frente al reto final.
Reto 5 (final)	Principios 1 y 2	5’	El quinto reto se corresponde con el reto final. Para llevarlo a cabo, se dispondrá de un tiempo base al que se le sumará el tiempo obtenido en el reto 4. El objetivo es clasificar ocho tarjetas con situaciones digitales cotidianas según se consideren seguras o peligrosas, para conseguir finalizar el juego.

Nota. Elaboración propia.

Tal como están definidos los retos, a continuación, en el detalle de los mismos, se supone una disponibilidad de ordenadores y conexión a Internet adecuada. En un contexto diferente, se

puede plantear el reto con imprimibles, candados, etc. Esto responde tanto al principio 1 como al principio 2 del DUA, de proporcionar múltiples medios de representación y múltiples medios de acción y expresión. En este sentido, también cabe destacar que ofrecer retos diversos en cuanto a contenido y soporte utilizado se alinea con los tres principios del DUA.

Reto 1: Contraseñas y autenticación

El primer reto está relacionado con los contenidos de contraseñas y autenticación. Cada grupo recibe un email con el enlace a un Formulario de Google (ver Anexo III). Los estudiantes deben seguir las instrucciones que se indican para resolver el reto. En la Tabla 12, se indican el nombre, el objetivo y el escenario del reto 1. Además, a continuación, se detallan los diferentes desafíos que se deben resolver.

Tabla 12

Detalles del reto 1

Nombre del reto	El cifrado de la contraseña maestra
Objetivo	Conseguir la contraseña maestra, de 4 dígitos ($D_1D_2D_3D_4$), resolviendo cuatro desafíos.
Escenario	Una gran cantidad de datos del centro se han visto comprometidos con un intento de phishing. Se requiere una contraseña maestra para desactivar el cifrado del atacante. Cada dígito se obtiene al resolver un desafío sobre buenas prácticas de contraseñas y autenticación.

Nota. Elaboración propia.

Desafío 1: La contraseña más fuerte

El atacante ha dejado una lista de cuatro contraseñas que intentó usar. Solo una cumple con los requisitos de seguridad. El dígito D_1 es el número de la opción de la contraseña más fuerte.

Tabla 13

Opciones del desafío 1 (reto 1)

Opción	**Contraseña**
1	Digitalizacion4ESO
2	P4$$w0rd_4ESO!
3	Cib3rs3guridad
4	1234567890

Nota. Elaboración propia.

Solución para D_1: la opción más fuerte es la 2.

Desafío 2: Tipos de factor de autenticación

La autenticación de dos factores (2FA) es un método de seguridad que requiere dos formas de verificación, de entre tres categorías: algo que sabes (contraseña), algo que tienes (móvil, token) y algo que eres (biometría). El dígito D_2 es el número de la opción que identifica correctamente el factor basado en "algo que tienes" en un sistema 2FA.

Tabla 14

Opciones del desafío 2 (reto 1)

Opción	Descripción
1	La huella dactilar o el reconocimiento facial.
2	El código temporal que genera una aplicación de autenticación (TOTP) en tu teléfono móvil.
3	La contraseña que recuerdas.
4	La respuesta a una pregunta secreta.

Nota. Elaboración propia.

Solución para D_2: El código temporal que genera una aplicación de autenticación (TOTP) en tu teléfono móvil es un factor de "algo que tienes", por tanto, es la opción 2.

Desafío 3: Gestión y reutilización

Usar una misma contraseña en múltiples sitios supone un gran riesgo. El dígito D_3 es el número de la opción que describe la principal amenaza de la reutilización de contraseñas.

Tabla 15

Opciones del desafío 3 (reto 1)

Opción	Descripción
1	La contraseña se detectará como insegura por el navegador.
2	Tarda más en ser descifrada por un ataque de fuerza bruta.
3	Si un sitio web sufre una brecha de seguridad, todas tus cuentas estarán en peligro.
4	Es más fácil de recordar, lo que la hace más débil.

Nota. Elaboración propia.

Solución para D_3: La principal amenaza es que una brecha de seguridad en un sitio compromete al resto de tus cuentas, por tanto, es la opción 3.

Desafío 4: Identificación de amenazas

Recibes un correo electrónico que parece ser del departamento de informática, pidiéndote que hagas clic en un enlace "urgente" para "confirmar" tu contraseña. La dirección del remitente es extraña (informatica@escuelagmail.com).

El dígito D_4 es el número de la opción que nombra correctamente esta técnica de robo de credenciales.

Tabla 16

Opciones del desafío 4 (reto 1)

Opción	**Ataque**
1	Ataque de denegación de servicio (DoS)
2	Malware (virus informático)
3	Ataque de fuerza bruta (Brute Force)
4	Phishing

Nota. Elaboración propia.

Solución para D_4: El acto de suplantar una entidad de confianza para engañar se llama phishing, por tanto, es la opción 4.

Clave final y conclusión

Una vez que el estudiante ha resuelto los cuatro desafíos, puede formar la contraseña maestra: 2234. Al introducir dicho código en el documento "Reto 2.docx", se accede a las instrucciones del siguiente reto.

Reto 2: Detección de phishing

El segundo reto está relacionado con el phishing. Después de superar el primer reto, los estudiantes han abierto el documento "Reto 2.docx" con la contraseña maestra, donde se encuentra un enlace a una presentación de Genially (ver Anexo IV). En la Tabla 17, se indican el nombre, el objetivo y el escenario del reto 2. Además, a continuación, se detallan las diferentes pruebas que deben resolver los alumnos.

Tabla 17

Detalles del reto 2

Nombre del reto	El cebo
Objetivo	Analizar tres intentos de phishing diferentes (un email, un WhatsApp, y un sitio web falso) para encontrar una clave oculta que solo se revela al detectar correctamente los indicadores de peligro en cada uno.
Escenario	Los alumnos forman parte del equipo de seguridad del centro y han recibido reportes de actividad sospechosa. Se les presentan tres pantallas simuladas. Por cada una, deben seleccionar los indicadores claves de phishing. Cada detección correcta desbloquea una parte de la clave final.

Nota. Elaboración propia.

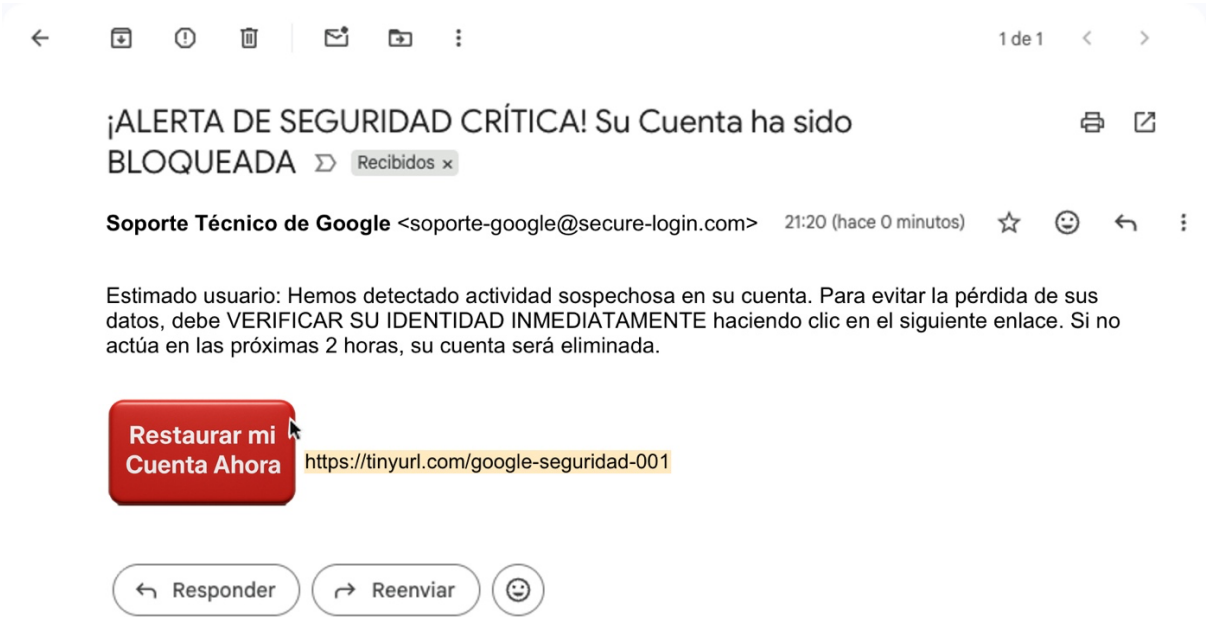
Evidencia 1: Email urgente

Se muestra una captura de pantalla de un email urgente, con la siguiente información:

- DE: Soporte Técnico de Google <soporte-google@secure-login.com>
- ASUNTO: ¡ALERTA DE SEGURIDAD CRÍTICA! Su Cuenta ha sido BLOQUEADA
- MENSAJE: Estimado usuario: Hemos detectado actividad sospechosa en su cuenta. Para evitar la pérdida de sus datos, debe VERIFICAR SU IDENTIDAD INMEDIATAMENTE haciendo clic en el siguiente enlace. Si no actúan en las próximas 2 horas, su cuenta será eliminada. [Botón grande: Restaurar mi Cuenta Ahora]
- ENLACE DEL BOTÓN: Al pasar el ratón, se ve la URL https://tinyurl.com/google-seguridad-001

Figura 5

Captura de pantalla de la evidencia 1 (reto 2)



Nota. Elaboración propia.

Se lanza la pregunta clave: ¿Cuáles son los cuatro principales indicadores de que este email es un ataque de phishing?

Tabla 18

Opciones de la evidencia 1 (reto 2)

Opción	Razón del peligro	Clave oculta
A	El uso de mayúsculas en el asunto.	
B	La dirección de email del remitente es sospechosa.	G
C	El enlace no coincide con la dirección web oficial de la empresa que supuestamente lo envía.	I

D	Menciona una “Alerta de seguridad crítica” y exige una acción inmediata y urgente.	I
E	El diseño gráfico del email no es profesional.	

Nota. Elaboración propia.

Solución: Los alumnos deben seleccionar las opciones B, C y D, desbloqueando las letras G, I e I de la clave oculta.

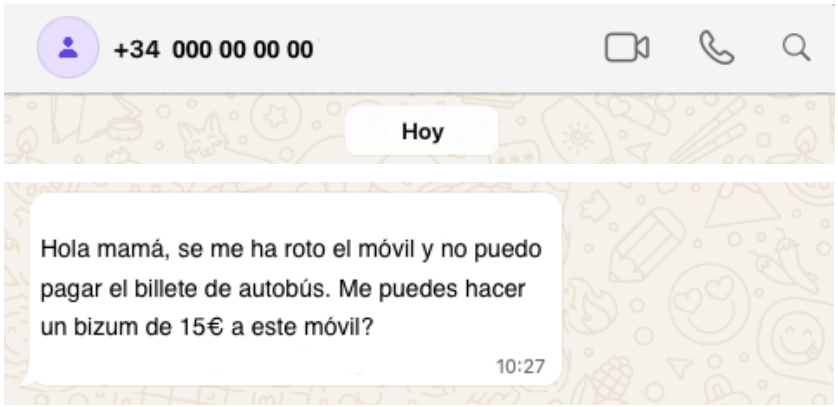
Evidencia 2: WhatsApp de un amigo cercano o familiar pidiendo ayuda

Se muestra un mensaje de WhatsApp de un número desconocido, haciéndose pasar por un amigo cercano o familiar, fingiendo estar en una emergencia y necesitar dinero. El mensaje contiene la siguiente información:

- REMITENTE: +34 6## ### ### (contacto desconocido)
- MENSAJE: Hola mamá, se me ha roto el móvil y no puedo pagar el billete de autobús. Me puedes hacer un bizum de 15 € a este móvil?

