



UNIVERSIDAD DE TALCA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA EN DESARROLLO DE
VIDEOJUEGOS Y REALIDAD VIRTUAL

CyberSafety: Videojuego 2D para la Autoconciencia de Ciberseguridad

MATIAS ALVARADO GRANDON

Profesor Guía: FELIPE BESOIAN PINO

Profesor Co-guía: CLAUDIO ALFREDO RUBIO NARANJO

Memoria para optar al título de
Ingeniero en Desarrollo de Videojuegos y Realidad Virtual

Talca – Chile
Julio, 2026



UNIVERSIDAD DE TALCA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA EN DESARROLLO DE
VIDEOJUEGOS Y REALIDAD VIRTUAL

CyberSafety: Videojuego 2D para la
Autoconciencia de Ciberseguridad

MATIAS ALVARADO GRANDON

Profesor Guía: FELIPE BESOIAN PINO

Profesor Co-guía: CLAUDIO ALFREDO RUBIO NARANJO

Miembro Comisión Examinadora: NICOLAS BARRIGA

Memoria para optar al título de
Ingeniero en Desarrollo de Videojuegos y Realidad Virtual

El presente documento fue calificado con nota: _____

Talca – Chile

Julio, 2026

TABLA DE CONTENIDOS

	página
Tabla de Contenidos	I
Índice de Figuras	IV
Índice de Tablas	V
Resumen	VI
1. Introducción	1
2. Marco Teórico	4
2.1. Fundamentos de la Ciberseguridad	4
2.1.1. Panorama actual en Chile y Latinoamérica	4
2.1.2. Usuarios vulnerables	7
2.2. Educación y Alfabetización Digital	7
2.2.1. Brecha entre acceso a internet y conocimientos en seguridad digital	8
2.2.2. Estrategias tradicionales de capacitación	8
2.2.3. Limitaciones detectadas	9
2.3. Videojuegos Educativos y Definiciones	10
2.3.1. Serious Games	10
2.3.2. Gamificación	10
2.3.3. Ventajas Pedagógicas	10
3. Metodología	12
3.1. Concientización del Problema	13
3.2. Propuesta de Solución	14
3.3. Desarrollo del Artefacto	15
3.4. Evaluación	18
3.5. Conclusión	20
3.6. Carta Gantt	21

4. Diseño	23
4.1. Mecánicas	23
4.1.1. Correos electrónicos	23
4.1.2. Estructura de Niveles	24
4.1.3. Sistema de Correos y Puntaje	24
4.1.4. Sistema de Objetivos	24
4.1.5. Sistema del Manual	25
4.1.6. Temporizadores (Versión alternativa)	25
4.2. Dinámicas	25
4.3. Estética	26
4.3.1. Simulador de Computadora	26
4.3.2. Aspecto Visual	26
4.3.3. Aspecto Sonoro	27
4.3.4. Sensación de Inmersión	27
4.3.5. Tensión y Responsabilidad	27
4.3.6. Satisfacción y Aprendizaje	27
5. Implementación	28
5.1. Prototipo	28
5.1.1. Interfaz Principal	29
5.1.2. Interfaz de Configuraciones	29
5.1.3. Interfaz de Niveles	29
5.1.4. Interfaz de Escritorio	30
5.1.5. Interfaz de Tareas	31
5.1.6. Interfaz de Correos	31
5.1.7. Interfaz de Resultados	31
5.1.8. Versión Alternativa: Modo Temporizador	32
5.2. Preparación y Encuestas para Pruebas con Usuarios	32
5.2.1. Encuesta Propia	32
5.2.2. Procedimiento de Pruebas	33
5.2.3. Resultados	33
6. Conclusión	39
Glosario	41

Bibliografía	43
: Apéndice	48
7.1. Detalles de usuarios vulnerables	48
7.2. Juegos de Ciberseguridad	49
7.2.1. Riskio	49
7.2.2. Control-Alt-Hack	50
7.2.3. Hacked Time	51
7.2.4. Tabla Comparativa de Juegos de Ciberseguridad	51
7.3. Tablas de Diseño	52
7.3.1. Tablas de Correos electrónicos	52
7.3.2. Tablas de Estructura de Niveles	54
7.3.3. Tablas de Sistema de Correos y Puntaje	56
7.3.4. Tablas de Sistema de Objetivos	57
7.3.5. Tablas de Sistema del Manual	58
7.3.6. Tablas de Temporizadores	59
7.3.7. Tablas de Dinámicas	60
7.4. Diagramas de Diseño	62
7.4.1. Diagrama de Interfaz Principal	62
7.4.2. Diagrama de Interfaz de Configuraciones	63
7.4.3. Diagrama de Interfaz de Niveles	64
7.4.4. Diagrama de Interfaz de Tareas	65
7.4.5. Diagrama de Interfaz de Correos	66
7.4.6. Diagrama de Interfaz de Resultados	68
7.4.7. Diagrama de Versión Alternativa: Modo Temporizador	69
7.5. Preguntas de Encuesta Propia	69
7.6. Gráficos de sesión de resultados	70
7.7. Video Gameplay	71
7.8. Resultados de encuestas	71
7.9. Resultados de sesiones	71

ÍNDICE DE FIGURAS

	página
3.1. Ciclo general del diseño en Design Science Research	13
3.2. Ciclo de Iteración de la Metodología Ágil	15
5.1. Diagrama de Interfaz de Escritorio	30
5.2. Gráfico de comparación de campos UEQ con t-test	34
5.3. Gráfico de comparación de promedios SUS	35
5.4. Gráfico de comparación de promedios SUS por ítem	36
5.5. Gráfico de comparación de respuestas de Cuestionario Propio	37
7.1. Diagrama de Interfaz Principal	62
7.2. Diagrama de Interfaz de Configuraciones	63
7.3. Diagrama de Interfaz de Niveles	64
7.4. Diagrama de Interfaz de Tareas	65
7.5. Diagrama del Contenido del Correo	66
7.6. Diagrama de Responder Email	67
7.7. Diagrama del Panel de Reportes	67
7.8. Diagrama de Interfaz de Resultados	68
7.9. Diagrama de Modo Temporizador	69
7.10. Gráfico de promedios de acciones y puntaje de pruebas sin temporizador	70
7.11. Gráfico de promedios de acciones y puntaje de pruebas con temporizador	71

ÍNDICE DE TABLAS

	página
3.1. Carta Gantt del proyecto CyberSafety	21
7.1. Comparativa de Videojuegos enfocados en la enseñanza de Ciberse- guridad	51
7.2. Atributos de los correos electrónicos	52
7.3. Tipos de correos electrónicos	53
7.4. Estructura y atributos de los niveles del videojuego	54
7.5. Datos de los Niveles	55
7.6. Acciones en el sistema de correos	56
7.7. Reglas del sistema de puntaje	57
7.8. Tipos de Objetivos	57
7.9. Condiciones de Finalización del Nivel	58
7.10. Criterios para la identificación de Correos Maliciosos	58
7.11. Rasgos del Modo Temporizador	59
7.12. Dinámicas de interacción del jugador con la interfaz del sistema . . .	60
7.13. Dinámicas de comportamiento del jugador	61

RESUMEN

La ciberseguridad se ha convertido en un aspecto esencial de la vida cotidiana debido al uso constante de dispositivos digitales e internet. Millones de personas acceden diariamente a la red sin considerar que su seguridad digital puede verse comprometida por métodos maliciosos que, aunque simples a primera vista, resultan efectivos ante la falta de experiencia o de atención. Esto puede resultar en la pérdida de información personal, financiera o confidencial. Entre las amenazas más frecuentes destaca el *phishing*, una técnica de ciberamenaza por correo ampliamente conocida pero aún subestimada por muchos usuarios, especialmente jóvenes y adultos mayores, quienes presentan mayor vulnerabilidad al interactuar con entornos digitales.

Con el objetivo de fortalecer la concientización preventiva en ciberseguridad, se propone el desarrollo de un videojuego tipo *Serious Game*, nombrado *CyberSafety*, orientado a la identificación y comprensión de intentos de *phishing* en un entorno simulado de computador. A través de las acciones interactivas y actividades prácticas, se busca que los usuarios adquieran experiencia y confianza para reconocer y evitar este tipo de amenazas fuera del entorno del juego, contribuyendo así a una mayor concientización y resiliencia digital, además de identificar la efectividad del producto digital. A través de una evaluación con diferentes instrumentos de encuesta como el Sistema de Usabilidad (SUS) y el Cuestionario de Experiencia de Usuario (UEQ), se busca probar dos versiones del videojuego (con temporizador, sin temporizador), para determinar qué versión es más efectiva para la experiencia del jugador y su efectividad temática.

Los resultados obtenidos con usuarios de prueba lograron demostrar que la versión sin temporizador es mucho más favorecida por los jugadores, ya que provee la libertad y similitud de lo que podría ser una experiencia real. Reconocen las posibles ventajas del videojuego como un elemento de enseñanza a usuarios con poca experiencia en *phishing*, y logra ser lo suficientemente claro para su uso sin necesidad de información técnica. El modo temporizador genera una presión externa y limitante que solo fuerza a los jugadores a tomar decisiones más aceleradas con menor desempeño general, con el mayor dato diferenciable entre las versiones siendo la confianza y estimulación, siendo la más baja y más alta en la versión con temporizador, respectivamente.

1. Introducción

En las últimas décadas, la creciente dependencia de tecnologías digitales en la vida cotidiana y el trabajo ha incrementado la exposición de estos usuarios a ciberamenazas como el *phishing* (correos electrónicos falsos), *spoofing* (correos disfrazándose de correos legítimos) y *malware* (virus de computadora, consultar *Glosario*). Estas estrategias maliciosas buscan como objetivo final obtener acceso a información sensible de los usuarios o comprometer sus dispositivos, y su ubicuidad ha hecho que estos dispositivos digitales sean mucho más comunes y naturales en nuestros ambientes diarios, por lo que no terminamos de cuestionar su propósito. Aún así, persiste una brecha digital entre el uso tecnológico y el conocimiento necesario para una navegación segura para evitar ciberataques y mejorar su ciberseguridad. Esto afecta especialmente a grupos con menor alfabetización digital, como adultos mayores y jóvenes [1].

Los usuarios comunes tienden a sobreestimar su capacidad para detectar ataques cibernéticos, lo que los hace vulnerables incluso después de recibir advertencias o capacitaciones convencionales, ya sea por falta de experiencia o falta de práctica constante, y aunque pueden sospechar de intentos de ciberamenazas, aún pueden llegar a cometer errores [2]. Los métodos tradicionales solo llegan a ser concientizadores y no logran otorgar mayor experiencia en presencia de estos ataques, por lo que deja en evidencia la necesidad de métodos educativos más interactivos para entrenar a los usuarios, uno capaz de simular escenarios reales y fomentar el aprendizaje experiencial.

Este problema general se basa en la inexperiencia en ciberseguridad de los usuarios que usan dispositivos digitales de manera regular, expuestos a ataques por métodos cotidianos como *phishing*, páginas web y descargar contenido no seguro, como

contenido malicioso o malware; que tratan de obtener su información personal o bancaria. Un usuario puede también tener experiencia en el uso tecnológico de varios dispositivos, pero no poseer concientización sobre su propia ciberseguridad o reconocer amenazas. Por la inocuidad de estos productos digitales en la vida cotidiana, uno siempre se encuentra expuesto a estas amenazas de manera constante.

Analizando este problema, se ha visto una metodología que puede cubrir este ámbito para obtener experiencia sobre la ciberseguridad sin estar expuesto a sus riesgos y consecuencias. 'Serious Games' son videojuegos cuyo propósito principal es enseñar, entrenar o tener otro propósito aparte de entretener, y forman parte de los videojuegos educativos. Aunque hay ciertas limitaciones de estos métodos, como solo dirigidos a cierto público de usuarios, como trabajadores tecnológicos u organizaciones, en vez de ser más generales. Los ataques de ciberseguridad no son solo para las organizaciones, sino para todos los usuarios. Aunque estos casos son bastante cotidianos, la gente desconoce cómo estos actos maliciosos ocurren en el sentido de cómo son ocasionados o cómo la víctima accidentalmente da sus datos al atacante. Esta experiencia se puede otorgar por un videojuego [3].

La primera parte de la solución para abordar este problema de enseñanza de ciberseguridad es hacerlo accesible a una mayor parte del público y usar un elemento común y no técnico que es parte cotidiana de actos fraudulentos. Como respuesta a esta problemática, se propone el desarrollo de un videojuego educativo 2D, denominado **CyberSafety**, cuyo objetivo es entrenar a los usuarios en la identificación y correcta reacción frente a amenazas cibernéticas. El juego simulará un entorno de computadora, en un escritorio digital, donde el jugador deberá reconocer y clasificar correos electrónicos como fraudulentos o legítimos, aplicando criterios de análisis prácticos. Esto forma parte de la identificación principal ante correos convincentes que son similares a correos maliciosos reales, pero dando guías para identificar activamente cuáles son fraudulentos para reportarlos.

Se espera que esta propuesta contribuya al fortalecimiento del reconocimiento de peligros digitales y la ciberseguridad personal, ya que a través de un programa que simule y enseñe estas experiencias, los usuarios pueden enfrentarse ante estos actos fraudulentos, que a pesar de ser bastante comunes, aún no hay gran concientización de ello.

Parte del impacto potencial proyecta que los usuarios que interactúen con el videojuego aumenten significativamente su capacidad de detectar intentos de fraude

digital en comparación con métodos tradicionales de aprendizaje. También se espera llevar a cabo el diseño de esta herramienta pedagógica innovadora para ser aplicada en contextos educativos, laborales y familiares.

Esta propuesta se trabajará como una **Memoria Tecnológica** durante su desarrollo y mediante la creación de un prototipo funcional para la prueba con usuarios.

Pregunta de Investigación: ¿Cómo puede un *serious game* diseñado para promover prácticas seguras de ciberseguridad impactar en la percepción de las personas hacia la ciberseguridad?

Objetivo general: Desarrollar y evaluar un videojuego serio 2D enfocado en las amenazas comunes de ciberseguridad, como phishing, mediante un entorno simulado de escritorio de computadora, orientado a la concientización y entrenamiento de usuarios inexpertos o con poca experiencia en prácticas de ciberseguridad.

Objetivo específico 1: Diseñar un entorno de escritorio de computadora simulado que represente situaciones relacionadas con *phishing*, *spoofing* y malware.

Objetivo específico 2: Implementar mecánicas de juego y niveles progresivos de dificultad orientados a la interacción y familiarización del usuario con situaciones comunes de ciberseguridad.

Objetivo específico 3: Evaluar el videojuego mediante pruebas con usuarios, considerando aspectos relacionados con la usabilidad, experiencia de usuario e interacción con el producto.

Objetivo específico 4: Analizar los resultados obtenidos de las pruebas de usuario para determinar la percepción, usabilidad y experiencia general del videojuego, identificando fortalezas y aspectos susceptibles de mejora del producto.

2. Marco Teórico

2.1. Fundamentos de la Ciberseguridad

Uno de los principales objetivos de una amenaza digital es implantar un *malware* o virus informático en los dispositivos de las víctimas, con el propósito de obtener acceso a información crítica o comprometer el sistema. El ciberdelincuente busca adquirir control o privilegios sobre el equipo a través de dicho software malicioso, el cual suele distribuirse mediante ataques cibernéticos dirigidos, como correos electrónicos fraudulentos de tipo *phishing*. Incluso si el usuario final no es el objetivo directo, puede verse afectado por la infiltración de malware en empresas o servicios a los que pertenece, lo que permite accesos no autorizados o el uso de información interna para enviar campañas de phishing más convincentes hacia los clientes, como puede ocurrir con entidades bancarias comprometidas [4].

2.1.1. Panorama actual en Chile y Latinoamérica

En los últimos años, se ha visto un creciente riesgo de exposición a amenazas digitales relacionadas con la extracción y recopilación de información personal de los usuarios que usan internet. Desde junio de 2022 a julio de 2023, en Latinoamérica, hubo un incremento de 617% en intentos de ataques de phishing y troyanos bancarios en comparación con los 12 meses anteriores, y en Chile, se registraron 10,5 millones de ataques de phishing. [5].

Esta alza de ataques tiene que ver, por una parte, con el hecho de que los computadores y dispositivos móviles se han vuelto una parte natural de nuestras vidas. Es difícil pensar en alguien que no posea al menos un teléfono celular o smartphone, incluso en los adultos mayores, aunque no posean el conocimiento para usarlos a su

completo potencial. Esta ubicuidad computacional se ha vuelto casi invisible en la vida cotidiana y en su conocimiento general, con su transición pensada desde 1991, como reemplazos naturales de pizarras por el uso de pantallas o proyectores, o, en este caso, el reemplazo de correos físicos por correos electrónicos [6].

Ya que la gente tiene gran acceso a estos dispositivos, uno de sus principales usos es acceder a internet. Pero con su utilidad y la interacción online, uno de los conocimientos que aún no se ha vuelto cotidiano o natural es la ciberseguridad personal con estos elementos electrónicos. Esto se hace mucho más relevante cuando se considera que las personas usan internet de manera diaria gracias al mayor acceso a smartphones y computadores. Durante el 2023 en Chile, desde el 26 de agosto hasta el 14 de noviembre, de un grupo de 50 mil encuestados, 92.5 % indican que usan internet todos los días [7]. Esto significa una constante exposición a posibles amenazas que hagan objetivo a estos usuarios, y solo se necesita equivocarse una vez para sufrir las consecuencias de perder información personal.

En Chile, ha habido intentos de progreso en adaptar nuevas políticas para reforzar la ciberseguridad tanto del Estado como de los usuarios comunes y la población en general.

- En **2017**, el Gobierno de Chile publicó la Política Nacional de Ciberseguridad, que tiene como objetivo “desarrollar una estrategia de seguridad digital que proteja a los usuarios privados y públicos”, apuntando a lograr un ciberespacio libre, abierto, seguro y resiliente para el año 2022 [8].
- En **2018**, el presidente de la República dictó el Instructivo Presidencial 8, del 23 de octubre de 2018, a través del cual se impartieron instrucciones urgentes en materia de ciberseguridad para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado [9].

