UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Diseño y desarrollo de un videojuego educativo para la concientización y prevención de amenazas digitales

TESIS

Que para obtener el título de

Ingeniera en Computación

P R E S E N T A

Mildred Janelly Alvarez Valdez

DIRECTORA DE TESIS

M.C. María Jaquelina López Barrientos

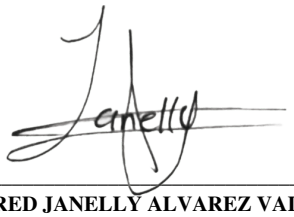
Ciudad Universitaria, Cd. Mx., 2026

PROTESTA UNIVERSITARIA DE INTEGRIDAD Y HONESTIDAD ACADÉMICA Y PROFESIONAL
(Titulación con trabajo escrito)

De conformidad con lo dispuesto en los artículos 87, fracción V, del Estatuto General, 68, primer párrafo, del Reglamento General de Estudios Universitarios y 26, fracción I, y 35 del Reglamento General de Exámenes, me comprometo en todo tiempo a honrar a la institución y a cumplir con los principios establecidos en el Código de Ética de la Universidad Nacional Autónoma de México, especialmente con los de integridad y honestidad académica.

De acuerdo con lo anterior, manifiesto que el trabajo escrito titulado DISEÑO Y DESARROLLO DE UN VIDEOJUEGO EDUCATIVO PARA LA CONCIENTIZACION Y PREVENCION DE AMENAZAS DIGITALES que presenté para obtener el titulo de INGENIERA EN COMPUTACIÓN es original, de mi autoría y lo realicé con el rigor metodológico exigido por mi Entidad Académica, citando las fuentes de ideas, textos, imágenes, gráficos u otro tipo de obras empleadas para su desarrollo.

En consecuencia, acepto que la falta de cumplimiento de las disposiciones reglamentarias y normativas de la Universidad, en particular las ya referidas en el Código de Ética, llevará a la nulidad de los actos de carácter académico administrativo del proceso de titulación.



MILDRED JANELLY ALVAREZ VALDEZ
Número de cuenta: 314056445

Índice

Capítulo I. Introducción

1.1 Planteamiento del problema

Prevenir es un acto que practicamos en distintos ámbitos de nuestra vida, ya sea en el doméstico, laboral, en la salud, entre otros. Por ejemplo, al salir de casa la gente siempre revisa que todo esté apagado y/o cerrado, con el fin de evitar algún peligro, sin embargo, se vuelve importante saber qué significa la palabra prevención, de acuerdo con la Real Academia Española, se define como “Preparación y disposición que se hace anticipadamente para evitar un riesgo o ejecutar algo”, pero, ¿Se hace lo mismo con la información, datos o dispositivos?, es decir, ¿las personas toman alguna medida preventiva en este ámbito?, preguntas cómo estás son las que se vuelven importantes para reflexionar y saber en qué nivel de seguridad se encuentra hoy día la población.

El Índice Global de Ciberseguridad (GCI) fue lanzado en 2015 por la Unión Internacional de Telecomunicaciones (UIT), organismo especializado de las Naciones Unidas responsable de las tecnologías de la información y la comunicación. El índice evalúa el compromiso de los países en materia de ciberseguridad a través de cinco pilares: jurídico, técnico, organizativo, desarrollo de capacidades y cooperación. Su elaboración involucra a expertos nacionales e internacionales de los países miembros, quienes documentan y verifican de manera independiente las medidas adoptadas en cada pilar. Dada la complejidad del proceso de recopilación, verificación y análisis de datos a escala global, el informe se publica aproximadamente cada dos o tres años; la edición más reciente corresponde a septiembre de 2024 y constituye la quinta edición del índice. La edición anterior había sido publicada en 2021.

Actualmente México se encuentra en el Tier 2 – Advancing del Índice de Ciberseguridad Global (ICG) de la Unión Internacional de Telecomunicaciones (UIT), lo que indica un avance significativo en la implementación de estrategias de ciberseguridad. No obstante, uno de los principales problemas persiste: la falta de concientización y educación sobre ciberseguridad entre la población mexicana, lo que la hace vulnerable a la pérdida de datos (Infobae México, 2024).
En este contexto, el factor humano representa la causa principal de incidentes de ciberseguridad, siendo responsable del 74% de los casos registrados en México. Errores como el uso de contraseñas débiles, la falta de actualizaciones y la exposición involuntaria de información facilitan el trabajo de los ciberdelincuentes. Además, con el avance de la inteligencia artificial, las amenazas se han vuelto más sofisticadas: desde la recreación de voces para cometer fraudes por mensajería instantánea, hasta campañas de phishing automatizadas. A pesar del creciente número de ataques, la información sobre ciberseguridad no siempre resulta accesible o comprensible, lo que genera apatía e inacción en la adopción de medidas preventivas.

Ante este panorama surge la siguiente pregunta de investigación:

¿Cómo puede un videojuego serio mejorar el nivel de concientización en ciberseguridad en usuarios finales?

1.2 Justificación

La ciberseguridad no es únicamente un problema técnico, sino cultural. La evidencia muestra que el comportamiento humano -actitudes, hábitos e impulsividad de los usuarios- constituye el principal factor de riesgo ante incidentes de seguridad digital, por encima de las deficiencias en soluciones tecnológicas (Hadlington, 2017). Invertir en firewalls y software de detección avanzada resulta insuficiente si los usuarios continúan incurriendo en prácticas de riesgo básicas. Por ello, se requieren estrategias de educación accesibles, atractivas y efectivas.

Los videojuegos serios son herramientas eficaces para el aprendizaje: la evidencia empírica acumulada en más de cien estudios demuestra su impacto positivo en la adquisición de conocimientos, el desarrollo de habilidades, la mejora en la motivación intrínseca y el cambio de actitudes en los usuarios (Connolly et al., 2012). Estos recursos combinan motivación intrínseca, retroalimentación inmediata, y un entorno seguro donde el usuario puede cometer errores sin consecuencias reales. Su uso en áreas como la salud, el ámbito militar y la educación avala su potencial como medio de concientización. En este trabajo se propone aprovechar estos beneficios para abordar la brecha de conocimiento en ciberseguridad.

1.3 Objetivos

1.3.1 Objetivo general

Diseñar y desarrollar un videojuego educativo que fomente la sensibilización y el aprendizaje sobre prácticas básicas de ciberseguridad, brindando herramientas para identificar y prevenir riesgos en el ciberespacio.

1.3.2 Objetivos específicos

A) Crear un sistema de niveles y desafíos que permita a los jugadores aprender gradualmente conceptos clave de ciberseguridad.

B) Diseñar una interfaz amigable e interactiva que facilite la comprensión y retención del contenido educativo.

C) Generar conciencia sobre la importancia de las contraseñas seguras, la navegación responsable y el uso adecuado de herramientas tecnológicas.

1.4 Hipótesis

El uso de un videojuego educativo como herramienta de aprendizaje interactivo incrementará la sensibilización y el conocimiento sobre ciberseguridad en las personas que participen, fomentando mejores prácticas y reduciendo su exposición a ciberataques.

1.5 Alcances y limitaciones

1.5.1 Alcances

- El videojuego cubre nueve áreas temáticas fundamentales de ciberseguridad: contraseñas, navegación segura, ataques de ingeniería social, malware, sistemas operativos, videoconferencia, uso seguro de la nube, copias de seguridad y antivirus.
- El producto fue desarrollado y validado con una muestra de 203 estudiantes de licenciatura.
- El videojuego se exportó para la plataforma Windows con fines de prueba y evaluación.
- Los resultados incluyen evidencia de mejora en la autopercepción del conocimiento en ciberseguridad antes y después de jugar

1.5.2 Limitaciones

- La evaluación del aprendizaje se basó en la autopercepción de los usuarios mediante encuesta, no en un instrumento validado externamente ni en pruebas estadísticas formales (pre-test/post-test con prueba t de Student o equivalente). En consecuencia, los resultados reflejan percepción subjetiva y no pueden aseverar un cambio estadísticamente significativo en el conocimiento real.
- El estudio no incluye medición de retención del conocimiento a mediano plazo.
- La muestra está compuesta por estudiantes universitarios de entre 19 y 24 años, por lo que los resultados no son generalizables a toda la población.
- El videojuego fue exportado únicamente para Windows, lo que restringe su alcance a usuarios de dicha plataforma.

1.6 Metodología

Para el desarrollo del videojuego se utilizó un enfoque basado en fases iterativas. El tipo de estudio es descriptivo-exploratorio con evaluación empírica de usuarios. La evaluación se llevó a cabo con estudiantes de Ingeniería en Computación que cursan las asignaturas de Redes y Seguridad a inicios de semestre, ya que como parte de su formación son los conocimientos básicos de ciberseguridad que deben conocer. Las etapas del proceso fueron las siguientes:

A. Conceptualización e investigación. Revisión de literatura sobre videojuegos serios, gamificación y ciberseguridad.

B. Definición de temáticas y estructura de niveles. Identificación y organización de los nueve temas clave en niveles de dificultad creciente.

C. Elaboración del Game Design Document (GDD). Documentación de la mecánica, personajes, niveles y objetivos del videojuego.

D. Desarrollo del prototipo. Implementación en Unity con C# y ajustes iterativos en mecánica e interfaz.

E. Pruebas funcionales. Pruebas de volumen, integración y testers externos.

F. Prueba de usuarios. Aplicación del videojuego con 203 estudiantes universitarios y recolección de retroalimentación mediante encuesta digital (Google Forms) que incluyó preguntas sobre nivel de conocimiento previo y posterior a la experiencia.

G. Análisis de resultados y documentación. Interpretación de datos y redacción del presente trabajo.

Nota: La evaluación del aprendizaje se realizó a través de la autopercepción de los usuarios. Dado que no se aplicó un instrumento validado ni una prueba estadística formal, los resultados deben interpretarse como indicadores exploratorios y no como evidencia concluyente de aprendizaje.

Capítulo II. Marco teórico y estado del arte

2.1 Ciberseguridad

Dentro de la ciberseguridad existen tres conceptos importantes que se deben tener presentes, los cuales de acuerdo con Moreno (2012) se describen a continuación:

- Activo. Todo aquello que posee un valor importante. Según Bertolín (2008), son aquellos elementos relacionados con el entorno.

- Amenaza. Todo aquello que pueda provocar un daño a nuestro activo.

- Vulnerabilidad. Son las inseguridades que posee el activo.

- Riesgo. Es la probabilidad de que una amenaza aproveche una vulnerabilidad.

Enseguida se presenta una imagen (Figura 3) donde se observa la relación entre estos conceptos.

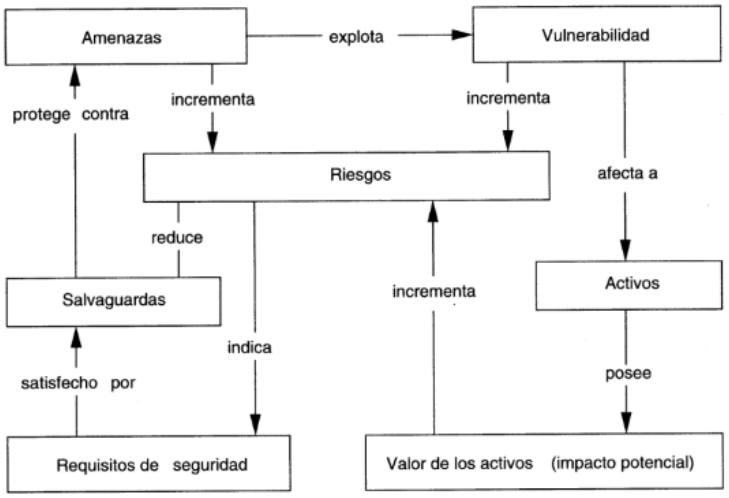


Figura 1. Relación entre los conceptos de activo, vulnerabilidad, amenaza y riesgo. Nota. Adaptado de Relación entre componentes de la gestión de la seguridad, por Bertolín Javier, 2008, Google libros.

(J.L. Barrientos, comunicación personal, 23 de noviembre de 2021) considera que existen cinco fuentes de amenaza, enseguida se muestra su clasificación:

I. Factor Humano.
Las amenazas de este tipo surgen por ignorancia en el manejo de la información, descuido o negligencia. Sabemos que la debilidad de los activos es el factor humano, puesto que se realizan varias prácticas para que el usuario caiga en la trampa. Algunas de estas prácticas que se realizan son:

 Ingeniería social. Práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.

 Robo. Apoderamiento de bienes ajenos.

 Fraude. Engaño económico con la intención de conseguir beneficios.

 Sabotaje. Proceso por el cual se realiza una modificación, destrucción, obstrucción o cualquier intervención con el propósito de obtener un beneficio y dañar a un grupo contrario.

 Juego de roles. Pretende ser un servicio de ayuda, un empleado, un técnico, un usuario importante, o un indefenso y persuadir a alguien a revelar información.

 Caballo de troya. Se engaña a la víctima para descargar un archivo malicioso, que en la ejecución crea una puerta trasera en el equipo y el atacante puede entrar en un futuro y obtener información delicada.

 Phishing. Crear sitios web o emails parecidos a los de sitios, instituciones financieras, agencias gubernamentales o negocios legítimos para engañar a los usuarios para que revelen su información personal o laboral que se utilizará en el robo de identidad.

II. Hardware.
Las amenazas de hardware se pueden clasificar en fallas físicas o por desperfectos.

 Fallas físicas. Problemas se suministró de energía eléctrica, bajo voltaje, ruido electromagnético, distorsión, alto voltaje, variación de frecuencia.

 Desperfecto. Bajo rendimiento, pérdida del mismo dispositivo físico por deterioro o incorrecto funcionamiento, pérdida total o parcial del equipo por sobrecalentamiento, problemas con cargas estáticas, entre otros.

Los apagones afectan a los sistemas operativos o hardware. Recordemos que apagar un servidor repentinamente sin los procedimientos adecuados de cierre puede generar problemas con el sistema de operación para reiniciar. Los cambios bruscos en el voltaje también pueden dañar muchas partes de la computadora, es por ello que cuando conectamos algún dispositivo en algún lugar nuevo, nos informemos y aseguremos que la corriente a la que lo vamos a conectar sea la adecuada.

III. Red.
Las amenazas de red se presentan cuando no se calcula bien el flujo de información que circulará por el canal de comunicación, (Un atacante podría saturar el canal de comunicación provocando la no disponibilidad de la red), si bien dentro del hogar nosotros no tenemos este control, sigue siendo una amenaza. Se clasifica en aspecto físico y lógico.

 Físico. Interferencia, cables cortados o dañados que pueden alterar la integridad de los datos.

 Lógico. Se presentan amenazas de monitorización, escaneo, ataques de autenticación, obtención de contraseñas, denegación de servicio, vulnerabilidades en los navegadores, virus de correo electrónico, virus fantasmas – conocidos como hoax-, señuelos, escaneo de la conexión TCP, escuchar detrás de las puertas, fisgoneo, descargas, engaño DNS, engaño de web, secuestro, uso de diccionarios electrónicos para obtener contraseñas.

IV. Software.
Se refiere al malware, que es básicamente un software destinado a realizar un proceso no autorizado que tendrá impacto sobre la confidencialidad, integridad o disponibilidad de un sistema de información. Este código malicioso explota los flujos de información en los sistemas operativos y software asociado; además, explota la configuración insegura, la mayoría de

los sistemas son entregados con configuración insegura y eso se debe a que es más fácil de instalar y utilizar.

V. Desastres.
Se trata de desastres naturales, son amenazas directas puesto que repercuten directamente en el funcionamiento físico de los equipos de cómputo, redes, instalaciones, líneas de comunicación, etc. También es muy importante mantener el sitio a la temperatura que los fabricantes de los equipos especificaron para su buen desempeño. Los desastres que se pueden presentar son rayos, fallas eléctricas o picos de potencia, el polvo, la humedad o la temperatura excesiva, entre otros están:

 Fuego. Una de las principales amenazas contra la seguridad, es considerado el enemigo número uno de las computadoras, ya que puede destruir fácilmente los archivos de información y programas. Se puede dar por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el incorrecto almacenamiento o traslado de sustancias peligrosas.

 Inundaciones. Exceso de escurrimientos superficiales o acumulación de agua en terrenos planos (por la falta de drenaje natural o artificial), o una inundación por lluvia o provocada por la necesidad de apagar un incendio en un piso superior.

 Terremotos. Causan destrucción de edificios, de equipo y hasta pérdidas humanas. El problema es que, en la actualidad, estos fenómenos están ocurriendo en lugares donde no se tenían previstos.

De acuerdo a un artículo publicado el 1 de diciembre de 2021 por el portal Kaspersky latam, algunos de los métodos más comúnmente utilizados para amenazar la ciberseguridad son: malware (en sus diferentes tipos), inyección de código SQL, phishing, ataque de tipo “Man-in-the-middle” y ataque de denegación de servicio. De igual importancia, en un mapa otorgado por Kaspersky para visualizar las ciberamenazas en tiempo real en todo el mundo, México varía entre la posición 12 y 13, del ranking mundial, en la figura tres consultada el día 3 de junio del 2025 podemos apreciar las últimas cifras registradas de cada sección.

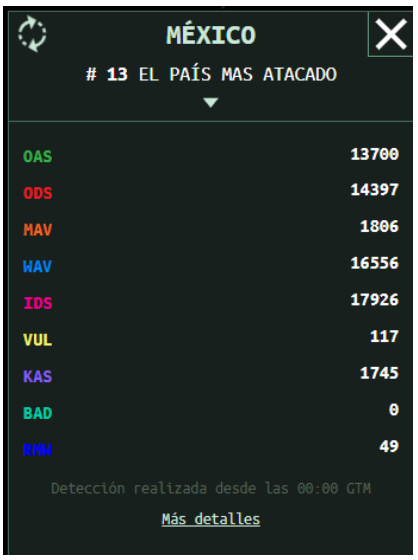


Figura 2. Posición de México en cuanto a ciberamenazas en tiempo real.

Nota. Adaptado de mapa en tiempo real de ciberamenazas en el mundo, de, Kaspersky Lab, 2025, Kaspersky (https://cybermap.kaspersky.com/es)

Para resaltar la importancia de estos temas y las consecuencias que se pueden generar si no se siguen las buenas prácticas de seguridad, se tiene como ejemplo el caso del ataque hacia la Comisión de Seguros y Finanzas (CNSF). Una noticia publicada el 29 de noviembre de 2021 por el periódico “El economista”, nos relata que a través de redes sociales se dio a conocer el ataque, en el cual, los ciberdelincuentes tuvieron acceso a los sistemas informáticos de este organismo afectando su continuidad operativa. El sistema fue vulnerado a través de un ransomware denominado “LockBit” diseñado para bloquear el acceso de los usuarios a los sistemas informáticos y pedir un pago de rescate para restablecerlo, este ransomware busca automáticamente objetivos valiosos, propaga la infección y cifra todos los sistemas informáticos accesibles en una red. Los ataques de LockBit pueden entenderse en tres etapas; explotación, infiltración e implementación. La etapa de explotación consiste justamente en explotar las vulnerabilidades de una red, y esto se puede lograr por medio de tácticas de ingeniería social como el phishing. Una vez explotadas las vulnerabilidades el ransomware actúa por sí sólo desactivando los programas de seguridad y de cualquier otra infraestructura que pudiera permitir la recuperación del sistema, por último, la etapa de implementación se encarga de cifrar todos los archivos del sistema.