Figura 6

Captura de pantalla de la evidencia 2 (reto 2)



Nota. Elaboración propia.

Se lanza la pregunta clave: ¿Por qué no debes realizar ninguna acción sobre este mensaje?

Tabla 19

Opciones de la evidencia 2 (reto 2)

Opción	**Razón del peligro**	**Clave oculta**
A	No tienes el número de teléfono en tus contactos.	
B	Presión por hacer un pago inmediato.	O
C	Responder al mensaje confirma que tu número está activo, favoreciendo el intento de otros engaños.	N
D	El mensaje se recibe en la aplicación de WhatsApp.	

Nota. Elaboración propia.

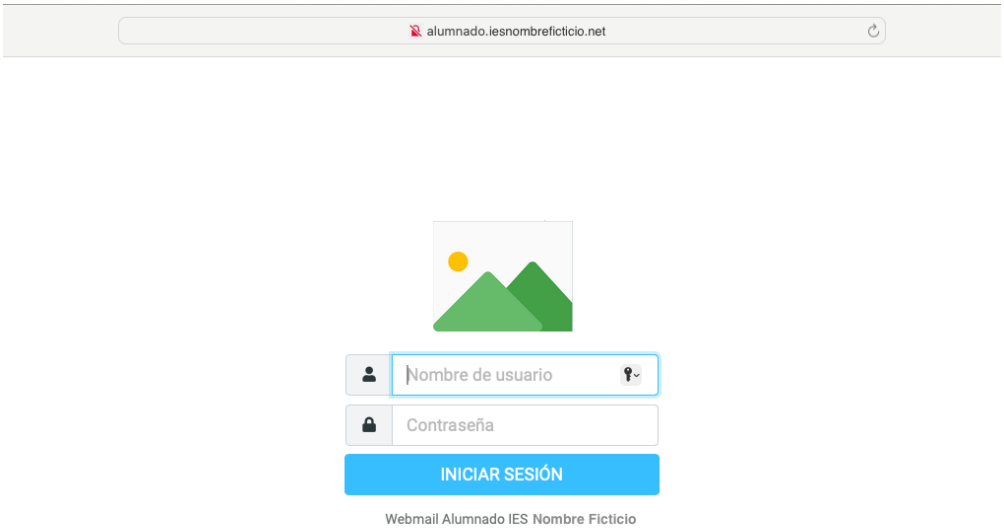
Solución: Los alumnos deben seleccionar las opciones B y C, desbloqueando las letras O y N de la clave oculta.

Evidencia 3: Página de inicio de sesión falsa

Se muestra una imagen de una página de inicio de sesión que simula ser el portal del instituto, pero con fallos. En la barra de direcciones se muestra una URL muy similar y el contenido de la página es idéntico, pero la imagen de fondo está borrosa y hay un error de carga del logo.

Figura 7

Captura de pantalla de la evidencia 3 (reto 2)



Nota. Elaboración propia.

Se lanza la pregunta clave: ¿Si fueras a introducir tu contraseña en esta página, ¿qué detalle crucial te indicaría que es una página falsa?

Tabla 20

Opciones de la evidencia 3 (reto 2)

Opción	Razón del peligro	Clave oculta
A	La URL es demasiado larga.	
B	El dominio de la URL no es el oficial del instituto (es .net en lugar de .edu).	E
C	El icono del candado de seguridad no aparece o está roto.	N
D	La página tarda mucho en cargar.	

Nota. Elaboración propia.

Solución: Los alumnos deben seleccionar las opciones B y C, desbloqueando las letras E y N de la clave oculta.

Clave final y conclusión

Una vez se tienen todas las letras de la clave oculta, los alumnos tienen acceso al acertijo:

> Soy chispa que no se ve pero mueve la mano,
> puedo fabricar ideas o azúcar en terreno cubano.
> Nace en la mente, trabaja en la fábrica y en el corazón,
> me nombran cuando hay astucia, invención y creación.
> ¿Qué palabra soy?

En este acertijo, se pueden proporcionar las siguientes pistas:

1. A la vez nombre de talento y de industria tradicional.
2. Lo que usó el inventor para crear su máquina.
3. Empiezo por I y termino por O.

Con la palabra clave, INGENIO, los estudiantes deben buscar en el directorio del ordenador el documento "INGENIO.docx", donde pueden ver las instrucciones del siguiente reto.

Reto 3: Malware

El tercer reto está relacionado con malware y buenas prácticas de seguridad. Después de superar el segundo reto, los estudiantes han encontrado y abierto el documento "INGENIO.docx" (ver Anexo V). En la Tabla 21, se indican el nombre, el objetivo y el escenario del reto 3. Además, a continuación, se detallan las diferentes pruebas que deben resolver los alumnos.

Tabla 21

Detalles del reto 3

Nombre del reto	Infección en el instituto
Objetivo	Identificar el tipo de malware que ha infectado el sistema del instituto y aplicar medidas correctas para detenerlo, obteniendo un código final de desbloqueo.
Escenario	El sistema informático del instituto ha sido atacado. Los ordenadores se comportan de forma extraña, aparecen ventanas inesperadas y algunos archivos han desaparecido. El equipo de ciberseguridad (el alumnado) tiene 10 minutos antes de que el sistema se bloquee por completo.

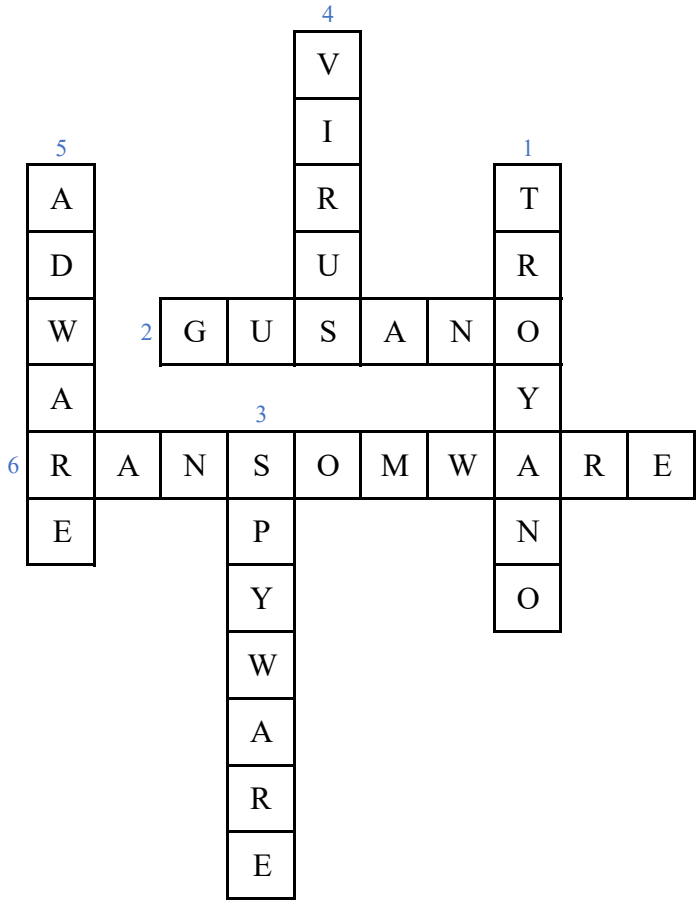
Nota. Elaboración propia.

Prueba 1: Síntomas sospechosos

Esta prueba consiste en resolver el crucigrama (ver Figura 8) que se encuentra en el documento "INGENIO.docx". Para ello, se muestran distintas características de los malware, y se debe indicar el tipo de malware correcto.

Figura 8

Crucigrama de la prueba 1 (reto 3)



Nota. Elaboración propia.

Las características que se indican para resolver el crucigrama son las siguientes:

1. Se oculta dentro de un programa.
2. Se copia automáticamente por la red.
3. Roba información sin que lo notes.
4. Se replica e infecta otros archivos o sistemas sin consentimiento.
5. Muestra publicidad no deseada o engañosa de forma intrusiva.
6. Pide dinero para recuperar archivos.

En caso de requerirse, y tras un tiempo determinado de transcurso de la prueba 1, se puede ofrecer como pista el listado de palabras que componen el crucigrama, sin relacionar con su definición correspondiente.

En el mismo documento, en la página siguiente, los estudiantes tienen disponible la sección Código de desbloqueo, con el siguiente contenido:

12 - 24 - 32 - 42 - 52 - 65

Descubre una parte del código final de desbloqueo utilizando el crucigrama.

De la misma manera, se puede ofrecer alguna pista al alumnado para descifrar la parte del código de desbloqueo.

Solución: La parte del código de desbloqueo correspondiente a la prueba 1 es RÁPIDO, que corresponde a la 2ª letra de la 1ª palabra + la 4ª letra de la 2ª palabra + la 2ª letra de la 3ª palabra + la 2ª letra de la 4ª palabra + la 2ª letra de la 5ª palabra + la 5ª letra de la 6ª palabra.

Prueba 2: ¿Cómo nos protegemos?

Esta prueba consiste en un ejercicio de selección múltiple. En la siguiente página del documento, se listan las siguientes acciones, y se debe seleccionar cuáles de ellas se corresponden con acciones seguras:

- Descargar archivos piratas
- Usar antivirus actualizado
- Abrir enlaces desconocidos
- Actualizar el sistema
- Hacer copias de seguridad

Solución: La posición de cada acción correcta se corresponde con un dígito del código final de desbloqueo. En este caso, 245.

Prueba 3: El laboratorio

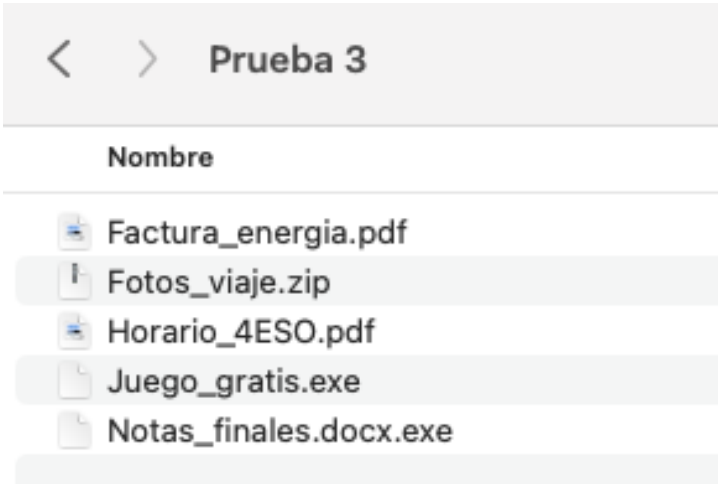
Esta prueba consiste en diferenciar qué archivos pueden estar potencialmente infectados. En el documento, se indica al alumnado que acceda a una carpeta del ordenador que contiene los siguientes archivos y debe eliminar aquellos que resulten sospechosos.