A pesar de estas políticas que se han tratado de aplicar, no ha habido grandes cambios recientes en organizaciones, compañías o grupos para dar enfoque a la ciberseguridad como un punto vital que se deba manejar o aplicar para el correcto funcionamiento de la navegación por internet. En sí, estas normativas son aplicadas por unas pocas instituciones: entidades fiscalizadoras en mercados regulados, como la Subsecretaría de Telecomunicaciones, la Comisión para el Mercado Financiero y la Superintendencia de Pensiones, entre otras. Estas entidades han dictado sus propias normas, relacionadas con aspectos técnicos y organizativos para abordar los

riesgos en el ciberespacio y sus efectos en los datos personales de los usuarios, que esencialmente es la concientización por la ciberseguridad dentro de la compañía. En el ambiente público, la regulación es escasa pero hay esfuerzos para que se mejore mediante la tramitación del proyecto de ley sobre delitos informáticos.

Ciertas organizaciones gubernamentales, tales como el **Registro Civil de Identificación, el Fondo Nacional de Salud, hospitales, la red de atención primaria, ministerios**, entre otros, manejan una gran cantidad de datos personales y biométricos que son vitales para sus usuarios y que con frecuencia son objetivo de varios ciberataques para extraer información sensible para su uso en otros crímenes [10].

Una de las posibles razones por las que la ciberseguridad no es considerada un punto a abordar por las compañías o grupos con acceso a internet es por la falta de percepción del grado de las amenazas o de cómo estas pueden afectar a los usuarios. Tan solo el hecho de que solo unas compañías han aplicado estas normas por su propia cuenta indica que la ciberseguridad es solo relevante a grupos que ya han migrado a espacios tecnológicos más avanzados que requieren el resguardo de su información digital, a comparación de otras entidades, pero que aún así el daño por permitir una ciberamenaza a un sistema, independiente del tamaño de la entidad afectada, sigue siendo un punto vulnerable de seguridad y funcionamiento.

Estos se vuelven mucho más relevantes cuando las propuestas de proyectos para fomentar la organización de directivas de ciberseguridad por parte del Estado de Chile se consideran secundarias hasta que ocurre un incidente que fuerza su atención a leyes relacionadas con este ámbito, que muestra la importancia de los datos personales que pueden ser vulnerados por un ciberataque hacia los organismos públicos. Esto hace que varias organizaciones solo se muestren reactivas en vez de proactivas ante amenazas de este tipo.

Durante el 2020, en la semana del 5 al 11 de octubre, los sistemas informáticos de la **Clave Única de la División de Desarrollo Digital de Chile** fueron vulnerados por un ciberataque que robó esta información desde la misma organización gubernamental, con 17 millones de usuarios chilenos afectados. Por este caso, aumentó la preocupación por poner urgencia a los proyectos de ley sobre delitos informáticos, sobre protección de datos personales por parte de la nueva Agencia de Protección de Datos Personales e ingresar la nueva ley del Sistema Nacional de Ciberseguridad. Estos proyectos buscan actualizar la legislación de Chile para en-

frentar los desafíos del cibercrimen y mejorar la protección de datos personales. El único plan de recuperación ante esto fue la sugerencia de cambiar la Clave Única tan pronto y constantemente como fuera posible por parte de los usuarios [11].

2.1.2. Usuarios vulnerables

Aquí definiremos a los **usuarios vulnerables** como aquellos que están más expuestos a amenazas digitales y suelen ser objetivos frecuentes de los ciberataques, divididos tanto por su posición como por su edad.

Los grupos que son más vulnerables son los usuarios comunes de la sociedad sin gran especialización o enfoque en el uso de computadoras o aparatos tecnológicos. Esta falta de interacción constante con lo tecnológico da la sensación de que no necesitan aprender acerca de la ciberseguridad, ya sea para el uso doméstico o en el área de trabajo con aparatos digitales. Este cubre todo el rango de edad de los sujetos, pero quita a aquellos que trabajan en TI, computación u otro ámbito similar. Aunque también existen divisiones por género, solo se considerarán los grupos por su rango de edad y posición de trabajo, excluyendo rasgos de investigación psicológica [12].

Aparte, los **niños y estudiantes** son grupos vulnerables, pero no los consideramos parte de esta agrupación general, ya que existe menos acceso al uso de internet y más uso en su recreación u ocio que para la comunicación o búsqueda de archivos, que además es supervisada por los apoderados del joven.

En este caso, podemos definir los siguientes tipos de usuarios vulnerables: **jóvenes** que recién están entrando en el mundo tecnológico, los **adultos mayores** que están adaptándose al uso de aparatos electrónicos, y los **usuarios empleados** cuya posición de trabajo los hace más expuestos a ciberataques por formar parte de una organización crítica, como una gubernamental o tecnológica. En el *Anexo 7.1* se explora en más detalle su comportamiento.

2.2. Educación y Alfabetización Digital

Para que exista una respuesta apropiada por parte de los usuarios, estos deben estar educados en el ámbito digital para poder saber cómo utilizar la tecnología y cómo evitar riesgos dentro de ella. Sin importar qué tan seguro sea un programa, todo aparato digital requiere conocimiento del usuario para su uso apropiado.

2.2.1. Brecha entre acceso a internet y conocimientos en seguridad digital

La **brecha digital** se entiende como la diferencia en la competencia de los individuos o grupos para utilizar tecnologías digitales de manera efectiva. Una mayor brecha indica que poseen menos capacidad efectiva para su uso y una menor indica mejor efectividad en su uso. Esto explica las situaciones donde el mero hecho de tener conexión a internet no implica necesariamente que una persona pueda usarlo de forma crítica, segura, o productiva [1].

Dentro de este marco, se destaca la existencia de una brecha de competencias digitales, que abarca especialmente los conocimientos sobre seguridad informática y protección de la información personal. Aunque los programas de inclusión digital han ampliado el acceso, muchas personas siguen siendo vulnerables frente a amenazas por falta de conocimiento tecnológico para actuar contra estos peligros, como el phishing, el spoofing, o el malware.

Debido a esta carencia, producto de la falta de formación en seguridad digital, los usuarios no saben cómo reaccionar frente a estos errores, impidiendo el desarrollo de hábitos seguros y la capacidad de reconocer riesgos. Esto requiere mejores políticas y estrategias educativas para detectar amenazas digitales que combinen conectividad con alfabetización digital integral, que enfaticen la formación práctica y que sean contextualizadas con la ciberseguridad como un componente esencial para poder acortar la brecha entre el 'uso' y la 'protección' dentro del entorno digital.

2.2.2. Estrategias tradicionales de capacitación

Para reducir las brechas digitales, se han desarrollado diversos programas de formación tecnológica orientados a la capacitación en ciberseguridad y, particularmente, en la prevención del phishing. Estos **entrenamientos tradicionales** suelen combinar cursos presenciales o en línea, materiales estáticos como folletos o videos, y simulaciones de phishing para reforzar el reconocimiento de amenazas y los protocolos de seguridad. Generalmente, el proceso consiste en una sesión teórica seguida de ejercicios prácticos de detección de correos fraudulentos [13].

Estos métodos comparten características comunes: se organizan como capacitaciones puntuales, utilizan materiales genéricos y simulaciones poco adaptadas al perfil de cada usuario. La revisión literaria señala que, aunque estas estrategias ge-

neran efectos positivos a corto plazo, la retención del conocimiento y el cambio de comportamiento requieren entrenamiento continuo y seguimiento. Asimismo, el entrenamiento integrado proporciona retroalimentación durante la práctica cuando el usuario comete un error; sin embargo, continúa dependiendo de escenarios predefinidos y poco variables, limitando la personalización y la exposición a situaciones más específicas.

2.2.3. Limitaciones detectadas

A pesar del uso de estos formatos, las estrategias tradicionales de capacitación en ciberseguridad presentan limitaciones en su efectividad a largo plazo. Los usuarios tienden a olvidar los contenidos pocas semanas después de la formación, especialmente cuando esta se basa en material teórico o exposiciones sin práctica. La **falta de interactividad y de contextos realistas** dificulta la aplicación del conocimiento, generando una brecha entre saber y actuar.

Adicionalmente, los entrenamientos basados únicamente en charlas o material audiovisual **no favorecen una comprensión profunda de las tácticas de los atacantes ni el reconocimiento de amenazas reales**. La repetición de ejemplos similares también reduce la motivación y aumenta la fatiga cognitiva.

Otra limitación es la **escasa personalización y retroalimentación inmediata**. Las simulaciones de phishing suelen utilizar casos generales que no consideran las diferencias de experiencia o contexto de los usuarios, reduciendo su impacto educativo. Además, la falta de escenarios variados y de explicaciones inmediatas frente a los errores limita el aprendizaje y el cambio de comportamiento.

En este contexto, los *Serious Games* surgen como una alternativa al combinar aprendizaje activo, retroalimentación inmediata y motivación en un entorno interactivo. Mediante escenarios simulados y controlados, este permite que los usuarios aprendan haciendo, favoreciendo la retención del conocimiento y la adopción de conductas más seguras frente a amenazas de ciberseguridad.

2.3. Videojuegos Educativos y Definiciones

2.3.1. Serious Games

Los ‘**Serious Games**’ o ‘Juegos Serios’ son juegos diseñados con un **propósito principal distinto al entretenimiento**, como la educación, la salud o la formación profesional. Aunque conservan elementos característicos de los juegos, como narrativa, mecánicas, objetivos y retroalimentación, estos videojuegos se enfocan en promover el aprendizaje, el entrenamiento o la concientización en un área específica. De esta forma, combinan una experiencia lúdica e inmersiva otorgada por los videojuegos con fines pedagógicos, constituyéndose en herramientas eficaces para abordar problemáticas complejas como la ciberseguridad, lo cual requiere mayor especialización o experiencia real para combatirlas [3].

El *Anexo 7.2* presenta una serie de videojuegos adicionales que también han demostrado resultados positivos en la concientización de la ciberseguridad.

2.3.2. Gamificación

La ‘**Gamificación**’ es un tipo de técnica que consiste en la incorporación de elementos y dinámicas propias del diseño de videojuegos en contextos y situaciones no lúdicas, como actividades de trabajo, para volverlas más atractivas e interesantes a los usuarios [3]. Usualmente, el método más común usado es asignar puntajes a actividades hechas por su rendimiento, al igual que otorgar medallas o tablas de puntuación. Estos se pueden aplicar a procesos como la productividad laboral, el aprendizaje y ciertas campañas, con el fin de aumentar la motivación y el compromiso de los participantes. La gamificación no requiere la creación de un juego completo, ya que solo toma la implementación de elementos y mecánicas de juego, y las aplica a otro ambiente, situación o actividad.

2.3.3. Ventajas Pedagógicas

Los Serious Games han sido usados en áreas pedagógicas para mejoras en entrenamiento de diferentes habilidades y tratamientos de ciertos comportamientos psicológicos, como el TDAH (ADHD), con resultados positivos en reducción de errores y post-tratamiento.

Como un caso, un estudio se enfocó en el desarrollo de un producto, *StegAdventure*, un serious game narrativo enfocado en enseñar esteganografía (la práctica de ocultar mensajes dentro de otros medios digitales) a estudiantes de educación superior, y se comparó su uso con un recurso tradicional basado en texto. Los resultados mostraron que el grupo que usó StegAdventure mostró niveles significativamente mayores de compromiso y atención hacia el contenido, pero aunque no se mostraron diferencias significativas por un examen de conocimiento a corto plazo, la interactividad y experiencia narrativa sugieren mayor interés y retención de información a largo plazo [14].

Otro estudio realizado en Cataluña, España, comparó dos formas de entrenamiento atencional en niños de 8 a 10 años con diagnóstico de TDAH: una versión en formato videojuego educacional (Serious Games) y otra tradicional con lápiz y papel, con actividades equivalentes en contenido tales como selección de estímulos, diferencias visuales, laberintos y memorizar dibujos. Los resultados mostraron que ambos grupos mejoraron en su atención selectiva, concentración general y capacidad de atención sostenida, pero el grupo que usó Serious Games presentó mejoras significativamente mayores en los errores de comisión (elemento que refleja dificultad con la impulsividad o el control atencional) en comparación con el grupo convencional [15].

Esto sugiere que los Serious Games no solo refuerzan la motivación y la adhesión al entrenamiento, sino que también resultan más eficaces en ciertos componentes concretos del control cognitivo.

3. Metodología

En este proyecto se emplea la metodología **Design and Creation** [16], un método orientado a la creación de artefactos tecnológicos que permiten resolver un problema práctico mediante diseño, construcción y evaluación sistemática. Esta metodología es adecuada para esta investigación tecnológica donde se busca desarrollar herramientas de software, prototipos interactivos o sistemas destinados a mejorar un proceso existente. El programa de software interactivo es denominado ‘artefacto’ a través de esta etapa.

Esta metodología se estructura en cinco etapas fundamentales para guiar el proceso de diseño y validación del artefacto [17] (Figura 3.1):

- **Awareness** (Concientización): Identificación del problema central y revisión preliminar del estado del arte, estableciendo la necesidad de mejorar la capacitación en phishing.
- **Suggestion** (Propuesta): Definición conceptual de la solución mediante el diseño de un Serious Game simulador de correos, sus objetivos mecánicos y sus principales funcionalidades.
- **Development** (Desarrollo): Construcción del prototipo del videojuego mediante un proceso iterativo, integrando interfaz, mecánicas y retroalimentación.
- **Evaluation** (Evaluación): Aplicación de pruebas de usabilidad para medir la efectividad del prototipo con un grupo de control y un grupo experimental mediante una prueba t-Test [18].

- **Conclusion** (Conclusión): Análisis de los resultados obtenidos y reflexión sobre el aporte del artefacto, así como oportunidades de mejora y continuidad del proyecto.

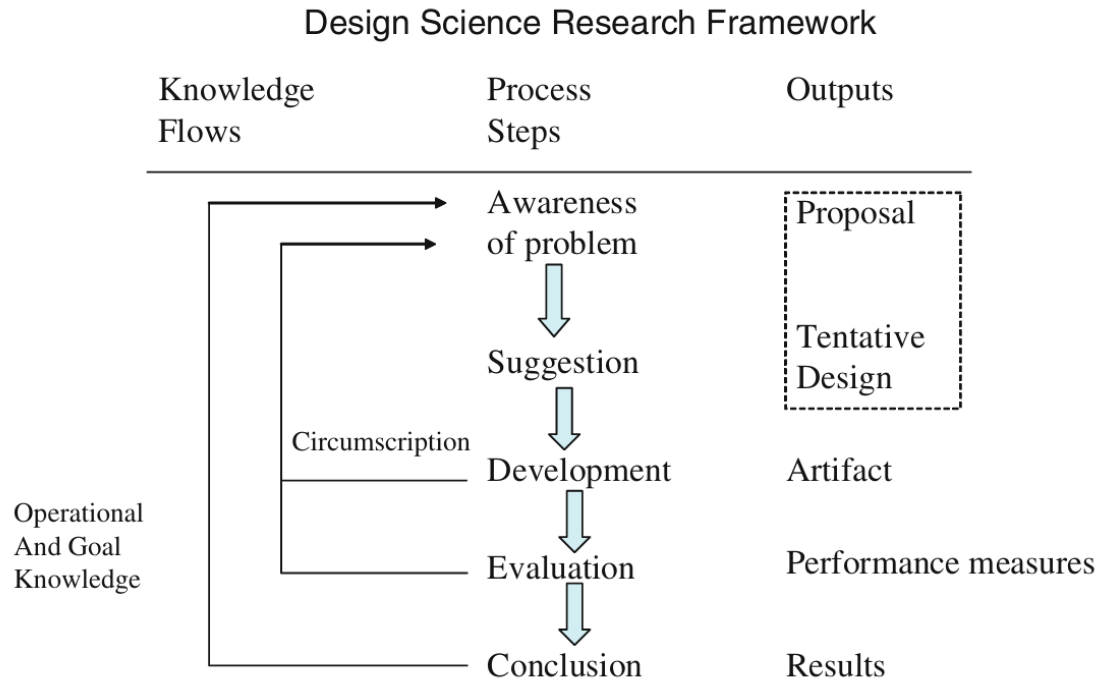


Figura 3.1: Ciclo general del diseño en Design Science Research

Fuente: Hevner, Alan. Design Research in Information Systems, pág. 27.

3.1. Concientización del Problema

La dificultad que presentan usuarios jóvenes y adultos para reconocer intentos de phishing, debido a brechas en alfabetización digital y a la ineficacia relativa de los métodos tradicionales de capacitación.

Este análisis ya se cubrió en el **Marco Teórico** en detalle. En resumen, se realizó mediante un análisis de literatura científica que abarcó temas como amenazas digitales, aumento de ataques de ingeniería social, brechas en educación digital, vulnerabilidades comunes, y enfoques pedagógicos aplicados a la ciberseguridad. Tal análisis

permitió comprender que, aunque existe abundante información sobre cómo abordar la ciberseguridad, muchos usuarios no logran aplicarla de manera efectiva al enfrentarse a escenarios reales. Este diagnóstico fundamenta la necesidad de herramientas más atractivas, prácticas y motivadoras para reforzar habilidades de identificación de amenazas, justificando la elección de un **Serious Game** como una posible solución a esta problemática, ya que cubre el uso de software.

3.2. Propuesta de Solución

En esta etapa se diseñará la solución conceptual del artefacto en mayor detalle: un videojuego Serious Game que simula un entorno de computadora y de correos electrónicos, donde el usuario debe distinguir entre mensajes legítimos y mensajes maliciosos. En un concepto general, la propuesta de solución propone y define los siguientes aspectos de este programa:

- **Plataforma: Videojuego para PC desarrollado en Unity.** Se eligió el uso de un motor de videojuegos en vez de una interfaz de cliente de correos para tener mayor control del flujo del gameplay y la expansión de sus mecánicas.
- **Objetivo:** Entrenar al usuario para que pueda identificar señales comunes de phishing mediante práctica repetida y retroalimentación por métodos lúdicos (objetivos, puntaje, modificadores).
- **Concepto General:** Un videojuego del género simulación donde el jugador debe verificar los correos que recibe si son maliciosos o seguros, reportando o respondiendo de vuelta cuando sea necesario. Una vez se completa una cierta cantidad y se cumplen los objetivos, se puede terminar el nivel para evaluar la cantidad de acciones correctas.

Esta propuesta se sustenta en un documento previo de Ingeniería de Software realizado para este mismo proyecto, donde se describen modelos, diagramas y requisitos que guían la construcción del prototipo.¹ A partir de esta conceptualización, se establecen las bases funcionales y pedagógicas para la etapa siguiente.