2.2 Cibercultura

Para que se pueda entender mejor qué es la cibercultura, primero se debe tener claro qué significa cultura. La palabra cultura tiene diversos conceptos dependiendo de las necesidades y elaboraciones de disciplinas específicas, para este trabajo se hará uso de los conceptos antropológicos y sociológicos.

De acuerdo con Millán (2000) desde el concepto antropológico, la cultura es el sustantivo común “que indica una forma particular de vida, de gente, de un período o de un grupo humano”; está ligado a la apreciación y análisis de elementos tales

como valores, costumbres, normas, estilos de vida. Mientras que desde el concepto sociológico se entiende como "el concepto abstracto que describe procesos de desarrollo intelectual, espiritual y estéticos" del acontecer humano, incluyendo la ciencia y la tecnología.

Por otra parte, la Real Academia Española define la palabra cibercultura como “el conjunto de hábitos generados por el uso continuado de los recursos informáticos”.

Por lo que, la transición de la cultura a cibercultura sólo se diferencia por los recursos tecnológicos que las personas incorporan a su vida y la interacción de las personas con el ciberespacio. Albornoz (2008) señala que, en el mundo actual, donde la tecnología predomina en múltiples áreas de la sociedad, se descuidan las buenas prácticas o prevenciones que se suelen tomar fuera de la red para proteger la privacidad, las personas dejan de distinguir entre lo público y lo privado mientras navegan en el ciberespacio (PP. 44 - 50).

Al igual que en la cultura, de la cibercultura se desprenden diversos enfoques, a continuación, se abordarán algunos de ellos.

- Educación.

  En cuanto a la educación, las Tecnologías de la Información y Comunicación (TIC) han sido sumamente útiles en la vida del estudiante, puesto que le facilita el acceso a la información y automatiza algunos procesos. Hoy en día los más pequeños saben manejar muchas de estas tecnologías, se les facilita el manejo de diversos dispositivos teniendo así nuevas maneras de presentar y acceder al conocimiento, sin embargo, Levy (2000) señala que los sistemas de educación y formación deben afrontar dos grandes reformas; la primera es la adaptación e integración de los dispositivos y la filosofía del AAD (Aprendizaje abierto y a distancia) a las prácticas habituales de la educación. El AAD utiliza ciertas técnicas de enseñanza a distancia, incluyendo los hipermedios, redes de comunicación interactivas y todas las tecnologías intelectuales de la cibercultura. Pero lo esencial reside en un nuevo estilo pedagógico, que favorece, al mismo tiempo, el aprendizaje personalizado y el aprendizaje cooperativo en red.

  La segunda reforma se refiere al reconocimiento de lo adquirido. Si las personas aprenden en sus experiencias sociales y profesionales, si la escuela y la universidad pierden progresivamente su monopolio en la creación y transmisión de conocimientos, los sistemas de educación pueden asumir una nueva misión: orientar las carreras individuales en los espacios del saber y contribuir al reconocimiento del conjunto de capacidades de los individuos, incluidos los conocimientos no académicos.

  Es importante mencionar que aún existe una brecha entre las TIC y la educación, Bonilla (2005) señala que impide sean implementadas completamente, algunas de estas barreras son: a) No hay docentes lo suficientemente preparados en su manejo; b) Algunos softwares educativos son costosos; c) Falta de concientización en la población; d) Poco conocimiento de las leyes o reformas dirigidas a los delitos cibernéticos.

- Ético, antropológico y social.

  Con la llegada de las nuevas tecnologías, el ser humano queda expuesto a todo tipo de información, por lo que una Comunidad de Conocimiento (CC) se integra por grupos de personas que tienen la posibilidad de compartir información y experiencias sobre aspectos o áreas de interés común. (Drucker 2008, citado por Fuentes y Duarte 2016).

  Esto se aprecia mejor cuando se navega en el ciberespacio, ya que en diversos medios como los juegos en línea o redes sociales se encuentran comunidades o grupos que comparten intereses y con los cuáles se sienten incluidos, por consiguiente, existe la posibilidad de que las personas no interactúen de la misma manera estando detrás de una pantalla que en la vida real, esto también puede derivar en la creación de falsas identidades.

  Fuentes y Duarte (2016) señalan que, desde una aproximación constructiva, las Tecnologías de la Información y Comunicación (TIC) pueden utilizarse para generar conocimiento y cambios sociales significativos. Tal es el caso de la ley Olimpia en México, publicada el 22 de enero del 2020 por el gobierno de la Ciudad de México, esta ley surge a raíz de la difusión de un video de contenido sexual no autorizado de una mujer en el estado de Puebla; derivado de ello se impulsó una iniciativa para reformar el Código Penal de dicha entidad y tipificar tales conductas como violación a la intimidad. La “Ley Olimpia” hace referencia a un conjunto de reformas legislativas encaminadas a reconocer la violencia digital y sancionar los delitos que violen la intimidad sexual de las personas a través de medios digitales, también conocida como ciber violencia.

  Otro aspecto que se debe tomar en cuenta al navegar, es que así como se tiene acceso a todo tipo de información, el ser humano también queda expuesto al conocimiento de otras culturas, por lo que al interactuar en línea con personas de diversas partes del mundo pueden existir choques culturales, porque no en todos lados se comparten las mismas costumbres o hábitos y no se tiene la misma definición para el bien o el mal, esto dependerá de las personas que integren las sociedad, estas diferencias pueden pasar desapercibidas o en algunos casos derivar en un conflicto.

- Organizaciones.

  Para Bonilla (2005)

  Desde la llegada de las Tecnologías de la Información y Comunicación (TIC), al buscar un trabajo independientemente del área estudiada, se requiere saber manejar herramientas de software: un procesador de palabra, una hoja electrónica, un programa para presentaciones y otro de mensajería instantánea, un administrador de correo electrónico y, por supuesto, navegar por internet. (P.181)

  Actualmente y derivado de la pandemia de Covid-19, han aumentado las herramientas de software que se deben saber manejar, ya que se sumaron programas de teleconferencias, gestión de proyectos, automatización (más enfocado en el área de marketing), gestores de contraseñas, entre otros. Es

deber de las empresas mantenerse actualizadas en cuánto al manejo de información, así como tener capacitado a su personal en el manejo de las nuevas herramientas que ofrece el avance tecnológico.

La Secretaría de Seguridad y Protección Ciudadana (SSPC), perteneciente al gobierno de la Ciudad de México, el 25 de octubre de 2021 puso a disposición una ciberguía con el objetivo de que las personas integrantes de la sociedad naveguen de manera segura y que la protección en el ciberespacio se vuelva cultura, los temas principales de esta ciberguía son:

- Seguridad durante el teletrabajo.
- Contraseñas seguras.
- Malware y Ransomware.
- Phishing: Estafas de suplantación de identidad.
- Noticias falsas.
- Técnicas de Ingeniería Social.
- Fraude electrónico.
- La reputación en el ciberespacio.
- Seguridad en dispositivos móviles.
- Lineamientos para identificar y reportar páginas falsas.
- Ley Olimpia.
- Seguridad en redes sociales y comunidades virtuales.
- Seguridad en el uso del correo electrónico.

Está guía se complementa con el Decálogo de Ciberseguridad de la SSPC, que consta de lo siguiente:

1. Protegerás tu identidad digital.
2. Utilizarás medidas de seguridad durante el teletrabajo.
3. Usarás contraseñas seguras.
4. Cuidarás los datos personales que se exponen en el ciberespacio.
5. No compartirás noticias falsas.
6. Pondrás más atención cuando compartas datos personales.
7. Verificarás ofertas y proveedores cuando se trate de comercio digital.
8. Protegerás todos los equipos informáticos.
9. Evitarás el ciberacoso.
10. Denunciarás.

Estas recomendaciones pueden llegar a parecer obvias, sin embargo, muchas veces se pasan por alto, en junio del 2022 Christopher Calderón publicó un artículo en el periódico “El financiero” citando un informe de la empresa mexicana Silikn, refiriendo que en los primeros seis meses de este año México sufrió 85 mil millones de intentos de ciberataques representando un alza de 41.9% con respecto a los 60 mil millones de tentativas del mismo periodo del 2021. De acuerdo con dicho informe el 48.6% de los intentos de ciberataque fueron a través de las conexiones de acceso remotas poco seguras, y que en el 39% de los casos el acceso fue a través de correos electrónicos de phishing.

“A raíz de la pandemia crecieron significativamente los ataques de ingeniería social, particularmente ataques de phishing y malware, es decir, que los hackers se enfocan

en atacar las redes de los usuarios finales, lo que derivó en un incremento de hasta 300 por ciento en ciberataques, de los cuales, más del 60 por ciento estuvieron dirigidos a ataques de banca en línea" (Castillo, citado por Calderón 2022).

El 5 de noviembre del 2025 Viviana Hernández publicó un artículo en el portal "W Radio" citando al director de ciberseguridad en KIO IT Services, en relación con los más de 237 mil ataques de ransomware entre agosto de 2024 y junio de 2025, convirtiendo al país en el más atacado de América Latina, sólo detrás de Brasil.

Con la llegada de la Inteligencia Artificial, se ha abierto un nuevo panorama, ya que ahora los ciberdelincuentes la utilizan para automatizar campañas de phishing, clonar voces y rostros mediante deep fakes, y propagar desinformación a velocidades imposibles para un humano. En respuesta, las empresas emplean la misma tecnología para detectar patrones anómalos, anticipar amenazas y responder en tiempo real.

Los especialistas coinciden en un punto: el eslabón más débil sigue siendo el humano. La conciencia digital es tan importante como la tecnología. Hacer inversiones en firewalls y software de detección avanzada no servirá si los usuarios siguen cayendo en trampas básicas. La ciberseguridad no es un asunto técnico, sino cultural.

Se puede concluir entonces que la cibercultura sólo existe en el ciberespacio ya que surge a partir de la interacción de las personas con los recursos tecnológicos, ya que conforme se van incorporando a la vida, se van modificando nuestras costumbres, hábitos, comportamientos e interacciones con otras personas. Como ya se mencionó anteriormente, al estar en el ciberespacio se encuentra la posibilidad de que no se interactúe de la misma forma que en presencial, en diversas ocasiones puede que sean falsas identidades y por ello es importante que se tomen precauciones en cuanto a la información que se comparte dentro de las comunidades en línea.

De igual forma es importante mencionar que en cuanto a las organizaciones, es deber de las empresas mantenerse actualizadas en cuanto al manejo de información, así como tener capacitados a sus empleados en el manejo de las nuevas herramientas que ofrece el avance tecnológico.

Por lo tanto, la principal característica de la cibercultura es el conocimiento, es decir, la información que posee el usuario es el principal recurso valioso, por eso es importante que se tenga en cuenta y se integren las buenas prácticas de seguridad indicadas en el decálogo de la Ciberseguridad, así como conocer y entender la ciberguía para tener el conocimiento de la forma en la que actúan los atacantes y así estar prevenidos ante cualquier amenaza.

2.3 Videojuegos serios

Crawford (1982) señala que el juego crea una visión subjetiva simplificada de la realidad en representación de la misma.

Ferrer (2018) define juego como “ejercicio lúdico delimitado por normas ejercido de forma voluntaria”

El concepto de videojuego, presenta cierta similitud con el concepto de juego, de este modo, Lin y Lepper (1987) resaltan tres elementos que los diferencian: componente tecnológico, tipo de videojuego y soporte en que se juega.

Videojuego se define como todo tipo de juego digital interactivo, con independencia de su soporte (ROM interno, cartucho, disco magnético u óptico, on-line) y plataforma tecnológica (máquina de bolsillo, videoconsola conectable a la T.V., teléfono móvil, máquina recreativa, microordenador, ordenador de mano, video interactivo) (Marqués, 2000).

Malone (1981) señala que los videojuegos logran captar y mantener la atención como consecuencia de la motivación que despiertan en el jugador. Esta motivación, que califica como intrínseca al propio juego, se fundamenta a su vez en tres aspectos fundamentales que son retos, fantasía y curiosidad. De igual importancia, Malone y Lepper (1987) identifican dos tipos de motivaciones: individuales e interpersonales. En la primera de ellas añaden el concepto de control a los mencionados anteriormente (retos, fantasía y curiosidad). Por otra parte, los factores que se incluyen en el tipo de motivación interpersonal son la cooperación, competencia y reconocimiento.

Los juegos y videojuegos serios son aquellos que se utilizan para fines educativos y distintos a sólo entretenimiento (Susi, Johannesson y Blacklund, 2007). Una de las principales ventajas de los videojuegos serios es que promueven jugar. Como resultado, el aprendizaje que se realiza a través del juego conlleva un proceso más atractivo y motivador para el estudiante (Gros, 2009).

Los primeros campos en los que se utilizaron los videojuegos serios fueron el militar, la seguridad y la medicina. A partir de ahí, estos se han trasladado a otros campos hasta llegar a todos los niveles de educación, desde el infantil hasta la universidad (Tasci, 2016).

Las primeras evidencias que se tienen acerca del origen de los videojuegos serios se dan después de la segunda guerra mundial, en 1947, cuando Thomas T. Goldsmith y Estle Ray Mann crearon una simulación de pantalla que buscaba asemejar un radar del ejército, la cual tuvo el nombre de “lanzamiento de misiles”, dado que el mecanismo consistía en lanzar misiles hacia targets virtuales (Gigante, 2009, p.46, citado por Espadas, 2018). Simultáneamente durante los años 40, técnicos americanos desarrollaron el primer simulador de vuelo, destinado al entrenamiento de pilotos (Balerdi, 2011).

Durante el año de 1951 se desarrolló NIM, considerado uno de los primeros videojuegos, se trata de un juego matemático de estrategia que se jugaba en la computadora NIMROD contra una inteligencia artificial (Gómez, Espinosa y Albajes, 2012).

Conforme fue avanzando la tecnología en cuánto a ordenadores, procesadores, memorias y periféricos, entre otros, también evolucionaron los videojuegos, lo que ocasionó que diversos investigadores se plantearon la idea de integrar los videojuegos como una herramienta que ayude y permita a los estudiantes mejorar su aprendizaje (Antonio, 2015).

De acuerdo con Prieto, Medina y López (2016) dentro de los juegos serios existen tres tipos de interacción los cuales se describen a continuación:

A. Interacción activa. El jugador realiza la interacción con el videojuego utilizando su cuerpo, para ello hace uso de una serie de dispositivos que utilizan sensores giroscópicos o acelerómetros para captar los movimientos. Un ejemplo de este tipo de interacción serían los Exergaming, algunos dispositivos que permiten este tipo de interacción son la Wii de Nintendo y el Kinect de Xbox.

B. Interacción pervasiva. Es el tipo más reciente, en este tipo de interacción se persigue integrar el videojuego y el contexto personal del jugador, es decir, una parte importante de la experiencia del videojuego interactúa con objetos del mundo real. Un ejemplo de este tipo de interacción sería el videojuego Pokémon Go.

C. Interacción estándar. En este tipo de interacción el jugador utiliza en la gran mayoría de los casos los dedos para controlar el videojuego. Esta interacción contempla dos subcategorías según el usuario utilice periféricos comunes o periféricos especiales, tales como pedales, cascos de realidad virtual, joysticks, entre otros. Respecto a los periféricos comunes la interacción se subdivide en:

    a. Interacción táctil. Se asocia con smartphones, tabletas y algunos ordenadores personales que permiten un manejo táctil.

    b. Interacción tradicional. La interacción más habitual donde se controla el videojuego a través de un teclado y un ratón en el caso de los ordenadores, y con un mando en el caso de las consolas.

En la siguiente imagen (Figura 3) se muestran las diferentes tipologías.

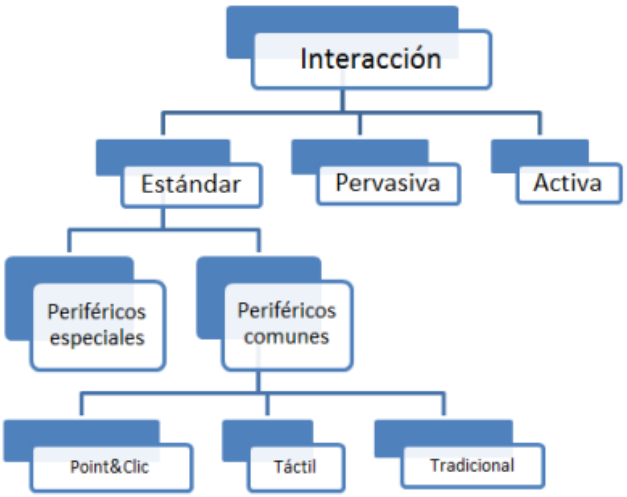


Figura 3. Tipos de interacciones.

Nota. Lope., R. P., Medina., N. M., & López., J. M. (2016). Tipos de interacciones. [Diagrama]. Research Gate. https://www.researchgate.net/profile/Francisco-Garcia-Penalvo/publication/308063240_Actas_del_XVII_Congreso_Internacional_de_Interaccion_Persona-Ordenador_-_Interaccion_2016/links/57d8885b08ae601b39afad1b/Actas-del-XVII-Congreso-Internacional-de-Interaccion-Persona-Ordenador-Interaccion-2016.pdf#page=41

Cada vez existen más aplicaciones docentes, entre ellas muchos videojuegos, sin embargo, la tendencia futura es que los videojuegos serios de nueva generación vayan ligados a libros de texto y material docente predeterminado por las propias editoriales con base a contenido específico y como apoyo a las lecciones didácticas o bien como lecciones únicamente dictadas por el videojuego (Pitarch, 2018).

Finalmente, los videojuegos pueden ser un inicio para acercar progresivamente a las personas a temas que se quieren abordar de una manera más atractiva e interactiva, puesto que nos dan la motivación de seguir adelante y se crean experiencias en las cuales es más intuitivo aprender.

Asimismo se observa que el aprendizaje lúdico ha estado presente durante largo tiempo, como sucedió con los primeros videojuegos durante los años cuarenta, mencionados con anterioridad en este trabajo, su objetivo fue que los usuarios adquirirán conocimientos por medio de escenarios simulados, creando así un ambiente amable y seguro en el cual se pueden cometer errores sin sufrir las consecuencias de la vida real, para que al momento de llevarlo a la práctica, exista un menor margen de error.

2.4 Teorías de aprendizaje

El aprendizaje es un proceso complejo que ha sido estudiado desde diversas perspectivas psicológicas y pedagógicas. Para el diseño de herramientas educativas digitales, resulta fundamental comprender cómo las personas adquieren, procesan y retienen conocimiento nuevo, con el fin de tomar decisiones de diseño que favorezcan una experiencia de aprendizaje efectiva y significativa.