- Horario_4ESO.pdf
- Fotos_viaje.zip
- Juego_gratis.exe 
- Notas_finales.docx.exe 
- Factura_energia.pdf

Solución: Al eliminar los archivos sospechosos (Juego_gratis.exe y Notas_finales.docx.exe), los alumnos deben acceder a cada uno de los archivos restantes y construir la dirección del directorio del ordenador donde se ubica el documento “Sistema desbloqueado.docx”, donde se debe introducir la clave alfanumérica obtenida en las pruebas 1 y 2 (RÁPIDO245).

Figura 9

Captura de pantalla de la carpeta de la prueba 3 (reto 3)



Nota. Elaboración propia.

Reto 4: Huella digital y privacidad

El cuarto reto está relacionado con la huella digital y la privacidad. Después de superar el tercer reto, los estudiantes han abierto el documento "Sistema desbloqueado.docx", donde se encontrará el acceso a un cuestionario en el aula virtual. En la Tabla 22, se indican el nombre, el objetivo y el escenario del reto 4. Además, a continuación, se detalla la prueba que deben resolver los alumnos.

Tabla 22

Detalles del reto 4

Nombre del reto	El anonimato: desafío de privacidad
Objetivo	Responder un cuestionario de diez preguntas sobre la huella digital y la privacidad, obteniendo tiempo extra a un tiempo base de 30" para afrontar el reto final.
Escenario	Has sido atrapado en una simulación de una base de datos de una inteligencia artificial maliciosa llamada EDD (Extractora de Datos Digitales). Para escapar, debes probar que todavía tienes control sobre tu propia información.

Nota. Elaboración propia.

En esta prueba, el alumnado deberá responder a un cuestionario de diez preguntas, con cuatro opciones de respuesta. Las preguntas son las siguientes (ver Anexo VI para ver el detalle de opciones de respuesta y retroalimentación).

1. ¿Cuál de las siguientes acciones contribuye directamente a tu huella digital pasiva?

a. Aceptar las cookies por defecto en una página web sin leer la política
b. Subir tu currículum a un portal de empleo
c. Firmar una petición en línea con tu nombre completo y correo electrónico
d. Publicar una foto de tus vacaciones en Instagram

Respuesta correcta: a

2. Estás configurando la privacidad de tu perfil en una red social. ¿Qué opción es la más segura para proteger tu intimidad y limitar tu huella?
    a. Configurar el perfil como 'Solo amigos' y desactivar la geolocalización de las publicaciones
    b. Dejar la configuración por defecto de la plataforma, ya que la red social ya te protege
    c. Configurar el perfil como 'Público', pero evitar publicar información muy personal
    d. Configurar el perfil como 'Público' y usar un nombre de usuario falso

Respuesta correcta: a

3. Has descubierto que una foto embarazosa tuya de hace tres años sigue disponible en un foro antiguo. ¿Qué derecho, reconocido por el Reglamento General de Protección de Datos (RGPD), te permitiría solicitar su eliminación?
    a. Derecho de acceso
    b. Derecho de supresión (o 'derecho al olvido')
    c. Derecho de rectificación
    d. Derecho de oposición

Respuesta correcta: b

4. Un inversor revisa tu perfil de red social para un posible empleo futuro y encuentra comentarios de hace 5 años con opiniones muy radicales. Esto es un ejemplo de riesgo de la huella digital en el ámbito de:
    a. Riesgo de phishing
    b. Riesgo de malware
    c. Riesgo en la reputación digital
    d. Riesgo de suplantación de identidad

Respuesta correcta: c

5. Estás realizando una investigación sensible y no quieres que tu proveedor de servicios de internet (ISP) o los sitios web sepan tu ubicación geográfica. ¿Qué herramienta de privacidad avanzada deberías usar?

a. Usar un gestor de contraseñas
b. Usar el modo de navegación 'Incógnito' o 'Privada'
c. Conectarte a través de una VPN
d. Instalar un software antivirus

Respuesta correcta: c

6. Si una aplicación gratuita te pide acceso a tu micrófono, cámara, contactos y ubicación, y su función principal es una linterna, ¿cuál debería ser tu acción prioritaria desde el punto de vista de la privacidad?
    a. Aceptar todos los permisos para que la aplicación funcione correctamente
    b. Denegar todos los permisos innecesarios y buscar una alternativa si no funciona sin ellos
    c. Aceptar todos los permisos, pero instalar un antivirus que la supervise
    d. Aceptar solo los permisos de la ubicación, ya que es el menos sensible

Respuesta correcta: b

7. ¿Qué tipo de dato personal es considerado sensible bajo la ley de protección de datos, y requiere una protección especial?
    a. Tu fecha de nacimiento
    b. Tu dirección de correo electrónico
    c. Tu grupo sanguíneo y alergias
    d. Tu número de teléfono

Respuesta correcta: c

8. Para evitar que los ciberdelincuentes puedan acceder a tus cuentas incluso si descubren tu contraseña, ¿qué medida de seguridad es la más efectiva para implementar inmediatamente?
    a. Cambiar la contraseña cada semana
    b. Activar la autenticación de dos factores (2FA)
    c. Usar el nombre de una mascota como parte de la contraseña
    d. Usar la misma contraseña en todas las cuentas, pero muy larga

Respuesta correcta: b

9. Al visitar un sitio web, este utiliza cookies de seguimiento que registran tus hábitos de compra para mostrarte anuncios personalizados. ¿A qué aspecto de la huella digital está directamente relacionado este proceso?
    a. A la huella digital pasiva, ya que el sitio web registra tus acciones automáticamente

b. A la divulgación de datos sensibles, porque tu historial de navegación es sensible
c. A la huella digital activa, porque estás comprando productos
d. A la suplantación de identidad, ya que pueden robar tu historial de compras

Respuesta correcta: a

10. Para reducir al máximo tu huella digital y proteger tu privacidad, ¿cuál de estas acciones tiene el mayor impacto en el largo plazo?
    a. Borrar el historial de navegación de tu móvil cada noche
    b. Usar un apodo o alias en lugar de tu nombre real en foros públicos
    c. Desactivar la función de 'recordar contraseña' en el navegador
    d. Revisar y ajustar periódicamente la configuración de privacidad y seguridad de todas las plataformas que usas (redes sociales, apps, correo)

Respuesta correcta: d

Solución: A la hora de pasar al reto final, cada grupo de estudiantes dispondrá de 30” de tiempo base, al cual se le sumará el tiempo obtenido en el reto 4. Cada respuesta correcta, sumará 10” al tiempo base, mientras que, cada respuesta incorrecta, restará 2,5”. Si no se responde la pregunta, no se sumará ni se restará ningún tiempo. El tiempo mínimo con el que se puede llegar al reto final es el tiempo base (30”), y el tiempo máximo es de 130” (2’ 10”).

Reto 5: Reto final para concluir el juego

El quinto reto se corresponde con el reto final. Para llevarlo a cabo, se dispondrá del tiempo base (30”) + el tiempo obtenido en el reto 4, por tanto, se puede disponer entre 30” y 130” para realizar la prueba. En la Tabla 23, se indican el nombre, el objetivo y el escenario del reto final. Además, a continuación, se detalla la prueba que deben resolver los alumnos.

Tabla 23

Detalles del reto final

Nombre del reto	¿Humano o amenaza?
Objetivo	Clasificar ocho tarjetas con situaciones digitales cotidianas según se consideren seguras o peligrosas, en un tiempo limitado, para llegar al final del juego.
Escenario	El sistema de seguridad ha activado un protocolo de emergencia: una inteligencia artificial debe decidir qué acciones son seguras y cuáles son amenazas reales. ¿El problema? La IA está dañada y el alumnado debe tomar las decisiones correctas antes de que el sistema bloquee todo.

Nota. Elaboración propia.

En un Genially (ver Anexo VII), en pantalla, aparecen ocho tarjetas con situaciones digitales cotidianas y un temporizador de cuenta atrás. Cada grupo debe clasificarlas rápidamente en dos columnas: seguro y peligro. Al clasificarlas correctamente, se desbloquea el código final.

Las tarjetas que se muestran en pantalla son las siguientes, según su clasificación en seguro y peligro[3]:

Seguro

- Contraseña: "P3rr0$!2024" + verificación por móvil
- Perfil privado solo para amigos
- Activar doble factor en redes sociales
- Revisar permisos de una app antes de instalarla

Peligro

- Correo del banco con enlace acortado
- Programa gratuito para "mejorar el móvil"
- Publicar tu ubicación en tiempo real
- Archivo adjunto de un contacto desconocido

Solución: Al clasificar correctamente las tarjetas, se muestra un mensaje de enhorabuena por finalizar el juego.

4.4.4. Fase 3: cierre y reflexión

Los objetivos de la tercera fase, de cierre y reflexión, se basan en consolidar y dar sentido a los aprendizajes obtenidos, mediante la reflexión sobre lo aprendido y el proceso seguido.

En la Tabla 24 se detallan cada una de las tareas que se llevan a cabo, especificando su temporalización y su vinculación con los principios del DUA.

Tabla 24

Relación de tareas que componen la tercera fase

Tarea	Principio DUA	Temporalización	Descripción general
Síntesis y organización de contenidos	Principios 1 y 3	10'	El docente comparte un mapa conceptual con los diferentes contenidos que se han abordado a lo largo del juego. También está a disposición de los estudiantes un resumen de los contenidos y un vídeo breve explicativo.

[3] En pantalla, las tarjetas se muestran desordenadas de una manera aleatoria.

Reflexión metacognitiva	Principio 3	10’	El docente abre un breve debate sobre la temática tratada y la forma en la que se han adquirido conocimientos.
Valoración de logros y dificultades	Principio 3	5’	El docente lanza una cuestión sobre aquellos logros y dificultades encontrados durante la realización de la actividad por parte de los estudiantes.
Relación del aprendizaje con la realidad	Principio 3	10’	El docente reproduce un vídeo corto y abre un breve debate sobre la conexión de lo aprendido con la realidad actual.

Nota. Elaboración propia.

La temporalización total de la tercera fase es de 35 minutos. A continuación, se detallan cada una de las tareas de la fase 3.

En primer lugar, la síntesis y organización de contenidos pretende proporcionar el contenido de una manera estructurada para afianzar la adquisición de los mismos durante la realización de la actividad. La aplicación del principio 1 del DUA se basa en la representación de los mismos contenidos de diferentes maneras (mapa conceptual, resumen y vídeo), de forma que los estudiantes puedan seleccionar aquella que les resulte más cómoda para su comprensión.