¹Documento 'CyberSafety' de Ingeniería de Software disponible en: <https://drive.google.com/file/d/1zHUw4wcYj1uhYoBREZDgw6fBQ0ZFEOA/view?usp=sharing>

3.3. Desarrollo del Artefacto

El desarrollo del videojuego se realizará utilizando un enfoque iterativo basado en metodología ágil [19][20], cuyos pasos se muestran en la Figura 3.2. Cada ciclo incorpora análisis, diseño, desarrollo, validación, y despliegue, permitiendo construir versiones funcionales tempranas y mejorar continuamente la experiencia del usuario.

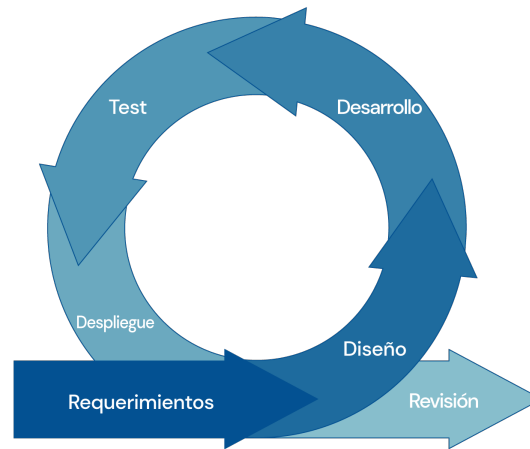


Figura 3.2: Ciclo de Iteración de la Metodología Ágil

Fuente: Extraída de “Metodología Waterfall vs Metodología Ágil”, DoneTonic.com.

El proceso iterativo se estructura en cuatro pasos principales:

1. **Análisis o Requerimientos:** Se identifican los requisitos funcionales del videojuego, considerando los objetivos establecidos en la propuesta de solución. Esto incluye el tipo de simulación, los patrones de phishing a representar, la complejidad esperada por nivel y las opciones para el usuario final.
2. **Diseño:** Se definen los elementos conceptuales del artefacto: estructura de niveles, flujo de interacción, diseño general de la interfaz, organización de los correos, modelo de retroalimentación y criterios de evaluación del jugador. Esta etapa traduce los requisitos del análisis en un plan concreto para la implementación de la iteración.
3. **Desarrollo:** En esta etapa se construyen las funcionalidades planificadas para cada iteración. Aquí se implementan los componentes principales del prototipo,

que incluyen:

- **Interfaz gráfica básica del simulador de correo electrónico**, simulando un entorno de escritorio donde el usuario puede revisar, responder o reportar correos.
 - **Base de datos local** para almacenar información de correos, niveles, objetivos, y datos guardados, permitiendo modularidad y escalabilidad futura.
 - **Conjunto inicial de correos legítimos y fraudulentos**, diseñados para representar múltiples temas de phishing.
 - **Sistema de tutorial interactivo** que introduce al usuario a las mecánicas, controles y elementos clave de la simulación.
 - **Mecanismo de retroalimentación por puntaje y objetivos**, que evalúa las decisiones del usuario al final del nivel.
 - **Sistema de progresión por niveles**, aumentando la dificultad mediante mayor complejidad y sutileza en los correos.
 - **Glosario, menú de ayuda y opciones de accesibilidad**, como categorías de correos (bancarios, concursos, familiares, juegos) y ajustes de tamaño de fuente.
4. **Pruebas y Validación:** Cada iteración se somete a pruebas internas orientadas a detectar errores, evaluar usabilidad y medir claridad de las mecánicas. Los resultados permiten refinar la interfaz, ajustar el comportamiento de los correos y mejorar la retroalimentación antes de avanzar a la siguiente iteración.
5. **Despliegue:** Con una iteración finalizada, esta se guarda como una versión/build del software y se puede empezar una nueva iteración del software para avanzar a una versión mejorada, o decidir si este es el estado del software que se usará como prototipo final.

La metodología ágil se seleccionó para este proyecto debido a su capacidad de adaptarse a cambios, permitir mejoras continuas y facilitar el desarrollo de prototipos funcionales en etapas tempranas. A diferencia de metodologías tradicionales más rígidas como la metodología de cascada [21], la naturaleza iterativa del enfoque

ágil resulta especialmente adecuada para el desarrollo de Serious Games, donde la usabilidad, la claridad de la interfaz y la efectividad de la experiencia requieren múltiples ciclos de refinamiento.

En cada iteración se realizarán pruebas internas orientadas a:

- Detectar errores funcionales.
- Evaluar la claridad y coherencia de la interfaz.
- Mejorar la usabilidad general del sistema.
- Ajustar, corregir o balancear las mecánicas del videojuego.

Este enfoque permite refinar progresivamente los elementos interactivos y educativos del videojuego, asegurando que cada ciclo incremente la calidad del prototipo en términos de estabilidad, accesibilidad y efectividad instructiva. Las iteraciones continuarán mientras existan *requisitos pendientes*, problemas de funcionalidad o mejoras necesarias identificadas durante las pruebas internas.

El proceso iterativo culminará cuando el prototipo alcance un estado estable en el que:

- Todas las funcionalidades esenciales están implementadas.
- La interfaz cumple criterios mínimos de claridad y usabilidad.
- Las mecánicas funcionan sin errores críticos.
- La experiencia del usuario es coherente con los objetivos formativos del proyecto.

En ese punto, el artefacto se considerará suficientemente aceptable para avanzar hacia la fase de evaluación formal con usuarios. El propósito final de esta etapa es obtener una versión robusta que permita medir adecuadamente su usabilidad y su impacto en las experiencias sobre el phishing.

El objetivo esperado del proyecto es alcanzar un nivel de madurez tecnológica **TRL 4**, correspondiente a la validación de un prototipo bajo condiciones de laboratorio, lo cual implica que el videojuego debe encontrarse en un estado suficientemente estable y funcional para que se consideren sus características similares a las de su aplicación final y que haya sido validado con usuarios dentro de un ambiente de laboratorio.

3.4. Evaluación

La fase de evaluación corresponde al proceso en el que se pondrá a prueba el prototipo para determinar su usabilidad, funcionalidad y efectividad educativa. Dado que esta etapa requiere la participación de usuarios, el diseño descrito a continuación constituye una planificación preliminar y sus tiempos e instrumentos podrán ajustarse según las necesidades del estudio.

- **Participantes y materiales:** Se trabajará con **20–30 participantes**, idealmente jóvenes adultos o estudiantes universitarios, con familiaridad general con dispositivos digitales. Esta cantidad es obtenida de un curso de estudiantes que tienen acceso a los computadores de laboratorio, están familiarizados con sistemas de videojuegos y reconocen la ciberseguridad como un tema serio. Esta es una prueba exploratoria con el objetivo de asegurar la usabilidad del producto previo a ser presentado en grupos más grandes. Los participantes se asignarán aleatoriamente a dos grupos: (a) **Grupo Experimental**, que utilizará el videojuego simulador de correos; (b) **Grupo de Control**, que utilizará el mismo simulador de correos con una versión alternativa. Es necesario tener dos grupos para evaluar la comparación de las métricas de usabilidad, experiencia de usuario y actitudes para verificar qué versión del videojuego posee mayor efectividad en la experiencia del videojuego y la concientización acerca de la ciberseguridad [22].

La edad se registrará únicamente como **rango general del conjunto** (aprox. **20–30 años**), sin almacenar datos personales identificables. Toda la información recopilada será completamente anónima y se limitará exclusivamente a variables relevantes para este proyecto.

Cada participante utilizará un computador con el prototipo instalado, junto con un formulario de consentimiento informado y los cuestionarios respectivos. Las sesiones se realizarán en una sala aislada, con el participante y un guía encargado de explicar el procedimiento.

- **Procedimiento y diseño:** El estudio seguirá un diseño experimental entre grupos (Control vs. Experimental). Cada sesión tendrá una duración estimada de **10–12 minutos**, aunque estos tiempos son aproximados y pueden variar. El procedimiento será:

1. **Introducción y consentimiento** (2–3 minutos): explicación del estudio y firma del consentimiento informado.
 2. **Intervención** (5 minutos):
 - **Grupo Experimental:** Videojuego enfocado en la promoción de la ciberseguridad a través de un simulador de correos.
 - **Grupo de Control:** Videojuego simulador de correos, versión alternativa donde hay mayores restricciones o condiciones de victoria.
 3. **Cuestionarios posteriores** (3–4 minutos): aplicación de instrumentos de evaluación.
- **Variables independientes:** La variable independiente será el **tipo de intervención**:
 - (a) **Videojuego de ciberseguridad de simulador de correos** (grupo experimental),
 - (b) **Videojuego de ciberseguridad de simulador de correos, versión alternativa** (grupo control).

Esto permitirá analizar si el carácter práctico y lúdico del prototipo genera una mejora significativa en el aprendizaje.

- **Variables dependientes:** Se usarán al menos dos de tres tipos principales de mediciones para recopilar datos significativos:
 - **SUS - Sistema de Usabilidad:** Evalúa la facilidad de uso, claridad y satisfacción general con el prototipo [23].
 - **UEQ - Cuestionario de Experiencia de Usuario:** Mide la experiencia pragmática y hedónica, evaluando dimensiones como atractivo, eficiencia, confiabilidad y estimulación [24].
 - **Encuesta propia:** Evalúa cambios en la habilidad y actitudes para identificar señales de phishing y comentarios acerca de la interacción con el programa.

Adicionalmente, para el grupo experimental se registrará el **porcentaje de correos clasificados correctamente** durante la prueba como indicador objetivo de desempeño.

Todos los resultados se almacenarán de manera anónima para su posterior análisis en la etapa de tratamiento de datos.

3.5. Conclusión

La etapa final consistirá en analizar los datos obtenidos durante la evaluación del prototipo con el objetivo de determinar su efectividad como herramienta de concientización para la identificación de amenazas digitales basadas en phishing. Para ello, todos los datos recopilados: Puntajes SUS, resultados del UEQ y respuestas de la encuesta propia serán organizados, limpiados y procesados utilizando **Python**, permitiendo estandarizar valores, generar estadísticas y producir visualizaciones de gráficos que faciliten la interpretación.

Dado que el estudio contempla un **grupo experimental** (Videojuego simulador de correos) y un **grupo de control** (Videojuego simulador de correos alternativo), el análisis estadístico se enfocará en comparar ambos conjuntos únicamente a partir de las mediciones **post-intervención**. Para cada instrumento se calcularán medias, medianas y desviaciones estándar por grupo, lo que permitirá observar tendencias generales en actitudes, experiencia de usuario y usabilidad.

Posteriormente, se aplicará un **t-Test para muestras independientes** con el fin de determinar si las diferencias observadas entre el grupo experimental y el grupo de control son estadísticamente significativas [25]. En el caso de la encuesta propia, que evalúa la capacidad para identificar señales de phishing, se calculará adicionalmente la **diferencia de medias intra-grupo**, con el objetivo de identificar si la intervención produjo mejoras coherentes dentro de cada grupo y si estas mejoras son superiores en el grupo experimental.

Finalmente, los puntajes EUQ y SUS serán transformados a su escala estandarizada para evaluar la usabilidad percibida del prototipo y determinar si cumple con los niveles aceptables según la literatura. Este análisis final permitirá establecer si el videojuego constituye un programa efectivo y con impacto en la actitud de los usuarios sobre la ciberseguridad.

3.6. Carta Gantt

Para lograr la realización completa de esta etapa de diseño hasta su conclusión de datos, se realizará una Carta Gantt para estructurar las etapas y sus tareas logradas a través del tiempo. Se espera hacer en Cuartiles en el año 2026, con un progreso previo en los últimos dos cuartiles del año 2025.

A continuación, la Tabla 3.1, muestra las tareas consideradas a realizar, que corresponden a las siguientes:

Tareas	2025						2026		
	Q3			Q4			Q1		
0. Propuesta de Memoria	X	X	X	X	X	X	-	-	-
0.1 Marco Teórico	X	X	X	-	-	-	-	-	-
0.2 Diseño y Metodología	-	-	-	X	X	X	-	-	-
1. Diseño del Videojuego	-	-	-	-	X	X	X	-	-
1.1 Elaboración de Mecánicas	-	-	-	-	X	X	-	-	-
1.2 Planificación de Sistema de Base de Datos y Correos	-	-	-	-	-	X	X	-	-
2. Implementación del Videojuego	-	-	-	-	-	-	X	-	-
2.1 Mecánicas Principales e Interfaz	-	-	-	-	-	-	X	-	-
2.2 Integración de Base de Datos, Puntaje y Niveles	-	-	-	-	-	-	X	-	-
2.3 Refinación y Mejoras	-	-	-	-	-	-	X	X	-
3. Play Testing	-	-	-	-	-	-	-	X	-
4. Recopilación de Datos	-	-	-	-	-	-	-	X	X
5. Tratamiento de Datos	-	-	-	-	-	-	-	-	X
6. Presentación Final	-	-	-	-	-	-	-	-	X

Tabla 3.1: Carta Gantt del proyecto CyberSafety

0. **Propuesta de Memoria:** Desarrollo inicial del documento base, organización del tema y delimitación del proyecto.
 - 0.1 **Marco Teórico:** Revisión bibliográfica sobre ciberseguridad, phishing y Serious Games.
 - 0.2 **Diseño y Metodología:** Definición de la metodología Design & Creation y estructura general del desarrollo.
1. **Diseño del Videojuego:** Creación del concepto general del artefacto, estructura de niveles, objetivos y flujo de interacción.
 - 1.1 **Elaboración de Mecánicas:** Diseño de las interacciones principales del simulador de correos.
 - 1.2 **Planificación de Sistema de Base de Datos y Correos:** Diseño de la estructura interna para almacenar correos, niveles y progreso.
2. **Implementación del Videojuego:** Desarrollo técnico del prototipo en Unity siguiendo metodologías ágiles.
 - 2.1 **Implementación de Mecánicas e Interfaz:** Construcción funcional del simulador, interfaz y controles básicos.
 - 2.2 **Integración de Base de Datos, Puntaje y Niveles:** Incorporación de sistemas de almacenamiento, análisis de correos y retroalimentación.
 - 2.3 **Refinación y Mejoras:** Ajustes finales, corrección de errores y optimización general del prototipo.
3. **Play Testing:** Pruebas internas para validar la jugabilidad, claridad de la interfaz y balance de mecánicas.
4. **Recopilación de Datos:** Aplicación de los instrumentos de evaluación (SUS, UEQ y encuesta propia) a los participantes del estudio.
5. **Tratamiento de Datos:** Limpieza, normalización y análisis estadístico mediante Python, incluyendo comparación entre grupos.
6. **Presentación Final:** Preparación del documento final y defensa del proyecto.

4. Diseño

En este diseño se seguirá la metodología **MDA** (Mecánicas, Dinámicas y Estéticas), un marco de diseño formal enfocado en comprender el diseño de videojuegos dividido en tres componentes clave: **Mecánicas**, que cubren reglas, funcionamiento y código; **Dinámicas**, que cubren el comportamiento del gameplay en tiempo real; y **Estéticas**, que cubren el aspecto visual y sonoro para inmersir al jugador. Este diseño permite combinar en rasgos generales la representación del juego, cómo funciona, la experiencia del jugador y la estética del juego. [26]

4.1. Mecánicas

Las mecánicas corresponden a las reglas, sistemas y componentes lógicos que estructuran el funcionamiento del videojuego en su forma de código.

4.1.1. Correos electrónicos

El sistema principal del videojuego se basa en la gestión de correos electrónicos y su interacción para identificar si es malicioso o no. Cada correo está definido por atributos como nombre, contenido, y si es malicioso o no, que permiten construir distintos tipos de correos y variar su complejidad a lo largo del juego. Estos correos se encuentran en una base de datos, donde cada nivel puede sacar correos al azar de este listado para variar sus contenidos. Además, ciertos correos poseen diferentes características durante el gameplay que los hacen distintivos de otros, como ser persistentes o spam.

En el *Anexo 7.3.1* se encuentran tablas de los tipos de correos y sus atributos.

4.1.2. Estructura de Niveles

El videojuego se organiza en niveles dentro del sistema simulado de computadora. Estos niveles se seleccionan dentro de una interfaz de niveles, con el primero desbloqueado. El siguiente nivel se desbloquea al completar exitosamente el nivel anterior. Existen 3 niveles con dificultad creciente, agregando nuevos tipos de correos en cada nivel nuevo, como correos phishing persistentes en el nivel 2 y correos spam en el nivel 3.

En el *Anexo 7.3.2* se encuentran tablas de los tipos de correos y sus atributos.

4.1.3. Sistema de Correos y Puntaje

El videojuego posee un botón en el escritorio para acceder al sistema de correos. El jugador puede visualizar los correos recibidos en un listado y seleccionar uno para revisar su remitente y contenido. Los correos se reciben progresivamente durante el nivel para simular un flujo continuo.

Cada correo dispone de elementos interactivables, como responder o reportar, cuyas acciones son evaluadas por el sistema de puntaje. Las acciones correctas otorgan puntos y las incorrectas los quitan, siendo necesario reconocer los rasgos de correos maliciosos para completar el nivel con éxito.

En el *Anexo 7.3.3* se encuentran tablas de los tipos de acciones y las reglas del puntaje.

4.1.4. Sistema de Objetivos

Cada nivel presenta una lista de objetivos a los que se puede acceder por un botón en el fondo del escritorio. Este contiene actividades que el jugador debe completar para poder finalizar el nivel. Los objetivos no otorgan puntaje en sí, sino que guían al jugador a hacer acciones correctas para poder completar el nivel con el puntaje mínimo requerido, ya que se puede responder a un correo malicioso o legítimo y se contará aún para el objetivo.

El nivel no finaliza automáticamente al completar los objetivos. El jugador puede continuar interactuando con los correos restantes para obtener puntos adicionales. Una vez cumplidos los objetivos, se habilita un botón de finalización manual dentro del botón de inicio (parte inferior izquierda de la pantalla), que llevará a la pantalla de resultados para evaluar el puntaje y el resultado del nivel. Si no se completan los

objetivos y no quedan más correos que responder, se permite completar el nivel para ir a los resultados. Un nivel completado con éxito desbloquea el siguiente nivel.

En el *Anexo 7.3.4* se encuentran tablas de los tipos de objetivos y de las condiciones de finalización.