Dentro de las corrientes del aprendizaje, el constructivismo sostiene que el conocimiento no se transmite de manera pasiva, sino que es construido activamente por el aprendiz a partir de su interacción con el entorno y sus experiencias previas (Piaget, 1952). Esta perspectiva resulta especialmente relevante en el contexto de los videojuegos educativos, ya que el usuario no es un receptor pasivo de información, sino un agente activo que explora, toma decisiones y aprende de las consecuencias de sus acciones dentro del entorno del juego.

2.4.1 Aprendizaje significativo

Una de las teorías más influyentes en el diseño de materiales educativos es la teoría del aprendizaje significativo, propuesta por David Ausubel en 1963. Esta teoría establece que el aprendizaje ocurre de manera más efectiva cuando el nuevo conocimiento se relaciona de forma deliberada y sustancial con conceptos o experiencias que el aprendiz ya posee en su estructura cognitiva, a los que Ausubel denomina 'conocimientos previos' o 'ideas ancla' (Ausubel, 1963).

A diferencia del aprendizaje memorístico o mecánico, en el que la información se almacena de forma aislada y tiende a olvidarse con rapidez, el aprendizaje significativo genera conexiones duraderas que facilitan la comprensión profunda y la transferencia del conocimiento a nuevas situaciones. Para que este tipo de aprendizaje ocurra, Ausubel identifica tres condiciones fundamentales: que el material sea potencialmente significativo, que el aprendiz disponga de conocimientos previos relevantes con los cuales relacionarlo, y que exista una disposición activa del aprendiz hacia el aprendizaje (Ausubel, Novak y Hanesian, 1983).

En el contexto de CyberQuest, la teoría del aprendizaje significativo se operacionaliza mediante la selección de temáticas asociadas a situaciones cotidianas del usuario —como el uso de contraseñas, la navegación en internet o la recepción de correos electrónicos sospechosos— lo que permite que el jugador establezca conexiones entre el contenido del juego y sus experiencias digitales previas. De este modo, el aprendizaje no se limita al desempeño dentro del juego, sino que favorece la reflexión y la adopción de buenas prácticas en la vida real.

2.5 Gamificación educativa

La gamificación se define como la aplicación de elementos y mecánicas propias de los juegos en contextos que no son juegos, con el propósito de incrementar la motivación, el compromiso y el comportamiento deseado en los participantes (Deterding, Dixon, Khaled y Nacke, 2011). A diferencia de los videojuegos serios, que son juegos completos diseñados con un propósito educativo o de entrenamiento, la gamificación toma elementos específicos del juego —como puntos, insignias, tablas de clasificación o narrativas— y los integra en actividades de aprendizaje o procesos organizacionales.

En el ámbito educativo, la gamificación ha demostrado tener un impacto positivo en la motivación intrínseca de los estudiantes, en su nivel de participación y en la retención del conocimiento. Kapp (2012) señala que los elementos del juego generan en el aprendiz un estado de flujo —concepto acuñado por Csikszentmihalyi (1990)— caracterizado por una concentración profunda y una sensación de disfrute

que favorece el aprendizaje. Este estado se alcanza cuando el nivel de desafío de la tarea corresponde con las capacidades del usuario: si el reto es demasiado bajo, el usuario se aburre; si es demasiado alto, se frustra.

Los elementos de gamificación más comúnmente utilizados en entornos educativos incluyen los siguientes:

- Puntos y sistemas de puntuación. Proporcionan retroalimentación inmediata sobre el desempeño y generan una sensación de progreso constante.
- Insignias y logros. Funcionan como reconocimiento visible de las habilidades adquiridas, lo que refuerza la motivación y la autoeficacia del aprendiz.
- Niveles progresivos. Permiten estructurar el contenido de menor a mayor complejidad, facilitando una curva de aprendizaje gradual.
- Retroalimentación inmediata. Informa al usuario de manera instantánea sobre la corrección o incorrección de sus acciones, lo que facilita la corrección de errores y el aprendizaje por ensayo.
- Narrativa. Dota de contexto y significado a las actividades, aumentando el nivel de inmersión y la conexión emocional del usuario con el contenido.

En el caso de CyberQuest, la gamificación se materializa a través del sistema de trofeos otorgados al responder correctamente cada pregunta, el desbloqueo secuencial de niveles que introduce los temas de ciberseguridad de forma progresiva, la retroalimentación inmediata ante respuestas correctas e incorrectas, y la recomendación de artículos de repaso cuando el usuario no logra superar un nivel. Estos elementos, en conjunto, buscan mantener al usuario motivado y comprometido con el aprendizaje a lo largo de los nueve niveles del juego.

2.6 Conciencia situacional en ciberseguridad

La conciencia situacional (situational awareness) es un concepto originalmente desarrollado en el ámbito de la aviación y la psicología cognitiva, que describe la capacidad de una persona para percibir los elementos relevantes de su entorno, comprender su significado y proyectar su estado futuro con el fin de tomar decisiones informadas (Endsley, 1995). Este modelo ha sido ampliamente adoptado en el campo de la ciberseguridad para describir el nivel de comprensión que un usuario tiene respecto a los riesgos y amenazas presentes en el entorno digital.

Endsley (1995) propone que la conciencia situacional se desarrolla en tres niveles jerárquicos y progresivos:

- Nivel 1 – Percepción. El usuario es capaz de identificar y detectar los elementos relevantes del entorno, como reconocer un correo electrónico sospechoso, identificar una URL maliciosa o notar comportamientos inusuales en un sistema.
- Nivel 2 – Comprensión. El usuario no solo detecta los elementos, sino que comprende su significado y su potencial impacto. Por ejemplo, entiende que un enlace desconocido en un correo podría ser un intento de phishing y que hacer clic en él podría comprometer su información personal.

- Nivel 3 – Proyección. El usuario es capaz de anticipar cómo evolucionará una situación y tomar decisiones preventivas antes de que se materialice la amenaza. Este nivel representa el más alto grado de conciencia situacional y es el objetivo final de la educación en ciberseguridad.

En el contexto de la ciberseguridad para usuarios finales, diversos autores han señalado que la mayoría de los incidentes ocurren precisamente porque los usuarios operan en el Nivel 1 o incluso por debajo de él: no identifican las señales de alerta presentes en su entorno digital (Jajodia et al., 2010). La falta de conciencia situacional explica, en gran medida, por qué el factor humano continúa siendo el eslabón más débil en la cadena de seguridad, representando hasta el 74% de los incidentes de ciberseguridad en México según datos de Infobae México (2024).

CyberQuest aborda los tres niveles de conciencia situacional a través de su mecánica de juego: las preguntas de opción múltiple requieren que el usuario identifique situaciones de riesgo (Nivel 1), comprenda por qué representan una amenaza y cuáles son sus consecuencias (Nivel 2), y seleccione la acción preventiva correcta (Nivel 3). De este modo, el videojuego no solo evalúa el conocimiento factual del usuario, sino que entrena su capacidad de razonamiento ante escenarios reales de ciberseguridad.

2.7 Trabajos relacionados

El uso de videojuegos y entornos de escape room digitales como herramientas de educación en ciberseguridad ha experimentado un crecimiento notable en la última década. A continuación se presenta una revisión de los trabajos más relevantes en esta área, con el propósito de contextualizar el aporte de CyberQuest dentro del estado actual del conocimiento y destacar los elementos diferenciadores del presente trabajo.

EyesOnCS — Educational Escape Room Game to Develop Cybersecurity Skills

Spatafora et al. (2024) desarrollaron EyesOnCS, un videojuego de escape room educativo diseñado para mejorar la conciencia en ciberseguridad de empleados de pequeñas y medianas empresas (PyMEs). El juego sigue una narrativa en la que el jugador asume el rol de un nuevo empleado en el departamento de seguridad de un banco y enfrenta desafíos basados en situaciones reales, cubriendo temas como el reconocimiento de mensajes maliciosos, llamadas fraudulentas y correos de ingeniería social. El estudio fue evaluado con más de 200 participantes y utilizó el Game Experience Questionnaire (GEQ), un instrumento validado, para medir la experiencia de juego.

Este trabajo es especialmente relevante para CyberQuest porque comparte la mecánica de escape room, los temas de ciberseguridad orientados a usuarios no especializados y un tamaño de muestra comparable. La principal diferencia radica en el contexto de aplicación: EyesOnCS está orientado al entorno empresarial, mientras que CyberQuest está dirigido a estudiantes universitarios en México. Adicionalmente, EyesOnCS empleó un instrumento validado para la evaluación, lo

que constituye una fortaleza metodológica que puede considerarse como una dirección de mejora para trabajos futuros de CyberQuest.

2.8 Análisis de necesidades

Con base en la previa investigación, se observa que dentro de las áreas que engloba la ciberseguridad existen diversas vulnerabilidades y amenazas, que a su vez implican riesgos. Una de las cinco fuentes de amenaza es el factor humano, este se considera uno de los mayores retos, puesto que es el factor más impredecible, debido a que las personas actúan con base en lo que conocen y en muchas ocasiones el conocimiento que poseen es limitado, por ello es importante acercar a las personas a estos temas de una manera agradable y entretenida.

En la actualidad gran parte de la población mundial almacena información personal en línea, como datos bancarios, información de identidad, correos electrónicos y datos en redes sociales, por lo que, una de las vulnerabilidades que se deben tomar en cuenta es el uso de contraseñas inseguras, ya que a causa de esto la información personal e identidad de cada individuo puede quedar expuesta a posibles amenazas.

Los ciberdelincuentes utilizan diversas técnicas para obtener contraseñas, por ejemplo, el phishing, el keylogging y la fuerza bruta por mencionar algunos, por lo que una vez que ganan acceso puede resultar en suplantación de identidad, robo de dinero, difundir información privada o daños a la reputación.

De igual importancia, cada vez que navegamos en el ciberespacio ya sea para realizar transacciones, almacenar información, comunicarnos con otras personas o cualquier otra actividad que se realice dentro del ciberespacio, estamos expuestos a diversos riesgos como sitios web maliciosos, ataques de phishing, descarga de malware, entre otros. Por lo antes mencionado es importante que se utilicen medidas de seguridad adecuadas ya que de no hacerlo puede derivar en diversas consecuencias, por ejemplo, una de las amenazas más frecuentes es el malware, el cual puede causar daños significativos, como: pérdida de información, espionaje e interrupción de servicios en línea.

Es necesario que se tenga conocimiento acerca de los diferentes ataques de ingeniería social, puesto que son técnicas comúnmente utilizadas por los atacantes para engañar a las personas y obtener acceso no autorizado a la información o a los sistemas.

Así mismo, la configuración de seguridad, las actualizaciones e identificar las vulnerabilidades de un sistema operativo nos puede ayudar a protegernos contra amenazas como lo son el malware o virus, esto es importante ya que son los responsables de controlar el acceso al hardware y a los recursos del sistema, por lo que sí resulta comprometido, el atacante puede tener acceso a todo el sistema y sus datos.

Actualmente y a raíz de la pandemia, las videoconferencias se volvieron algo común y una herramienta esencial para el trabajo remoto, sin embargo, su uso también

conlleva diversos riesgos que son importantes dar a conocer, por ejemplo, las plataformas utilizadas pueden tener vulnerabilidades que podrían ser explotadas por ciberdelincuentes, puede existir fuga de información al momento de compartir pantallas o documentos que contengan información confidencial o en otros casos los ciberdelincuentes pueden enviar malware a través de la plataforma.

A la vez que se volvió común el uso de herramientas para videoconferencia, también incrementó el uso de la nube para diversas necesidades, y así como la tecnología está en constante evolución, los ciberataques también van evolucionando y volviéndose más sofisticados, por ello, al hacer uso de la nube también debemos mantenernos prevenidos asegurándonos de que nuestros datos estén protegidos de posibles accesos no autorizados, verificar que sólo las personas autorizadas tengan acceso a la información compartida, conocer las regulaciones existentes y tener un respaldo en caso de alguna falla en el sistema o error humano.

Tener copias de seguridad también es importante ya que son una medida de protección contra la pérdida de datos, ya sea debido a errores humanos, fallas del sistema, desastres naturales y ataques cibernéticos.

Un elemento que también se considera esencial poseer en un antivirus, puesto que son una capa de protección para los dispositivos, así como para la información del usuario ante cualquier ataque de un software malicioso.

En resumen, cada vez confiamos más en la tecnología y la conectividad, y aun cuando los responsables de esto hacen los esfuerzos necesarios para mantenerlos seguros, es responsabilidad de los usuarios aplicar las buenas prácticas, ya que de lo contrario se está más expuestos a riesgos en línea. Por lo tanto, es fundamental proteger nuestra información y privacidad y prevenir posibles ataques y fraudes.

Tomando en cuenta las necesidades identificadas anteriormente, se seleccionaron los siguientes temas que se consideran más relevantes para dar a conocer y llevar a cabo la prevención de ataques y concientización:

- ➔ Contraseñas.

  Una contraseña segura es difícil de adivinar o descifrar, dificulta que una persona mal intencionada acceda a nuestras cuentas.

- ➔ Navegación segura.

  Ayuda a proteger nuestra información personal y nuestra privacidad en línea, así como prevenir fraudes y ataques cibernéticos.

- ➔ Ataques de ingeniería social.

  Al conocer el funcionamiento de estos ataques, se pueden tomar medidas preventivas.

- ➔ Malware.

  Al conocer cómo funciona y se propaga, se pueden tomar medidas preventivas y así reducir el riesgo de infección.

- ➔ Sistemas Operativos.

Si los configuramos adecuadamente y los actualizamos de manera constante, podemos estar mejor protegidos.

➔ Videoconferencia.

Si tenemos cuidado al hacer uso de estas herramientas, podemos tomar medidas para evitar fugas de información.

➔ Uso seguro de la nube.

Si se conocen los riesgos al usar la nube podemos tomar medidas preventivas.

➔ Copias de seguridad.

Al reconocer su importancia podemos tener resguardada y respaldada nuestra información.

➔ Antivirus.

Nos ayudan a mantenernos seguros en contra de ataques y a proteger nuestros datos.

Se puede concluir que las personas somos el eslabón más débil dentro de la ciberseguridad, por lo que resulta importante y prioritario que adquieran los conocimientos teóricos y prácticos para invitarles a reflexionar de una manera lúdica, además de que se lleve a cabo en un entorno seguro y conocer el modo de operar de los ciberdelincuentes es indispensable para tomar las medidas necesarias. De esta manera se invita a los usuarios a mejorar su seguridad y con ello corregir las vulnerabilidades prioritarias al navegar por el ciberespacio y así lograr una reducción en los ataques.

Capítulo III. Diseño y desarrollo

3.1 Alternativas de solución

Hoy en día, los estudiantes tienen acceso a una gran cantidad de información a través de diversas alternativas tecnológicas, que nos permiten aplicar estrategias de aprendizaje, es por ello que el contexto educativo en el que vivimos actualmente, donde las tecnologías como medios para la educación y la era digital están en constante y acelerada evolución, requiere un aprendizaje dinámico y desarrollo de nuevas competencias.

Existen diversas estrategias de aprendizaje para llegar al objetivo, a continuación se mencionan algunas de ellas:

- Tutoriales. De acuerdo con Gonzalez Y., el tutorial es un método para transferir conocimiento, es una guía paso a paso que nos ayuda a realizar una tarea específica. Los tutoriales requieren de una planeación para que puedan ser incorporados en el aprendizaje, ya que su éxito va a depender de que el material sea atractivo y que los objetivos estén alineados al mensaje que se desea abordar. Según Boschi L., está basado en la estrategia de

enseñanza denominada aprendizaje por descubrimiento, en esta estrategia el estudiante/aprendiz se apropia del proceso.

Alicia B. y Zulema B., dicen que los tutoriales son bastante útiles en aquellas áreas del conocimiento donde la solución a los problemas requiere determinado procedimiento o proceso paso a paso, y para que un tutorial pueda considerarse recurso educativo debe cumplir con las siguientes características:

- ➢ El contenido debe estar adaptado al nivel de conocimientos del público.
- ➢ Debe poseer una clara estructuración de la información.
- ➢ Debe tener una estrategia para mostrar y explicar el contenido.
- ➢ Si bien el tutorial ha sido constantemente utilizado, se han desarrollado vídeos para mostrar la ejecución de cada uno de los pasos para que se pueda realizar determinada tarea o exponer un tema de manera más clarificada.

- Videos.Han ganado popularidad como herramientas de enseñanza y aprendizaje, debido a que transmiten información de manera visual y atractiva, lo que puede facilitar la comprensión y retención de contenido. Pueden abordar diversos temas y vienen en diferentes formatos como conferencias, documentales, animaciones, entre otros.

  De acuerdo con diversos autores, la efectividad de los vídeos como método de aprendizaje está en su capacidad de combinar diferentes estímulos sensoriales, presentar ejemplos prácticos además de fomentar la participación activa y el aprendizaje. Aunado a esto los vídeos como método de aprendizaje tienen la característica de ser pausados, retrocedidos y reproducidos permitiendo controlar su ritmo de aprendizaje, sin embargo, también existen diversos factores que resultan contraproducentes, como la calidad del vídeo, la relevancia del contenido y la duración del vídeo.

  Según Gonzalez Y. Los vídeos deben contar con las siguientes características:

  - ➢ Organización de contenidos.
  - ➢ Análisis de formas para presentar la información.
  - ➢ Gráficos para representar las situaciones.
  - ➢ Debe servir como material de consulta.

- Artículos. Este método de aprendizaje se refiere a la lectura de textos académicos, científicos o educativos para adquirir conocimiento y aprender sobre un tema en específico. Son una de las principales fuentes de información y proporcionan análisis e investigaciones detalladas sobre varios temas. Al usar este método se tiene información precisa, actualizada y respaldada por evidencia científica, presentan un formato estructurado con introducción, metodología, resultados y conclusiones lo que facilita la organización y comprensión del conocimiento.

  De acuerdo con Day y Bamford, la lectura de artículos como método de aprendizaje requiere habilidades de comprensión lectora, capacidad para evaluar la calidad y la relevancia del contenido, así como una actitud crítica hacia la información presentada.

  Según Mata L. Un artículo debe cumplir con las siguientes características:

  - ➢ Presentar una estructura formal coherente con una secuencia lógica en que se organizan las etapas del proceso de investigación.
  - ➢ Brindar una amplia síntesis de procesos investigativos efectuados.
  - ➢ Permitir la visualización de manera accesible y la interrelación del conjunto de etapas del procesos de investigación.

- Juegos. Como mencionan Cristina M., Fanny P., Aleira O. y Gladys C. en su artículo “El juego como método de aprendizaje” el juego es innato en el humano. Todos los seres han aprendido desde su nacimiento a relacionarse con su familia y el mundo exterior a través del juego. Es una actividad necesaria para los seres humanos ya que es una herramienta útil para adquirir y desarrollar capacidades intelectuales, motoras o afectivas. Todo ello se debe realizar de forma gustosa y placentera, sin sentir obligación de ningún tipo y con el tiempo y el espacio necesarios.