En segundo lugar, el docente abre un breve debate sobre la temática de la ciberseguridad y la forma en la que se ha abordado, favoreciendo una reflexión metacognitiva. Cuando jugamos, en muchas ocasiones, el cerebro entra en “piloto automático”, lo que se conoce como estado de flujo. El hecho de llevar a cabo un proceso reflexivo sobre la actividad permite movilizar al pensamiento consciente aquellos aprendizajes que se han realizado de manera inconsciente.

Una tercera tarea es la valoración de logros y dificultades, la cual se trata de una forma de retroalimentación, en la que tanto los estudiantes como el docente se permiten aprender de sus debilidades para mejorarlas.

Por último, con el objetivo de contextualizar lo aprendido en el mundo real, el docente reproduce el vídeo *Privacidad en Internet* sobre la campaña para concienciar a niños, niñas y adolescentes sobre la importancia de la protección de la identidad y la privacidad en Internet y redes sociales [enlace: https://youtu.be/CXmjnNoDrTI] (UNICEF #educaDerechos, 2020) y se abre un breve debate en el que el alumnado puede compartir experiencias, creencias o ideas relacionadas con la temática.

La aplicación del principio 3 del DUA durante toda esta tercera fase radica en el incremento de la conexión de los intereses de los estudiantes con los contenidos, dado que el material se ofrece de una manera que se adapta a sus necesidades, se ofrece un espacio para reflexionar sobre lo aprendido, así como de los logros y dificultades encontradas, y se presenta una conexión con la realidad.

4.4.5. Evaluación de la intervención

La evaluación formativa se concibe, según Muñoz et al. (2022), como una metodología clave para la mejora continua de los aprendizajes, transformando el aula en un espacio de comunicación activa donde el estudiante es el protagonista de su propio progreso. Además, se trata de una herramienta reguladora y reflexiva que busca trascender el modelo tradicional para fomentar la autorregulación del alumnado y optimizar la práctica docente mediante la retroalimentación constante.

En el marco de la propuesta, la evaluación no se limita a la comprobación final de los aprendizajes adquiridos, sino que se integra de forma transversal en el desarrollo del juego. Durante toda la actividad, el docente actúa como guía del proceso de aprendizaje, por lo que, mediante la observación continua, debe realizar los ajustes necesarios para asegurar la comprensión y la adquisición de aprendizajes.

Empezando por la activación de conocimientos previos, en la primera fase, el docente lanza las preguntas "¿Qué es la seguridad digital?" y "¿Qué es el bienestar digital?" y provoca una discusión controlada para encaminar las respuestas de las mismas, favoreciendo el pensamiento crítico.

En cada uno de los retos de la segunda fase se produce una retroalimentación inmediata, de manera que los estudiantes son capaces de autorregularse en el avance de la actividad. Los retos están configurados de manera que solo se pueda avanzar con respuestas acertadas, por lo que aquellas respuestas erróneas plantean un momento de autoevaluación. Además, en algunos de los retos, se da la posibilidad de acceder a pistas, ya sea de manera autónoma por los estudiantes o facilitadas por el docente, el cual observa y registra de manera sistemática el comportamiento, las interacciones y el desempeño de los grupos durante la actividad.

En la tercera fase, de cierre y reflexión, la síntesis y organización de contenidos, la reflexión metacognitiva y la valoración de logros y dificultades crean un espacio de retroalimentación inmediata, autoevaluación y coevaluación, en el que los estudiantes mejoran su comprensión, reflexionan sobre su trabajo, identificando fortalezas y debilidades, y se promueve el aprendizaje colaborativo. Además, tras la reproducción del vídeo que pretende relacionar lo aprendido con la realidad, se plantea un debate en el que se favorece el pensamiento crítico y

se afianza lo aprendido.

Por último, a nivel global, se plantea una rúbrica de evaluación (ver Anexo VIII), que integra la valoración de conocimientos específicos y competencias transversales. Esta rúbrica se comparte con el alumnado desde el inicio de la actividad, con el fin de hacer explícitos los criterios de evaluación y promover la implicación activa en su propio proceso de aprendizaje. Los criterios de evaluación que se tienen en cuenta son los conocimientos sobre ciberseguridad, la resolución de problemas, el pensamiento crítico, el trabajo en equipo, la comunicación y la autonomía y autorregulación. Este documento debe ser completado por cada estudiante, a modo de autoevaluación, y por el docente.

En resumen, la evaluación de la intervención se configura como un proceso dinámico, participativo y orientado a la mejora continua.

5. Conclusiones y valoración crítica

El presente Trabajo de Fin de Máster ha tenido como objetivo principal el diseño de un escape room educativo digital para la enseñanza de ciberseguridad en la materia Digitalización de 4º ESO, con el fin de favorecer el desarrollo de la competencia digital y la concienciación sobre el uso seguro, responsable y crítico de la tecnología. A partir del análisis realizado y del diseño de la propuesta, se considera que los objetivos plateados al inicio del trabajo han sido alcanzados de manera satisfactoria.

A continuación, se presentan las principales conclusiones derivadas del estudio teórico que fundamenta el diseño de la actividad.

1. Adecuación curricular de la propuesta. El análisis del marco normativo y curricular de la materia Digitalización de 4º ESO confirma que la ciberseguridad se trata de un contenido integrado en el currículo vigente. El escape room diseñado se alinea de forma coherente con las competencias específicas, los saberes básicos y los criterios de evaluación establecidos en el RD 217/2022, lo que refuerza su viabilidad y adecuación como recurso didáctico.
2. Base teórica sólida. La revisión de literatura diversa sobre metodologías activas, gamificación, Aprendizaje Basado en Retos y escape room educativos pone de manifiesto su potencial para promover el aprendizaje significativo, aumentar la motivación del alumnado y favorecer el desarrollo de competencias transversales, como el trabajo en equipo, el pensamiento crítico y la autonomía. La integración de estos enfoques en el diseño del escape room responde a los principios pedagógicos que sitúan al alumnado como protagonista de su propio aprendizaje.
3. Selección adecuada de contenidos de ciberseguridad. Los contenidos abordados en el escape room (gestión de contraseñas, phishing, malware, huella digital y privacidad) han sido seleccionados atendiendo a su relevancia, su adecuación al nivel del alumnado y su vinculación con situaciones reales cotidianas. Esta selección permite trabajar la ciberseguridad de una manera aplicada y preventiva, sobrepasando el enfoque puramente teórico.
4. Potencial del escape room como recurso didáctico innovador. El diseño del escape room educativo digital, que usa una narrativa gamificada y retos secuenciados, demuestra que este tipo de recurso puede ser una herramienta eficaz para trabajar la ciberseguridad en la ESO. La resolución de problemas, el trabajo cooperativo, la toma de decisiones y la retroalimentación inmediata favorecen un aprendizaje activo y significativo.

5. Contribución al desarrollo de la competencia digital del alumnado. La propuesta diseñada permite trabajar varias áreas de la competencia digital, como la seguridad, la resolución de problemas o el pensamiento crítico. Con esta actividad, el alumnado no solo adquiere conocimientos sobre ciberseguridad, sino que desarrolla una actitud preventiva, responsable y crítica ante los riesgos que presenta el entorno digital. Estos aspectos son fundamentales en la formación de una ciudadanía digital competente.
6. Importancia del rol docente. El diseño del escape room pone de manifiesto la importancia de la competencia digital docente y de la capacidad del profesorado para diseñar, adaptar y evaluar experiencias de aprendizaje innovadoras. El rol de guía y facilitador resulta clave para obtener un equilibrio lúdico-educativo, así como para atender a la diversidad del aula.

La elaboración de este Trabajo de Fin de Máster ha supuesto una experiencia altamente significativa, tanto a nivel académico como personal, al permitirme adoptar una perspectiva centrada en el alumnado y en sus procesos de aprendizaje. Además, al trabajar la temática de la ciberseguridad, se ha intensificado mi creencia sobre su importancia en el mundo actual, caracterizado por un crecimiento abrumador de la digitalización. En este sentido, se espera que este trabajo resulte enriquecedor también para quienes lo lean.

Entre las principales fortalezas del trabajo, destaca la coherencia entre el marco teórico, los objetivos y la propuesta didáctica diseñada, así como la adaptación al currículo vigente y a las necesidades reales del alumnado de educación secundaria. En esta línea, el diseño detallado del escape room, la integración de metodologías activas y la alineación con los principios del DUA refuerzan el valor pedagógico de la propuesta. No obstante, se identifican debilidades. En primer lugar, al tratarse de un trabajo centrado en el diseño de una propuesta, no se ha llevado a cabo una implementación real en el aula, lo que imposibilita medir su impacto en el aprendizaje del alumnado. Además, la puesta en práctica de un escape room digital puede verse altamente condicionada por factores externos, como la dotación tecnológica del centro, la conectividad o el nivel de competencia digital, tanto del alumnado como del profesorado. Por último, resulta imprescindible destacar que, pese a haber conseguido una base teórica sólida y un diseño con un alto nivel de detalle, cada iteración realizada sobre el mismo ha dado lugar a mejoras y ampliaciones, lo que, visto desde el punto de vista de la mejora continua, abre un abanico de posibilidades respecto a la actividad.

Desde el punto de vista del aprendizaje personal, la profundización en el marco teórico que rodea el recurso me ha permitido conocer con detalle las metodologías activas y sus diferencias respecto a metodologías tradicionales, comprender la importancia de la planificación didáctica

y reflexionar sobre el papel docente en la educación digital. Si bien es cierto que los beneficios de las situaciones de aprendizaje innovadoras pueden resultar evidentes, he comprendido que no todo vale y que un mal uso de las mismas puede provocar los resultados contrarios a los deseados, y es por esto que se hace especial hincapié en la formación del profesorado. Asimismo, el desarrollo de este trabajo ha reforzado el pensamiento sobre la necesidad de formar al alumnado no solo en el uso de la tecnología, sino en su uso seguro, crítico y responsable.

La propuesta realizada presenta una serie de limitaciones que es conveniente destacar para poner en contexto sus aportaciones. En primer lugar, el diseño del escape room digital se ha planteado desde un enfoque teórico, sin una implementación en un contexto educativo real que permita evaluar su impacto en el aprendizaje del alumnado. En consecuencia, no se dispone de datos cuantitativos ni cualitativos que permitan hacer mediciones del desarrollo competencial o de la adquisición de conocimientos de ciberseguridad. De otra parte, la propuesta se dirige de manera específica al alumnado de 4º ESO, lo que limita su generalización a otros niveles educativos sin una adaptación previa de contenidos y complejidad. Del mismo modo, se parte de una disposición de dispositivos digitales y conectividad "ideales", lo que no coincide con la realidad de todos los centros educativos y que puede condicionar su aplicabilidad. Por último, un factor clave para asegurar el éxito de la propuesta es un adecuado nivel de competencia digital del profesorado.