4.1.5. Sistema del Manual

El videojuego incorpora una ventana de **Manual**, accesible mediante un botón en el escritorio, que reúne información sobre el funcionamiento del sistema y los criterios para identificar correos maliciosos. La identificación de estos correos se basa en diversas características, donde la presencia de uno o más indicadores aumenta la probabilidad de que un correo sea malicioso.

El manual incluye secciones de ayuda y listas de entidades confiables, las cuales varían entre niveles para introducir nuevas mecánicas y aumentar progresivamente la dificultad.

En el *Anexo 7.3.5* se encuentra la tabla que indica los criterios de identificación de correos maliciosos.

4.1.6. Temporizadores (Versión alternativa)

El videojuego incluye una variante con **límite de tiempo**, que se aplica a todos los niveles. Este limita el tiempo que el jugador puede tomar al tratar de completar un nivel y priorizar ciertas acciones. Este modificador general aplica una duración límite a los correos y niveles del juego. En el *Anexo 7.3.6* se encuentra la tabla del modo temporizador con detalles específicos.

4.2. Dinámicas

Las dinámicas corresponden a las interacciones de los jugadores con las mecánicas del sistema, cómo se presenta y se siente esta experiencia, y cómo la jugabilidad está diseñada para estos tipos de comportamientos. Estos detalles son para indicaciones específicas de los elementos de la interfaz, sus botones y cómo funcionan de forma similar a un sistema de escritorio de computadora.

Las tablas asociadas a estos detalles se encuentran en el *Anexo 7.3.7*.

4.3. Estética

Las estéticas corresponden a los componentes visuales y sonoros que se usan dentro del videojuego y a la percepción del uso de estos elementos para influir en las experiencias emocionales y perceptibles que el jugador obtiene al interactuar con el juego. El enfoque de la estética busca inmersir al jugador en un simulador de computadora, como un oficinista o trabajador que requiere la revisión constante de correos.

4.3.1. Simulador de Computadora

El videojuego busca recrear la experiencia de usar un computador personal. Para ello, se implementará una interfaz basada en un escritorio de computadora, donde las distintas funcionalidades se presentan mediante ventanas, botones de escritorio y barra de tareas, imitando el comportamiento de un sistema operativo, como Windows XP.

Este enfoque permite generar una experiencia cercana a un contexto real, facilitando la transferencia del aprendizaje a situaciones cotidianas relacionadas con el uso del correo electrónico.

4.3.2. Aspecto Visual

El aspecto visual está inspirado en los sistemas operativos más reconocibles (Windows XP, Windows 95, Linux), caracterizados por:

- Interfaces basadas en ventanas de computadora.
- Uso de iconografía simple y reconocible.
- Distribución estructurada de elementos en pantalla, como botones de fondo y las múltiples ventanas.

Este estilo busca ser intuitivo para el jugador, evitando sobrecarga visual y favoreciendo la comprensión de las acciones disponibles, además de su aspecto nostálgico y diferente de los sistemas actuales.

4.3.3. Aspecto Sonoro

El aspecto sonoro se basa en la utilización de efectos digitales simples y familiares para las múltiples interacciones dentro del sistema, tales como:

- Notificación de la llegada de correos electrónicos.
- Interacción con botones y ventanas.
- Alertas asociadas a acciones del sistema.

Estos elementos refuerzan la inmersión del jugador dentro del entorno simulado y dan retroalimentación sonora cuando el sistema responde, pero sin generar distracciones innecesarias.

4.3.4. Sensación de Inmersión

La combinación de elementos visuales y sonoros permite al jugador sentirse dentro del escritorio de un computador, a pesar de ser un simulador, para permitir una experiencia cercana a la realidad, lo que favorece la atención y el compromiso con las tareas propuestas. Además, se le otorga un 'rol' como personaje, ya que los contenidos de los correos se refieren al jugador, pero como un personaje oficinista que usa este sistema.

4.3.5. Tensión y Responsabilidad

El jugador experimenta una sensación de tensión al enfrentarse a los correos, producto de que solo se comprueba si eran maliciosos o no al final del nivel una vez se otorga el puntaje. Esto genera más responsabilidad con las acciones del jugador para no cometer equivocaciones. En la versión con límite de tiempo, esta sensación se intensifica mediante la presión por tomar decisiones rápidas.

4.3.6. Satisfacción y Aprendizaje

La correcta identificación de correos legítimos y maliciosos genera una sensación de logro en el jugador, demostrada por el puntaje obtenido al final. A su vez, el proceso de prueba y error contribuye a una experiencia de aprendizaje significativa dentro del progreso del juego para acomodarlo a los niveles futuros.

5. Implementación

Dentro de esta sección se demostrará el progreso final del prototipo para la prueba con usuarios y cómo se realizarán estas.

5.1. Prototipo

El prototipo desarrollado para las pruebas corresponde a una versión funcional del videojuego y sus mecánicas principales, incluyendo el sistema de gestión de correos electrónicos y sus múltiples interacciones.

Actualmente, el sistema incluye diferentes funcionalidades descritas por el diseño:

- Interfaz de escritorio y múltiples ventanas.
- Sistema de correos.
- Acciones de responder, eliminar, bloquear, y marcar como spam.
- Sistema de puntaje y objetivos.
- Modo alternativo de Temporizador.
- Incluye 3 niveles con mecánicas progresivas y alrededor de 50 correos diferentes.

En el **Anexo 7.7** se muestran dos videos del gameplay del videojuego: Versión sin temporizador y versión con temporizador,

5.1.1. Interfaz Principal

La interfaz principal es donde el jugador comienza el videojuego. Tiene una escena inicial para la inmersión, mostrando una consola con múltiples líneas de comandos antes de que se muestre la interfaz principal y su título en la ventana principal. Solo con los botones de la ventana se puede interactuar, mientras que los otros solo producen un sonido de error.

Desde aquí se puede acceder a la interfaz de niveles, configuraciones, o salir del videojuego y cerrar la aplicación.

En el **Anexo 7.4.1** se encuentra el diagrama de la interfaz principal.

5.1.2. Interfaz de Configuraciones

La interfaz de Configuraciones permite al jugador hacer cambios menores al videojuego como cambiar el tamaño de la letra, el idioma del programa, y activar/desactivar el modo temporizador, aunque este modo se va a bloquear su cambio para las pruebas con usuarios.

Finalmente, el jugador puede eliminar los datos guardados, que incluyen los niveles desbloqueados y el tutorial terminado, lo que solo deja que el jugador vuelva a tener solo el primer nivel desbloqueado y que deba completar el tutorial otra vez. Esta acción requiere una confirmación en una ventana emergente.

Solo se puede devolver a la interfaz principal desde aquí. En el **Anexo 7.4.2** se encuentra el diagrama de la interfaz de configuraciones.

5.1.3. Interfaz de Niveles

La interfaz de Niveles permite al jugador escoger el nivel para poder jugar al videojuego, dentro de una nueva ventana. Los niveles se encuentran en la parte superior central, y solo el primer nivel estará desbloqueado al principio de una nueva partida sin datos previos. Se debe seleccionar un nivel para proseguir. Al medio de la ventana hay un espacio que describe el nivel seleccionado y si posee mecánicas nuevas.

Una vez seleccionado un nivel, se puede seleccionar empezar para ir a la interfaz de escritorio para comenzar el juego. En otro caso, se puede volver atrás al menú principal. En el **Anexo 7.4.3** se encuentra el diagrama de la interfaz de niveles.

5.1.4. Interfaz de Escritorio

La interfaz de Escritorio corresponde al área principal de juego. Al iniciar el nivel 1 por primera vez, se presenta un tutorial que introduce las mecánicas, ventanas y acciones disponibles. Una vez finalizado, comienza el nivel.

Durante el nivel, los correos se reciben progresivamente en intervalos de tiempo cortos y aleatorios. Estos se gestionan mediante la ventana de Correos, junto con las ventanas de Tareas y Manual, que proporcionan la información necesaria para el desarrollo del juego.

Para completar el nivel, el jugador debe alcanzar los objetivos indicados en la ventana de Tareas antes de quedarse sin correos disponibles. En la esquina inferior izquierda se encuentra el botón de salida, que permite abandonar el nivel o finalizarlo una vez cumplidos los objetivos o cuando ya no queden correos por responder.



Figura 5.1: Diagrama de Interfaz de Escritorio

5.1.5. Interfaz de Tareas

Se encuentra conectada a la interfaz de Escritorio como una ventana adicional. Dentro de esta se encuentran objetivos como responder X correos o reportar X correos. Si el modo Temporizador está activo, este también aparece como un objetivo para mostrar cuánto tiempo se tiene.

Al completar todos los objetivos o no haber más correos que responder, el botón para terminar el nivel se desbloquea. En el **Anexo 7.4.4** se encuentra el diagrama de la interfaz de tareas.

5.1.6. Interfaz de Correos

La interfaz de Correos recibe progresivamente correos legítimos y maliciosos durante el nivel. Al seleccionar uno desde la lista, se muestran su contenido, remitente, asunto y los botones de acción.

Las acciones disponibles son **Reportar**, que despliega un panel con las opciones Eliminar, Bloquear y Marcar como Spam (desbloqueadas progresivamente según el nivel), y **Responder**, utilizada para contestar correos legítimos.

El contenido, junto con el asunto y el remitente, constituye el principal medio para identificar amenazas. Algunos correos incluyen enlaces maliciosos que, al seleccionarlos, provocan errores visuales y descuentan puntaje.

Las acciones correctas otorgan puntos, mientras que las incorrectas los reducen. El puntaje acumulado solo se presenta al finalizar el nivel mediante la pantalla de resultados.

Finalmente, algunos correos maliciosos son persistentes que requieren ser bloqueados, mientras que un correo spam debe marcarse como tal para eliminarlo.

En el **Anexo 7.4.5** se encuentran los diagramas de la interfaz de correos.

5.1.7. Interfaz de Resultados

La interfaz de Resultados es la última interfaz del videojuego y donde el jugador puede ver sus datos de rendimiento, las acciones que tomó, el tiempo que demoró, y su puntaje total. Cada acción correcta muestra un valor positivo mientras las incorrectas muestran valores negativos. Otros valores con acciones no indican suma o resta de puntaje (como spam, que no progresa puntos ni objetivos). Si se llegó al puntaje mínimo del nivel, entonces se desbloqueará el siguiente nivel si existe.

Desde aquí, el jugador puede volver a la pantalla principal, reintentar el nivel o avanzar al siguiente si hay uno desbloqueado. En el **Anexo 7.4.6** se encuentra el diagrama de la interfaz de resultados.

5.1.8. Versión Alternativa: Modo Temporizador

Ubicado como una opción en las configuraciones, el Modo Temporizador agrega un temporizador al nivel que depende de cada nivel, y agrega una duración limitada a cada correo cuando aparece, mostrada por un círculo verde que se vuelve más rojo al perder más segmentos en sí, y si pierde toda la duración, el correo se quita y resta 1 punto si no es spam. Si se agota el tiempo en el nivel, este acaba inmediatamente y lleva al jugador a la pantalla de resultados.

En las pruebas, los usuarios no ajustarán esta configuración, ya que solo usarán una sola versión, al azar, sin conocimiento de la otra. En el **Anexo 7.4.7** se encuentra el diagrama del temporizador.

5.2. Preparación y Encuestas para Pruebas con Usuarios

El prototipo considera la aplicación de tres instrumentos de evaluación dirigidos a los usuarios luego de terminar el videojuego. Estas métricas de evaluación son: **Cuestionario de Experiencia de Usuario**, **Encuesta de Usabilidad del Sistema**, y **Encuesta propia enfocada en ciberseguridad**.

Además, se recopilarán datos demográficos básicos de los participantes, tales como código de grupo (obtenido del juego), edad, género y cargo/empleo.

5.2.1. Encuesta Propia

La encuesta propia tiene como objetivo evaluar la percepción del jugador respecto a la ciberseguridad y su experiencia con el videojuego. Parte de esta encuesta está basada en preguntas ya hechas en otro estudio similar acerca de la conciencia de la ciberseguridad [27].

Se utilizará una encuesta con base en la escala Likert de 1 a 7, donde 1 corresponde a “Muy en desacuerdo” y 7 a “Muy de acuerdo”. Las preguntas se encuentran en el **Anexo 7.5**.

5.2.2. Procedimiento de Pruebas

Las pruebas con usuarios se realizaron dentro del laboratorio 3D de la escuela de Ingeniería en Desarrollo de Videojuegos y Realidad Virtual de la Universidad de Talca. El videojuego se instaló en los equipos del laboratorio, separando los equipos para que tengan solo 1 versión del videojuego (con o sin temporizador). Los participantes de prueba fueron informados del procedimiento y de que la prueba está enfocada en la efectividad del producto para la concientización de la ciberseguridad, pero para asegurar respuestas no influenciadas, no se informó acerca de la existencia de estas versiones o de cuál están probando. La duración de la prueba del videojuego fue de alrededor de 15-20 minutos y, al finalizar el juego, los resultados de la sesión se exportaron a un archivo de Excel y el usuario fue enviado a un cuestionario, donde tuvo que ingresar datos demográficos y responder 3 diferentes encuestas, con una duración de 5-10 minutos, además de ingresar el archivo de resultados. Las pruebas finalizaron una vez que completaron y enviaron la encuesta.

5.2.3. Resultados

Se hicieron pruebas con 30 usuarios dentro del rango de edad de 20-30 años, con cargo de universitario o estudiante, obteniendo 16 respuestas para la versión sin temporizador y 14 respuestas para la versión con temporizador. Con estos resultados, se busca obtener datos relevantes de la experiencia de usuario para determinar qué versión es más efectiva para la concientización de la ciberseguridad.

Estos resultados se pueden revisar en los Anexos 7.8 y 7.9, que incluyen las encuestas, estadísticas de sesiones, y retroalimentación de usuarios.

Análisis Exploratorio de Datos

Los resultados de las sesiones de juego cuentan con los siguientes datos notables (El gráfico de datos obtenidos se encuentra en el *Anexo 7.6.1*):

Duración de niveles: Se observa mayor dispersión de resultados en las pruebas sin temporizador entre 1-4 minutos, mientras que con temporizador se observa un progreso creciente por niveles que dura 70-150 segundos, con menor tiempo invertido en comparación con las sin temporizador. Indica que los jugadores se toman el tiempo necesario para completar sus objetivos cuando no hay presión externa.

Puntaje y acciones: En general, el puntaje y las acciones correctas (responder correos legítimos, reportar correos maliciosos) tienen un promedio relativamente mayor sin temporizador que con temporizador, aunque sufren una baja de puntaje en el tercer nivel. Esto indica que se logró cumplir con el entrenamiento para reconocer phishing (un puntaje promedio menor a 5 indica fallos graves). Los comentarios de retroalimentación dados en la encuesta propia indican experiencias similares.

Respuestas de Experiencia de Usuario (UEQ)

UEQ presenta su evaluación de datos en 6 campos de escala (Atractivo, Eficiencia, Claridad, Fiabilidad, Estimulación y Novedad). La versión sin temporizador obtuvo un mejor puntaje que la con temporizador, excepto en el campo de estimulación, donde la versión con temporizador tiene una puntuación ligeramente mejor, pero sus datos son mucho más dispersos. Los resultados sin temporizador presentan menor dispersión que los de la versión con temporizador. La evaluación t-test con estos campos no mostró diferencias estadísticamente significativas entre los grupos, ya que la mayoría obtuvo un rango de t entre 0.20 y 1.47, que indica que las diferencias son pequeñas o insuficientes.

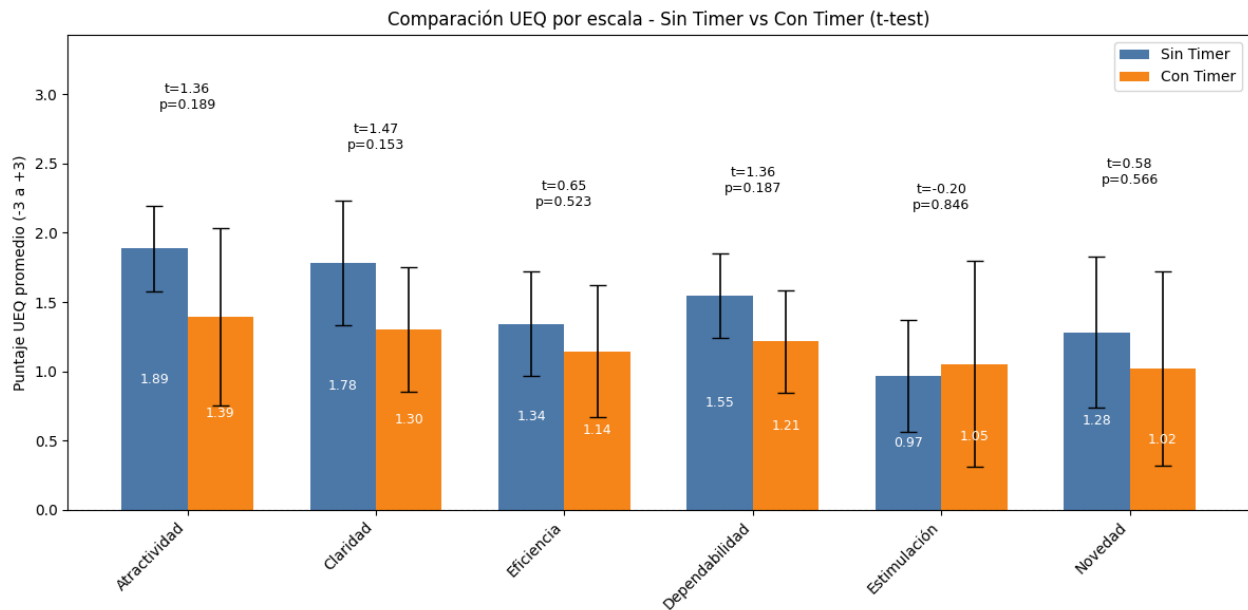


Figura 5.2: Gráfico de comparación de campos UEQ con t-test

Respuestas de Usabilidad de Sistema (SUS)

El puntaje promedio obtenido sin temporizador en la escala de Sistema de Usabilidad es de 83.3, mientras que con temporizador fue 76.4, indicando una diferencia de 6.9 puntos hacia el primero y que el videojuego es mejor en su usabilidad sin la presión del temporizador. Con un t-test, no se lograron obtener diferencias estadísticamente significativas con el promedio ($t = 1.61$, $p = 0.123$). Los datos obtenidos para la versión con temporizador muestran estar más dispersos que los de la versión sin temporizador, que se encuentra más consistente.

