
# Cyberman en la red

## Herramienta digital gamificada para potenciar el conocimiento en ciberseguridad y prevención del phishing

**Proyecto de Grado**

Valeria Rodriguez Villamizar

**Bogotá D. C., 2025**

# Cyberman en la red

## Herramienta digital gamificada para potenciar el conocimiento en ciberseguridad y prevención del phishing

Proyecto de grado presentado como requisito parcial para optar al título de:
**Diseñador Digital y Multimedia**

Director (a):

Andrés Felipe Parra Vela

Línea de énfasis:

Videojuegos

Universidad Colegio Mayor de Cundinamarca
Facultad de Ingeniería y Arquitectura
Programa de Diseño Digital y Multimedia
Bogotá D. C., 2025

# Aval del Proyecto

_____

Firma del Director(a) de proyecto de grado

_____

_____

_____

_____

Firmas de los jurados

Bogotá D. C., noviembre de 2025

La Universidad Colegio Mayor de Cundinamarca respeta los conceptos académicos emitidos por los estudiantes de la Facultad de Ingeniería y Arquitectura a través de sus proyectos de investigación y no se hace responsable de su contenido.

Las ideas expresadas en los citados trabajos no constituyen compromiso institucional y son responsabilidad exclusiva de cada autor.

Atentamente,

FLORINDA SÁNCHEZ MORENO
Decana Facultad de Ingeniería y Arquitectura

NOMBRE Y FIRMA
Valeria Rodriguez Villamizar

## Dedicatoria

Este proyecto, producto de largas horas de esfuerzo, noches sin dormir e información desbordante, se lo dedico a quienes estuvieron ahí desde el primer día, mis padres. Gracias a ellos por creer en mis capacidades incluso cuando yo dudaba, y por ser la fuente de cariño y motivación que me impulsó a culminar esta etapa.

A mi hermano por su sabiduría y su paciencia,  por los consejos, las ideas y la enorme ayuda que me brindo a lo largo del desarrollo de este proyecto.

Y por último, pero no menos importante, a cuantos vean el tema de ciberseguridad como algo relevante e importe en la actualidad.

## Agradecimientos

Sin lugar a duda, el agradecimiento más importante, grande y profundo va dirigido a mi hermano. Sin él, nada de este proyecto habría sido posible. Sus conocimientos, consejos, charlas e ideas fueron la guía necesaria en medio de mis dudas y preguntas. Extiendo también mi agradecimiento a mis padres por su apoyo, comprensión y, sobre todo, por el cariño y la ternura que me ofrecen a diario.

También agradezco con todo el corazón a los compañeros del grupo estudiantil de ciberseguridad de la Universidad Nacional, Uqbar, por inspirarme y por brindar su conocimiento y ayuda en la temática de este proyecto.

Un sincero agradecimiento a los profesores y tutores, quienes brindaron orientación y guía a lo largo de este proceso. Sus observaciones, siempre tan acertadas, ayudaron a forjar un proyecto mucho más sólido y coherente.

Agradezco también al colegio Gimnasio Santa Rocío por abrirme sus puertas y por su constante disposición para colaborar, así como a los estudiantes, quienes fueron amables y participativos en cada charla, reunión o conversación que tuvimos.

Por último, agradezco a mis compañeros, quienes fueron una fuente de inspiración constante y, con su optimismo y compromiso, me motivaron a seguir adelante.

*“El eslabón más débil de la cadena de seguridad es el elemento humano”*

*Kevin Mitnick*

## Resumen

Constantemente estamos expuestos a amenazas digitales en este mundo hiperconectado, aún más aquellas personas que están más tiempo en línea como lo son los adolescentes de 15 a 17 años, quienes, a pesar de pasar horas en la red, y tener conocimientos basados en lógica, aun les cuesta identificar las formas de los ciberataques a los que están expuestos, por ende, no adoptan de protección adecuadas.

Como respuesta a esta problemática, se plantea el proyecto llamado “Cyberman en la red” que tiene como principal objetivo el desarrollo de un videojuego para el fomento de habilidades digitales direccionadas a la ciberseguridad. Empleando una metodología iterativa como lo es el doble diamante, donde se habla con el usuario y expertos temáticos, se llevó a cabo una investigación con la cual se buscó dejar claro los lineamientos y requerimientos del usuario. El mínimo producto viable (MVP) busca precisamente presentar una solución alineada al usuario y a la problemática.