A partir de las limitaciones detectadas, se abren diversas líneas de investigación futuras que permitirían ampliar el alcance de esta propuesta, entre las que se pueden señalar:

- La implementación del recurso en contextos educativos reales, acompañada de una investigación que analice su impacto en el desarrollo competencial y en la adquisición de conocimientos.
- El estudio comparativo entre metodologías tradicionales y experiencias gamificadas en la enseñanza de ciberseguridad.
- La adaptación del recurso a otros contextos o niveles educativos o fortaleciendo la atención a la diversidad del alumnado, validando su carácter transversal.
- La formación del profesorado en el diseño y uso de escape room educativos como herramienta innovadora.

En conclusión, el presente Trabajo de Fin de Máster pone de manifiesto la viabilidad del escape room educativo digital como propuesta didáctica innovadora y su alto potencial para la enseñanza de ciberseguridad en la educación secundaria, contribuyendo al desarrollo de la competencia digital y a la formación de una ciudadanía digital crítica, segura y responsable.

6. Referencias

Apple. (2011). Challenge based learning: A classroom guide. Recuperado de: http://www.apple.com/br/education/docs/CBL_Classroom_Guide_Jan_2011.pdf

BeChallenge. (2022, 5 de mayo). *¿Qué es el Aprendizaje Significativo? Importancia y Beneficios*. https://blog.bechallenge.io/que-es-el-aprendizaje-significativo/

Cabrera, J. I. (2017). Nativos digitales que no lo son tanto. *Revista de estudios de juventud*, (117), 199-207. https://bit.ly/4i2ZLRj

Contreras-Espinosa, R. S., & Eguia, J. L. (2017). *Experiencias de gamificación en las aulas*. InCom-UAB, 15. https://dialnet.unirioja.es/servlet/libro?codigo=713370

Cuesta, L. (2024, 30 de septiembre). *Bienestar digital: equilibrar, no erradicar la tecnología*. El Español. https://bit.ly/3XuD2o2

educaDUA. (2016, 23 de marzo). *Sobre el DUA: Principios del DUA*. https://www.educadua.es/html/dua/pautasDUA/dua_principios.html

EscapeUp. (2022, 5 de abril). *El origen de los escape rooms*. https://escapeup.es/blog/origen-escape-rooms/

Gaitan, M. A., & de la Cruz, R. (2024). Impacto de las metodologías activas en la motivación y rendimiento académico de estudiantes en educación secundaria. *Pedagogical Constellations, 3*(1), 127- 146. https://doi.org/10.69821/constellations.v3i1.32

García, M., Romero, S., Castro, G. J., & Buendía-Oliva, M. (2024). Propuestas para el diseño de estrategias didácticas en entornos digitales a partir de la teoría de autodeterminación y la gamificación. *RIDE Revista Iberoamericana para la Investigación y el Desarrollo Educativo, 14*(28). https://doi.org/10.23913/ride.v14i28.1841

González, G. (2021, 9 de octubre). Origen e historia de los escape rooms. E*scape Room Lover*. https://bit.ly/3WVBRxG

Gutiérrez, L. (2012). Conectivismo como teoría de aprendizaje: conceptos, ideas, y posibles limitaciones. *Revista Educación y Tecnología,* (1), 111-122. https://dialnet.unirioja.es/servlet/articulo?codigo=4169414

Guzmán, V. del C., Naranjo, A. L., Oña, J. E., & Barona, S. M. (2025). El aprendizaje basado en retos como estrategia para fomentar la motivación y el compromiso académico. *Polo del Conocimiento, 10*(6), 1842-1862. https://doi.org/10.23857/pc.v10i6.9755

Instituto de la Juventud de Extremadura. (2018). *Manual de diseño de un juego de escape*. https://bit.ly/3Y2msvO

Lejárraga, A. M., Lucas, E. M., & Nieto, J. (2023). Metodologías para la innovación educativa. En N. Sánchez (Ed.), *Aspectos esenciales para la docencia del siglo XXI: innovar e investigar* (pp. 25-70). Centro de Estudios Financieros. http://hdl.handle.net/20.500.12226/2097

Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación. https://www.boe.es/eli/es/lo/2020/12/29/3/con

López, G. F., Naranjo, M. B., Vera, M.D., & Naranjo, Z. M. (2025). Gamificación en la educación: avances, beneficios y limitaciones en el aprendizaje escolar. *Imaginario Social, 8*(3). 53-69. https://revista-imaginariosocial.com/index.php/es/article/view/324

Lozano-Monterrubio, N., Cuartielles, R., Carrillo-Pérez, N., & Montagut, M. (2024). Escape rooms como metodología educativa para combatir la desinformación en alumnos de primaria y secundaria: el caso de Learn to Escape. *Revista Latina de Comunicación Social*, (82), 1-21. https://www.doi.org/10.4185/RLCS-2024-2243

Macías-Guillén, A., Montes, R., & Borrás-Gené, O. (2023). Escape Room Educativo Digital para el aprendizaje en docencia híbrida. *Campus Virtuales, 12*(2), 19-30. https://doi.org/10.54988/cv.2023.2.1160

Microsoft. (2024, 25 de mayo). *¿Qué es la ciberseguridad?* https://bit.ly/47Lbh0k

Muñoz, V. A., Figueroa, E. C., & Ortecho, Z. C. (2022). La evaluación formativa una oportunidad de mejora en los aprendizajes. *TecnoHumanismo, 2*(3), 1-21. https://dialnet.unirioja.es/servlet/articulo?codigo=8754067

Navarro-Mateos, C., Pérez-López, I. J., & Femia, P. (2021). La gamificación en el ámbito educativo español: revisión sistemática (Gamification in the Spanish educational field: a systematic review). *Retos, 42*, 507-516. https://doi.org/10.47197/retos.v42i0.87384

Negre, C., & Carrión, S. (2020). *Desafío en el aula*. PAIDÓS Educación.

Orrego, V. (2022). Innovación educativa: Propuesta conceptual, paradigmática y dimensiones de acción. *Revista Ensayos Pedagógicos, 17*(2), 95-116. http://doi.org/10.15359/rep.17-2.5

Pérez, E., & Gértrudix-Barrio, F. (2021). Ventajas de la gamificación en el ámbito de la educación formal en España. Una revisión bibliográfica en el periodo de 2015-2020. *Contextos Educativos. Revista De Educación*, (28), 203–227. https://doi.org/10.18172/con.4741

Pozo-Sánchez, S., Lampropoulos, G., & López-Belmonte, J. (2022). Comparing Gamification Models in Higher Education Using Face-to-Face and Virtual Escape Rooms. *Journal of New Approaches in Educational Research, 11*(2), 307-322.

https://doi.org/10.7821/naer.2022.7.1025

Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1. *On the Horizon, 9*(5), 1-6. https://doi.org/10.1108/10748120110424816

Qualia. (2023, 9 de diciembre). *¿Sabes cuándo y por qué nacieron los escape room?* https://bit.ly/3LJU9PW

Real Academia Española. (s.f.). Lúdico. En *Diccionario de la lengua española*. Recuperado en 3 de noviembre de 2025, de https://dle.rae.es/lúdico

Real Decreto 217/2022, de 29 de marzo, por el que se establece la ordenación y las enseñanzas mínimas de la Educación Secundaria Obligatoria. https://www.boe.es/eli/es/rd/2022/03/29/217/con

Redecker, C. (2020). *Marco Europeo para la Competencia Digital de los Educadores: DigCompEdu*. (Trad. Fundación Universia y Ministerio de Educación y Formación Profesional de España). Secretaría General Técnica del Ministerio de Educación y Formación Profesional de España (Original publicado en 2017)

Saldarriaga-Zambrano, P. J., Bravo-Cedeño, G. del R., & Loor-Rivadeneira, M. R. (2016). La teoría constructivista de Jean Piaget y su significación para la pedagogía contemporánea. *Dominio de las Ciencias, 2*(3 Especial), 127-137. https://doi.org/10.23857/dc.v2i3%20Especial.298

Somos Digital. (2022). *DigComp 2.2: Marco de competencias digitales para la ciudadanía*. https://bit.ly/480PrVv

Úbeda, C. (2025, 6 de octubre). *"L'última moneda": el escape room con el que los jóvenes aprenden a gestionar su dinero*. https://bit.ly/49gbMiv

UNICEF #educaDerechos. (2020, 28 de enero). *Privacidad en Internet* [Video]. YouTube. https://youtu.be/CXmjnNoDrTI

Universidad Europea. (2024, 16 de septiembre). *¿Qué es el aprendizaje basado en retos?* https://universidadeuropea.com/blog/aprendizaje-basado-retos/

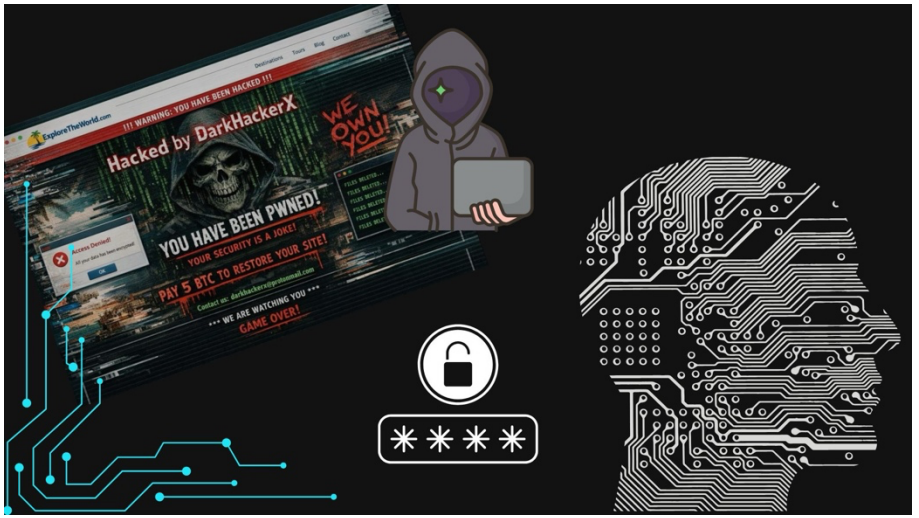
Universidad Europea. (2023, 3 de febrero). *¿Qué es el constructivismo en educación?* https://universidadeuropea.com/blog/constructivismo-educacion

Universidad Internacional de La Rioja. (2022, 6 de septiembre). *¿Qué es la innovación educativa y cómo se aplica en el aula?* https://www.unir.net/revista/educacion/innovacion-educativa/