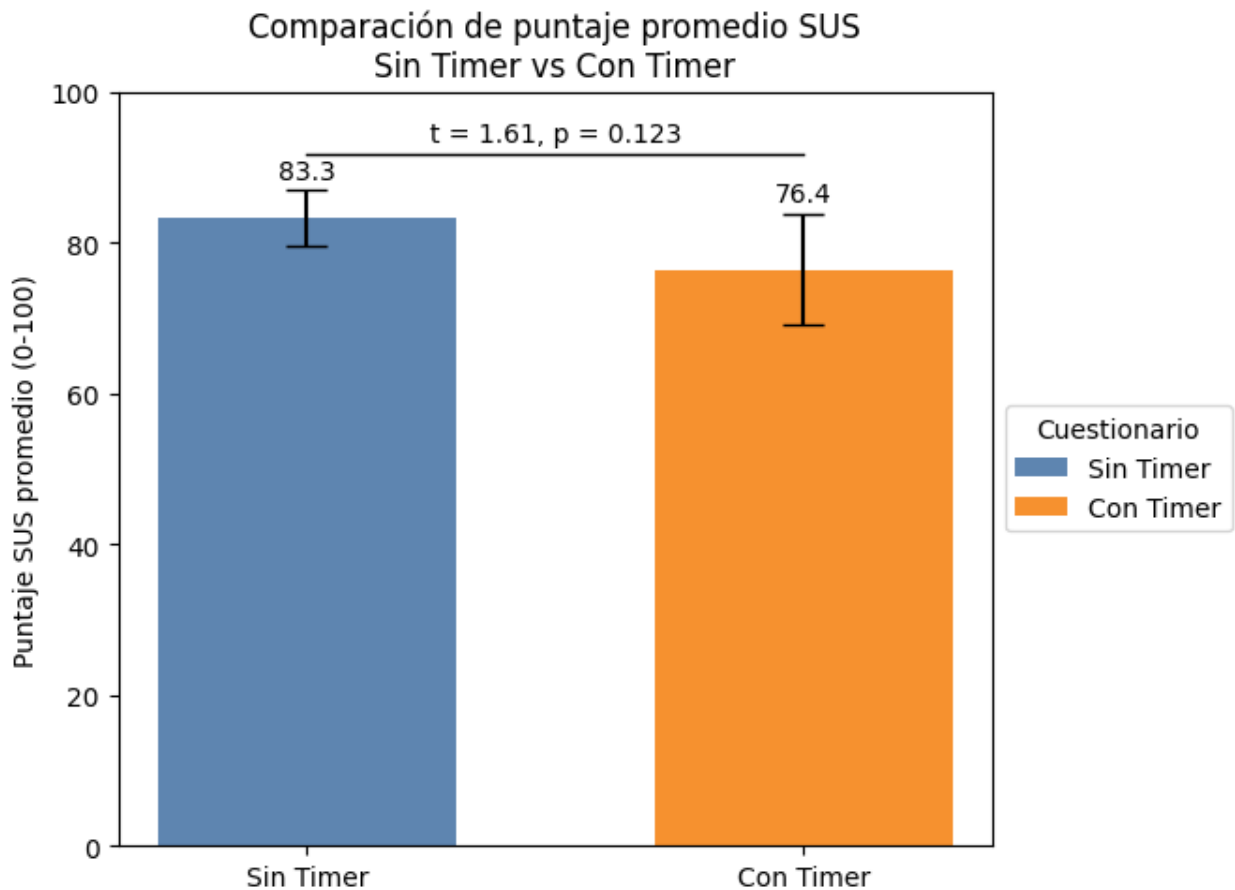


Figura 5.3: Gráfico de comparación de promedios SUS

Separando cada ítem de la prueba de usabilidad, se puede demostrar que la versión sin temporizador tiene una mejora significativa de puntajes respecto a la

versión con temporizador, tanto en los puntajes positivos como en los invertidos. El único ítem que posee un puntaje menor que en la versión con temporizador es el ítem 10, aprendizaje previo, por una diferencia ligera. Con un t-test, se pudo analizar que de los 10 ítems, solo el ítem 9 (confianza) muestra tener una diferencia estadística significativa ($t = 2.97$, $p = 0.009$), que está basado en la pregunta 'Me sentí seguro usando este sistema', que indica que en la versión sin temporizador, los usuarios se sintieron mucho más confiados en usar el sistema que aquellos usando la versión con temporizador.

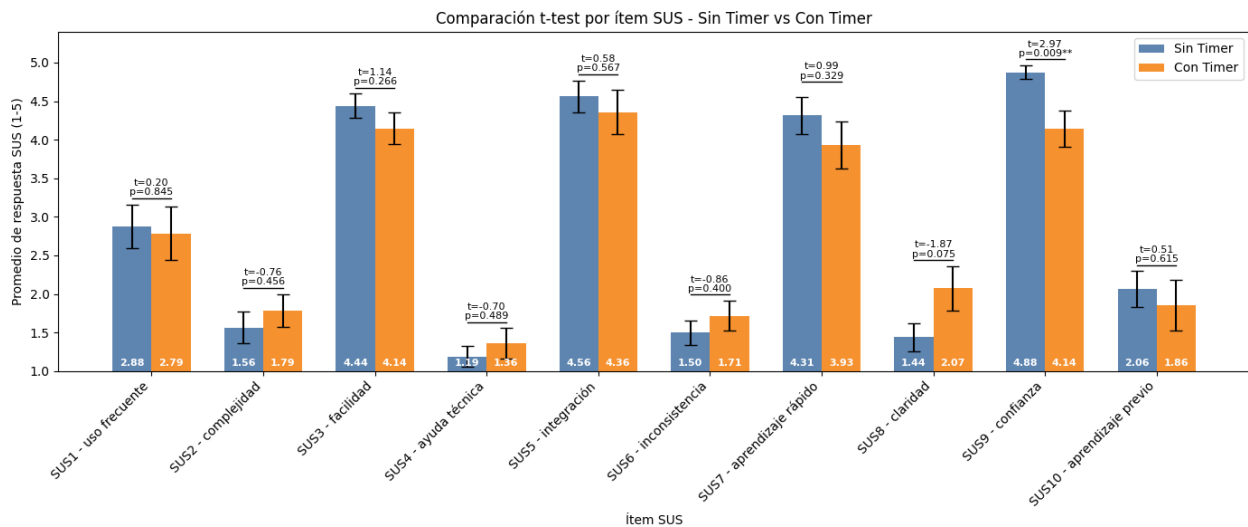


Figura 5.4: Gráfico de comparación de promedios SUS por ítem

Respuestas de Encuesta Propia

Dentro de las respuestas del cuestionario propio, no se encontraron datos generalmente relevantes que cambien la percepción de amenazas digitales o el comportamiento del usuario dentro del videojuego. Se puede asumir que el comportamiento de los jugadores dentro del juego se basó en sus respuestas en este cuestionario, identificando una mayor seguridad en las respuestas, haciendo que las respuestas sin temporizador sean en general más altas que aquellas con temporizador, excepto en el ítem 5, desconfianza de desconocidos ('Desconfío de correos de desconocidos').

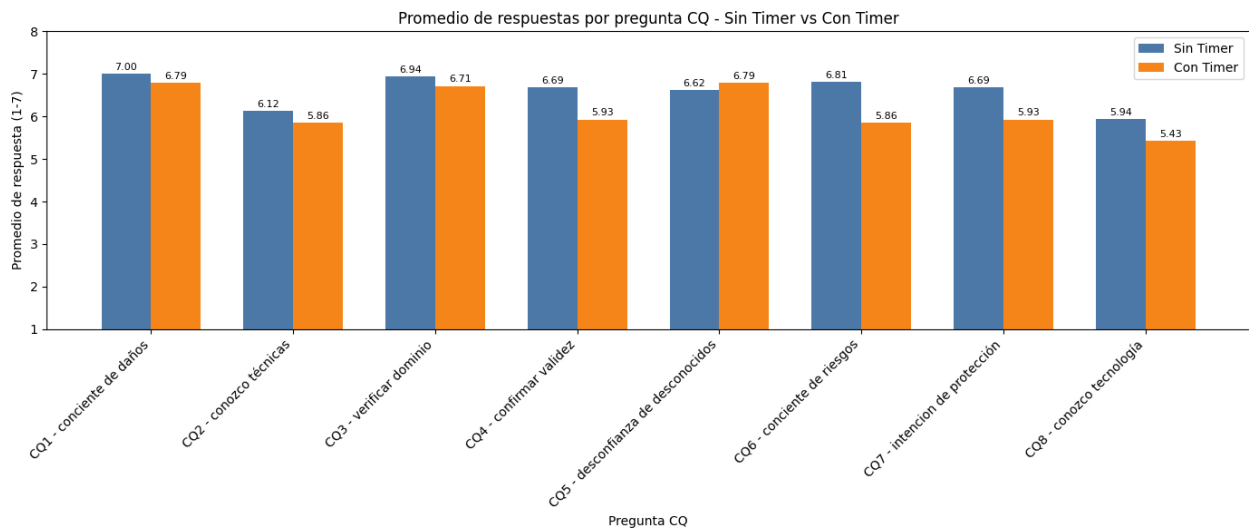


Figura 5.5: Gráfico de comparación de respuestas de Cuestionario Propio

Entre las respuestas abiertas obtenidas, ciertos datos y comentarios notables fueron:

- Varios usuarios valoraron que la experiencia es bastante cercana a la realidad y que se encuentra clara la identificación de correos maliciosos gracias a las instrucciones del manual.
- La experiencia fue percibida como más agradable sin temporizador, a diferencia de la con temporizador, donde se encontró más desafiante.
- El temporizador es un elemento controversial para la prueba, ya que se criticó su uso para forzar la obligación de responder más rápido, contradice el objetivo educativo y genera ansiedad para completar los objetivos.
- Se obtuvieron más comentarios acerca del foco de aprendizaje en la versión sin temporizador, indicando que el videojuego serviría para adultos mayores, niños y personas con pocos conocimientos computacionales, y que los correos son similares a situaciones reales. Con temporizador, se reconoce en menor medida por esta función.

- Las observaciones de usabilidad y funciones fueron similares entre las versiones, como diferenciar claramente entre Eliminar y Bloquear, mover o minimizar ventanas, y consultar el manual más fácilmente.
- Las sugerencias de contenidos fueron muy parecidas entre los grupos, en general, siendo acerca de nuevas ciberamenazas (malware, robo de cuentas, llamadas telefónicas fraudulentas), y también acerca de ideas sobre qué hacer después de cometer un error, como recuperar una cuenta, cambiar contraseñas o contactar soporte.

Discusión de Resultados

Ambas versiones del videojuego fueron percibidas positivamente por los participantes, obteniendo puntajes favorables tanto en experiencia de usuario (UEQ) como en usabilidad (SUS). No obstante, la versión sin temporizador presentó una tendencia consistente hacia mejores evaluaciones en la mayoría de las métricas analizadas.

En el UEQ, la versión sin temporizador obtuvo mayores puntajes promedio en casi todas las dimensiones, aunque las diferencias entre ambas versiones no fueron estadísticamente significativas. De forma similar, en la escala SUS alcanzó un puntaje promedio de 83.3 frente a 76.4 de la versión con temporizador, calificando positivamente en la escala SUS. Solo el ítem 9, 'confianza del sistema', se mostró estadísticamente relevante, por tener una mejora significativa en la versión sin temporizador.

Las respuestas abiertas respaldan estos resultados, describiendo la versión sin temporizador como una experiencia más relajada y adecuada para el aprendizaje, mientras que la versión con temporizador fue percibida como más desafiante debido a la presión del tiempo. Ambos grupos coincidieron además en sugerencias relacionadas con mejoras de interfaz y la incorporación de nuevos escenarios de ciberseguridad.

Los resultados cuantitativos y cualitativos muestran una tendencia consistente a favor de la **versión sin temporizador** como una experiencia mejor valorada por los usuarios, aunque las diferencias estadísticas entre ambas versiones fueron insuficientes.

6. Conclusión

Este proyecto ha permitido lograr la evaluación del videojuego 'CyberSafety', orientado a la concientización de la ciberseguridad, explorando cómo diferentes versiones afectan el producto y pueden influir en la experiencia del usuario y en la percepción de su calidad. A lo largo del proceso, el diseño y la producción del videojuego fueron hechos para proporcionar una experiencia inmersiva para las prácticas contra el phishing, cuya alza de ataques es la razón e idea general que dio origen a este videojuego. Para que este programa pueda otorgar la experiencia de un videojuego serio, el objetivo no es únicamente entretener, sino también fomentar la comprensión sobre las ciberamenazas, por lo cual la experiencia y el uso son vitales para definir y refinar.

Entre las pruebas con la versión con temporizador (Correos y niveles con duración limitada) y sin temporizador, los resultados generales del estudio, usando los cuestionarios UEQ, SUS y cuestionario propio, reflejan que favorece la versión sin temporizador, ya que una experiencia más pausada y libre de presión temporal otorga una mejor recepción del contenido, permitiendo a los usuarios interactuar de manera más reflexiva con las mecánicas propuestas. Esto sugiere que la usabilidad y la claridad de la interacción pueden ser más determinantes que la incorporación de elementos de estrés o desafío temporal, como el temporizador.

Sin embargo, la inclusión de mecanismos como temporizadores no es estrictamente negativa, sino que depende del contexto de aplicación, ya que los datos obtenidos no fueron estadísticamente significativos, con leves decrementos de puntaje general pero aún con una valoración buena por métricas del SUS y del UEQ. Este modo de juego puede aportar valor mayor cuando los jugadores están más experimentados y adaptados al sistema, en vez de tratar de adaptarlos al comienzo del juego, donde aún no reconocen la mayoría de las funciones y reglas.

En términos generales, se puede concluir que el videojuego desarrollado cumple con su propósito de concientización en ciberseguridad, con una experiencia de juego efectiva y como producto tecnológico evaluado para el progreso en futuras versiones. Este proyecto refuerza la importancia de iterar el diseño en función de la experiencia del usuario, priorizando el equilibrio entre jugabilidad, accesibilidad y objetivos del videojuego. A partir de la retroalimentación de los usuarios por respuestas de la encuesta propia, también se pudo confirmar que pudieron identificar los correos maliciosos de los normales.

Finalmente, gracias a varios comentarios obtenidos de la encuesta propia, este trabajo posee múltiples futuras mejoras orientadas a expandir el contenido acerca de ciberamenazas (virus, llamadas fraudulentas), diversificar escenarios de ciberseguridad (restablecer contraseñas, recuperar cuenta) y ajustar progresivamente la dificultad, con el fin de mejorar la experiencia e inmersión para un público objetivo que podría beneficiarse de una herramienta interactiva en formato de un videojuego serio, como adultos mayores y niños.

Glosario

Ciberseguridad: Se refiere a todas las tecnologías, prácticas y políticas para prevenir los ciberataques o mitigar su impacto, y tiene como objetivo proteger los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra el ransomware y otros malware, las estafas de phishing, el robo de datos y otras ciberamenazas.

Ciberataques: Cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital.

Phishing: Una táctica de ciberdelincuencia (actos criminales por dispositivos electrónicos) en la que los atacantes engañan a las personas para que revelen información confidencial (por ejemplo, contraseñas, datos bancarios) a través de correos electrónicos, mensajes o sitios web engañosos.

Spoofing: Es cuando alguien o algo se hace pasar por otra cosa en un intento de ganarse la confianza del usuario para obtener acceso a sus sistemas, robar datos, robar dinero o propagar malware. Los ataques de suplantación de identidad pueden adoptar muchas formas, como suplantación de correos electrónicos, sitios web, mensajes, llamadas, etc.

Malware: También llamado “software malicioso”, es un término abarcador que describe cualquier programa o código malicioso que es dañino para los sistemas. Este busca invadir, dañar o deshabilitar computadoras, sistemas informáticos, redes, tabletas y dispositivos móviles, a menudo controlando parcialmente las operaciones de un dispositivo, robar sus datos e interfiriendo con el funcionamiento normal.

Ransomware: Es un tipo de malware que retiene como rehenes los datos confidenciales o el dispositivo de una víctima, amenazando con mantenerlos bloqueados, eliminarlos o divulgarlos, a menos que la víctima pague un rescate en forma monetaria al atacante.

STRIDE: Es una taxonomía creada por Microsoft[28] que cubre las amenazas de ciberseguridad descritas por su acrónimo:

Spoofing: Falsificación de credenciales de usuario.

Tampering: Manipulación, modificación maligna de información.

Repudiation: Repudio, acciones negadas de un usuario el cual no se pueden comprobar por otras entidades.

Information Disclosure: Divulgación de información, información accedida por usuarios que no deben tener autorización para ello.

Denial of Service: DoS, Denegación de servicio, ataques de denegación de servicio impiden a usuarios autorizados a ocupar el sistema.

Elevation of Privilege: Elevación de privilegios, usuarios que se han vuelto autorizados más allá de las defensas del sistema.