  Al utilizar el juego como método de aprendizaje, se desarrollan diversos procesos cognitivos como: la observación, la atención, la concentración y la memoria. Es esencial tener presente que el juego como método de aprendizaje tiene una intención, una planificación y objetivos específicos.

  De acuerdo a diversos autores los juegos como método de aprendizaje deben cumplir en esencia, las siguientes características:

  - ➢ Resolución interactiva de problemas.
  - ➢ Metas y reglas específicas.
  - ➢ Retos.
  - ➢ Control del ritmo de aprendizaje.
  - ➢ Feedback.
  - ➢ Estímulos sensoriales.

Después de haber revisado los diferentes métodos de aprendizaje, se presenta un análisis comparativo en la tabla 1.0.

Tabla 1.0 . Análisis comparativo de los métodos de aprendizaje.

	Tutoriales	Videos	Artículos	Juegos
Divertido	✗	✓	✗	✓
Diferentes estímulos sensoriales	✗	✓	✗	✓
Controlar ritmo aprendizaje.	✓	✓	✓	✓
Monótono	✓	✓	✓	✗
Requiere habilidades previas	✗	✗	✓	✗
Es retador.	✗	✗	✗	✓
El contenido está adaptado para el nivel de conocimiento del público.	✓	✓	✓	✓
Organización de contenidos.	✓	✓	✓	✓
Resolución interactiva de problemas.	✓	✓	✗	✓

Estos son sólo algunos caminos que nos permiten aplicar las estrategias de aprendizaje, cada uno se adapta a las distintas necesidades de las personas, sin embargo, en este trabajo se seleccionó el juego, ya que, como se observa en la tabla 1.0 “Análisis comparativo de los métodos de aprendizaje”, cumple con diversas características que lo hacen más interesante, como la resolución de interactiva de problemas, los retos que se presentan, son divertidos ya que comúnmente se hace de forma gustosa y sin sentir algún tipo de obligación.

Es por ello que: “La enseñanza y el aprendizaje son procesos que se presentan juntos, es decir, las estrategias que se emplean para la instrucción inciden en los aprendizajes” (Monereo, 2000).

La tecnología y el aprendizaje es algo que nos acompaña día a día, ya sea como estudiantes o en el ámbito laboral, por ello es deseable que los usuarios tengan conocimiento de conceptos básicos de ciberseguridad para que puedan saber cómo, cuándo y por qué deben utilizarlos.

3.2 Necesidades y estructura del juego

Con base en la previa investigación realizada, se lograron identificar las siguientes necesidades para el juego:

- Desafíos en cada área. Habrá diferentes desafíos para poder mantener el interés y motivar a las personas a seguir aprendiendo.

- Recompensas y progresión. Debe tener algún tipo de recompensa al superar algún desafío para satisfacer el deseo de progreso y mejorar la experiencia.
- Curva de aprendizaje. Identificar la cantidad de niveles que son necesarios para que las personas obtengan un conocimiento básico en ciberseguridad.
- Sensación de logro. Los logros deben sentirse significativos superando los diversos desafíos (Niveles)
- Exploración y descubrimiento. Debe tener una estructura que fomente la exploración para satisfacer su curiosidad en un ambiente seguro donde se puedan cometer errores.
- Retroalimentación positiva. Utilizará una estructura que da retroalimentación positiva cuando se tiene un respuesta errónea o completan tareas.

En cuánto a su estructura:

- Niveles o escenarios. El juego cuenta con nueve niveles, que son los temas que se requieren para que una persona adquiera un conocimiento básico en ciberseguridad.
- Objetivos. El objetivo general del juego es que los usuarios obtengan los fundamentos necesarios para tener buenas prácticas en ciberseguridad, así como adentrarse más en este ámbito y a tomar conciencia sobre la importancia de estar protegidos en el ciberespacio.
- Personajes. El juego consta de un único personaje con perspectiva en primera persona, es decir, el jugador verá a través de los ojos de uno de los personajes que está bajo su control y que se mueve en el espacio del juego.
- Sistema de puntuación y progreso. Se asignará un trofeo por cada pregunta que es respondida correctamente, al obtener todos los trofeos de cada nivel, se podrá pasar al siguiente, de lo contrario se dará retroalimentación.
- Mecánica del juego. En cada nivel habrá preguntas ocultas, dependiendo del tema que se aborde en cada nivel, es la cantidad de preguntas que se tendrán que resolver, ya que los temas no son igual de extensos y no se pueden abordar con la misma cantidad de preguntas. Al encontrar las preguntas ocultas deberán responderlas, si lo hacen de manera correcta se les entregará un trofeo, si se responden todas las preguntas de manera correcta podrán avanzar al siguiente nivel, de lo contrario se les dará retroalimentación.
- Interfaz de usuario. (Cómo se presenta la información al jugador.) La información será presentada a través de tarjetas que contienen preguntas relacionadas al tema del nivel y con opción múltiple de respuestas.
- Modo de juego. Un único jugador con perspectiva en primera persona.

3.3 Requerimientos técnicos

Con base en los requerimientos identificados en el capítulo anterior, es necesario determinar qué herramientas se usarán para crear el videojuego, considerando esencialmente herramientas de software y hardware.
Para las herramientas de software se necesita principalmente un motor de videojuegos, de los cuales en el mercado existe una gran variedad, sin embargo, la búsqueda se enfocará en aquellos que ofrezcan lenguaje de programación universal y con versiones gratuitas. Después de haber revisado diferentes motores de

videojuegos, se presenta un análisis comparativo de los encontrados con las características mencionadas en la tabla 2.0.

Tabla 2.0 Análisis comparativo de motores de videojuego

Motor de Juego	**Lenguajes de programación soportados**	**Plataformas soportadas**	**Curva de aprendizaje**
Unity	C#, UnityScript (descontinuado)	Múltiples, incluyendo PC, consolas, móviles, VR y web	Moderada - Fácil para principiantes, pero profunda para expertos.
Unreal Engine	C++, Blueprints (lenguaje visual)	Múltiples, incluyendo PC, consolas, móviles y VR	Más enfocada para principiantes, pero poderosa.
Godot	GDScript, C#, VisualScript.	Múltiples, incluyendo PC, consolas, móviles y web	Moderada - Fácil para principiantes.
CryEngine	C++, C# (a través de plugins)	PC, consolas, VR	Más enfocada para principiantes
Lumberyard	C++, Lua (a través de plugins)	PC, consolas, VR	Más enfocada para principiantes

Motor de Juego	**Comunidad y recursos**	**Precio**	**Requerimientos de Hardware**
Unity	Gran comunidad, abundancia de tutoriales y activa Asset Store	Gratis (versión personal) o con licencia Pro	Mínimos: -Procesador (CPU):Compatible con SSE2 -Tarjeta gráfica (GPU): Con capacidad para DirectX 10 y Shader Model 4.0. -RAM: 4 GB de RAM. -Espacio en disco duro: 10 GB de espacio libre.

			-Sistema Operativo: Windows 7 SP1+, macOS 10.12+, Ubuntu 16.04+.
			Recomendados: -Procesador (CPU): Quad-core Intel o AMD. -Tarjeta gráfica (GPU): NVIDIA GeForce 600 Series o AMD Radeon HD 7000 Series con OpenGL 3.2 soporte. -RAM: 8 GB o más de RAM -Espacio en disco duro:SSD para un rendimiento óptimo. -Sistema Operativo: Windows10, macOS 10.14+, Ubuntu 18.04+.
Unreal Engine	Comunidad sólida y abundancia de recursos, Marketplace activo	Gratis (hasta cierto umbral de ingresos, luego regalías)	Mínimos: -Procesador (CPU): Quad-core Intel o AMD, 2.5 GHz o más rápido. -Tarjeta gráfica (GPU):NVIDIA GeForce 470 GTX o AMD Radeon 6870 HD series o superior -RAM:8 GB de RAM. -Espacio en disco duro:145 GB de espacio libre. -Sistema Operativo: Windows 7 de 64 bits o macOS 10.14.6 o superior.
			Recomendados: -Procesador (CPU):Intel Core i7 3.5 GHz o AMD FX-8350 4.0 GHz. -Tarjeta gráfica (GPU):NVIDIA

			GeForce GTX 970 o AMD Radeon R9 290 o superior. -RAM:16 GB de RAM o más. -Espacio en disco duro:SSD con 145 GB de espacio libre -Sistema Operativo: Windows 10 de 64 bits.
Godot	Comunidad en crecimiento, documentación sólida	Código abierto y gratuito	Mínimos: -Procesador (CPU): Dual-core. -Tarjeta gráfica (GPU): Compatible con OpenGL ES 3.0/3.1. -RAM: 2 GB de RAM. -Espacio en disco duro: Depende del tamaño del proyecto. -Sistema operativo: Variado (Windows, macOS, Linux).
			Recomendados: -Procesador (CPU): Quad-core. -Tarjeta gráfica (GPU): NVIDIA GeForce GTX 660 o AMD Radeon HD 7870. -RAM: 4 GB de RAM. -Espacio en disco duro: Depende del tamaño del proyecto. -Sistema operativo: Variado (Windows, macOS, Linux).
CryEngine	Comunidad más pequeña, recursos limitados	Gratis con regalías	Mínimos: -Procesador (CPU): Intel Dual-Core 2 GHz o AMD Dual-Core 2 GHz. -Tarjeta gráfica (GPU): NVIDIA

			GeForce 770 o AMD Radeon 7970. -RAM: 8 GB de RAM. -Espacio en disco duro: 8 GB de espacio libre. -Sistema operativo: Windows 7 de 64 bits o superior.
			Recomendados: -Procesador (CPU): Intel Quad-Core 3 GHz o AMD Ryzen 5 1600. -Tarjeta gráfica (GPU): NVIDIA GeForce GTX 1060 o AMD Radeon RX 580. -RAM: 16 GB de RAM. -Espacio en disco duro: SSD con 8 GB de espacio libre. -Sistema operativo: Windows 10 de 64 bits.
Lumberyard	Comunidad en crecimiento, recursos limitados	Gratis con regalías	Mínimos: -Procesador (CPU): Quad-core Intel o AMD. -Tarjeta gráfica (GPU): NVIDIA GeForce 470 GTX o AMD Radeon 6870 HD series o superior. -RAM: 8 GB de RAM. -Espacio en disco duro: 200 GB de espacio libre en SSD. -Sistema operativo: Windows 10 de 64 bits.
			Recomendados: -Procesador (CPU): Intel Core i7 4.0 GHz o AMD Ryzen

			7 1800X. -Tarjeta gráfica (GPU): NVIDIA GeForce GTX 1060 o AMD Radeon RX 580. -RAM: 16 GB de RAM. -Espacio en disco duro: 200 GB de espacio libre en SSD. -Sistema operativo: Windows 10 de 64 bits.

Estos son sólo algunos motores que permiten desarrollar videojuegos, cada uno se adapta a distintas necesidades, sin embargo, en este trabajo se seleccionó Unity, ya que, como se muestra en la tabla 2.0, cumple con las siguientes características:

- Amplia Compatibilidad: Unity es conocido por su amplia compatibilidad con una variedad de plataformas, lo que facilita el desarrollo multiplataforma.

- Lenguaje C#: El lenguaje de programación C# Es ampliamente utilizado en la industria y es relativamente fácil de aprender, lo que hace que Unity sea accesible para programadores principiantes.

- Gran Comunidad y Recursos: Unity tiene una comunidad de usuarios activa y una gran cantidad de recursos en línea, incluyendo tutoriales y una tienda de activos que facilita el desarrollo de juegos.

- Modelo de Precios Flexible: Unity ofrece una versión personal gratuita y opciones de licencia asequibles para pequeños equipos, lo que lo hace más accesible para desarrolladores independientes y estudios pequeños.

- Versatilidad en Géneros de Juegos: Unity ha sido utilizado para desarrollar una amplia variedad de géneros de juegos, desde juegos 2D simples hasta títulos AAA en 3D.

Dentro de la tabla 2.0 que se muestra anteriormente podemos encontrar las características de hardware mínimas y recomendadas, estas pueden variar dependiendo del tipo de juego que se desarrollará.

A continuación se muestran las capacidades del dispositivo donde se desarrolla el video juego.

- Procesador (CPU): Intel(R) Core(TM) i7-10750H
- Tarjeta gráfica (GPU): NVIDIA GeForce GTX 1660 Ti
- RAM: 16 GB de RAM.
- Espacio en disco duro: 500 GB de espacio en SSD, 293 disponibles.

- Sistema operativo: Windows 10 de 64 bits.

Además de todas estas características se puede exportar a diversas plataformas como:

- PC (Windows, MAC y Linux)
- Consolas (Play, xBox y Nintendo)
- Dispositivos móviles (Android, IoS)
- Realidad Virtual y Realidad Aumentada.
- Navegadores Web.
- Plataformas de Transmisión de Streaming.

A pesar de que el juego puede exportarse a múltiples plataformas, por el momento se realizó la exportación únicamente para Windows con el objetivo de facilitar las pruebas, ya que es el sistema operativo más estándar y ampliamente utilizado, lo que garantiza mayor compatibilidad y acceso durante el proceso.

Las capacidades de software y hardware necesarias para ejecutar un juego desarrollado en Unity varían según la complejidad y los requisitos específicos del juego, para éste juego se muestran las características que se deben cumplir:

- Sistema Operativo: Windows 10 o superior.
- Procesador mínimo recomendado: Intel Core i3 (2 núcleos) o equivalente AMD.
- Memoria RAM: 4GB.
- Almacenamiento: Al menos 500 MB libres.
- Resolución recomendada: 1920 x 1080 (HD).

3.4 Diseño

3.4.1 Diseño de interfaz

La interfaz se diseñó con el objetivo de que el usuario tenga una experiencia clara y de forma continua, considerando que el juego está enfocado a la enseñanza y refuerzo de conceptos de ciberseguridad. Se decidió que la interfaz debe ser una vista sencilla y accesible que permita al jugador priorizar su concentración en las preguntas y en la resolución de los niveles sin que los elementos visuales generen distracción.
La interfaz emplea una base de colores suaves que aporta una apariencia visual equilibrada y amigable, complementada con tonos contrastantes utilizados para destacar elementos interactivos como botones y mensajes informativos. Esta combinación mejora la legibilidad de los textos y facilita la identificación de acciones disponibles, al mismo tiempo que crea un ambiente visual armónico.

La distribución de los elementos en pantalla se definió bajo principios de usabilidad: botones de gran tamaño y alta legibilidad, menús fáciles de identificar y un flujo visual que guía al usuario de manera natural. El menú principal presenta los niveles de forma ordenada y mostrando los que están desbloqueados y los que no, facilitando la progresión y evitando confusiones. Asimismo, se cuidó el uso de

tipografías claras y consistentes en todo el sistema para mantener uniformidad y facilitar la lectura durante el límite de tiempo establecido en cada nivel.

3.4.2 Diseño de escenarios

El diseño de escenarios se enfocó en recrear un ambiente que alude la temática de un escape room digital, incorporando elementos visuales que refuerzan la identidad del juego sin sobrecargar el espacio. Cada escenario fue planteado para tener una estructura visual uniforme: un fondo neutro que permita destacar los objetos interactivos, tarjetas de preguntas bien delimitadas y una estructura visual que organiza los elementos sin generar ruido cognitivo.

El escenario principal corresponde al menú inicial, donde se presentan los nueve niveles del juego con el objetivo de orientar al usuario desde el primer momento, mostrando el avance logrado mediante la visualización de niveles bloqueados y desbloqueados.
En las pantallas internas de los niveles se mantuvo un enfoque homogéneo, utilizando fondos en su mayoría de colores suaves, paneles limpios y una disposición centrada de las tarjetas de preguntas al abrirlas. Esta consistencia visual favorece que el usuario se enfoque en la tarea principal: resolver correctamente las tarjetas dentro del tiempo asignado. Además, el menú de pausa se creó como una interfaz secundaria que aparece superpuesto, manteniendo la coherencia gráfica del resto del juego.

3.4.3 Diseño de mecánica del juego

La mecánica del juego se diseñó con la intención de integrar un proceso de aprendizaje estructurado a través de niveles progresivos. Cada nivel contiene cinco tarjetas de preguntas que deben resolverse de manera correcta para avanzar al siguiente. Se estableció un límite de tiempo de diez minutos por nivel como parte del desafío, incentivando la concentración y la gestión del tiempo del jugador.

La navegación dentro del nivel incorpora un botón de pausa que permite reanudar, reiniciar o salir del juego; sin embargo, este menú sólo puede activarse cuando no hay una tarjeta abierta, a fin de evitar interrupciones en mitad de una pregunta. El sistema implementa además una mecánica de reinicio automático en caso de interrupciones o cierre inesperado, garantizando la integridad del progreso y la consistencia del desafío.

El desbloqueo de niveles es secuencial: el jugador accede inicialmente solo al primer nivel y avanza conforme complete satisfactoriamente cada etapa. En caso de responder incorrectamente, el juego ofrece dos alternativas: reiniciar el nivel o consultar un artículo de repaso, fortaleciendo el objetivo educativo del proyecto.

3.4.4 Diseño de preguntas

El diseño de las preguntas conforman una parte fundamental del desarrollo, ya que representan el contenido educativo que sustenta el aprendizaje del usuario. Para ello, se seleccionaron temas clave de ciberseguridad, incluyendo contraseñas

seguras, ingeniería social, malware, navegación segura y manejo de información personal. La organización de los temas sigue una progresión lógica que permite al usuario avanzar desde conceptos básicos hasta temas más complejos.

Las preguntas fueron elaboradas en formato de opción múltiple para facilitar su integración al sistema y permitir una evaluación rápida dentro del límite de tiempo. Además, se buscó que cada reactivo promoviera la reflexión, evitando respuestas triviales. Se cuidó que el lenguaje empleado fuera claro y accesible, sin tecnicismos innecesarios, para asegurar la comprensión incluso en usuarios con conocimientos limitados en el área.

Finalmente, la estructura de retroalimentación en caso de respuestas incorrectas —que incluye la opción de consultar un artículo adicional— se integró como una estrategia que refuerza el aprendizaje significativo y motiva al usuario a corregir sus errores antes de continuar.

3.4.5 Diseño de vistas de los objetos

Este apartado se centró en la representación visual de los objetos interactivos del juego, buscando mantener una estética uniforme y funcional. Las tarjetas de preguntas fueron diseñadas con un contorno claro y bordes redondeados, destacándose sobre el fondo mediante un contraste adecuado para mejorar la legibilidad. Cada tarjeta incluye el enunciado, las opciones de respuesta y un diseño ordenado que facilita la interacción rápida.

Los botones —como los presentes en el menú principal, en el menú de pausa o en las pantallas de confirmación— se diseñaron con tamaños amplios, tipografía clara y estados visuales diferenciados (normal, resaltado y presionado) que brindan al usuario retroalimentación inmediata al interactuar. Esto mejora la experiencia y reduce errores de navegación.