7. Anexos

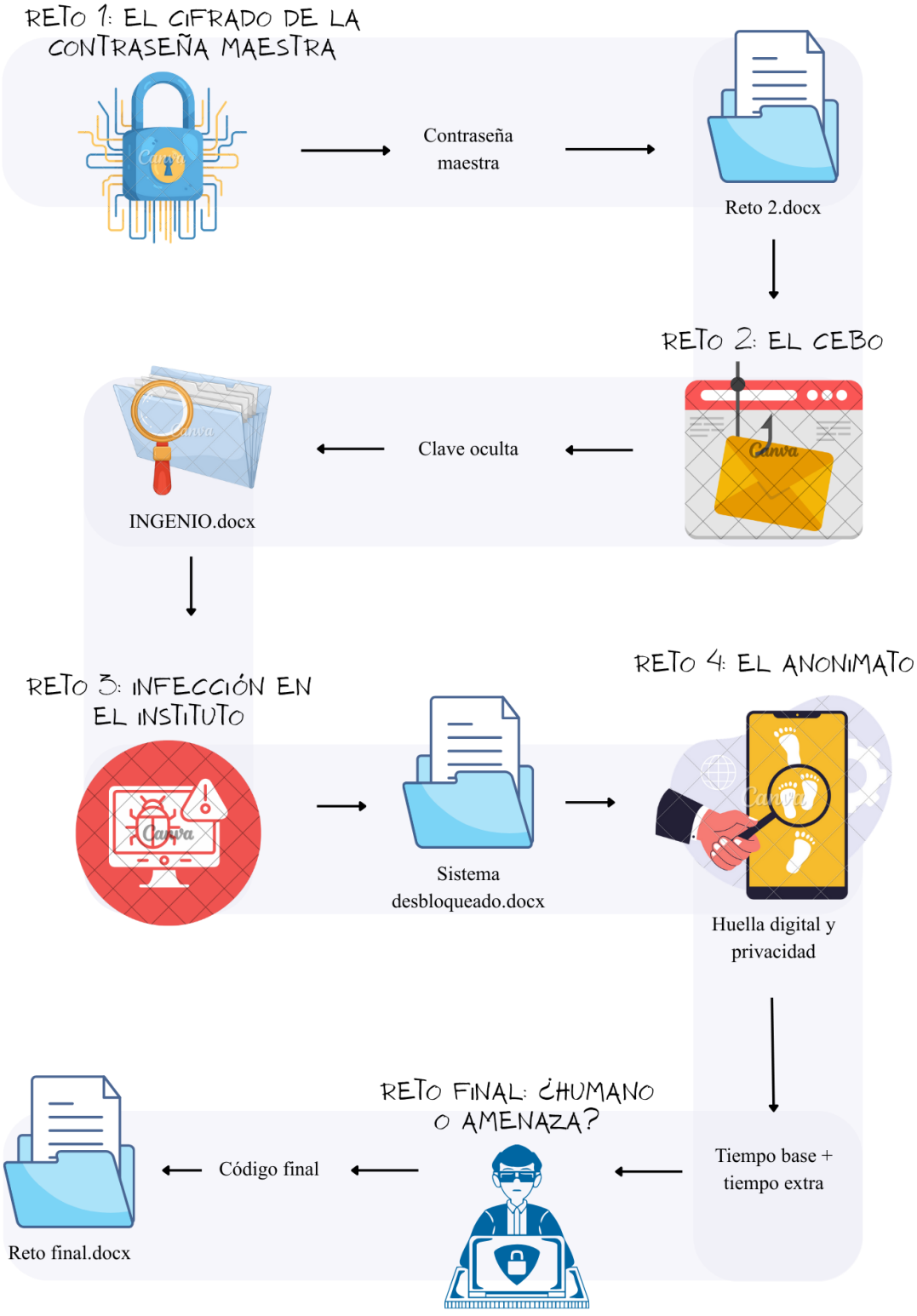
Anexo I. Escenas del video de la fase 1 para introducir a la narrativa


30
Descubre quién está detrás...


!!! WARNING: YOU HAVE BEEN HACKED !!!
Hacked by DarkHackerX
WE OWN YOU!
YOU HAVE BEEN PWNED!
YOUR SECURITY IS A JOKE!
YOUR SITE!
PAY 5 BTC TO RESTORE
*** WE ARE WATCHING YOU ***
GAME OVER!
****


¡QUE NO TE
PESQUEN!

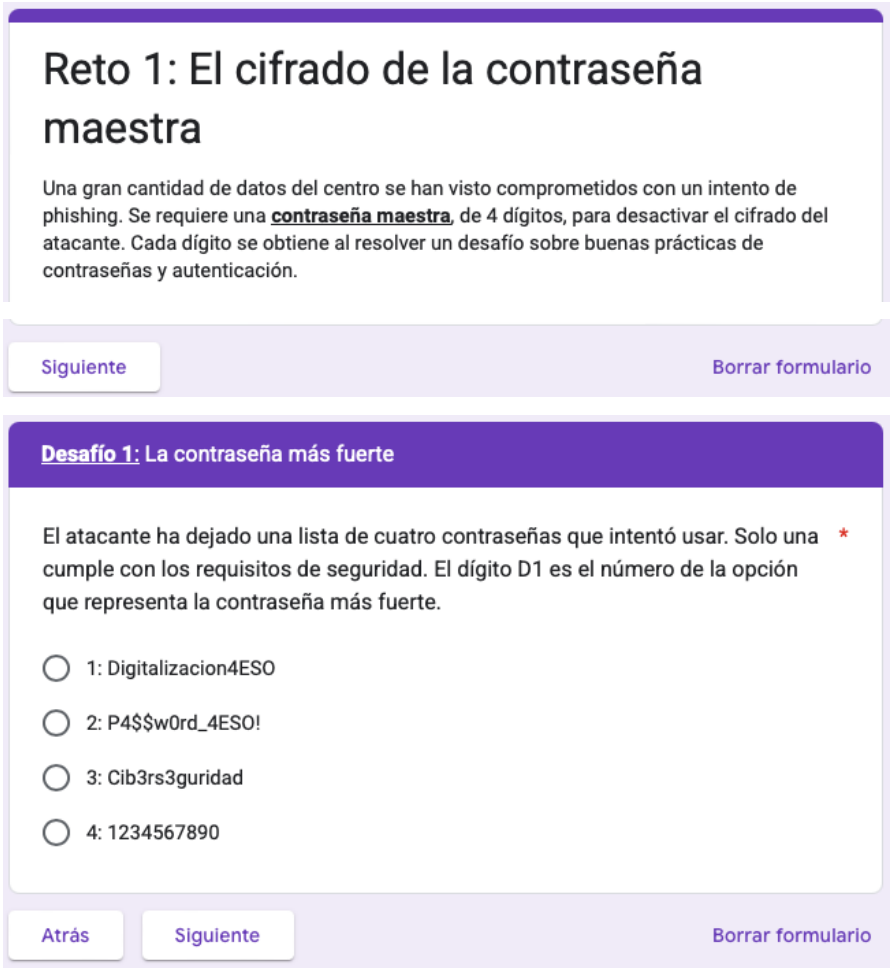
Anexo II. Esquema del escape room



Anexo III. Material para el reto 1

Formulario de Google del reto 1:

https://forms.gle/svwU5RfUGZu31KcP8



Reto 1: El cifrado de la contraseña maestra

Una gran cantidad de datos del centro se han visto comprometidos con un intento de phishing. Se requiere una **contraseña maestra**, de 4 dígitos, para desactivar el cifrado del atacante. Cada dígito se obtiene al resolver un desafío sobre buenas prácticas de contraseñas y autenticación.

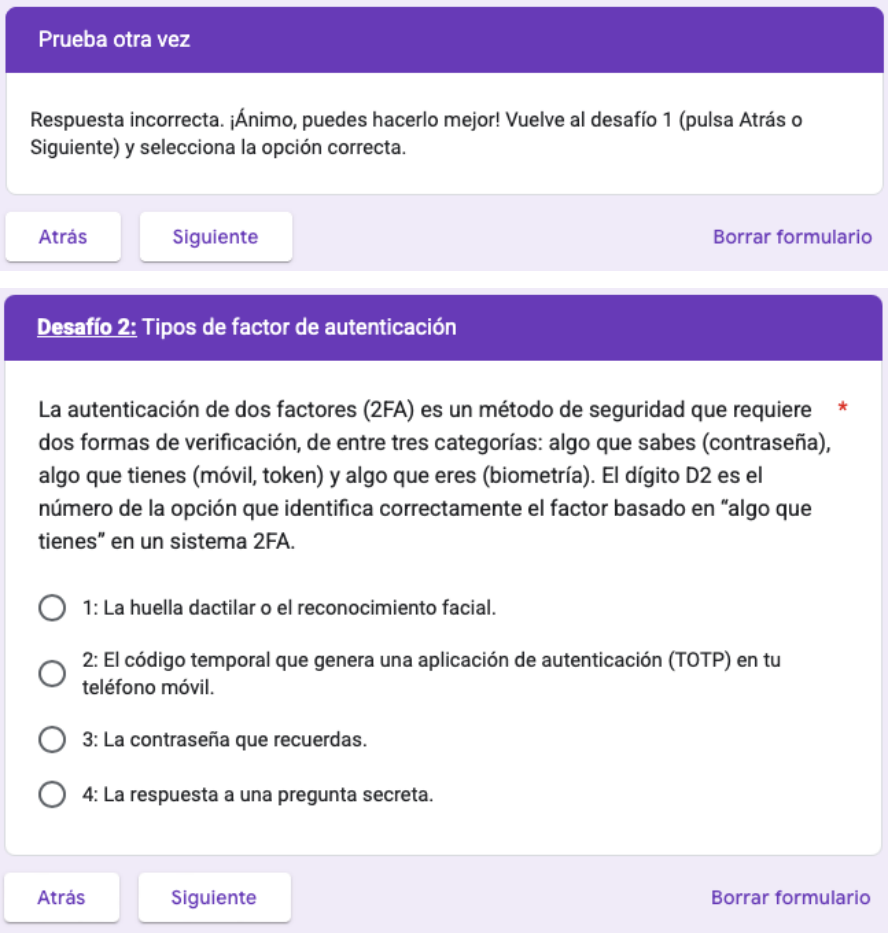
Siguiente Borrar formulario

Desafío 1: La contraseña más fuerte

El atacante ha dejado una lista de cuatro contraseñas que intentó usar. Solo una cumple con los requisitos de seguridad. El dígito D1 es el número de la opción que representa la contraseña más fuerte. *

- 1: Digitalizacion4ESO
- 2: P4$$w0rd_4ESO!
- 3: Cib3rs3guridad
- 4: 1234567890

Atrás Siguiente Borrar formulario



Prueba otra vez

Respuesta incorrecta. ¡Ánimo, puedes hacerlo mejor! Vuelve al desafío 1 (pulsa Atrás o Siguiente) y selecciona la opción correcta.

Atrás Siguiente Borrar formulario

Desafío 2: Tipos de factor de autenticación

La autenticación de dos factores (2FA) es un método de seguridad que requiere dos formas de verificación, de entre tres categorías: algo que sabes (contraseña), algo que tienes (móvil, token) y algo que eres (biometría). El dígito D2 es el número de la opción que identifica correctamente el factor basado en "algo que tienes" en un sistema 2FA. *

- 1: La huella dactilar o el reconocimiento facial.
- 2: El código temporal que genera una aplicación de autenticación (TOTP) en tu teléfono móvil.
- 3: La contraseña que recuerdas.
- 4: La respuesta a una pregunta secreta.

Atrás Siguiente Borrar formulario

Prueba otra vez

Respuesta incorrecta. ¡Ánimo, puedes hacerlo mejor! Vuelve al desafío 2 (pulsa Atrás o Siguiente) y selecciona la opción correcta.