Bibliografía

- [1] S. Lythreathis, S. K. Singh, and A.-N. El-Kassar, “The digital divide: A review and future research agenda,” *Technological Forecasting and Social Change*, vol. 175, p. 121359, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0040162521007903>
- [2] Z. M. Hakim, N. C. Ebner, D. S. Oliveira, S. J. Getz, B. E. Levin, T. Lin, K. Lloyd, V. T. Lai, M. D. Grilli, and R. C. Wilson, “The phishing email suspicion test (pest) a lab-based task for evaluating the cognitive mechanisms of phishing detection,” *Behavior research methods*, vol. 53, no. 3, pp. 1342–1352, 2021. [Online]. Available: <https://link.springer.com/article/10.3758/s13428-020-01495-0>
- [3] C. Y. Ng and M. K. B. Hasan, “Cybersecurity serious games development: A systematic review,” *Computers Security*, vol. 150, 2025. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404824006138>
- [4] Entel, “Reporte ciberseguridad 5ta edición,” p. 104, 2025, accedido: 19-08-2025. [Online]. Available: https://enteldigital.cl/hubfs/ebooks/ciberseguridad/2025/Entel_Digital_Reporte_Ciberseguridad_2025_.pdf
- [5] Kaspersky. (2023) Nueva epidemia: el phishing se sextuplicó en américa latina con el reinicio de la actividad económica y el apoyo de la ia. Accedido: 19-08-2025. [Online]. Available: <https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/>
- [6] M. D. Weiser, “Ubiquitous computing,” pp. 197 530–197 680, 1994. [Online]. Available: <https://ieeexplore.ieee.org/iel4/4236/14762/x0086424.pdf>

- [7] CADEM, “Estudio décima encuesta sobre acceso, usos y usuarios de internet en Chile,” p. 41, 2023, accedido: 19-08-2025. [Online]. Available: https://www.subtel.gob.cl/wp-content/uploads/2024/03/Informe.Final.Acceso_y_uso.Internet.2023_VF.pdf
- [8] M. del Interior y Seguridad Pública (Chile). (2017) Política nacional de ciberseguridad 2017-2022. Accedido: 2025-10-20. [Online]. Available: <https://generoyparticipacion.interior.gob.cl/media/2023/02/Politica-Nacional-Ciberseguridad-2018-2022.pdf>
- [9] P. de la República de Chile. (2018) Instructivo presidencial n°8 del 23 de octubre de 2018 sobre ciberseguridad. Accedido: 2025-10-20. [Online]. Available: <https://digital.gob.cl/biblioteca/regulacion/instructivo-presidencial-no8-ciberseguridad/>
- [10] N. Jara Fuentealba and A. Jorquera Cruz, “La responsabilidad de la Administración del Estado por incidentes de ciberseguridad,” *Revista chilena de derecho y tecnología*, vol. 10, pp. 201 – 230, 06 2021. [Online]. Available: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842021000100201&nrm=iso
- [11] S. de la República de Chile. (2025) Hackeo a clave Única: demandan esclarecimiento de las circunstancias del ataque y sanciones a los responsables. Accedido: 2025-10-20. [Online]. Available: <https://www.senado.cl/comunicaciones/noticias/hackeo-clave-unica-demandan-esclarecimiento-de-las-circunstancias-del>
- [12] D. Branley-Bell, L. Coventry, M. Dixon, A. Joinson, and P. Briggs, “Exploring age and gender differences in ict cybersecurity behaviour,” *Human Behavior and Emerging Technologies*, vol. 2022, no. 1, p. 2693080, 2022. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/2693080>
- [13] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, “Don’t click: towards an effective anti-phishing training. a comparative literature review,” *Human-centric Computing and Information Sciences*, vol. 10, no. 1, p. 33, 2020. [Online]. Available: <https://link.springer.com/article/10.1186/s13673-020-00237-7>
- [14] F. G. Weijssenfeld and D. K. Sarmah, “Gamifying cybersecurity: A narrative-driven approach to teaching steganography,” *Computers and Education Open*, vol. 9, p. 100288, 2025. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2666557325000473>

- [15] R. Gallardo Vergara and M. M. Gallardo, “Serious games to improve attention in boys and girls with attention deficit hyperactivity disorder (adhd): A pilot study,” *Acta Colombiana de Psicología*, vol. 26, no. 2, pp. 33–49, 2023.
- [16] B. J. Oates, R. McLean, and M. Griffiths, “Researching information systems and computing,” 2022.
- [17] A. Hevner and S. Chatterjee, *Design research in information systems: theory and practice*. Springer Science & Business Media, 2010, vol. 22.
- [18] J. L. Rogers, K. I. Howard, and J. T. Vessey, “Using significance tests to evaluate equivalence between two experimental groups.” *Psychological bulletin*, vol. 113, no. 3, p. 553, 1993.
- [19] P. Abrahamsson, O. Salo, J. Ronkainen, and J. Warsta, “Agile software development methods: Review and analysis,” 2017. [Online]. Available: <https://arxiv.org/abs/1709.08439>
- [20] S. Al-Saqqa, S. Sawalha, and H. AbdelNabi, “Agile software development: Methodologies and trends.” *International Journal of Interactive Mobile Technologies*, vol. 14, no. 11, 2020.
- [21] A. A. Adenowo and B. A. Adenowo, “Software engineering methodologies: a review of the waterfall model and object-oriented approach,” *International Journal of Scientific & Engineering Research*, vol. 4, no. 7, pp. 427–434, 2013.
- [22] M. M. Pithon, “Importance of the control group in scientific research,” *Dental Press Journal of Orthodontics*, vol. 18, pp. 13–14, 2013.
- [23] J. Brooke, “Sus: a retrospective.” *Journal of usability studies*, vol. 8, no. 2, 2013.
- [24] B. Laugwitz, T. Held, and M. Schrepp, “Construction and evaluation of a user experience questionnaire,” in *Symposium of the Austrian HCI and usability engineering group*. Springer, 2008, pp. 63–76.
- [25] T. K. Kim, “T test as a parametric statistic,” *Korean journal of anesthesiology*, vol. 68, no. 6, pp. 540–546, 2015.

- [26] B. Kim, “Game mechanics, dynamics, and aesthetics,” *Library technology reports*, vol. 51, no. 2, pp. 17–19, 2015.
- [27] P. A. Wang, “Assessment of cybersecurity knowledge and behavior: an anti-phishing scenario,” in *Proc. IEEE Int. Conf. Internet Monitor. Protection (ICIMP)*, 2013, pp. 1–7.
- [28] Q. Rouland, B. Hamid, and J. Jaskolka, “Specification, detection, and treatment of stride threats for software components: Modeling, formal methods, and tool support,” *Journal of Systems Architecture*, vol. 117, p. 102073, 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1383762121000631>
- [29] M. Alanazi, M. Freeman, and H. Tootell, “Exploring the factors that influence the cybersecurity behaviors of young adults,” *Computers in Human Behavior*, vol. 136, p. 107376, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0747563222001984>
- [30] K. S., “Impact of cybersecurity self-efficacy on digital economic behaviors among older adults,” *INQUIRY: The Journal of Health Care Organization, Provision, and Financing*, p. 62, 2025. [Online]. Available: <https://journals.sagepub.com/doi/10.1177/00469580251370933>
- [31] V. Business. (2025) 2025 data breach investigations report (executive summary). Accedido: 2025-10-20. [Online]. Available: <https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf>
- [32] S. Hart, A. Margheri, F. Paci, and V. Sassone, “Riskio: A serious game for cyber security awareness and education,” *Computers Security*, vol. 95, p. 101827, 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404820301012>
- [33] T. Denning, A. Lerner, A. Shostack, and T. Kohno, “Control-alt-hack: the design and evaluation of a card game for computer security awareness and education,” in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS ’13. New York, NY, USA: Association for Computing Machinery, 2013, p. 915–928. [Online]. Available: <https://doi.org/10.1145/2508859.2516753>

- [34] T. Chen, M. Stewart, Z. Bai, E. Chen, L. Dabbish, and J. Hammer, “Hacked time: Design and evaluation of a self-efficacy based cybersecurity game,” in *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, ser. DIS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1737–1749. [Online]. Available: <https://doi.org/10.1145/3357236.3395522>

7. Apéndice

7.1. Detalles de usuarios vulnerables

- **Adolescentes o jóvenes:** Usuarios jóvenes (16-19 años) que recién se integran al mundo digital. Poseen habilidades básicas en el uso de dispositivos y navegación en internet, pero suelen carecer de una formación sólida en prácticas de ciberseguridad. Su curiosidad, confianza excesiva y búsqueda de interacción en redes sociales los vuelven especialmente vulnerables a engaños, suplantaciones o manipulación emocional por parte de atacantes que buscan obtener su información personal.

También tienden a utilizar contraseñas simples y a descargar software o videojuegos desde sitios no seguros, exponiéndose a malware o virus informáticos. Aunque representan un público vulnerable, su edad y capacidad de aprendizaje rápido los convierten en un grupo idóneo para programas de educación preventiva en ciberseguridad, donde la simulación y el aprendizaje interactivo pueden generar una conciencia más duradera [29].

- **Adultos mayores:** Los adultos mayores (65+ años) han debido adaptarse a un entorno digital que cambió drásticamente en comparación con su experiencia previa. Esta brecha tecnológica, junto con el uso de equipos obsoletos y la falta de formación digital, aumenta su susceptibilidad a fraudes en línea. Tienden a confiar en mensajes formales o que aparentan provenir de instituciones legítimas, lo cual los hace vulnerables a ataques de phishing y estafas telefónicas.

Además, suelen ser objetivos frecuentes por razones financieras, dado que poseen ahorros o pensiones que los atacantes buscan explotar. Si bien algunos pueden evitar riesgos al usar menos tecnología, esto no implica mayor conocimiento en ciberseguridad, sino una menor exposición a ciertos vectores de ataque digitales. La falta de entrenamiento práctico y la dificultad para asimilar nuevas herramientas refuerzan la necesidad de estrategias de aprendizaje simples, visuales e interactivas [30].

- **Empleados de Instituciones y Organizaciones:** Los empleados de empresas, bancos, hospitales o entidades gubernamentales se enfrentan a un tipo de amenaza distinta: ataques dirigidos por su rol y acceso a información sensible. Los atacantes emplean principalmente phishing corporativo e ingeniería social, personalizando mensajes para engañar a los trabajadores y obtener credenciales o acceso a redes internas. En este contexto, el error humano sigue siendo el eslabón más débil de la cadena de seguridad, incluso en instituciones con infraestructura robusta.

Aunque muchas organizaciones ofrecen charlas o capacitaciones, estas suelen ser teóricas y poco efectivas para modificar conductas. La ausencia de simulaciones o experiencias prácticas reduce la capacidad de los empleados para reaccionar ante ataques reales. Por ello, los métodos de aprendizaje basados en juegos o simulaciones pueden aumentar la conciencia y preparación frente a ciberataques en entornos laborales [31].

7.2. Juegos de Ciberseguridad

Para evaluar los proyectos hechos, se mostrarán varios otros juegos de ciberseguridad ya existentes. No es limitado a solo videojuegos, ya que existen juegos de tablero con el mismo propósito de enseñar seguridad, a diferentes niveles y rangos de comprensión. Se consideran sus ventajas y limitaciones al momento de su análisis.

7.2.1. Riskio

Riskio (2020-2021), desarrollado por la *Universidad de Southampton*, es un juego de mesa colaborativo para 3 a 5 jugadores y un Game Master, diseñado como herramienta educativa para identificar vulnerabilidades digitales y proponer defensas

adecuadas. Utiliza tableros, mazos de ataque y defensa, y el modelo STRIDE de Microsoft para categorizar amenazas como spoofing, tampering o denial of service. Los jugadores asumen roles dentro de una oficina simulada, alternando entre atacante y defensor, mientras el Game Master evalúa sus respuestas y orienta el aprendizaje. El juego busca fortalecer el pensamiento crítico y la conciencia sobre ciberamenazas mediante la interacción directa y la cooperación [32].

Su estructura simple y adaptable lo convierte en una herramienta valiosa para entrenamientos corporativos o académicos, permitiendo conectar la teoría con la práctica en entornos controlados y colaborativos. Aunque se destaca por su interacción y enfoque participativo, su efectividad depende de contar con un facilitador experto en ciberseguridad y jugadores con conocimientos previos sobre el tema. Esto limita su aplicación para públicos generales sin formación técnica, además de que su público objetivo es bastante limitado por la accesibilidad por conocimiento tecnológico.

7.2.2. Control-Alt-Hack

Control-Alt-Hack (2012-2013), creado por el laboratorio de investigación en seguridad y privacidad de la *Universidad de Washington*, es un juego de cartas para 3 a 6 jugadores que introduce conceptos de ciberseguridad desde un enfoque lúdico. Los participantes interpretan a “hackers de sombrero blanco” que realizan misiones de auditoría o pruebas de intrusión para avanzar y convertirse en el CEO de su propia empresa tecnológica. El juego combina atraktividad, competitividad y narrativa ligera para generar conciencia sobre seguridad digital sin requerir experiencia técnica, apuntando a jóvenes y público general [33].

A diferencia de otros juegos más técnicos, Control-Alt-Hack no busca enseñar habilidades prácticas o metodologías de defensa, sino sensibilizar a los jugadores sobre los riesgos y dilemas éticos en el mundo digital. Por ello, se le considera más un juego con temática de ciberseguridad y por lo tanto, *no es un Serious Game*. Su valor reside en despertar interés y conversación sobre seguridad informática, aunque su falta de entrenamiento interactivo limita su impacto en el desarrollo de competencias reales.

7.2.3. Hacked Time

Hacked Time (2020), desarrollado por la *Universidad de Carnegie* en Eindhoven, es un videojuego tipo puzzle/novela visual donde el jugador, en el rol de un detective temporal, ayuda a un estudiante a corregir malas prácticas de seguridad digital. A través de decisiones narrativas, diálogos y exploración, el jugador aprende sobre contraseñas seguras, autenticación en dos pasos y gestores de contraseñas. Basado en la Teoría de la Autoeficacia de Bandura, el juego busca fortalecer la confianza de los usuarios en su capacidad para aplicar hábitos de ciberseguridad, combinando exposición a riesgos, desarrollo de habilidades y práctica guiada [34].

Este videojuego está vinculado a un estudio experimental, realizado con 178 participantes, donde mostró mejoras significativas en la autoeficacia y la actitud hacia la ciberseguridad frente a grupos que solo leyeron información o no recibieron entrenamiento. Sin embargo, el juego no logró modificar la percepción de riesgo ni medir cambios de comportamiento a largo plazo. Sus resultados evidencian beneficios a corto plazo y refuerzan el valor de los videojuegos narrativos como herramientas educativas, aunque también la necesidad de evaluaciones longitudinales que midan el impacto sostenido en la conducta digital.

7.2.4. Tabla Comparativa de Juegos de Ciberseguridad

Tabla 7.1: Comparativa de Videojuegos enfocados en la enseñanza de Ciberseguridad

Nombre de Videojuego	Descripción	Año	Instituciones / Autores	Amenazas abordadas	Metodología / Mecánicas	Limitaciones
Riskio	Juego de mesa de múltiples jugadores y un Game Master, jugando cartas y explicando cómo tratan de sabotear o proteger ante una ciberamenaza para obtener puntos.	2020	University of Southampton	Spoofing, Manipulación, Repudio, Divulgación de información, Denegación de servicios (DoS), Elevación de privilegios.	Taxonomía STRIDE. Argumentación de ataque y defensa de ciberseguridad	Requiere un tutorial de taxonomía STRIDE. Público limitado a usuarios técnicos, empleados o universitarios.
Control-Alt-Hack	Juego de mesa de cartas donde los jugadores hackean por misiones técnicas para convertirse en CEOs de su propia compañía digital.	2012 – 2013	University of Washington; Tamara Denning, Tadayoshi Kohno, Adam Shostack.	Reconocimiento de terminología y concientización sobre ciberseguridad.	Diseño recreacional. Roles y uso de habilidades con términos de ciberseguridad.	Solo aborda la temática de forma lúdica sin aplicación real. Público objetivo con poca experiencia en informática.
Hacked Time	Videojuego de computador tipo novela interactiva y puzzle, donde el jugador, como detective viajero en el tiempo, ayuda a un estudiante a prevenir un ciberataque aplicando prácticas de ciberseguridad.	2020	Carnegie Mellon University; Tianying Chen, Margot Stewart, Zhiyu Bai, Eileen Chen, Laura Dabbish, Jessica Hammer.	Autoeficacia con la ciberseguridad, contraseñas débiles, almacenamiento inseguro de credenciales, y riesgos de brechas de información.	Teoría de autoeficacia de Bandura (información de riesgo, desarrollo de habilidades, práctica guiada). Exploración, diálogos, puzzles y simulación.	Cubre solo manejo de cuentas a corto plazo. Mide percepciones, no conductas reales. Impacto a largo plazo no comprobado.

7.3. Tablas de Diseño

7.3.1. Tablas de Correos electrónicos

Atributo	Descripción
Nombre o asunto del correo	Texto que representa el título del correo electrónico.
Dirección del receptor	Dirección de correo electrónico de quien recibe el mensaje (Usualmente el mismo correo).
Dirección del remitente	Dirección de correo electrónico del emisor del mensaje.
Contenido del mensaje	Cuerpo del correo, donde se presenta la información principal. Esta información puede poseer links que son maliciosos.
Respuesta Prehecha	La respuesta para el correo cuando se responde.
Etiquetas (tags)	Identificadores que representan características específicas del correo.
Clasificación interna	Categoría del correo: malicioso, spam o legítimo.
Nivel mínimo de aparición	En qué nivel empieza a aparecer y en niveles subsiguientes.

Tabla 7.2: Atributos de los correos electrónicos

Tipo de Correo	Descripción	Acciones	Puntaje
Correo legítimo	Correo válido sin intención maliciosa. No posee rasgos maliciosos.	Correcto: Responder Incorrecto: Reportar (cualquiera)	Correcto: +1 Incorrecto: -1
Correo malicioso	Correo con intención dañina o fraudulenta. Posee uno o múltiples rasgos maliciosos.	Correcto: Eliminar Incorrecto: Responder o hacer click en un link	Correcto: +1 Incorrecto: -1 Otra acción: 0
Phishing persistente	Variante de correo malicioso que continúa apareciendo hasta ser bloqueado.	Correcto: Bloquear Incorrecto: Responder o hacer click en un link	Correcto: +1 Incorrecto: -1 Otra acción: 0
Spam	Correo no malicioso que actúa como obstáculo. Aumenta si no se marca como Spam.	Correcto: Enviar a spam	No otorga puntos ni contribuye a objetivos

Tabla 7.3: Tipos de correos electrónicos

7.3.2. Tablas de Estructura de Niveles

Elemento	Descripción
Mensaje inicial	Mensaje introductorio que entrega contexto sobre el nivel, el estado del jugador u otros elementos relevantes.
Objetivos	Lista de tareas necesarias para completar el nivel, como reportar o responder una cantidad específica de correos.
Cantidad de correos	El conjunto de correos legítimos y maliciosos que son usados para este nivel, obtenidos de la base de datos de forma aleatoria. Cada tipo tiene un mínimo igual al requerido por los objetivos, pudiendo excederlo.
Modificadores del nivel	Variaciones o mecánicas únicas, como la inclusión de correos de phishing persistente o spam, u otras condiciones especiales.
Puntaje mínimo	El puntaje requerido para completar el nivel exitosamente y desbloquear el siguiente. Debe ser igual o superior.