Asimismo, se diseñaron iconos e indicadores visuales para representar acciones como pausar, reiniciar o salir. Estos elementos fueron seleccionados con base en su universalidad y facilidad de reconocimiento, de modo que el usuario pueda ubicarlos intuitivamente. La coherencia visual entre todos los objetos garantiza una navegación fluida en cada etapa del juego.

3.5 Desarrollo de las etapas de diseño identificadas

En esta etapa se llevó a cabo la implementación de los elementos definidos durante la fase de diseño, integrando la interfaz, los escenarios, la mecánica del juego y los objetos interactivos dentro del motor de desarrollo seleccionado. El proceso de desarrollo se centró en transformar los bocetos y propuestas visuales en un sistema funcional que respetara la estructura y los objetivos planteados previamente.

La interfaz del juego fue implementada conforme a los criterios establecidos, incorporando los menús de navegación, el sistema de selección de niveles y los

elementos visuales necesarios para guiar al usuario durante la experiencia de juego. Asimismo, se desarrollaron los escenarios correspondientes a cada nivel, integrando objetos decorativos e interactivos que permiten la exploración del entorno y la interacción con las tarjetas de preguntas.

En cuanto a la mecánica del juego, se programaron las reglas que regulan el avance entre niveles, el control del tiempo, el sistema de desbloqueo progresivo y la gestión de las opciones disponibles para el usuario, como pausar, reiniciar o salir del nivel. Cada uno de estos componentes fue integrado de manera coherente con el diseño propuesto, asegurando una experiencia continua y estructurada.

Finalmente, se incorporaron las vistas de los objetos interactivos, tales como tarjetas, botones e indicadores visuales, manteniendo una identidad gráfica uniforme en todo el sistema.
Las Figuras 15 a 33 muestran la implementación final de los escenarios y pantallas del juego, evidenciando la correspondencia entre el diseño planteado y el producto desarrollado.

- Interfaz

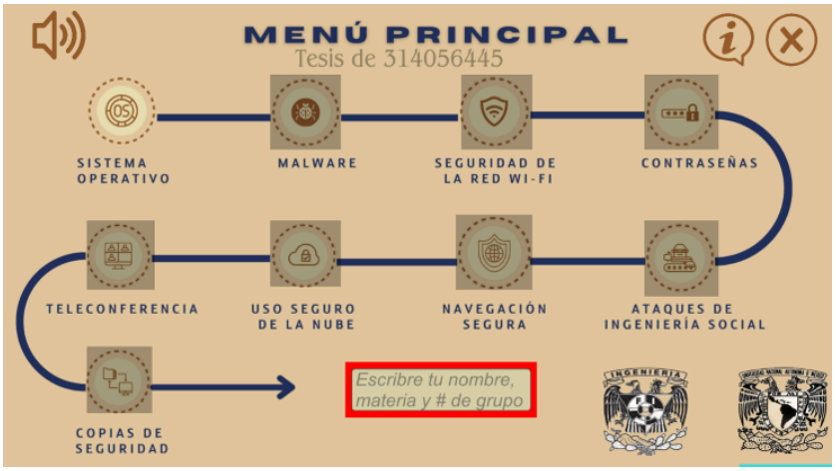


Figura 4. Vista del menú principal.

Figura 5. Botón para activar y desactivar sonido.

Figura 6. Botón de salida.

Figura 7. Botón para mostrar las instrucciones

Figura 8. Animación al iniciar el primer nivel

- Escenarios

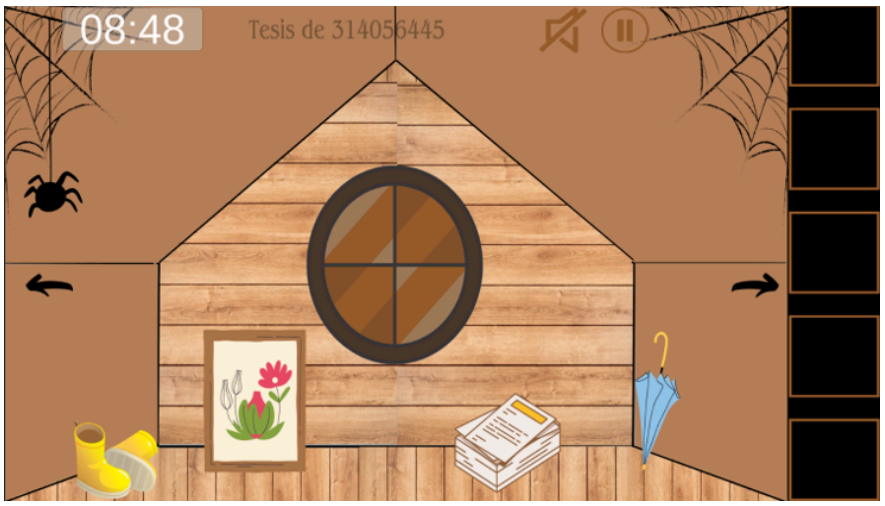


Figura 9. Primera vista del último nivel.

Figura 10. Segunda vista del último nivel.

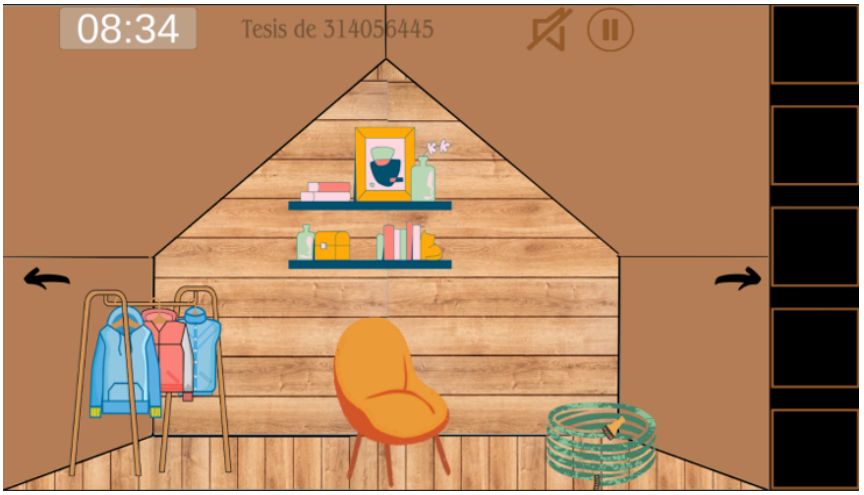


Figura 11. Tercera vista del último nivel.

Figura 12. Cuarta vista del último nivel,

Figura 13. Cambio de vista del primer nivel.

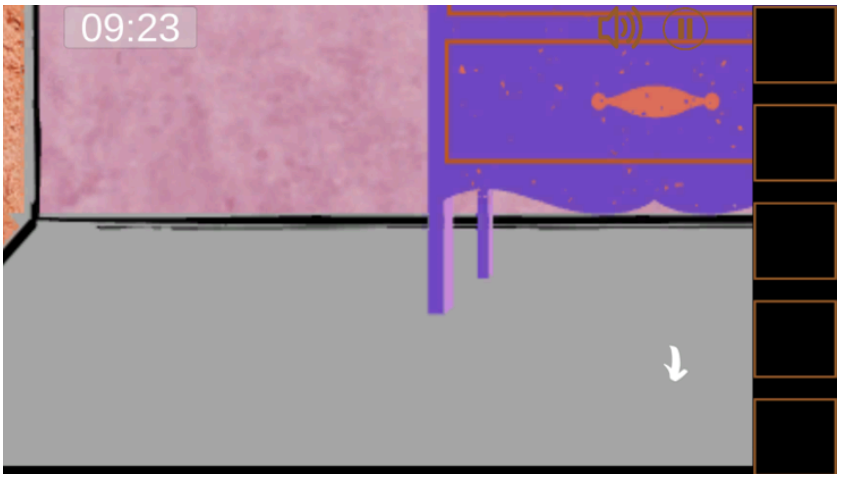


Figura 14. Zoom dentro del primer nivel.

- Mecánica del juego

Figura 15. Botón de pausa.

Figura 16. Mensaje y opciones al responder bien todas las preguntas.

- Preguntas

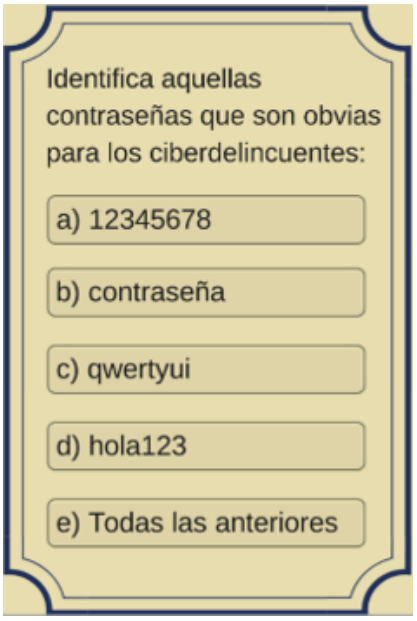


Figura 17. Tarjeta de pregunta.

Figura 18. Mensaje y opciones al responder mal una pregunta.

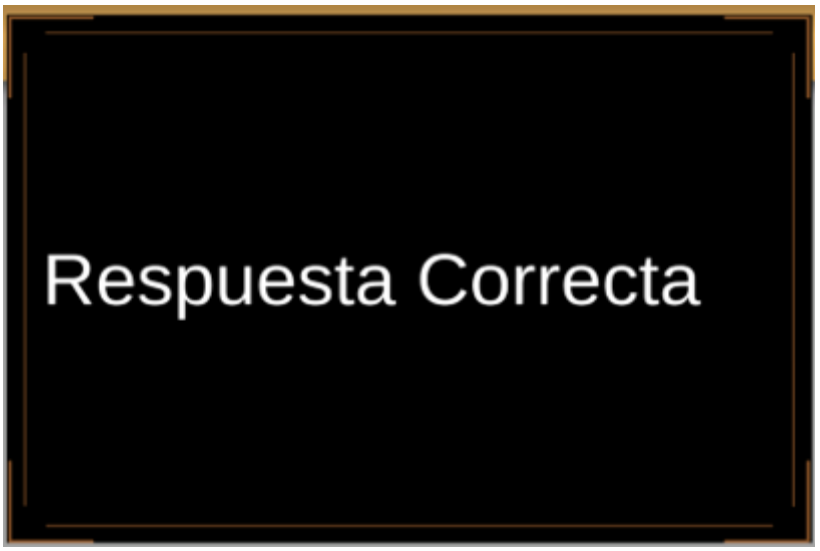


Figura 19. Mensaje al responder bien una pregunta.

- Vistas de los objetos

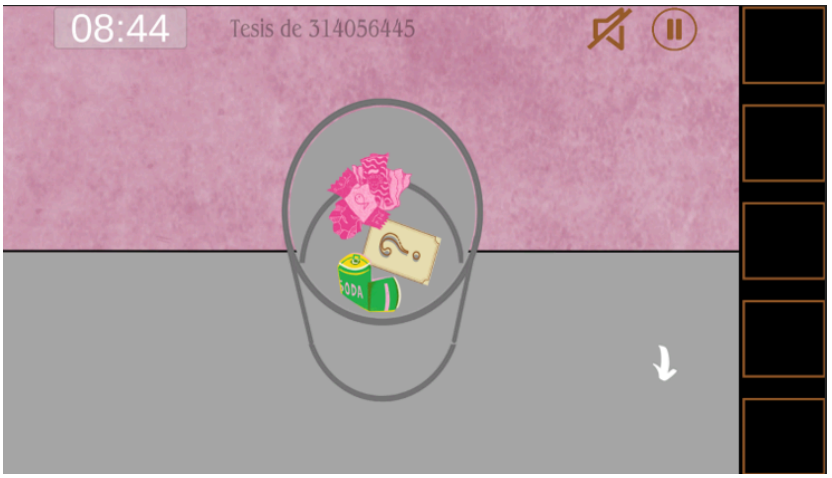


Figura 20. Vista de una tarjeta de pregunta en el primer nivel.

Figura 21. Botón de pausa.

Figura 22. Asignación de trofeos.

Capítulo IV. Plan de pruebas

Con la intención de asegurar que el videojuego funcione correctamente y brinde una experiencia de usuario fluida y sin errores, se lleva a cabo el proceso de pruebas, el cual considera: pruebas de volumen, pruebas de integración, pruebas de testers y pruebas de usuario, en las cuales se evalúan distintas funciones y características.

4.1 Pruebas de volumen

El juego demuestra una alta eficiencia en el uso de recursos:

Rendimiento:

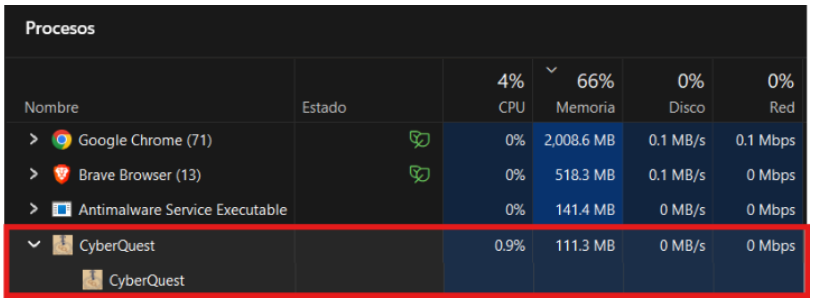


Figura 23. Uso de recursos usados por el videojuego.

- Uso de CPU. 0.9% indicando una carga mínima sobre el procesador.
- Uso de memoria RAM. 111.3 MB muestra una gestión optimizada de los recursos en ejecución.

- Uso de almacenamiento. 183 MB mantiene un tamaño ligero que facilita la instalación.

- Velocidad de carga del juego. 5.45 segundos, asegurando un inicio rápido y sin demoras perceptibles.

- Tiempo de respuesta de la interfaz de usuario. 0.24 milisegundos lo que permite una interacción inmediata y sin latencia.

  Calidad de audio :

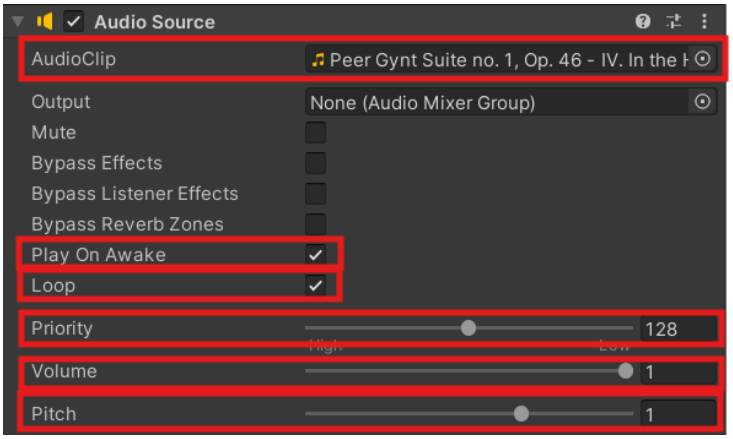


Figura 24. Configuración de sonido en la escena.

En la configuración de audio en Unity se muestran los parámetros esenciales que determinan el comportamiento del sonido en el videojuego. El valor “Volume” controla la intensidad con la que se reproduce el clip, permitiendo regular su presencia dentro de la escena. Por su parte, “Pitch” modifica la velocidad y tonalidad del audio; valores superiores a 1 aceleran y agudizan el sonido, mientras que valores menores lo hacen más grave y lento.

Las opciones “Loop y Play On Awake” definen el comportamiento temporal de la reproducción. Loop permite que el audio se repita de manera continua, lo cual es útil para ambientes o efectos prolongados. Play On Awake indica que el sonido debe iniciar automáticamente al cargar la escena, sin requerir interacción adicional.

Interfaz de usuario:

Facilidad de navegación. La navegación dentro del juego ha sido diseñada para ser intuitiva y fluida. Los comentarios recopilados en los formularios indican que los usuarios identifican rápidamente las funciones principales, comprenden la lógica de interacción entre objetos y transitan entre secciones de manera fluida.

Tiempo de carga de las diferentes secciones del juego. Tomando en cuenta la animación que se muestra al ingresar al primer nivel y la animación que se muestra al finalizar el último nivel fue de 3.83 segundos. Al cambiar de escenas e interactuar con los objetos y botones fue de 0.24 milisegundos.

4.2 Pruebas de integración

La prueba de integración es una fase esencial del desarrollo donde se evalúa cómo se comportan e interactúan los diversos elementos del juego cuando se combinan. Durante esta etapa, se asegura que los objetos añadidos, la interacción de los niveles, la mecánica del juego, entre otros componentes, trabajen de manera fluida y sin problemas. De la misma forma se pone especial atención a identificar y corregir los errores más comunes presentados durante el desarrollo del juego de los cuales sólo se presentan cuatro para este trabajo.

A continuación se enlistan los componentes evaluados durante las pruebas:

- Mecánica del juego. Verificar que los objetos añadidos y referenciados funcionen adecuadamente.

- Objetivos y logros. Verificar que los logros asociados al nivel se desbloquean correctamente al responder las preguntas.

- Interacción con niveles anteriores. Asegurarse que la transición al nuevo nivel sea fluida y sin errores visuales o de carga.

- Revisión de código. Realizar una revisión del código relacionado con las mecánicas y características específicas del nivel.

- Informes de Errores. Realizar una revisión de los errores mostrados por la consola de Unity.

De igual manera, se muestran los cuatro errores que se presentaron de manera más recurrente durante la realización del juego.

A. Zoom de objetos.

   Al integrar el segundo nivel, se presentaron algunos fallos con los objetos agregados, ya que no funcionaban como se esperaba; por ejemplo, un resultado satisfactorio, era que al seleccionar alguno de los objetos, hubiese un cambio de vista para simular una interacción real, y posteriormente al hacer click en una flecha para regresar a la vista de la escena, sin embargo, al hacer click en la flecha no permitía regresar a la escena original (Véase figura 25).