*Palabras clave:* Ciberseguridad, Phishing, Gamificación, Videojuego educativo, Design Thinking


**Línea(s) de profundización:**

Videojuegos

**Abstract**

We are constantly exposed to digital threats in this hyperconnected world — even more so those who spend more time online, such as adolescents aged 15 to 17. Despite spending hours on the internet and having logic-based knowledge, they still struggle to identify the different forms of cyberattacks to which they are exposed; therefore, they do not adopt adequate protection measures.

In response to this issue, the project “Cyberman en la red” (Cyberman on the Web) was proposed, with the main objective of developing a video game aimed at fostering digital skills related to cybersecurity. Using an iterative methodology such as the Double Diamond, which involves engaging with users and subject-matter experts, research was carried out to clearly define user guidelines and requirements. The Minimum Viable Product (MVP) aims to present a solution aligned with both the user and the identified problem.

*Keywords:* Cybersecurity, Phishing, Gamification, Educational Video Game, Design Thinking

**Research lines:**
Video games

## Tabla de contenido

## Listado de figuras

## Listado de tablas

# 1. Formulación del proyecto

## 1.1 Introducción

Habitar los entornos digitales es la nueva forma de vivir. Es allí donde las personas se relacionan, se comunican, muchos estudian, otros muchos trabajan, o todo al tiempo. Sin embargo, este crecimiento del espacio y del ciberespacio ha incrementado de manera exponencial los riesgos relacionados a la seguridad digital. Especialmente quienes carecen de los conocimientos y los hábitos necesarios para identificar y responder de manera oportuna las diferentes amenazas que se presentan en este entorno como lo es el phishing, este es un tipo de ataque que se basa en la manipulación y en la confianza que tienen las personas frente a la seguridad digital.

Ante este escenario un poco ajetreado, nace Cyberman en la red, que es una herramienta digital gamificada 2D, donde se ayuda a fortalecer las habilidades en ciberseguridad y a prevenir que las personas, particularmente adolescentes de 15 a 17 años, caigan en ataques de phishing.

El desarrollo del videojuego incluye varias etapas, como la caracterización del usuario, la identificación de las necesidades y requerimientos tanto de diseño como pedagógicos, técnicos y visuales. A partir de ellas se construyó una propuesta gamificada con el aprendizaje experiencial como base.

Este proyecto busca formar usuarios conscientes y críticos en

los entornos digitales. Que sepan cómo actuar frente a las ciiberamenazas y los ciberataques.

### 1.2 Justificación

En la actualidad, la plena integración de los medios digitales en las diferentes actividades de la cotidianidad no es un secreto ni un dato nuevo, de hecho, según DataReportal hay 5,64 mil millones de personas que usan internet un 2,6% más que el año anterior (We Are Social; Meltwater, 2025). En Colombia, los datos hasta principios del 2025 se dice que hay 41,1 millones de personas usan internet, un 77,3% de la población (Kemp, 2025), un aumento considerable si se tiene en cuenta que según la CRC, en 2020 la tasa de penetración fue del 64,4% (Comisión de Regulación de Comunicaciones, 2021), lo que evidencia el rápido incremento y la creciente necesidad de habitar los entornos virtuales, no obstante, esto dio más oportunidades a los ciberdelincuentes de atacar, es por ello que los ciberdelitos van en ascenso año tras año.

Particularmente en Colombia, la seguridad digital adquiere especial relevancia. Se estima que el promedio de tiempo en línea supera las 8 horas diarias, una cifra que se encuentra por encima del promedio mundial de aproximadamente 6 horas con 40 minutos (Statista, 2024). En el caso de niños, niñas y adolescentes en Colombia, el tiempo de conexión es aún mayor, según la investigación *Jóvenes en línea* (Durán Becerra y otros, 2024, pág. 17), ellos pasan en promedio 10 horas conectados, principalmente en plataformas de streaming, redes sociales y aplicaciones de mensajería.

Ahora bien, no se trata de aislarse ni de desconectarse de las tecnologías de la información y la comunicación (TIC), en lugar de eso, implica habitar los medios digitales con responsabilidad y mantenerse alerta frente a los posibles riesgos. Entre los más comunes se encuentran: el malware, correspondiente a software malicioso; el ransomware, un tipo de malware que “secuestra” datos a cambio de un rescate; el phishing, una forma de ingeniería social que engaña al usuario para obtener información sensible; y los ataques de Denegación de Servicio Distribuido (DDoS), que saturan servidores con tráfico excesivo para provocar su colapso (Lindemulder & Kosinski, ¿Qué es la ciberseguridad?, 2024).