Tabla 7.4: Estructura y atributos de los niveles del videojuego

Nivel	Descripción	Correos	Objetivos	Puntaje mínimo
1	Introducción al sistema de correos y mecánicas básicas. Si no se ha iniciado el Tutorial antes, se inicia aquí.	4–5 correos legítimos 3–4 correos maliciosos	Responde 3 correos Reporta 2 correos (Modo Temporizador): Termina el nivel dentro de 5 minutos	4
2	Mayor cantidad de correos y primera variación de correos maliciosos: Correos phishings persistente y como Bloquear estos correos.	4–5 correos legítimos 4–6 correos maliciosos	Responde 4 correos Reporta 3 correos (Modo Temporizador): Termina el nivel dentro de 4:30 minutos	6
3	Cantidad de correos aumentada con incorporación de spam y reportar como 'Marcar como Spam'. Se incluye mecánicas anteriores.	5–7 correos legítimos 6–8 correos maliciosos 3–4 correos spam	Responde 3 correos Reporta 5 correos (Modo Temporizador): Termina el nivel dentro de 4 minutos	8

Tabla 7.5: Datos de los Niveles

7.3.3. Tablas de Sistema de Correos y Puntaje

Acción	Descripción	Resultado en el sistema
Reportar	Botón con un signo de advertencia que abre el panel de reportes, permitiendo clasificar el correo según su tipo.	Permite usar acciones de reporte para registrar los correos maliciosos.
Responder	Permite escribir automáticamente y enviar una respuesta predefinida al correo.	El correo se considera respondido y se elimina del listado tras enviar la respuesta.
Eliminar	Parte del panel de reportes. Elimina el correo sin interactuar con su contenido.	El correo se considera reportado y eliminado del listado.
Bloquear	Parte del panel de reportes. Se desbloquea cuando hay correos phishing persistente. Elimina el correo y bloquea que el mismo remitente envíe más mensajes a tu correo.	El correo se considera reportado, eliminado del listado, y correos con el mismo nombre de remitente no podrán enviar más correos.
Marcar como Spam	Parte del panel de reportes. Se desbloquea cuando hay correos spam. Elimina el correo y lo envía a una bandeja de spam.	El correo se considera reportado, eliminado del listado, y enviado a Spam. Correos similares se consideran spam, reduciendo la probabilidad de recibir spam.
Link Malicioso	Puede aparecer en el contenido de un correo malicioso. Un enlace de texto con color diferente que llama la atención.	Se considera como acción incorrecta y se quita el correo del sistema.
Expirar	En el modo Temporizador, cuando la duración de un correo expira, se elimina por sí mismo.	Es una acción incorrecta (Si no es Spam) y se quita el correo del sistema.

Tabla 7.6: Acciones en el sistema de correos

Acción realizada	Puntaje
Responder un correo legítimo	+1 punto
Eliminar un correo malicioso (No phishing persistente)	+1 punto
Bloquear un correo phishing persistente	+1 punto
Hacer click en un link malicioso	-1 punto
Dejar que un correo no Spam expire (Modo Temporizador)	-1 punto
Realizar una acción incorrecta (Responder un correo malicioso, reportar un correo legítimo)	-1 punto
Otras acciones (Eliminar correo phishing persistente)	No otorga puntos
Cualquier acción con correos Spam	No otorga puntos ni contribuye a objetivos

Tabla 7.7: Reglas del sistema de puntaje

7.3.4. Tablas de Sistema de Objetivos

Tipo de objetivo	Descripción
Responder correos	El jugador debe responder una cantidad determinada de correos.
Reportar correos	El jugador debe reportar una cantidad determinada de correos. Esto incluye eliminar y bloquear. No incluye marcar como Spam.
Eliminar correos	El jugador debe eliminar una cantidad determinada de correos.
Bloquear correos	El jugador debe bloquear una cantidad determinada de correos.
Tiempo límite	Establece un tiempo máximo para completar el nivel y sus objetivos. Solo disponible cuando el modo Temporizador está activo.

Tabla 7.8: Tipos de Objetivos

Condición	Resultado
Objetivos completados	Se habilita la opción de finalización manual del nivel
Cumple todos los objetivos y mantiene un puntaje igual o superior al requerido	Nivel completado exitosamente
Cumple objetivos pero posee puntaje insuficiente o acciones incorrectas	Nivel finaliza en fallo
No cumple los objetivos dentro del tiempo límite (Modo Temporizador)	Nivel finaliza inmediatamente (Completado o fallo, dependiendo del puntaje obtenido)

Tabla 7.9: Condiciones de Finalización del Nivel

7.3.5. Tablas de Sistema del Manual

Criterio	Descripción
Solicitud de información personal	El correo solicita datos sensibles como contraseñas, información bancaria u otros datos personales.
Solicitudes urgentes	El mensaje utiliza lenguaje que presiona al usuario a actuar rápidamente, reduciendo su capacidad de análisis.
Presencia de enlaces externos desconocidos	El correo contiene enlaces/links de carácter sospechoso o no claro para extraer información. Dentro del juego, quita 1 punto.
Alertas de seguridad o amenazas	Se presentan advertencias alarmantes (como bloqueos de cuenta o accesos no autorizados) para inducir una reacción inmediata.
Archivos adjuntos desconocidos	Incluye archivos cuyo origen no es claro y que pueden contener software malicioso cuando se descargan.
Direcciones de correo sospechosas	El remitente presenta inconsistencias, errores o dominios poco confiables que no coinciden con entidades legítimas.

Tabla 7.10: Criterios para la identificación de Correos Maliciosos

7.3.6. Tablas de Temporizadores

Tipo de temporizador	Duración	Descripción y comportamiento
Temporizador de nivel	3 a 5 minutos	Ubicado en la parte inferior derecha de la pantalla. Limita el tiempo para completar el nivel. Comienza una vez que el jugador entra a un nivel. Si el tiempo se agota, el nivel finaliza inmediatamente.
Temporizador de correos	20 a 40 segundos por correo	Cada correo tiene un temporizador individual representado por un círculo de color verde al lado de su nombre en la lista de correos. Este indicador pierde segmentos progresivamente y vuelve más rojo, mostrando el tiempo restante. Al expirar, el correo se elimina automáticamente, y si no es spam, quita 1 punto.

Tabla 7.11: Rasgos del Modo Temporizador

7.3.7. Tablas de Dinámicas

Elemento de Interacción	Forma de Interacción	Efecto y retroalimentación
Botón de Acceso a Correos, Tareas y Manual	Abre o cierra las ventanas de correos, tareas o manual mediante un botón ubicado en el escritorio.	Muestra u oculta la interfaz correspondiente y reproduce un sonido.
Lista de Correos	Permite seleccionar un correo desde la lista de la ventana de correos.	Muestra u oculta el contenido del correo seleccionado y reproduce un sonido.
Botones de Acción	Ejecutan acciones sobre el correo (Responder, Eliminar, Bloquear o Marcar como Spam).	Eliminan el correo, actualizan los objetivos, registran la acción y reproducen un sonido.
Panel de Reportes	Despliega u oculta las opciones de reporte del correo.	Muestra u oculta el panel y reproduce un sonido.
Botones de Responder	Envían una respuesta predefinida y luego ejecutan la acción correspondiente sobre el correo.	Escriben y envían la respuesta automáticamente, eliminan el correo y actualizan los objetivos.
Botón de Finalización de Nivel	Permite finalizar el nivel cuando se cumplen los objetivos o no quedan correos pendientes. Cambia de color según su disponibilidad.	Si está bloqueado reproduce un sonido de error; de lo contrario, abre la pantalla de resultados y reproduce un sonido.
Indicadores de Temporizador	En el modo Temporizador muestran el tiempo restante del nivel y de cada correo.	Se actualizan automáticamente hasta procesar el correo o finalizar el nivel.

Tabla 7.12: Dinámicas de interacción del jugador con la interfaz del sistema

Dinámica de Comportamiento	Descripción	Impacto en el jugador
Toma de decisiones	El jugador evalúa la información de cada correo para clasificarlo como legítimo o malicioso antes de ejecutar una acción.	Fomenta el análisis crítico y la toma de decisiones informadas.
Reconocimiento de patrones	El jugador identifica características recurrentes en correos maliciosos a través de la repetición y experiencia.	Facilita la detección rápida y mejora el desempeño con el tiempo.
Aprendizaje progresivo	El sistema juega a base de prueba y error, donde los errores afectan el puntaje y motivan la revisión del manual, además de agregar contenido nuevo a medida que se progresa.	Refuerza la comprensión y adaptación a nuevas situaciones.
Gestión del tiempo y presión	La presencia de límites de tiempo obliga al jugador a tomar decisiones más rápidas.	Introduce presión que puede afectar la precisión y exige equilibrio entre velocidad y análisis.
Priorización de tareas	El jugador decide qué correos atender primero cuando existen múltiples disponibles o con temporizadores.	Desarrolla habilidades de organización y toma de decisiones bajo múltiples estímulos.
Atención selectiva	El jugador se enfoca en elementos clave del correo, ignorando información irrelevante o distracciones.	Mejora la capacidad de filtrar información y detectar intentos de engaño.
Consulta de información de apoyo	El jugador recurre al manual para verificar criterios o resolver dudas durante el juego.	Refuerza el aprendizaje y reduce la incertidumbre en la toma de decisiones.