Atrás Siguiente Borrar formulario

Desafío 3: Gestión y reutilización

Usar una misma contraseña en múltiples sitios supone un gran riesgo. El dígito D3 es el número de la opción que describe la principal amenaza de la reutilización de contraseñas, incluso si son muy complejas. *

- ◯ 1: La contraseña se detectará como insegura por el navegador.
- ◯ 2: Tarda más en ser descifrada por un ataque de fuerza bruta.
- ◯ 3: Si un sitio web sufre una brecha de seguridad, todas tus cuentas estarán en peligro.
- ◯ 4: Es más fácil de recordar, lo que la hace más débil.

Atrás Siguiente Borrar formulario

Prueba otra vez

Respuesta incorrecta. ¡Ánimo, puedes hacerlo mejor! Vuelve al desafío 3 (pulsa Atrás o Siguiente) y selecciona la opción correcta.

Desafío 4: Identificación de amenazas

Recibes un correo electrónico que parece ser del departamento de informática, pidiéndote que hagas clic en un enlace "urgente" para "confirmar" tu contraseña. La dirección del remitente es extraña (informatica@escuelagmail.com). El dígito D4 es el número de la opción que nombra correctamente esta técnica de robo de credenciales. *

- ◯ 1: Ataque de denegación de servicio (DoS)
- ◯ 2: Malware (virus informático)
- ◯ 3: Ataque de fuerza bruta (Brute Force)
- ◯ 4: Phishing

Atrás Siguiente Borrar formulario

Prueba otra vez

Respuesta incorrecta. ¡Ánimo, puedes hacerlo mejor! Vuelve al desafío 4 (pulsa Atrás o Siguiente) y selecciona la opción correcta.

Atrás Siguiente Borrar formulario

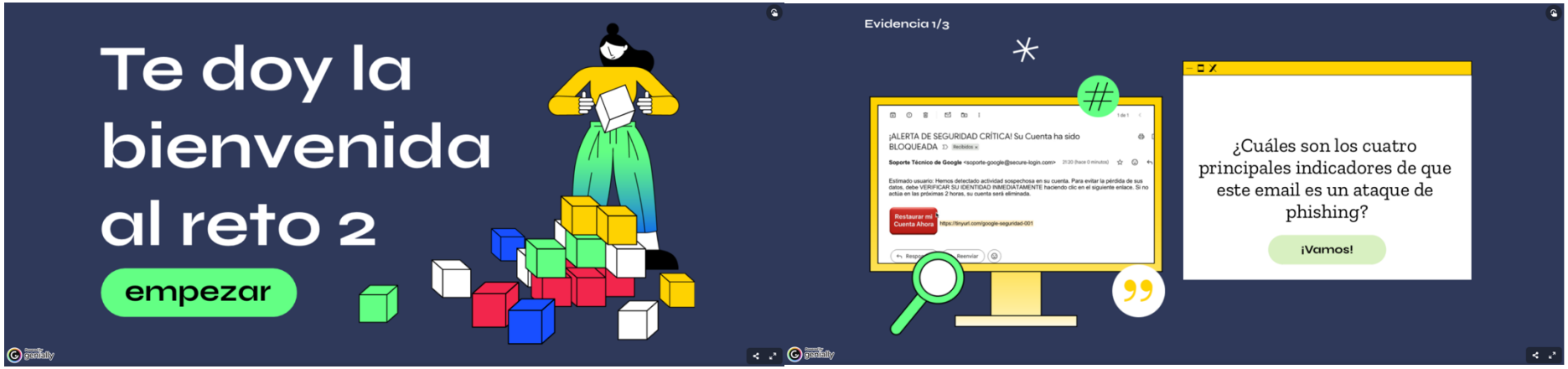
¡¡ENHORABUENA!!

Ahora ya puedes construir la contraseña maestra y abrir el documento Reto 2.docx.

Atrás Enviar Borrar formulario

Anexo IV. Material para el reto 2

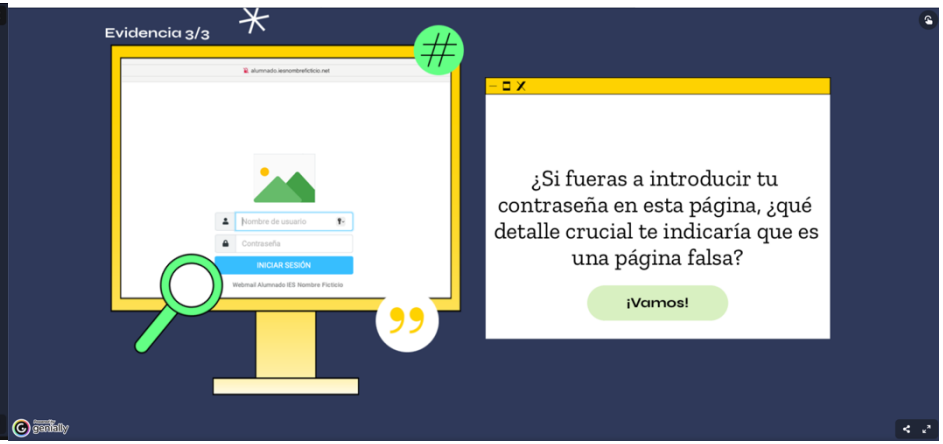
Presentación de Genially del reto 2: https://view.genially.com/69543b58c376eb6532e059ac/interactive-content-reto-2




Evidencia 2/3
+34 000 00 00 00
Hoy
Los mensajes y las llamadas están cifrados de extremo a extremo. Solo las personas en este chat pueden leerlos, escucharlos o compartirlos. Haz clic para obtener más información.
Hola mamá, se me ha roto el móvil y no puedo pagar el billete de autobús. Me puedes hacer un bizum de 15€ a este móvil?
10:27
¿Por qué no debes realizar ninguna acción sobre este mensaje?
¡Vamos!


WhatsApp pidiendo ayuda
Intentos:3
No tienes el número de teléfono en tus contactos.
Presión por hacer un pago inmediato.
Responder al mensaje confirma que tu número está activo, favoreciendo el intento de otros engaños.
El mensaje se recibe en la aplicación de WhatsApp.
Indicador de peligro
Nada que temer
Limpiar
Comprobar


WhatsApp pidiendo ayuda
Intentos:3
¡Excelente trabajo!
Has desbloqueado las lestras O y N.


Evidencia 3/3
Nombre de usuario
Contraseña
INICIAR SESIÓN
¿Si fueras a introducir tu contraseña en esta página, ¿qué detalle crucial te indicaría que es una página falsa?
¡Vamos!


Página de inicio de sesión
Intentos:3
Indicador de peligro
El icono del candado de seguridad no aparece o está roto.
El dominio de la URL no es el oficial del instituto (es .net en lugar de .edu).
Nada que temer
La URL es demasiado larga.
La página tarda mucho en cargar.
Limpiar
Comprobar
Página de inicio de sesión
Intentos:3
¡Excelente trabajo!
Has desbloqueado las lestras E y N.
Soy chispa que no se ve pero mueve la mano,
puedo fabricar ideas o azúcar en terreno cubano.
Nace en la mente, trabaja en la fábrica y en el corazón,
me nombran cuando hay astucia, invención y creación.
¿Qué palabra soy?
Palabra clave:
Escribe aquí tu respuesta.
Enviar
¡ENHORABUENA!
Ahora, en el directorio del ordenador, busca el archivo INGENIO.docx para acceder a las instrucciones del siguiente reto.
Palabra clave:
ingenio
Enviado

Anexo V. Material para el reto 3

RETO 3

¡Enhorabuena! Habéis llegado al tercer reto.

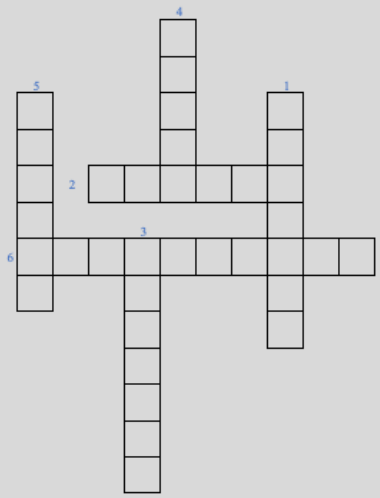
El sistema informático del instituto ha sido atacado. Los ordenadores se comportan de forma extraña, aparecen ventanas inesperadas y algunos archivos han desaparecido. El equipo de ciberseguridad (vosotros y vosotras) tiene **10 minutos** antes de que el sistema se bloquee por completo.

El objetivo de este reto consiste en resolver las tres pruebas que se encuentran en este documento para conseguir acceder y desbloquear el siguiente reto. Seguid las instrucciones que se os muestran para avanzar.

PRUEBA 1: SÍNTOMAS SOSPECHOSOS

Resolved el siguiente crucigrama con los tipos de malware a los que corresponden cada una de las siguientes características:

1. Se oculta dentro de un programa.
2. Se copia automáticamente por la red.
3. Roba información sin que lo notes.
4. Se replica e infecta otros archivos o sistemas sin consentimiento.
5. Muestra publicidad no deseada o engañosa de forma intrusiva.
6. Pide dinero para recuperar archivos.



Código de desbloqueo

12 - 24 - 32 - 42 - 52 - 65

Descubre una parte del código final de desbloqueo utilizando el crucigrama.

PRUEBA 2: ¿CÓMO NOS PROTEGEMOS?

¿Cuáles de las siguientes acciones se corresponden con acciones seguras?

- Descargar archivos piratas
- Usar antivirus actualizado
- Abrir enlaces desconocidos
- Actualizar el sistema
- Hacer copias de seguridad

Código de desbloqueo

La posición de cada acción segura se corresponde con un dígito del código final de desbloqueo.

PRUEBA 3: EL LABORATORIO

Id a la ubicación que se muestra a continuación y eliminad aquellos archivos que resulten sospechosos.

```
C:\Usuarios\instituto1\Documentos\Escape4\Prueba 3\
```

Código de desbloqueo

Acceded a cada uno de los archivos restantes y construid la ubicación del documento que os llevará al reto 4. Para abrirlo, deberéis introducir el código de desbloqueo que habéis obtenido en las dos pruebas anteriores.

Anexo VI. Material para el reto 4

Opciones de respuesta	Retroalimentación Respuesta correcta/Respuestas incorrectas
¿Cuál de las siguientes acciones contribuye directamente a tu huella digital pasiva?	
Aceptar las cookies por defecto en una página web sin leer la política	Al aceptar las cookies, permites que tu actividad de navegación sea rastreada por terceros, creando datos sobre ti sin tu interacción directa en la creación del contenido, lo cual es pasivo.
Subir tu currículum a un portal de empleo	Subir tu currículum es un acto consciente y voluntario. Tú decides qué información incluir (nombre, experiencia, contacto) y la entregas intencionalmente a la plataforma. Esta acción es un ejemplo de huella digital activa.
Firmar una petición en línea con tu nombre completo y correo electrónico	Esta acción es también parte de tu huella activa. Aunque la acción de "firmar" parezca mínima, estás introduciendo tus datos personales (nombre y correo) de forma deliberada para un propósito específico (la petición).
Publicar una foto de tus vacaciones en Instagram	Tu huella digital activa incluye todo el contenido que tú decides crear y compartir en redes, blogs o foros.
Estás configurando la privacidad de tu perfil en una red social. ¿Qué opción es la más segura para proteger tu intimidad y limitar tu huella?	
Configurar el perfil como 'Solo amigos' y desactivar la geolocalización de las publicaciones	Limitar la visibilidad solo a contactos conocidos y evitar la revelación de la ubicación son dos medidas clave para el control de la privacidad y la huella digital.
Dejar la configuración por defecto de la plataforma, ya que la red social ya te protege	Las configuraciones por defecto suelen ser las menos restrictivas, priorizando la difusión por encima de la privacidad del usuario.
Configurar el perfil como 'Público', pero evitar publicar información muy personal	La medida más segura es limitar la audiencia primero, y luego ser selectivo con lo que publicas.