Estas amenazas no son meramente hipotéticas, por ello la ciberseguridad surge como una respuesta indispensable ante los riesgos que enfrentan quienes están en el espacio virtual. De hecho, en 2024, los ciberataques aumentaron un 14 %, con un promedio diario de 467 mil incidentes reportados (Cyberpeace Tech, 2025). Según el informe IBM X-Force Threat Intelligence Index 2024, Latinoamérica representó el 12 % de todos los ciberataques registrados por X-Force, y dentro de esta cifra, Colombia concentró el 17 % de los ataques en la región durante 2023 (IBM Corporation, 2024).

La creciente preocupación se origina en la rápida evolución de las amenazas digitales. De acuerdo con el informe IBM X-Force 2025 Threat Intelligence Index, el principal método de acceso inicial utilizado por los atacantes fue el uso de credenciales válidas (usuario

y contraseña), en lugar de técnicas tradicionales de intrusión, “Hackers don’t break in, they log in”. Aunque el phishing clásico por correo electrónico mostró una disminución en su tasa de efectividad del 46 % en 2022 al 25 % en 2024, los atacantes han adaptado sus estrategias, como implementar Inteligencia Artificial (IA) para hacer señuelos más sofisticados. La tendencia a la baja también se observó en los correos electrónicos que contenían malware tipo backdoor, dado que la probabilidad de detección aumentó considerablemente, lo que hizo que los ciberdelincuentes tuvieran que modificar sus tácticas. Como respuesta, durante los primeros meses de 2025, el volumen de infostealers distribuidos mediante correos phishing aumentó en un 180% en comparación con 2023 (IBM Corporation, 2025, pág. 12), mediante una técnica sofisticada que consiste en ocultar el malware dentro de documentos adjuntos que aparentan ser legítimos, como archivos PDF, Excel o Word.

Es relevante destacar que este tipo de amenazas y ataques pueden afectar a toda persona que navegue en internet, actividad que, como se abordó anteriormente, más que una preferencia personal, es parte de una necesidad en los tiempos contemporáneos. En este sentido, llama la atención la situación de los usuarios jóvenes, el estudio antes citado, *Jóvenes en línea*, el 26.6 % de los niños, niñas y adolescentes encuestados afirmó que los riesgos digitales no les impiden navegar, y un 20.7 % dijo no saber a qué peligros están realmente expuestos (Durán Becerra y otros, 2024, pág. 59). Este desconocimiento amplía su vulnerabilidad y evidencia la falta de una

cultura de protección digital desde edades tempranas. Por ello, resulta interesante que el 43.4 % de las personas encuestadas por el DANE en el marco de la ENTIC (Encuesta de Tecnologías de la Información y las Comunicaciones) utilizan antivirus, y que el 60.9 % consideran que tienen una contraseña segura (Ministerio de Tecnologías de la Información y Comunicaciones de Colombia [MinTIC], 2023, pág. 24). Lo cual presenta un escenario llamativo, porque existe la creencia de que la seguridad técnica es más que suficiente, cuando no es así, y es obsoleta frente a las amenazas que atacan directamente al “eslabón más débil” de la seguridad de los sistemas, este eslabón es el usuario, que sumado a la sofisticación de los ciberataques actuales hace que se perpetue la vulnerabilidad en la que se encuentra la sociedad en general.

Por ello, es importante fortalecer las habilidades digitales en ciberseguridad entre los usuarios, y para ello el diseño digital y multimedia puede abordar esta necesidad desde diversos frentes. Con los datos sobre el aumento de ciberataques y ciber amenazas, la baja percepción de riesgo y medidas muy básicas e insuficientes de protección, se propone el desarrollo de un producto digital que mediante un entorno simulado que entrene al usuario en amenazas en los entornos digitales. Esto porque todos estamos expuestos en mayor o menor medida a diversos incidentes de seguridad que fácilmente pueden escalar a un ataque.

Para este proyecto se contempla en una primera etapa un enfoque que se centre en riesgos específicos, como lo es el phishing,

a través de una narrativa gamificada que propicie la identificación de estas amenazas. Sin embargo, se deja abierta la posibilidad de evolucionar progresivamente hacia la prevención de otros tópicos de ciberseguridad, para construir un recurso flexible y adaptativo frente al cambio constante del entorno digital.

### 1.3 Definición del problema

En la actualidad, los entornos digitales tienen tal importancia y trascendencia que están presentes en todos los aspectos de la vida, y, particularmente, los adolescentes tienen una presencia en línea bastante significativa. Este modo de habitar los medios virtuales ha hecho que todos, y de manera especial los más jóvenes, estén más expuestos a amenazas de seguridad. Bogotá registró en 2023 un uso de internet en personas de 5 y más años de un 85,9%, esto según la encuesta nacional de calidad de vida del DANE (2023), pero este nivel de uso no significa necesariamente que exista una educación en ciberseguridad efectiva, lo que hace que las vulnerabilidades y las amenazas digitales sigan en crecimiento con acciones más sofisticadas.