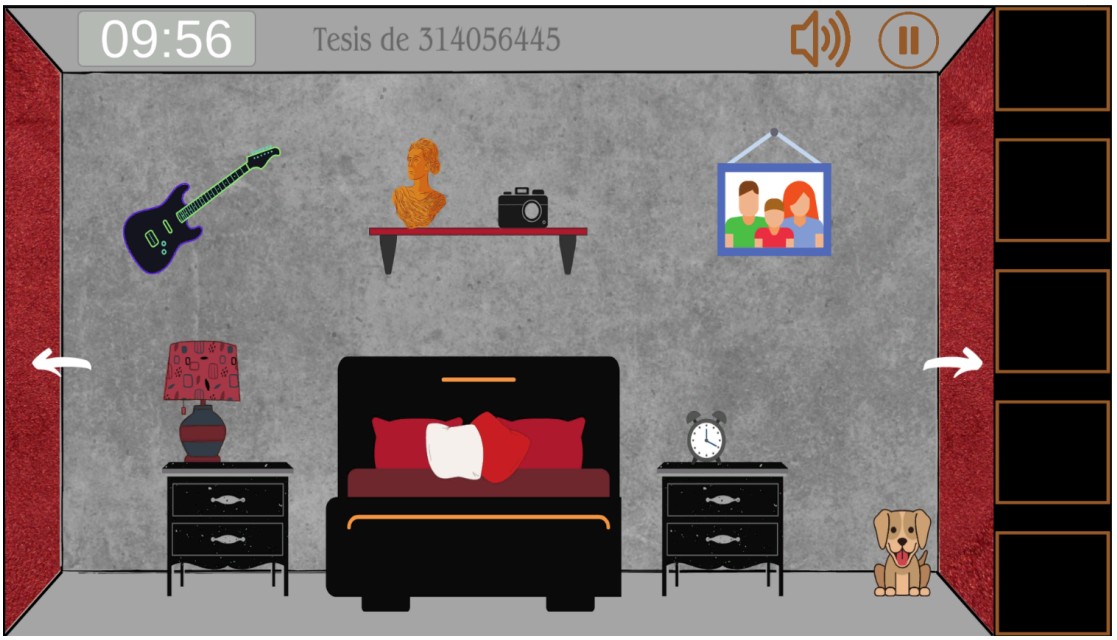


Figura 25. Primera escena del segundo nivel

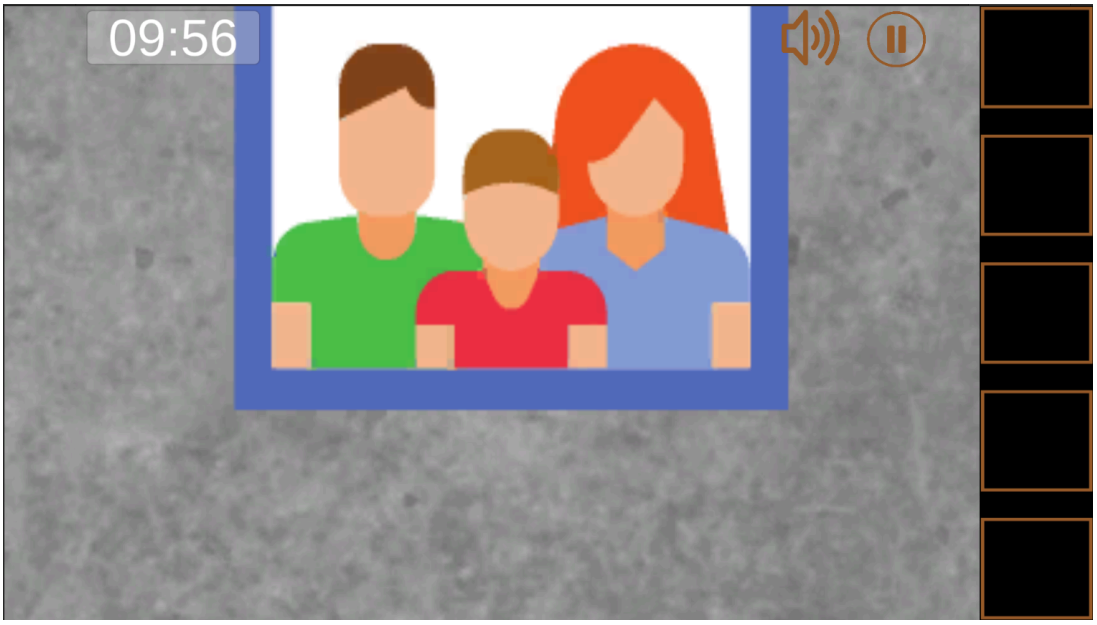


Figura 26. Cambió de vista para simular una interacción real.

B. Cambio de escenas.
Cada nivel es una habitación y cada habitación tiene cuatro escenas a modo de representación de las cuatro paredes, para hacer el cambio de escena simulando que el usuario recorre la habitación se debe presionar un botón en forma de flecha ya sea que se quiera dirigir hacia la derecha o la izquierda. Las escenas llevan un orden para que la simulación sea un poco más realista, el problema presentado es que al presionar cualquiera de las flechas las escenas se mostraban en desorden, lo que podría provocar confusión en el usuario acerca de qué escenas ya se habían recorrido.

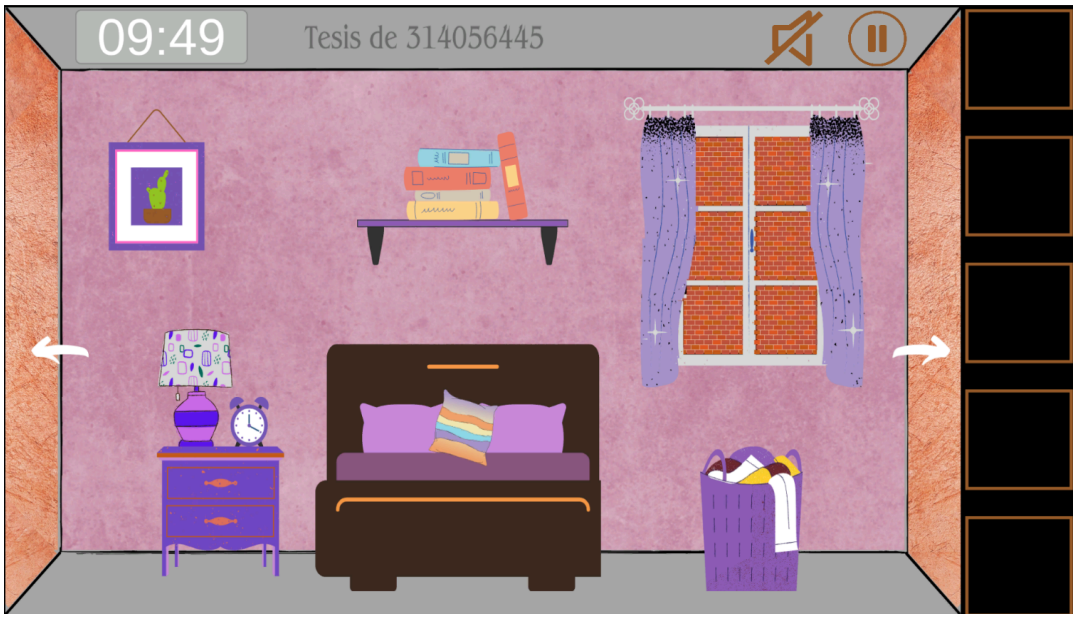


Figura 27. Escena de la primera habitación (nivel 1).

Figura 28. Mensaje que se ha completado el nivel.

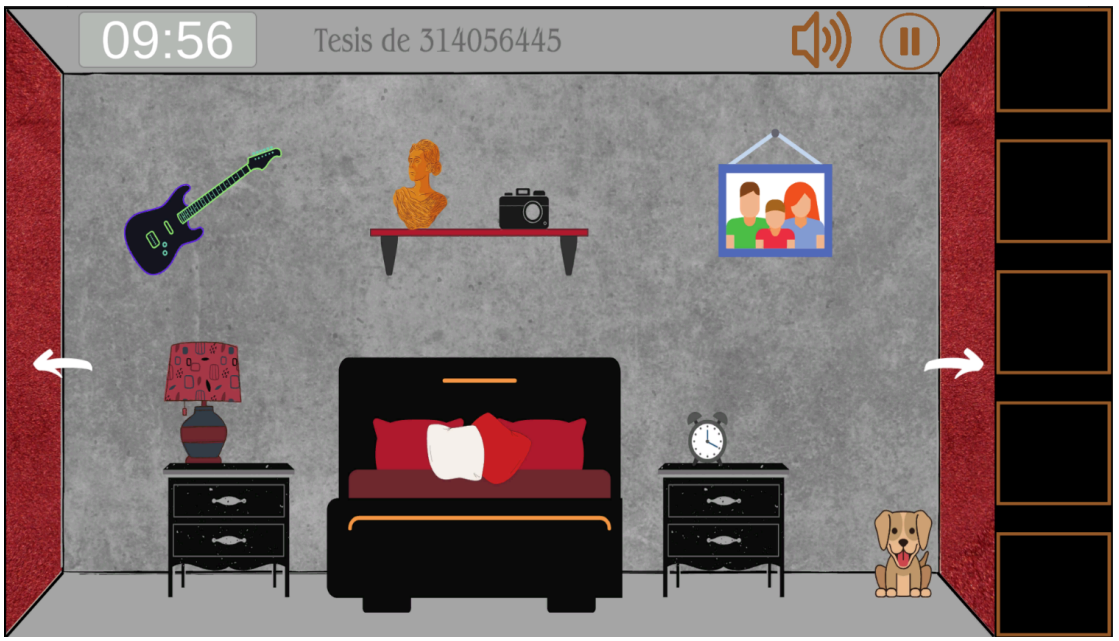


Figura 29. Escena de la segunda habitación (nivel 2).

C. Desbloqueo de logros.

Al integrar los logros en cada una de las escenas se presentaron algunos fallos, ya que al responder bien alguna pregunta, en un resultado satisfactoria es que se desbloquee un trofeo, sin embargo, no se reflejaba en el juego a pesar de que el mensaje mostraba que la respuesta era correcta(Véase la figura 30).

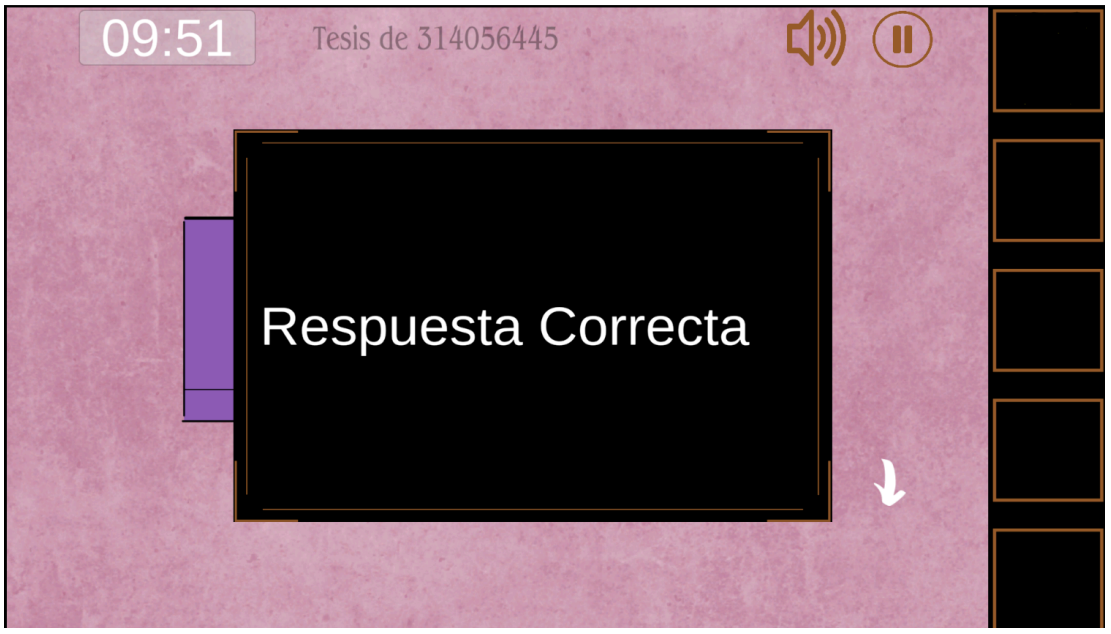


Figura 30. Respuesta correcta sin trofeo desbloqueado.

D. Presentación de diálogos.

Parte de la mecánica del juego es que al responder alguna pregunta aparezca un diálogo si la respuesta es o no correcta, al hacer la integración de estos diálogos se presentó el error de que al responder la pregunta se presentaba el diálogo, sin embargo, desaparecía de manera inmediata sin el tiempo necesario para poder leer el mensaje (Véase figura 23).

Figura 31. El diálogo desaparece rápidamente.

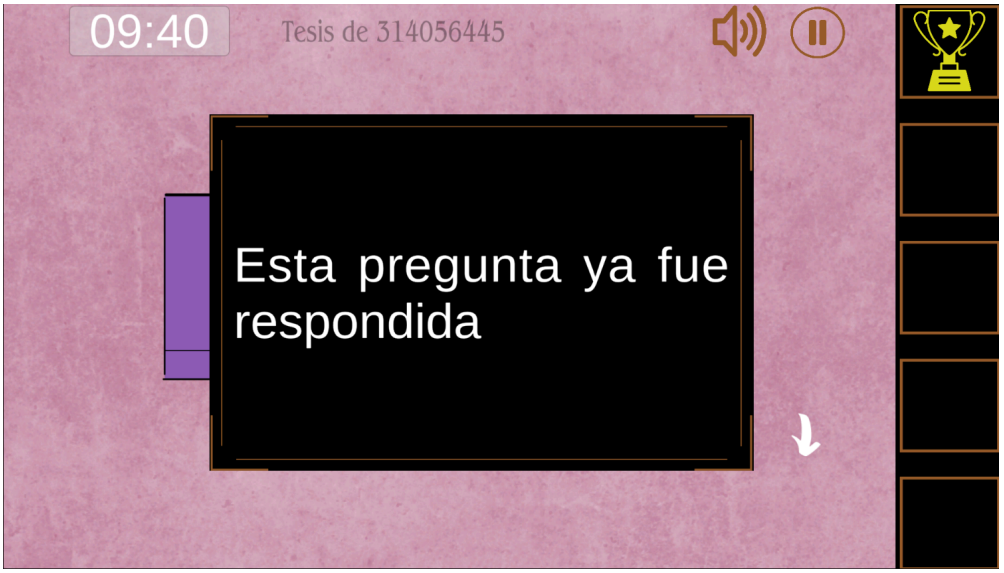


Figura 32. Diálogo que indica que la pregunta ya fue respondida.

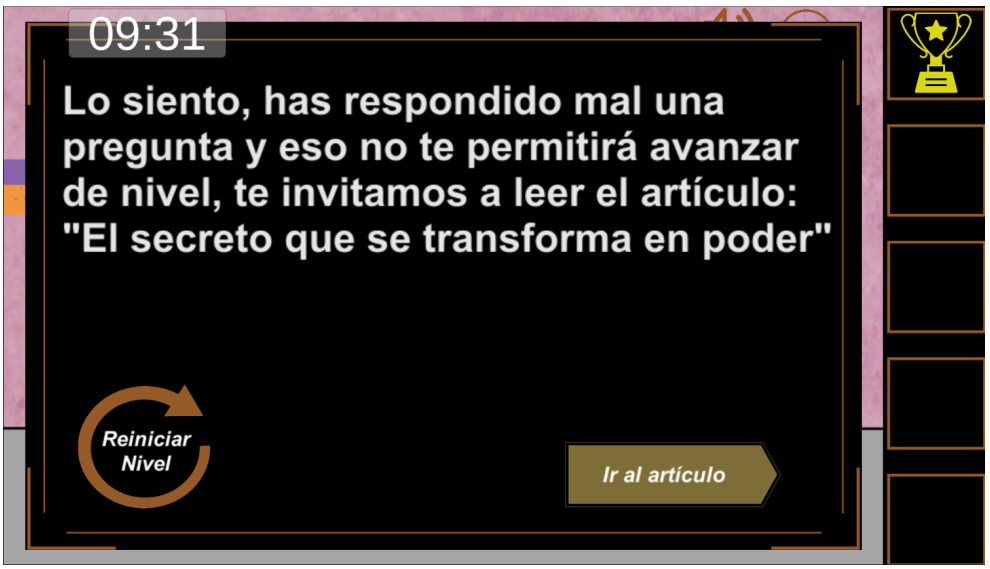


Figura 33. Diálogo que invita a leer el artículo en caso de responder mal.

4.3 Pruebas de Testers

Con el fin de garantizar la objetividad y la detección efectiva de errores, las pruebas funcionales fueron realizadas por tres personas externas al proceso de desarrollo. Esto permite evaluar el videojuego desde la perspectiva del usuario final y reducir el sesgo del desarrollador, quien puede pasar por alto fallos debido a su familiaridad con el código o la lógica interna del juego.

Las pruebas funcionales se dividen en tres fases, las cuales se describen a continuación:

•Primera Fase: Evaluación de los niveles del videojuego (1 al 9), menú principal.
•Segunda Fase: Evaluación de botones, sistema de guardado y carga así como animaciones inicial y final y efectos de sonido.

Primera Fase:

Fecha: mayo 5, 2024

Responsable: Vicente Hérnandez.

Funciones y características por evaluar:

a) Hay que asegurar que las preguntas aparezcan de forma correcta:

   - o Ortografía.
   - o Texto legible (tamaño y color de la fuente).

b) Verificar la funcionalidad del botón al seleccionar una respuesta y verificar que el artículo asignado sea el correspondiente a cada nivel.

c) Visualización de los mensajes para el usuario y con el tiempo adecuado para la lectura.

d) Comprobar que los objetivos en cada nivel se puedan completar.

e) Verificar que el cambio de nivel funcione correctamente al cumplir los objetivos.

Caso de prueba 1:

- Descripción: Hay que asegurar que las preguntas aparezcan de forma correcta, evaluando ortografía y legibilidad de los textos.
- Pasos:
    - Descargar el paquete de juego.
    - Iniciar el juego.
    - Verificar que el juego inicia correctamente sin falla.
    - Abrir las tarjetas de preguntas.
    - Revisar la ortografía de la pregunta.
    - Comprobar que el tamaño y color del texto sean legibles.
- Resultados esperados: Para que la pregunta no sea un obstáculo en el entendimiento del usuario y pueda responder de manera adecuada, en este caso de prueba se espera que, las preguntas sean lo suficientemente legibles y bien redactadas.

Caso de prueba 2:

- Descripción: Probar la funcionalidad de los botones en cada una de las tarjetas de preguntas al seleccionar la respuesta y verificar que los artículos recomendados sean los correspondientes a cada nivel.
- Pasos:
    - Iniciar el juego y verificar que inicia correctamente y sin falla.
    - Abrir las tarjetas de preguntas y probar el botón con la respuesta correcta.
    - Verificar que al presionar el botón aparezca un mensaje diciendo que la respuesta es correcta.
    - En otra tarjeta probar el botón con una respuesta incorrecta.
    - Verificar que al presionar el botón se termine el nivel y aparezca un mensaje diciendo que la respuesta es incorrecta e indicando el artículo correspondiente que se recomienda estudiar.
- Resultados esperados: Los mensajes deben aparecer después de presionar los botones con las respuestas y cada artículo recomendado al responder mal una pregunta debe ser el correspondiente al nivel que se está jugando.

Caso de prueba 3:

- Descripción: Corroborar que el tiempo de visualización de los mensajes sea el adecuado.
- Pasos:
    - Abrir las tarjetas de preguntas y seleccionar el botón con la respuesta correcta.
    - Verificar que el tiempo de visualización para el mensaje de “Respuesta correcta” sea adecuado para poder leer el mensaje.