Tabla 7.13: Dinámicas de comportamiento del jugador

7.4. Diagramas de Diseño

7.4.1. Diagrama de Interfaz Principal

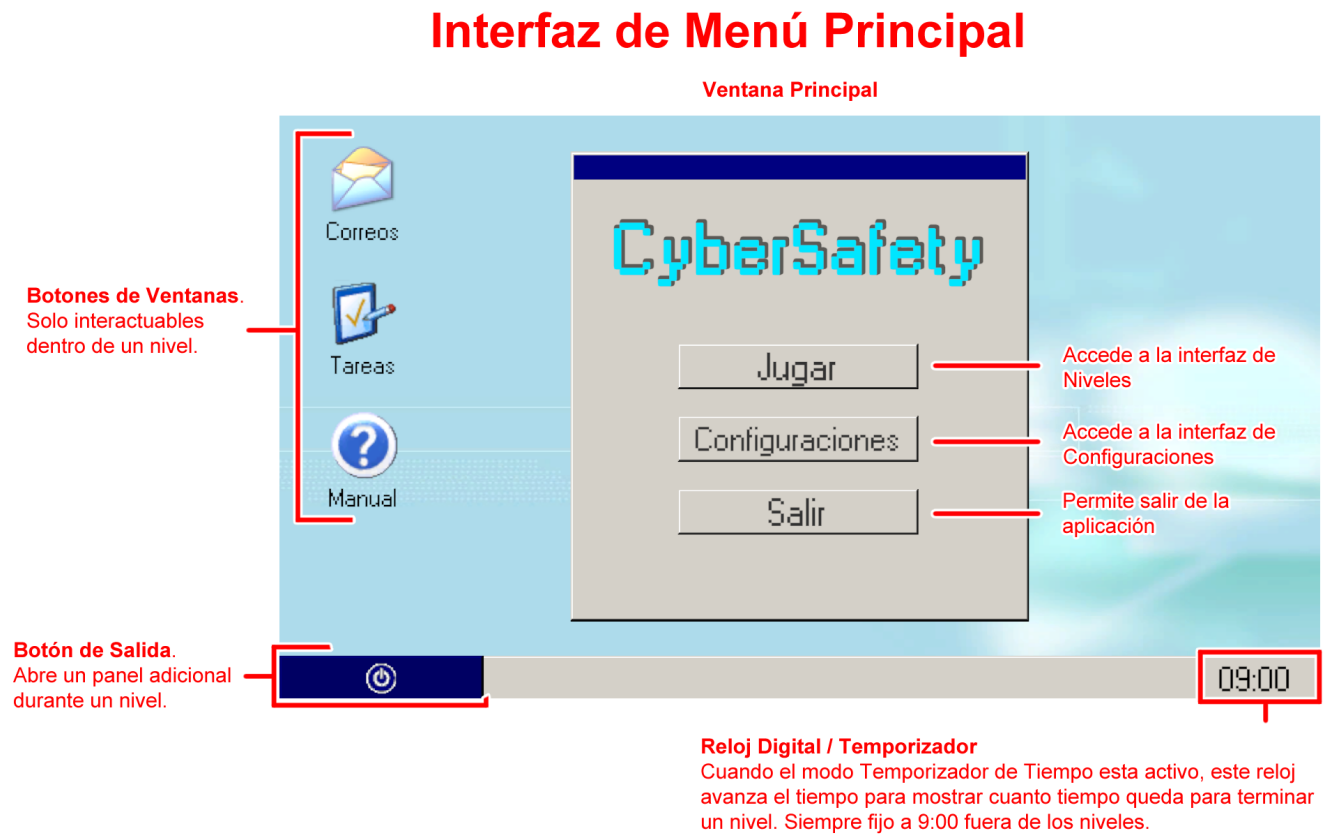


Figura 7.1: Diagrama de Interfaz Principal

7.4.2. Diagrama de Interfaz de Configuraciones

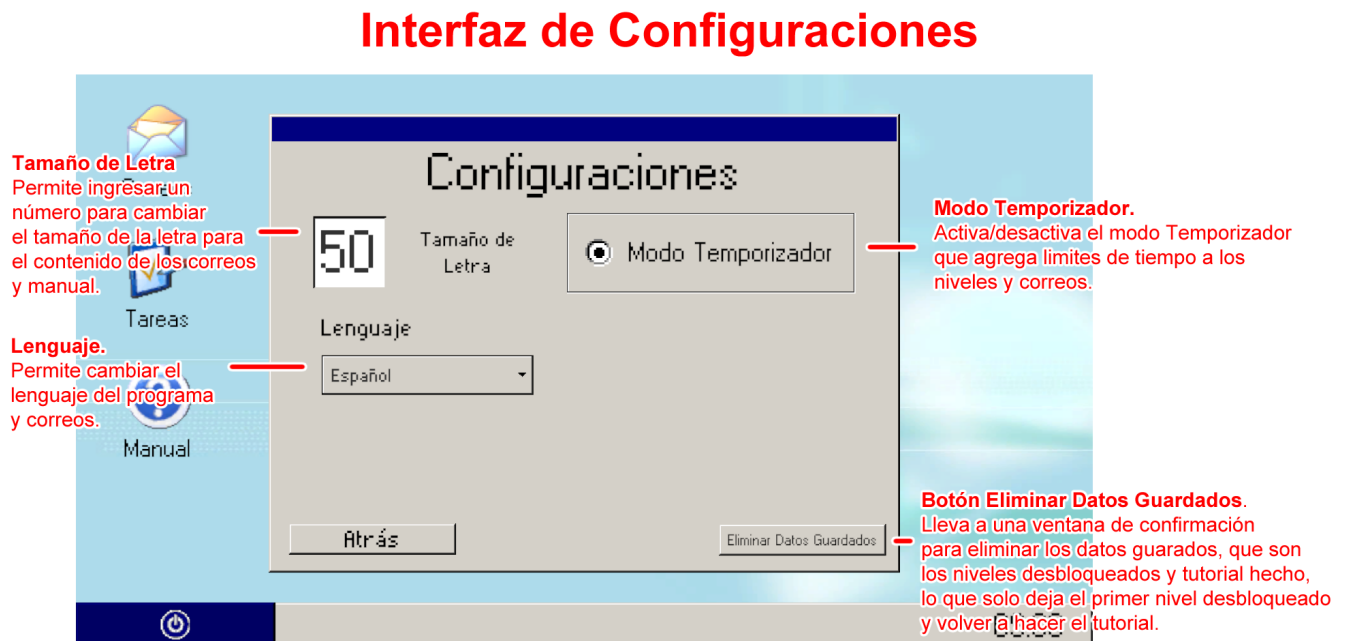


Figura 7.2: Diagrama de Interfaz de Configuraciones

7.4.3. Diagrama de Interfaz de Niveles

Interfaz de Niveles

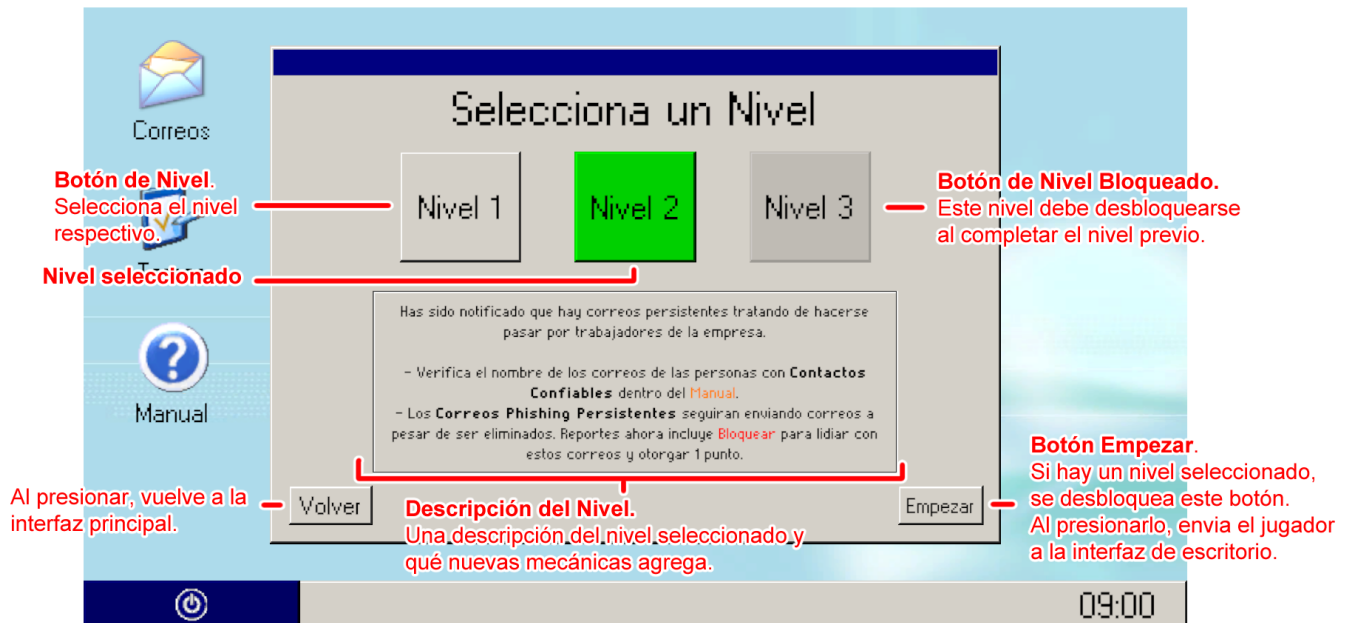


Figura 7.3: Diagrama de Interfaz de Niveles

7.4.4. Diagrama de Interfaz de Tareas

Interfaz de Tareas, Objetivos, y Panel de Salida

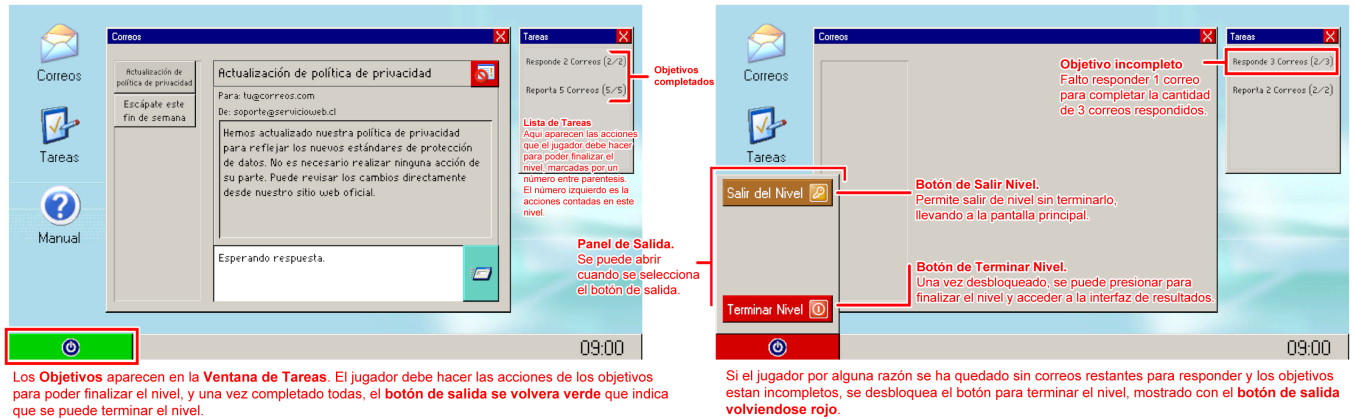


Figura 7.4: Diagrama de Interfaz de Tareas

7.4.5. Diagrama de Interfaz de Correos

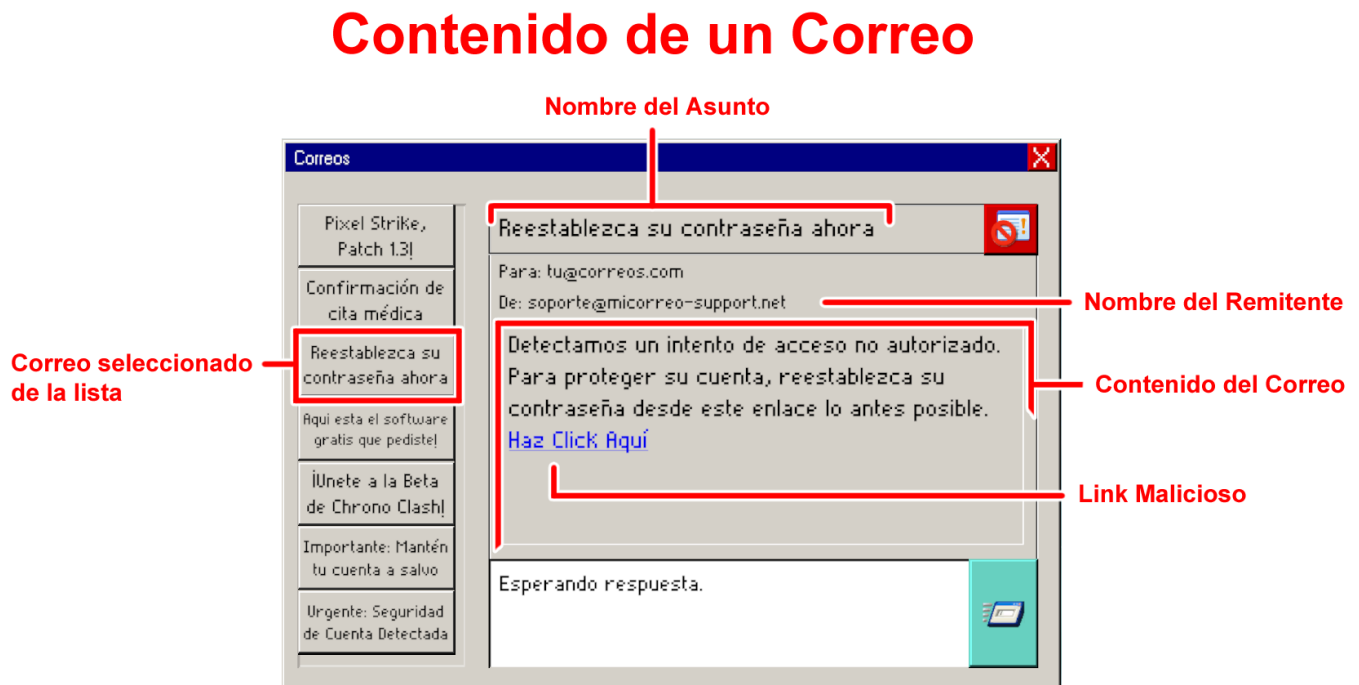
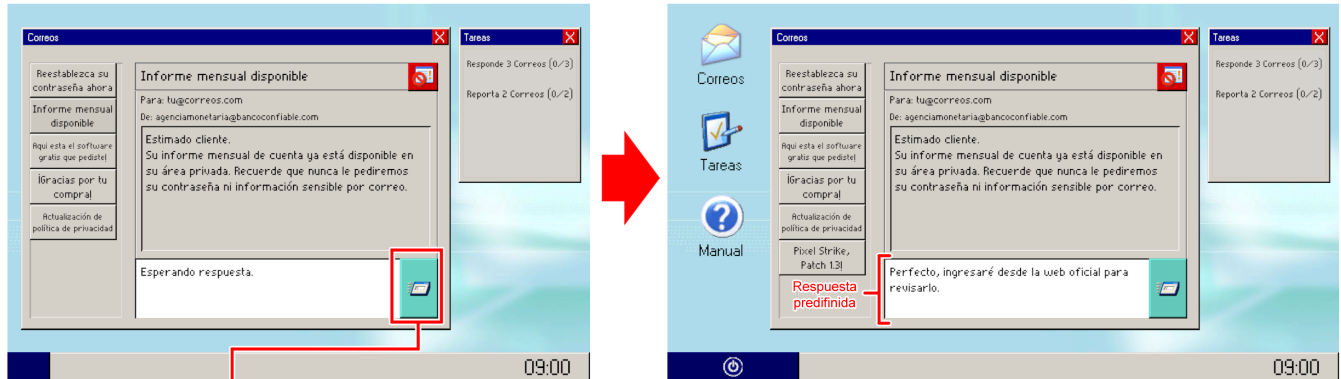


Figura 7.5: Diagrama del Contenido del Correo

Responder Email



El botón de **Responder**, cuando es presionado, escribe una respuesta predefinida para el correo durante unos segundos.

La respuesta tarda unos segundos en escribir y se envía automáticamente al terminar de escribir. No se puede hacer otras acciones (Como reportar) mientras aparece la respuesta. Si se cambia de correo, la respuesta se envía instantáneamente y el correo se remueve.

Figura 7.6: Diagrama de Responder Email

Panel de Reportes



Botón de Reporte. Al presionarlo, muestra/oculta la lista de opciones de reporte. Reportar un correo legítimo quita 1 punto.

Botón Eliminar. Remueve el correo de la lista. Otorga 1 punto al reportar un correo malicioso común.

Botón Bloquear. Remueve y previene ese correo de seguir enviando mensajes. Otorga 1 punto al reportar un correo phishing persistente.

Botón Marcar como Spam. Marca el correo como Spam y lo envía a otra carpeta, marcando correos similares como Spam. No otorga puntos, ya que los correos Spam son obstáculos y no parte de objetivos.

Los correos reportados son eliminados de la bandeja de entrada. Ciertos correos como los **phishing persistentes** o **spam** suelen reaparecer si no se ha hecho la acción correcta.

Figura 7.7: Diagrama del Panel de Reportes

7.4.6. Diagrama de Interfaz de Resultados

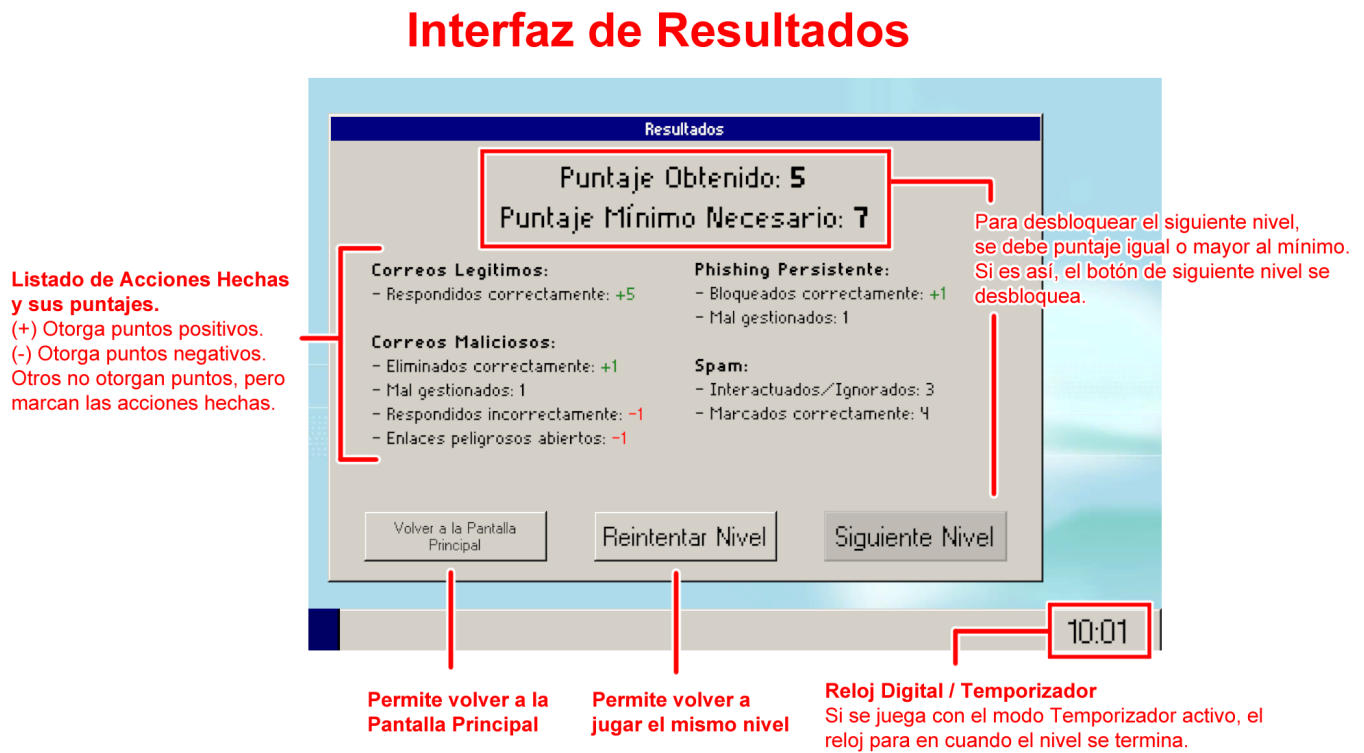


Figura 7.8: Diagrama de Interfaz de Resultados

7.4.7. Diagrama de Versión Alternativa: Modo Temporizador



Figura 7.9: Diagrama de Modo Temporizador

7.5. Preguntas de Encuesta Propia

1. Soy consciente de que los correos maliciosos pueden provocar robo de identidad y pérdidas económicas.
2. Conozco al menos una solución o técnica para protegerme contra los correos maliciosos.
3. Los dominios web y direcciones de correo son importantes a la hora de verificar si son seguros.
4. Antes de proporcionar mi información personal, busco una confirmación o certificado válido que acredite que la dirección de correo es correcta y segura.
5. Es poco probable que acepte invitaciones por correo electrónico de una fuente desconocida para compartir mi información personal.
6. Estoy bien informado sobre los riesgos de interactuar con correos maliciosos.
7. Tengo la intención de utilizar regularmente técnicas de protección eficaces contra los correos maliciosos / phishing en línea.

8. Estoy bien informado sobre la tecnología o técnicas contra correos maliciosos.
9. (Pregunta abierta) ¿Qué le pareció la experiencia completa del videojuego?
10. (Pregunta abierta) ¿Qué tema de ciberseguridad le hubiera interesado ver en la experiencia?

7.6. Gráficos de sesión de resultados

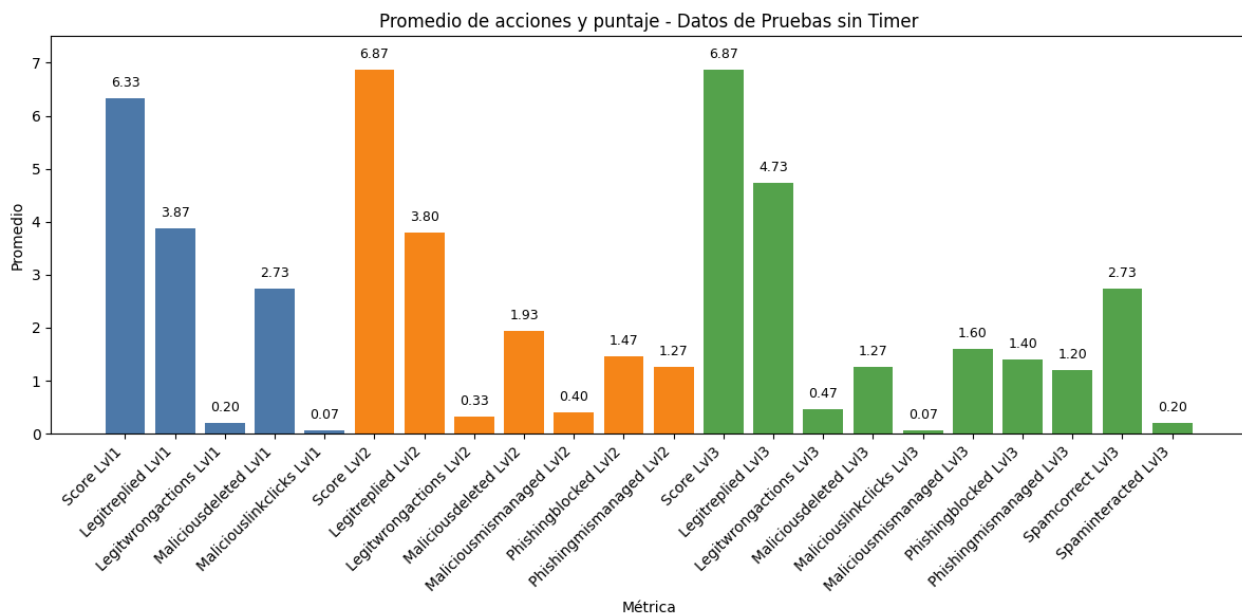


Figura 7.10: Gráfico de promedios de acciones y puntaje de pruebas sin temporizador

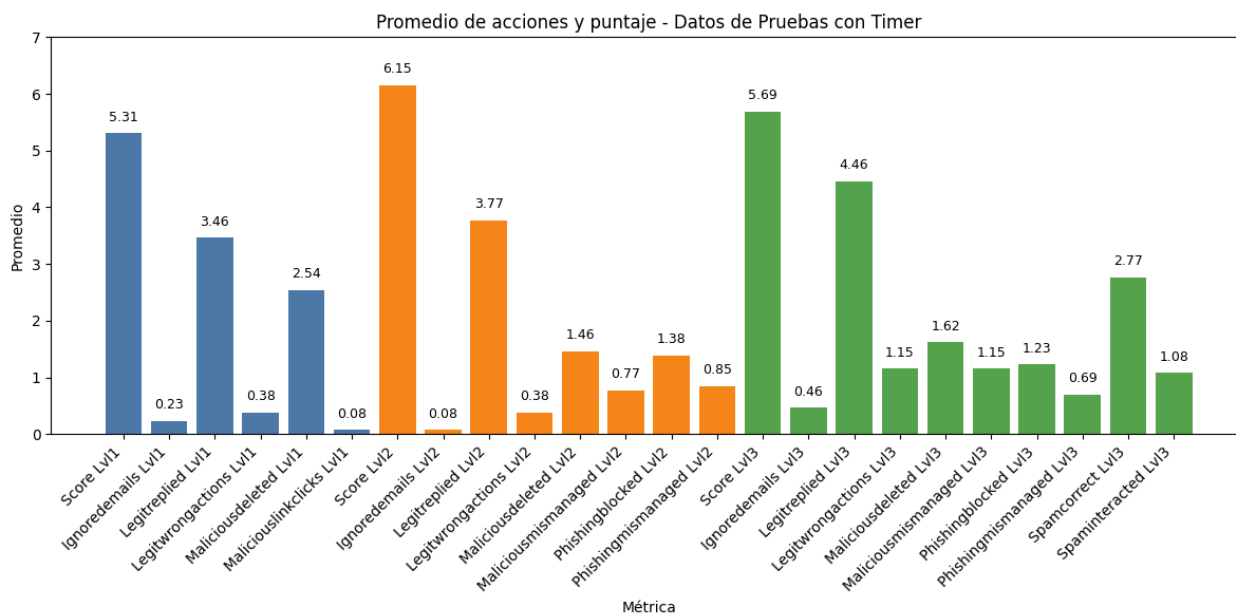


Figura 7.11: Gráfico de promedios de acciones y puntaje de pruebas con temporizador

7.7. Video Gameplay

Video de la versión sin temporizador: [Link de video](#)

Video de la versión con temporizador: [Link de video](#)

7.8. Resultados de encuestas

Sin temporizador: [Link de Excel](#)

Con temporizador: [Link de Excel](#)

7.9. Resultados de sesiones

Sin temporizador: [Link de Excel](#)

Con temporizador: [Link de Excel](#)