Esto necesita hábitos seguros de navegación y conocimiento sobre las amenazas digitales que, lastimosamente, no ha evolucionado al ritmo que se requiere. Esto genera una brecha entre este uso de las TIC y la falta de educación efectiva y útil en ciberseguridad, lo que ha provocado que los adolescentes entre los 15 y 17 años de Bogotá se conviertan en uno de los grupos más vulnerables frente a los ciberataques, como el phishing y otras formas

de ingeniería social moderna, además de otra serie de amenazas existentes en los entornos digitales.

Según David Chaparro, estudiante de Ingeniería de sistemas y computación en la Universidad Nacional y coordinador de Uqbar[1] la ingeniería social es la forma más fácil para atacar pues ataca directamente a las personas, pasando sobre todos los bloqueos técnicos que puedan haber, y lastimosamente las personas pasan por alto algunas señales importantes para reconocer un engaño resultando en robo de credenciales, un robo económico o se abra la puerta a ataques aún mayores (Anexo A).

Dentro de los factores que hacen de estos ataques algo que merece ser atendido es su rápida evolución, esto es producto de la combinación del uso de la tecnología de manera masiva e irresponsable y la ausencia o carente formación en ciberseguridad a la vanguardia, esto hace que los ciber atacantes prueben y perfeccionen nuevas técnicas de tal manera que logran acelerar la transformación de las vulneraciones e intrusión en los sistemas para exponer datos e información.

Es aquí donde el DDM se convierte en una herramienta capaz de transformar la forma en la que se comunican y apropian los temas relacionados a ciberseguridad. Esto se puede lograr mediante diferentes recursos, como lo podrían ser las narrativas digitales, la

[1] Uqbar: Grupo estudiantil de la Universidad Nacional de Colombia que se enfoca en el estudio y la divulgación de la seguridad digital por medio de cursos, material informativo y campañas de concientización

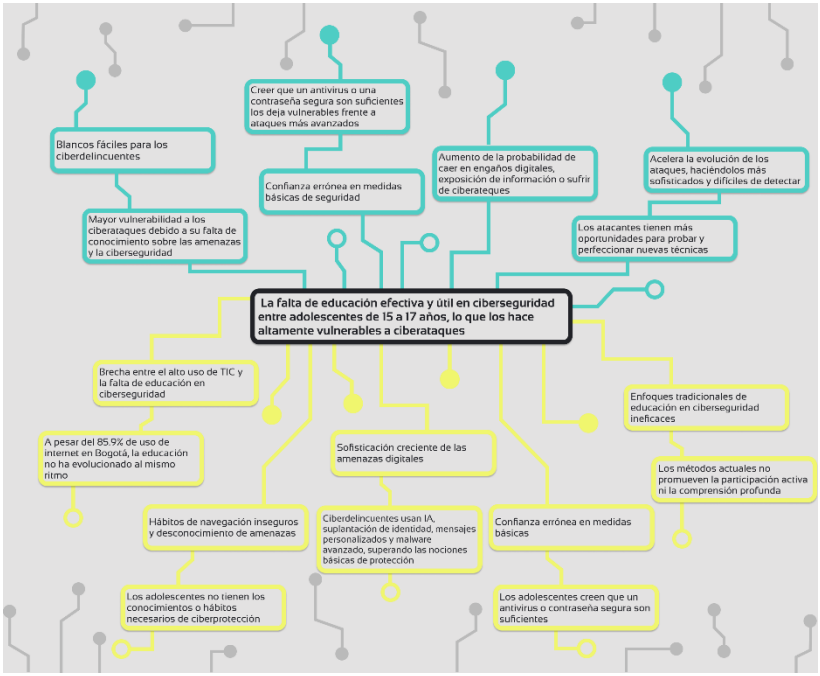
gamificación o experiencias interactivas que puedan facilitar la adopción de términos más complejos y fomentar el crecimiento de una cultura de ciberseguridad tan necesaria en los tiempos que corren.