    - Abrir la tarjeta de la misma pregunta.
    - Comprobar que el tiempo de visualización para el mensaje de “Esta pregunta ya fue respondida” sea el adecuado para poder leer el mensaje.
- Resultados esperados: El tiempo de visualización de los mensajes en pantalla, es el adecuado para que el usuario lea el mensaje.

Caso de prueba 4:

- Descripción: Cotejar la asignación de ítems al responder bien las preguntas.
- Pasos:
    - Abrir las cinco tarjetas de preguntas y seleccionar la respuesta correcta en cada una de ellas.
    - Comprobar que, al seleccionar la respuesta correcta, aparece un trofeo dentro del panel, para cada una de las preguntas.
- Resultados esperados: Al responder correctamente las preguntas se asignan los ítems correspondientes permitiendo cumplir los objetivos del nivel.

Caso de prueba 5:

- Descripción: Corroborar la funcionalidad del botón para pasar al siguiente nivel.
- Pasos:
    - Abrir las cinco tarjetas de preguntas y seleccionar la respuesta correcta en cada una de ellas.
    - Verificar que, al obtener todos los trofeos correspondientes a cada una de las preguntas, aparezca un letrero diciendo que podemos pasar al siguiente nivel, presionando el botón de “Siguiente nivel”.
    - Comprobar que, al seleccionar el botón, hace el cambio al nivel siguiente sin errores.
- Resultados esperados: Al responder correctamente todas las preguntas, aparece el botón de “siguiente nivel” y que permite cambiar al nivel siguiente sin errores.

Informe de resultados:

Durante las pruebas funcionales realizadas, se identificaron varios aspectos que requieren corrección, principalmente relacionados con la ortografía y caligrafía en el contenido del juego. Estos errores fueron detectados en diversos textos del juego, incluyendo diálogos, menús y mensajes emergentes. Aunque no afectan directamente la funcionalidad del juego, es esencial abordarlos para mejorar la calidad general y la experiencia del usuario. Se han planificado correcciones para asegurar que todos los textos estén libres de errores antes del lanzamiento final.

Segunda Fase:

Fecha: Septiembre 26, 2024

Responsables: Vicente Hérnandez, Samuel Dorantes y Hassiel Saucedo.

Funciones y características por evaluar:

a) Asegurar que el botón de pausa funcione correctamente en todos los niveles:

b) Verificar la funcionalidad de los botones de instrucciones y cerrar la aplicación que se encuentran dentro del menú.

c) Asegurar que los botones para ingresar a los niveles se desbloquean correctamente.

d) Verificar que cualquier interrupción durante un nivel sin haber finalizado provocará el reinicio del nivel.

Caso de prueba 1:

- Descripción: Verificar que al presionar el botón de pausa durante el juego, se muestre correctamente el menú de pausa con las opciones de Reanudar, Reiniciar y Salir del juego, y que cada opción funcione como se espera.
- Pasos:

1. Iniciar un nivel del juego.
2. Durante el juego, presionar el botón de pausa.
3. Verificar que se visualice el menú de pausa con las siguientes opciones:
    - *Reanudar*
    - *Reiniciar*
    - *Salir del juego*
4. Probar cada una de las opciones:
    - Seleccionar *Reanudar* y verificar que el juego continúa desde el punto donde fue pausado.
    - Seleccionar *Reiniciar* y verificar que el nivel se reinicia desde el principio.
    - Seleccionar *Salir del juego* y verificar que se cierra la aplicación.

- Resultados Esperados: Al presionar el botón de pausa, el menú de pausa debe mostrarse con las tres opciones disponibles.
    - Seleccionar *Reanudar* debe reanudar el juego correctamente.
    - Seleccionar *Reiniciar* debe reiniciar el nivel desde el inicio.
    - Seleccionar *Salir del juego* debe cerrar la aplicación sin problemas.

Caso de prueba 2:

- Descripción: Verificar que los botones de *Instrucciones* y *Cerrar la Aplicación* dentro del menú principal funcionen correctamente, mostrando las instrucciones del juego y cerrando la aplicación cuando se seleccionan, respectivamente.
- Pasos:
    - Iniciar el juego y acceder al menú principal.
    - Presionar el botón con el símbolo de signo de admiración.
    - Verificar que se muestren correctamente las instrucciones del juego, detallando cómo jugar y los controles.
    - Volver al menú principal.

    - Presionar el botón Cerrar la Aplicación.
    - Verificar que la aplicación se cierre de manera correcta, sin errores ni mensajes de advertencia.
- Resultados esperados: Al presionar el botón de signo de admiración, las instrucciones del juego deben mostrarse claramente y debe existir una forma de regresar y avanzar en los textos. Al presionar el botón con el signo de *X*, el juego debe cerrarse correctamente, finalizando la ejecución sin generar errores.

Caso de prueba 3:

- Descripción: Verificar que los botones de acceso a los niveles se desbloqueen correctamente cuando el jugador responde correctamente las 5 preguntas de un nivel, permitiendo el acceso al siguiente nivel.
- Pasos:
    - Iniciar el juego y acceder al primer nivel.
    - Responder correctamente las 5 preguntas del nivel.
    - Verificar que, al finalizar el nivel con todas las respuestas correctas, el siguiente nivel se desbloquee.
    - Acceder al siguiente nivel utilizando el botón desbloqueado.
    - Repetir el proceso para cada nivel disponible.
    - Verificar que si no se responden correctamente las 5 preguntas, el siguiente nivel permanezca bloqueado y no sea accesible.
- Resultados esperados: Al responder correctamente las 5 preguntas de un nivel, el botón para el siguiente nivel debe desbloquearse, permitiendo el acceso. Si no se completan correctamente las preguntas, el siguiente nivel debe permanecer bloqueado.

Caso de prueba 4:

- Descripción: Verificar que cualquier interrupción durante un nivel, antes de completar todas las preguntas, provoquen el reinicio del nivel al retomarlo, sin guardar ningún progreso parcial.
- Pasos:
    - Iniciar un nivel y comenzar a responder las preguntas.
    - Durante el nivel, antes de responder las 5 preguntas, provocar una interrupción.
        - Cerrar la aplicación.
        - Utilizar el botón de pausa y seleccionar Salir del juego.
        - Forzar el cierre de la aplicación de otra manera.
    - Reiniciar el juego y volver al nivel interrumpido.
    - Verificar que el nivel se reinicie desde el principio, sin conservar respuestas anteriores.
- Resultados esperados: Cualquier interrupción antes de finalizar el nivel debe provocar el reinicio completo del nivel, con todas las preguntas restablecidas y ningún progreso guardado.

Informe de resultados:

En esta fase de pruebas, se han identificado varias áreas de mejora, incluyendo ajustes en la visibilidad de algunos botones, mayor claridad en las instrucciones, y la adición de funciones como un botón de confirmación al salir, un botón de reinicio tras completar un nivel, y la reinicialización de niveles tras interrupciones. Además, se corregirá un error en el desbloqueo de niveles.

4.4 Pruebas de usuarios

En la fase final de desarrollo de CyberQuest: Desafío de ciberseguridad, se llevaron a cabo pruebas con usuarios finales, específicamente estudiantes universitarios, con el objetivo de evaluar la experiencia de uso del videojuego desde la perspectiva de su público objetivo. Estas pruebas permitieron identificar fortalezas, áreas de mejora y la percepción general del contenido educativo.

Objetivo
Recolectar información cualitativa y cuantitativa sobre la experiencia de los estudiantes al interactuar con el videojuego, para validar su efectividad como recurso educativo y realizar los ajustes finales antes de su publicación.

Metodología
Población objetivo: Estudiantes universitarios del área de tecnología o afines.

Modalidad: Presencial o remota, con acceso libre al videojuego.

Instrumento de evaluación: Encuesta digital mediante Google Forms.

Duración estimada de la prueba: 30 a 90 minutos de juego, seguido de 5 a 10 minutos para responder la encuesta.

Instrumento de Evaluación

Se diseñó una encuesta en Google Forms titulada “Evaluación de CyberQuest: Desafío de ciberseguridad”, con el propósito de obtener retroalimentación basada en la experiencia de los usuarios. La encuesta incluyó preguntas demográficas para contextualizar las respuestas y una serie de ítems que evaluaron aspectos específicos del videojuego.

Categorías evaluadas:

Datos demográficos:

Rango de edad.

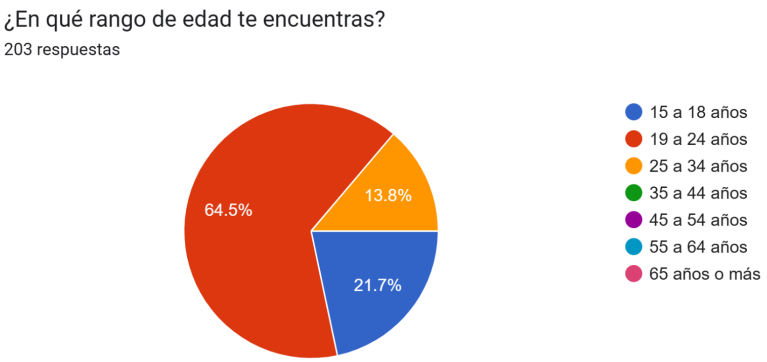


Figura 34. Gráfico de rango edad de los encuestados.

En la Figura 34 se observa la distribución por rango de edad de los 203 participantes que respondieron la encuesta. Los resultados muestran que la mayoría de los encuestados (64.5%) se encuentra en el rango de 19 a 24 años, seguido por un 21.7% en el rango de 15 a 18 años, mientras que el 13.8% restante pertenece al grupo de 25 a 34 años.

Esta distribución nos muestra que la mayor parte del público que evaluó el videojuego corresponde a jóvenes y adultos jóvenes, lo cual resulta coherente con el público objetivo del proyecto, orientado principalmente a estudiantes y personas en formación académica o profesional interesadas en temas de ciberseguridad.

Género.

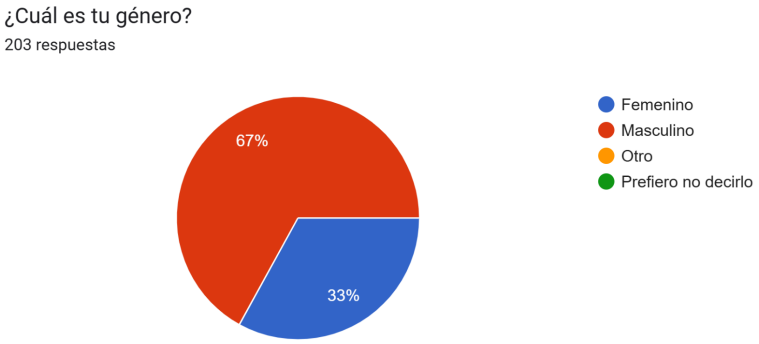


Figura 35. Gráfico de género de los encuestados.

En la Figura 35 se presenta la distribución por género de los 203 participantes que respondieron la encuesta. Los resultados muestran que el 67% de los encuestados se identifica como masculino, mientras que el 33% corresponde al género femenino. No se registraron respuestas en las categorías “Otro” ni “Prefiero no decirlo”.

Estos resultados evidencian una mayor participación masculina en la evaluación del videojuego, comportamiento que coincide con la brecha de género existente en el ámbito de

la ciberseguridad. Diversos estudios han señalado que las mujeres representan un porcentaje reducido dentro de esta área, lo que se refleja también en los resultados de los participantes del presente estudio.

Nivel escolar.

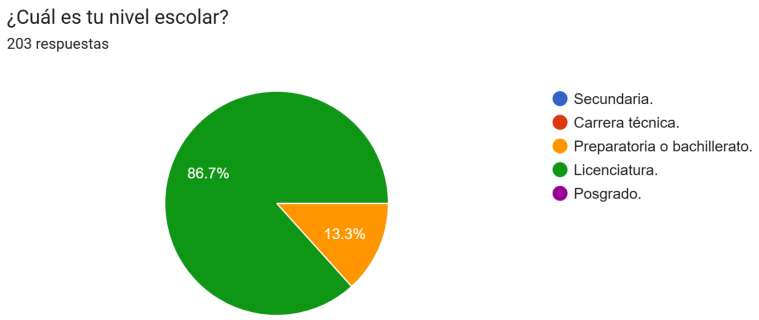


Figura 36. Gráfico de nivel escolar de los encuestados.

En la Figura 36 se muestra la distribución del nivel escolar de los 203 encuestados. Los resultados indican que el 86.7% reportó tener estudios de licenciatura, mientras que el 13.3% señaló haber cursado hasta preparatoria o bachillerato. No se registraron respuestas en los niveles de secundaria, carrera técnica o posgrado.
Sin embargo, es importante considerar que algunos participantes pudieron haber interpretado la pregunta en función de su último nivel concluido, y no del que actualmente cursan. Esto explicaría que varios estudiantes universitarios seleccionarán “preparatoria o bachillerato” como respuesta, a pesar de encontrarse en proceso de formación profesional. En general, la mayoría de los encuestados posee o está cursando estudios universitarios, lo que coincide con el perfil educativo esperado del público objetivo del videojuego.

Experiencia de juego:

Claridad de las instrucciones y preguntas.

Las preguntas en su mayoría se perciben claras y útiles, sin embargo, algunos comentarios señalan que ciertas preguntas eran algo confusas. En cuánto a las instrucciones varios jugadores señalan que sería agradable añadir una guía más interactiva para iniciar el juego, algo como un cursor que te vaya indicando para qué es cada botón.

Respecto a los artículos los encuestados consideran que son cortos y fáciles de entender, pero, sugieren ahondar más en las explicaciones dentro del juego, antes de ingresar al artículo.

En este apartado, al tratarse de una pregunta abierta se realizó un análisis mediante la identificación de patrones y categorías, es por eso que no se presentan gráficas, si no una narrativa de los resultados.

Nivel de dificultad.

Figura 37. Gráfico de dificultad del videojuego percibido por los encuestados.

En la Figura 37 se observa la percepción de los participantes respecto a la dificultad para superar los niveles del videojuego. La escala utilizada fue del 1 al 5, donde 1 representa “muy fácil” y 5 “muy difícil”.

Los resultados muestran que la mayoría de los encuestados consideró la dificultad como moderada, concentrándose principalmente en los valores 2 (33%) y 3 (37.4%). En comparación, sólo 10.8% de los participantes opinó que los niveles eran muy fáciles, mientras que 15.3% los percibió algo difíciles y apenas 3.4% los calificó como muy difíciles. En conjunto, estos datos indican que la dificultad del juego resulta equilibrada para la mayoría de los usuarios, lo que sugiere que el diseño de los retos y niveles ofrece un desafío adecuado sin generar frustración.

Valor educativo percibido.

Figura 38. Nivel de conocimiento antes de jugar.

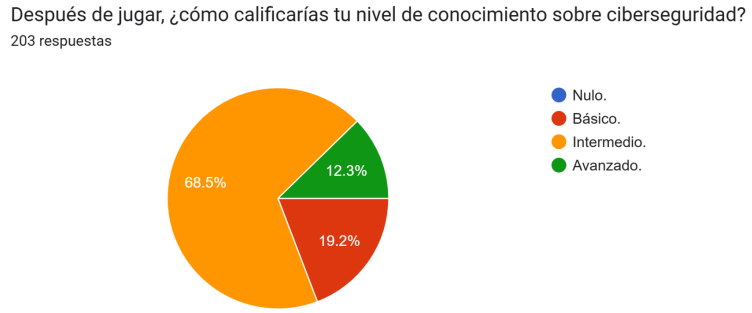


Figura 39. Nivel de conocimiento después de jugar.

Figura 40. Ayuda en la comprensión de los temas de ciberseguridad.

En las Figuras 38, 39 y 40 se presentan los resultados relacionados con el nivel de conocimiento sobre ciberseguridad antes y después de jugar el videojuego, así como la percepción de los participantes respecto a si este contribuyó a su aprendizaje.

Antes de la experiencia, la mayoría de los encuestados reportó tener un nivel bajo de conocimiento en ciberseguridad (58.6%), seguido de un nivel nulo (32.5%), mientras que solo un pequeño porcentaje indicó contar con un nivel intermedio o avanzado. Sin embargo, después de participar en la dinámica del videojuego, los resultados evidencian un cambio significativo: el 68.5% de los jugadores se ubicó en un nivel intermedio, mientras que el 12.3% se consideró en un nivel avanzado, lo que refleja una mejora en la autopercepción del conocimiento adquirido.

Asimismo, referente a la pregunta sobre si el videojuego ayudó a comprender mejor los temas de ciberseguridad, el 60.1% de los participantes afirmó que sí, mucho, y el 31% señaló que sí, en cierta medida.

Estos resultados permiten concluir que el videojuego tuvo un impacto educativo positivo, al facilitar la comprensión de conceptos fundamentales de ciberseguridad de manera dinámica y accesible. Además, refuerzan la idea de que los entornos interactivos pueden ser herramientas efectivas para la enseñanza y divulgación de temas técnicos.

Agradabilidad de la música y las animaciones.

La música en la mayoría de los comentarios se percibió agradable, algunos encuestados sugerían que se añadiera una melodía distinta en cada nivel, así como algún sonido al responder correcta o incorrectamente alguna pregunta. En cuánto a las animaciones, algunas opiniones expresan que sean más dinámicas y fluidas, ya que en algunos elementos se perciben repetitivos.
En este apartado, al tratarse de una pregunta abierta se realizó un análisis mediante la identificación de patrones y categorías, es por eso que no se presentan gráficas, si no una narrativa de los resultados.

Nivel de interés y motivación generado por el juego.

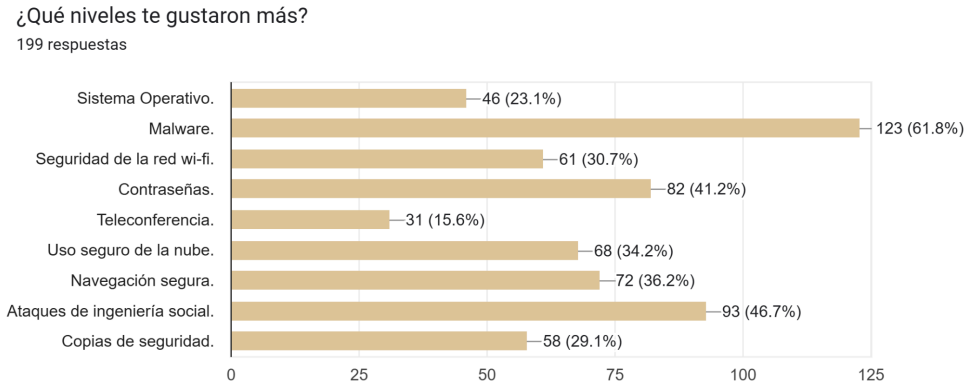


Figura 41. Niveles que tuvieron mejor recibimiento por parte de los participantes.