Configurar el perfil como 'Público' y usar un nombre de usuario falso	El nombre falso ofrece una falsa sensación de seguridad. Aunque dificulta la identificación inicial, este enfoque falla en el elemento de seguridad más crítico: el alcance de la visibilidad.
Has descubierto que una foto embarazosa tuya de hace tres años sigue disponible en un foro antiguo. ¿Qué derecho, reconocido por el Reglamento General de Protección de Datos (RGPD), te permitiría solicitar su eliminación?	
Derecho de acceso	Se trata de la capacidad que tienes como ciudadano para solicitar y obtener información del responsable del tratamiento sobre si tus datos personales están siendo tratados y, en caso afirmativo, cuáles son esos datos, para qué se utilizan y cómo lo hacen.
Derecho de supresión (o 'derecho al olvido')	Este derecho te permite solicitar la supresión de datos personales cuando, entre otras cosas, ya no son necesarios o cuando el interesado retira el consentimiento.
Derecho de rectificación	El derecho de rectificación permite corregir datos inexactos, pero no eliminar una foto, que se considera un dato veraz.
Derecho de oposición	Se trata del derecho que tiene un individuo a oponerse a que sus datos personales sean objeto de un tratamiento específico, o a que se dejen de tratar si se cumplen ciertas condiciones.
Un inversor revisa tu perfil de red social para un posible empleo futuro y encuentra comentarios de hace 5 años con opiniones muy radicales. Esto es un ejemplo de riesgo de la huella digital en el ámbito de:	
Riesgo de phishing	El phishing implica engaños para obtener información personal o confidencial.
Riesgo de malware	El malware se refiere a programas maliciosos que dañan dispositivos o sistemas.
Riesgo en la reputación digital	La reputación online es la imagen o prestigio de una persona en internet, y los comentarios pasados pueden afectarla, limitando oportunidades futuras.
Riesgo de suplantación de identidad	La suplantación de identidad ocurre cuando alguien se hace pasar por ti, no cuando se revisa tu contenido real.

Estás realizando una investigación sensible y no quieres que tu proveedor de servicios de Internet (ISP) o los sitios web sepan tu ubicación geográfica. ¿Qué herramienta de privacidad avanzada deberías usar?	
Usar un gestor de contraseñas	Un gestor de contraseñas mejora la seguridad de las cuentas, pero no la privacidad de la navegación en términos de rastreo de ubicación.
Usar el modo de navegación 'Incógnito' o 'Privada'	El modo incógnito solo evita que el navegador guarde el historial, cookies y formularios en el dispositivo local.
Conectarte a través de una VPN	Una VPN cifra tu tráfico y lo redirige a través de un servidor remoto, ocultando tu dirección IP real y, por lo tanto, tu ubicación, tanto a tu ISP como a los sitios web visitados.
Instalar un software antivirus	La suplantación de identidad ocurre cuando alguien se hace pasar por ti, no cuando se revisa tu contenido real.
Si una aplicación gratuita te pide acceso a tu micrófono, cámara, contactos y ubicación, y su función principal es una linterna, ¿cuál debería ser tu acción prioritaria desde el punto de vista de la privacidad?	
Aceptar todos los permisos para que la aplicación funcione correctamente	Aceptar permisos innecesarios es una práctica de alto riesgo que expone tus datos a la aplicación sin justificación.
Denegar todos los permisos innecesarios y buscar una alternativa si no funciona sin ellos	El principio de 'mínimo privilegio' o necesidad es fundamental en ciberseguridad y privacidad; solo se deben otorgar los permisos imprescindibles para la funcionalidad básica.
Aceptar todos los permisos, pero instalar un antivirus que la supervise	Un antivirus no justifica ni neutraliza un uso excesivo e innecesario de datos personales.
Aceptar solo los permisos de la ubicación, ya que es el menos sensible	La ubicación es un dato personal sensible y no es necesaria para la función principal de la aplicación.
¿Qué tipo de dato personal es considerado sensible bajo la ley de protección de datos, y requiere una protección especial?	

Tu fecha de nacimiento	La fecha de nacimiento es un dato personal ordinario, útil para verificación, pero no es de las categorías de datos especialmente protegidas.
Tu dirección de correo electrónico	La dirección de correo electrónico se clasifica como dato de identificación o contacto.
Tu grupo sanguíneo y alergias	Los datos relativos a la salud (incluyendo grupo sanguíneo y alergias) son datos de categoría especial o sensibles, y su tratamiento requiere consentimiento explícito y medidas de seguridad reforzadas.
Tu número de teléfono	El número de teléfono se clasifica como dato de identificación o contacto.
Para evitar que los ciberdelincuentes puedan acceder a tus cuentas incluso si descubren tu contraseña, ¿qué medida de seguridad es la más efectiva para implementar inmediatamente?	
Cambiar la contraseña cada semana	Cambiar la contraseña con mucha frecuencia no evita que un atacante acceda a la cuenta si ya conoce la contraseña actual.
Activar la autenticación de dos factores (2FA)	La 2FA requiere una segunda prueba de identidad (como un código enviado al móvil), lo que hace que la contraseña robada sea inútil sin el dispositivo físico del usuario.
Usar el nombre de una mascota como parte de la contraseña	Los nombres de mascotas son datos personales que a menudo se comparten en redes sociales y pueden ser fácilmente adivinados mediante ingeniería social.
Usar la misma contraseña en todas las cuentas, pero muy larga	Aunque una contraseña larga es mejor que una corta, reutilizarla en varias cuentas tiene un alto riesgo. Si una plataforma sufre una filtración, todas las demás cuentas quedan comprometidas.
Al visitar un sitio web, este utiliza cookies de seguimiento que registran tus hábitos de compra para mostrarte anuncios personalizados. ¿A qué aspecto de la huella digital está directamente relacionado este proceso?	
A la huella digital pasiva, ya que el sitio web registra tus acciones automáticamente	El rastreo de la navegación, las preferencias y los hábitos por las cookies sin la intención directa del usuario de 'crear' ese dato, es el corazón de la huella digital pasiva.

A la divulgación de datos sensibles, porque tu historial de navegación es sensible	El historial de navegación no se clasifica automáticamente como un dato sensible según las leyes de protección de datos.
A la huella digital activa, porque estás comprando productos	La huella digital activa se refiere a la información que el usuario comparte de forma consciente y voluntaria, como publicar comentarios, subir fotos o completar formularios.
A la suplantación de identidad, ya que pueden robar tu historial de compras	La suplantación de identidad implica que un tercero se haga pasar por una persona para cometer fraudes u otros delitos.
Para reducir al máximo tu huella digital y proteger tu privacidad, ¿cuál de estas acciones tiene el mayor impacto en el largo plazo?	
Borrar el historial de navegación de tu móvil cada noche	Borrar el historial solo elimina los registros almacenados en tu dispositivo, pero no borra la información que ya fue recopilada por sitios web, buscadores, redes sociales o proveedores de servicios.
Usar un apodo o alias en lugar de tu nombre real en foros públicos	Aunque usar un alias puede ayudar a proteger la identidad en ciertos contextos, no reduce de forma significativa la huella digital global.
Desactivar la función de 'recordar contraseña' en el navegador	Desactivar esta función mejora la seguridad local del dispositivo, pero no influye directamente en la cantidad de información personal que se genera o queda registrada en internet.
Revisar y ajustar periódicamente la configuración de privacidad y seguridad de todas las plataformas que usas (redes sociales, apps, correo)	Esta es la acción más efectiva, ya que permite controlar activamente quién ve, usa y almacena tu información, impactando directamente en la huella digital activa y pasiva.

Anexo VII. Material para el reto 5

Presentación de Genially del reto 5:
https://view.genially.com/6957efea65924c7731afa263/interactive-content-reto-final

Anexo VIII. Rúbrica de evaluación

Criterio de evaluación	Excelente	Adecuado	En proceso	Insuficiente
Conocimientos de ciberseguridad	Aplica correctamente y de forma autónoma los conceptos de ciberseguridad en todos los retos, justificando sus decisiones con argumentos sólidos.	Aplica correctamente la mayoría de los conceptos de ciberseguridad, con escasos errores y justificaciones básicas.	Aplica algunos conceptos, pero presenta errores frecuentes o necesita ayuda para avanzar en los retos.	Muestra un conocimiento muy limitado o incorrecto de los conceptos de ciberseguridad, incluso con apoyo.
Resolución de problemas	Analiza las situaciones planteadas, propone estrategias eficaces y ajusta sus decisiones cuando detecta errores.	Resuelve los retos siguiendo estrategias adecuadas, aunque con escasa reflexión sobre el proceso.	Tiene dificultades para plantear estrategias y necesita orientación frecuente para resolver los problemas.	No logra identificar el problema ni proponer estrategias para resolverlo.
Pensamiento crítico	Evalúa la información de forma crítica, detecta riesgos digitales y toma decisiones responsables y fundamentadas.	Identifica riesgos digitales y toma decisiones generalmente adecuadas, aunque con argumentaciones poco elaboradas.	Reconoce algunos riesgos, pero le cuesta analizar la información y justificar sus decisiones.	No identifica riesgos ni analiza la información de manera crítica.

Trabajo en equipo	Participa activamente, escucha a los demás, aporta ideas y favorece la cooperación y el consenso en el grupo.	Colabora de forma adecuada y respeta las normas del grupo, aunque su participación es irregular.	Participa de forma limitada o muestra dificultades para coordinarse con el grupo.	No colabora con el grupo o dificulta el trabajo conjunto.
Comunicación	Expresa ideas de forma clara y respetuosa, argumenta sus respuestas y utiliza un lenguaje adecuado al contexto digital.	Comunica sus ideas de manera comprensible, aunque con poca precisión o escasa argumentación.	Tiene dificultades para expresar sus ideas con claridad o para justificar sus respuestas.	No logra comunicar sus ideas de forma adecuada.
Autonomía y autorregulación	Gestiona eficazmente el tiempo y las tareas, reflexiona sobre sus errores y mejora su desempeño de forma autónoma.	Muestra autonomía básica y acepta la retroalimentación para mejorar.	Necesita apoyo frecuente para organizarse y mejorar su trabajo.	No muestra autonomía ni utiliza la retroalimentación recibida.