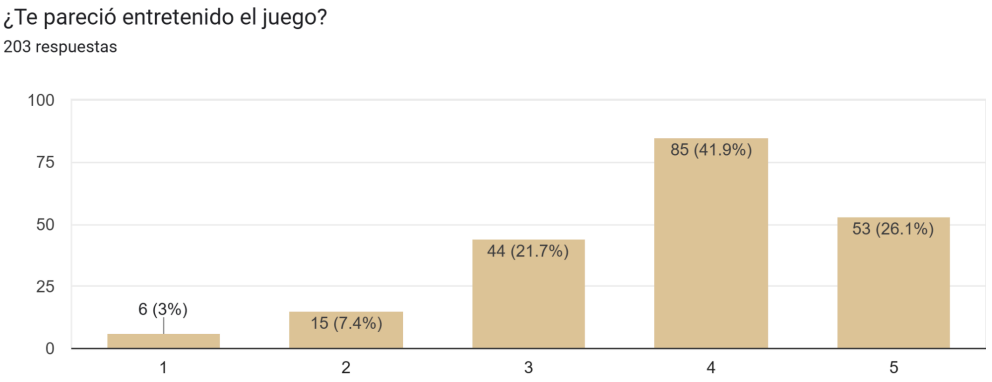


Figura 42. Nivel de entretenimiento del juego.

Figura 43. Incorporación de contenido adicional.

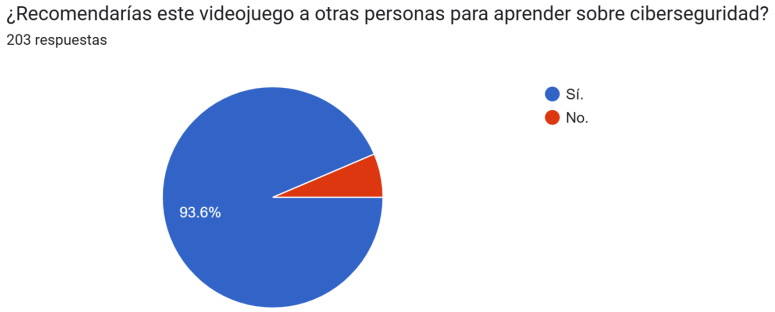


Figura 44. Recomendación a otras personas.

En las Figuras 41, 42, 43 y 44 se presentan los resultados relacionados con el nivel de interés y motivación generado por el videojuego. Estos datos permiten evaluar la percepción de los participantes respecto a la experiencia de juego, el grado de entretenimiento, así como su disposición para continuar aprendiendo mediante esta herramienta.

En cuanto a si les pareció o no entretenido el juego, la mayoría de los encuestados manifestó una valoración positiva: el 41.9% calificó el videojuego con 4 y el 26.1% con 5, lo que refleja que más de dos tercios de los jugadores consideraron la experiencia como divertida y atractiva. Solo un 10.4% otorgó puntuaciones bajas (1 o 2), lo que indica una buena aceptación general del juego como medio de aprendizaje lúdico.

Respecto a los niveles que resultaron más interesantes, sobresalen los temas de malware (81.8%), ataques de ingeniería social (46.7%) y contraseñas (41.2%), los cuales están ampliamente vinculados con eventos relacionados a ataques de ciberseguridad. Esto sugiere que los participantes se sintieron más motivados por contenidos con una aplicación práctica y directa en su vida cotidiana.
Por otro lado, el 44.3% de los jugadores expresó su interés en que se agreguen más niveles o contenido adicional, mientras que un 93.6% afirmó que recomendaría el videojuego a otras personas para aprender sobre ciberseguridad. Estos resultados evidencian un alto nivel de satisfacción e interés en seguir explorando la temática a través del juego.

En conjunto, los resultados reflejan que el videojuego no solo logró captar la atención de los participantes, sino que también generó motivación y entusiasmo por aprender, posicionándose como una herramienta efectiva para fomentar la educación en ciberseguridad de manera dinámica e interactiva.

Percepciones sobre la experiencia de uso.

Algunos de los problemas técnicos experimentados fueron:

- Textos cortados o mal escritos. De acuerdo a los encuestados, en las respuestas de algunas tarjetas, el texto aparecía cortado o incompleto, así cómo algunas cosas mal escritas en los botones como “meú” en lugar de “menú”

- Detección de clics poco intuitivo. Dentro de las opiniones se describe que algunas zonas son muy pequeñas o imprecisas para encontrar las tarjetas.

- Temporizador. El temporizador dentro del juego se percibió como frustrante ya que generaba presión dentro del juego.

En este apartado, al tratarse de una pregunta abierta se realizó un análisis mediante la identificación de patrones y categorías, es por eso que no se presentan gráficas, si no una narrativa de los resultados.

Capítulo V. Análisis de resultados

5.1 Resultados técnicos

El desarrollo del videojuego consiguió alcanzar los objetivos técnicos planteados al inicio del proyecto, logrando la implementación de un sistema funcional y estable que cumple con las mecánicas definidas. El juego presenta un comportamiento adecuado en cuanto a navegación, gestión de niveles, control del tiempo, retroalimentación al usuario y manejo de eventos como pausas, reinicios e interrupciones.

Desde el punto de vista del desarrollo, este proyecto representó un primer acercamiento formal a la programación de videojuegos, lo que implicó la adquisición de nuevos conocimientos relacionados con la programación orientada a objetos, la estructuración de scripts y la interacción entre componentes dentro del motor Unity. Asimismo, se aprendió el uso de herramientas propias del entorno de desarrollo, como la gestión de escenas, la integración de interfaces gráficas y el control de eventos.

Durante el proceso se llevaron a cabo pruebas técnicas que permitieron identificar y corregir errores relacionados con la interacción del usuario y el comportamiento del sistema, así como ajustes en la correcta visualización de los elementos en pantalla. Estas pruebas contribuyeron a mejorar la estabilidad del videojuego y a garantizar una experiencia de uso continua y funcional.

5.2 Resultados de aprendizaje

Al realizar este proyecto, se obtuvieron resultados significativos respecto al aprendizaje técnico, personal y académico. Durante el proceso se fortalecieron habilidades relacionadas con la planificación y gestión del tiempo, así como la organización de tareas mediante la división del proyecto en etapas más pequeñas y manejables.

De igual forma, se desarrollaron competencias en la gestión de proyectos, incluyendo la toma de decisiones, el seguimiento del avance y la adaptación ante dificultades técnicas o de diseño. La elaboración de documentación permitió mejorar las habilidades de redacción técnica y estructuración de información, facilitando la comunicación clara de las ideas y procesos implementados.

En el ámbito académico, el proyecto fomentó la investigación y verificación de fuentes confiables, especialmente en temas relacionados con la ciberseguridad, lo que contribuyó a un aprendizaje más sólido y fundamentado. En conjunto, estos aprendizajes complementaron la formación profesional, reforzando la capacidad de abordar proyectos complejos de manera autónoma y organizada.

Capítulo VI. Conclusiones y trabajo futuro

Los resultados obtenidos a lo largo del diseño, desarrollo y pruebas del videojuego educativo demuestran que la concientización en ciberseguridad puede fortalecerse de manera efectiva mediante estrategias lúdicas e interactivas. En un panorama donde las ciberestafas, la pérdida de datos y el uso malintencionado de tecnologías como la inteligencia artificial aumentan de forma acelerada, es crucial que los usuarios comprendan los riesgos asociados y adopten buenas prácticas para proteger su información. Tal como se menciona en el prólogo, incidentes como la recreación de voces mediante IA y el fraude por mensajería instantánea nos muestran la necesidad de promover mecanismos de verificación y fortalecer la cibercultura.

A partir del análisis del panorama general, se confirma que el conocimiento es el recurso más valioso dentro de la cibercultura. Sin embargo, en la investigación se detectó que el factor humano sigue siendo una fuente de amenaza y que el ser humano es el eslabón más débil en la cadena, debido al poco o nulo uso de buenas prácticas al navegar en el ciberespacio, desconocimiento y falta de interés en la adopción de medidas preventivas. Por ello, el videojuego se diseñó y desarrolló como una herramienta accesible que permitiera aprender y reforzar conocimientos en un entorno seguro, dinámico y atractivo, integrando principios del decálogo de la ciberseguridad y contenidos de la ciberguía para que los usuarios pudieran reconocer tácticas comunes de ataque y anticiparse a posibles amenazas.

Las pruebas realizadas apoyan la relevancia de esta propuesta. La dificultad fue percibida como moderada por la mayoría de los participantes, con una concentración significativa en valores intermedios, lo cual indica que los retos ofrecieron un estímulo adecuado sin resultar frustrantes. Asimismo, el impacto educativo del videojuego quedó demostrado con la mejora de la autopercepción del conocimiento en los encuestados: antes de la experiencia, la mayoría reportó un nivel bajo o nulo en ciberseguridad, mientras que después de interactuar con el juego, más del 80% manifestó haber alcanzado un nivel intermedio o avanzado.

Además, cerca del 60% afirmó que la dinámica les ayudó a comprender mejor los temas abordados, reflejando una comprensión real de la información.

De forma general, puede concluirse que el videojuego cumplió con su objetivo principal: facilitar la comprensión de conceptos esenciales de ciberseguridad e invitar a la reflexión sobre la importancia de adoptar prácticas seguras. La implementación de este tipo de recursos demuestra que la educación en ciberseguridad puede ser más accesible cuando se presenta mediante experiencias motivadoras que conectan con los hábitos digitales de los usuarios. Finalmente, se identifica como trabajo futuro la ampliación del contenido, la incorporación de métricas más precisas y la expansión del entorno hacia plataformas web, con el propósito de beneficiar a un mayor número de personas y continuar fomentando una cultura de seguridad digital.

Referencias bibliográficas

1. Milenio. (2024, 25 de marzo). *Criminales usan IA para recrear voz y estafar por WhatsApp.* Milenio.https://www.milenio.com/policia/criminales-usan-ia-para-recrear-voz-y-estafar-por-whatsapp
2. FortiGuard Labs. (2025). *Top countries by threat volume.* Fortinet. https://www.fortiguard.com/threat-research/map
3. Infobae México. (2024, 25 de marzo). El factor humano, causa principal de la pérdida de datos. *Infobae.* https://www.infobae.com/mexico/2024/03/25/el-factor-humano-causa-principal-de-la-perdida-de-datos/
4. UNAM-CERT. (s. f.). Concientizar para prevenir. *Revista .Seguridad.* https://revista.seguridad.unam.mx/numero-21/concienciar-para-prevenir
5. Unión Internacional de Telecomunicaciones (UIT). (2024). *Global Cybersecurity Index 2024.* https://www.itu.int/epublications/en/publication/global-cybersecurity-index-2024/en
6. Lab. (2025). *Mapa en tiempo real de ciberamenazas en el mundo* [Herramienta interactiva en línea]. Recuperado el 3 de junio de 2025 de https://cybermap.kaspersky.com/es
7. **9.** Redacción El Economista. (2020, 30 de noviembre). Comisión Nacional de Seguros y Fianzas sufre ciberataque. *El Economista.* https://www.eleconomista.com.mx/sectorfinanciero/Avisan-sobre-ciberataque-a-la-CNSF-organismo-reconoce-incidente-20201129-0030.html
8. Kaspersky. (2021). Ransomware LockBit: lo que necesitas saber. *Kaspersky Resource Center.* https://latam.kaspersky.com/resource-center/threats/lockbit-ransomware
9. Real Academia Española. (2022). Cultura. En *Diccionario de la lengua española* (edición del tricentenario). https://dle.rae.es/cultura

10. Quiñones Bonilla, F. (2005). De la cultura a la cibercultura. *Hallazgos, 2*(4), 174–190. https://www.redalyc.org/articulo.oa?id=413835163015
11. Lévy, P. (2000). *Cibercultura: la cultura de la sociedad digital.* Anthropos/Universidad Autónoma Metropolitana. http://hdl.handle.net/20.500.12209/7487
12. Millán, T. R. (2000). Para comprender el concepto de cultura. *UNAP Educación y Desarrollo, 1*(1), 1–11.
13. Calderón, C. (2022, 9 de junio). México "clientazo" de los ciberataques: crecen 42% amenazas por internet. *El Financiero.* https://www.elfinanciero.com.mx/empresas/2022/06/09/aumentan-42-los-ciberataques-con-85-mil-millones-de-intentos-en-mexico/
14. Secretaría de Gobernación, Unidad General de Asuntos Jurídicos. (s. f.). *Ficha técnica Ley Olimpia.* http://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf
15. Secretaría de Seguridad y Protección Ciudadana. (2021, 25 de octubre). *Ciberguía.* https://www.gob.mx/sspc/documentos/ciberguia?idiom=es
16. Albornoz, M. B. (2008). Cibercultura y las nuevas nociones de privacidad. *Nómadas,* (28), 44–50.
17. Hernández, V. (2025, 5 de noviembre). La IA impulsa la amenaza digital en México al ser el segundo país más atacado de la región. *W Radio.* https://wradio.com.mx/2025/11/05/la-ia-impulsa-la-amenaza-digital-en-mexico-al-ser-el-segundo-pais-mas-atacado-de-la-region
18. Prieto, R., Medina, N. M., & López, J. M. (2016). Interacción en videojuegos serios. En *Actas del XVII Congreso Internacional de Interacción Persona-Ordenador — Interacción 2016* (pp. 41–48). Research Gate. https://www.researchgate.net/publication/308063240
19. Casañ Pitarch, R. (2018). *Videojuegos serios en educación* [Diapositivas]. Research Gate. https://www.researchgate.net/publication/350967167
20. Ferrer, J. R. C. (2018). Juegos, videojuegos y juegos serios: Análisis de los factores que favorecen la diversión del jugador. *Miguel Hernández Communication Journal,* (9), 191–226. https://dialnet.unirioja.es/servlet/articulo?codigo=6268953
21. Pindado, J. (2005). Las posibilidades educativas de los videojuegos. Una revisión de los estudios más significativos. *Pixel-Bit. Revista de Medios y Educación, 26*, 55–67. https://idus.us.es/bitstream/handle/11441/45601/file_1.pdf
22. Etxeberría Balerdi, F. (2001). Videojuegos y educación. *Teoría de la Educación: Educación y Cultura en la Sociedad de la Información, 2*(2).

https://redined.educacion.gob.es/xmlui/bitstream/handle/11162/91630/00820113013570.pdf

23. Armendáriz Espadas, P., & Sánchez Camargo, M. (2018). *Los videojuegos educativos en México* [Tesis de licenciatura, Universidad de las Américas Puebla]. Repositorio UDLAP. http://catarina.udlap.mx/u_dl_a/tales/documentos/lnd/armendariz_espadas_p/
24. Eguía Gómez, J. L., Contreras Espinosa, R. S., & Solano Albajés, L. (2012). Videojuegos: conceptos, historia y su potencial como herramientas para la educación. *3C TIC, 1*(2), 1–14. http://dspace.uvic.cat/bitstream/handle/10854/2764/artconlli_a2012_contreras_ruth_videojuegos.pdf
25. Universidad Autónoma del Estado de Hidalgo. (s. f.). El video tutorial como herramienta de apoyo pedagógico. *Boletín Científico UAEH.* https://www.uaeh.edu.mx/scige/boletin/prepa4/n1/e8.html
26. Hernández-Martínez, L. E., & Rodríguez-Cantú, S. P. (s. f.). Tutoriales como apoyo en el aprendizaje del estudiante en el área de administración. *Vinculatégica EFAN, 4*(2), 710–715. https://doi.org/10.29105/vtga4.1-826
27. Kizilcec, R. F., Papadopoulos, K., & Sritanyaratana, L. (2014). Showing face in video instruction: Effects on information retention, video engagement, and affect. En *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2095–2102). ACM. https://doi.org/10.1145/2556288.2557207
28. Ou, C., Joyner, D. A., & Goel, A. K. (2019). Designing and developing videos for online learning: A 7-principle model. *Online Learning, 23*(2), 82–103. https://doi.org/10.24059/olj.v23i2.1449
29. Bayeck, R. Y. (2020). Exploring video games and learning in South Africa: An integrative review. *Educational Technology Research and Development, 68*(5), 2775–2795. https://doi.org/10.1007/s11423-020-09764-7
30. Chang, C., Chung, C., & Chang, J. A. (2020). Influence of problem-based learning games on effective computer programming learning in higher education. *Educational Technology Research and Development, 68*(5), 2615–2634. https://doi.org/10.1007/s11423-020-09784-3
31. Chen, H. M., & Thomas, M. (2020). Effects of lecture video styles on engagement and learning. *Educational Technology Research and Development, 68*(5), 2147–2164. https://doi.org/10.1007/s11423-020-09757-6
32. Chu, H., & Chang, S. (2014). Developing an educational computer game for migratory bird identification based on a two-tier test approach. *Educational Technology Research and Development, 62*(2), 147–161. https://doi.org/10.1007/s11423-013-9323-4

33. Lange, C., & Costley, J. (2020). Improving online video lectures: Learning challenges created by media. *International Journal of Educational Technology in Higher Education, 17*(1), 16. https://doi.org/10.1186/s41239-020-00190-6
34. Educación 3.0. (2024, 28 de octubre). Aprendizaje basado en el juego: pedagogías emergentes (V). *Educación 3.0.* https://www.educaciontrespuntocero.com/noticias/aprendizaje-basado-en-el-juego/
35. Boschi, C. (2014). Innovación docente mediante un método tutorial apoyado con recursos informáticos. *Revista Iberoamericana de Educación Superior, 5*(13), 55–64. https://doi.org/10.1016/s2007-2872(14)71953-5
36. Rodríguez Guardado, M. del S., & Platas-García, A. (2022). Uso de videos tutoriales en el proceso de aprendizaje de estudiantes universitarios. *Revista Electrónica de Investigación Educativa, 24*, e21. https://doi.org/10.24320/redie.2022.24.e21.4176
37. Javier, A. C. F. (s. f.). *El diseño y el arte en los videojuegos* [Trabajo fin de grado]. Archivo Digital UPM. https://oa.upm.es/50803/
38. Mata Solís, L. D. (2019, 10 de diciembre). Utilidad del artículo científico en enseñanza-aprendizaje. *Investigalia.* https://investigaliacr.com/educacion-e-investigacion/utilidad-del-articulo-cientifico-en-ensenanza-aprendizaje/
39. Paur, A. B., Rosanigo, Z. B., Bramati, P., Ortega, A., & Cerra, J. P. (2004). El uso de tutoriales interactivos en ambientes educativos: un caso práctico. En *Memorias del III Congreso de Tecnología en Educación y Educación en Tecnología.* Universidad Nacional de La Plata. http://sedici.unlp.edu.ar/handle/10915/22420
40. Quesnel, J. Q., Guerrero, H. G., & Ávila, N. A. (2017). *Manual: Desarrollo de videojuegos.* Secretaría de Cultura / Centro de Cultura Digital. https://vision.centroculturadigital.mx/media/done/manual%20videojuegos_ok_final.pdf
41. Connolly, T. M., Boyle, E. A., MacArthur, E., Hainey, T., & Boyle, J. M. (2012). A systematic literature review of empirical evidence on computer games and serious games. *Computers & Education, 59*(2), 661–686. https://doi.org/10.1016/j.compedu.2012.03.004
42. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346