La necesidad de un enfoque diferente se vuelve valioso si se considera que las amenazas digitales actuales ya no se limitan a técnicas simples, los ciberdelincuentes usan métodos cada vez más sofisticados, acompañados del uso de inteligencia artificial para suplantar identidades, generar mensajes personalizados o insertar malware en documentos aparentemente inofensivos. Esta complejidad supera con en muchas ocasiones las nociones básicas de protección que suelen manejar los adolescentes, quienes confían que con tener un antivirus activo o una contraseña segura son medidas suficientes ante estos riesgos, y esto no es del todo así

El problema está en la presencia de amenazas, al igual que en la falta de conocimiento para poder reconocerlas y actuar frente a ellas. Es por ello que el DDM da herramientas importantes para el fortalecimiento de habilidades digitales para la ciberseguridad, que va más allá del simple hecho de presentar la información. He aquí la diferencia con los enfoques más tradicionales y rígidos: el DDM promueve la participación activa de la persona en su proceso de aprendizaje, impulsa la comprensión de conceptos técnicos y puede incentivar hábitos digitales seguros de forma clara y consciente (figura 1).

**Figura 1**

*Árbol de problemas*




*Nota.* En el grafico se representa la relación del problema central con las causas y las consecuencias. *Fuente*: Elaboración propia.

Entonces, en esta investigación se genera esta pregunta: ¿Cómo puede el diseño digital y multimedia puede contribuir a fortalecer las habilidades digitales en ciberseguridad con base en el conocimiento y la prevención? Es importante decir que el enfoque, inicialmente, estará centrado en el phishing en particular, aunque no se descarta que, a futuro, se pueda ampliar a otras ciberamenazas.

Con este planteamiento, se busca contribuir al desarrollo de unas habilidades digitales capaces de responder a las amenazas actuales y reducir la vulnerabilidad de uno de los grupos más expuestos en el entorno digital contemporáneo.

## 1.4 Hipótesis de la investigación

### *1.4.1 Hipótesis explicativa*

Existe una relación entre la alta vulnerabilidad de los adolescentes de 15 a 17 años a diversas ciberamenazas, dentro de las cuales está el phishing y otros tipos de ingeniería social, y los proyectos educativos poco efectivos que tratan de fortalecer las habilidades digitales enfocadas en ciberseguridad desde edades en las cuales la permanencia en línea es mayor. La falta de conocimientos adecuados sobre amenazas cibernéticas, como la ingeniería social, contribuye a una exposición constante y desprotegida en los entornos digitales.

### *1.4.1 Hipótesis propositiva*

Si se implementan estrategias de DDM orientadas a la prevención del phishing, que integre recursos narrativos y participativos adaptados a las dinámicas que requieren adolescentes entre los 15 y 17 años, posiblemente se pueda fortalecer las habilidades en ciberseguridad entre adolescentes, para que su comprensión de los riesgos asociados a la ingeniería social sea mayor y puedan promover prácticas de navegación más seguras. Esto permitiría mejorar el reconocimiento de amenazas digitales actuales, y propiciar un cambio de comportamiento frente a la seguridad en línea.

## 1.5 Objetivos

### *1.5.1 Objetivo general*

Desarrollar un producto gamificado que permita a los adolescentes de 15 a 17 años mejorar su comprensión sobre los riesgos digitales, específicamente el phishing, y fomentar la adquisición de habilidades digitales que velen por su seguridad en línea, con el objetivo de reducir su vulnerabilidad frente a ataques cibernéticos.

### *1.5.2 Objetivos específicos*

- Caracterizar el perfil del usuario objetivo en relación con su conocimiento, percepción y hábitos frente a riesgos digitales como el phishing, mediante instrumentos de recolección de datos que permitan comprender su nivel de exposición y vulnerabilidad.
- Identificar los requerimientos clave para una propuesta que promueva la alfabetización en ciberseguridad, con especial atención en los hallazgos sobre las necesidades e intereses del público objetivo.
- Prototipar un recurso interactivo orientado a la prevención del phishing, donde se articulen elementos narrativos, visuales y de participación activa
- Evaluar el impacto de la propuesta a través de testeos con usuarios, donde se puedan observar los cambios en la percepción del riesgo, el aprendizaje adquirido y la disposición a aplicar prácticas seguras en línea

## 1.6 Planteamiento metodológico

La metodología es una parte transversal del proyecto ya que con este se determina la estructura y camino que se llevara a cabo. Este proyecto usara una metodología que tiene como base y columna vertebral la metodología de Doble Diamante desarrollada por el British Design Council en 2004, este modelo permite el diseño exitoso con una alta comprensión de las necesidades y los deseos de los usuarios, lo que lleva a soluciones efectivas y relevantes. El doble diamante brinda una estructura general que permite la exploración de problemas y el desarrollo de soluciones que requieren una sólida investigación .

Los pasos del Doble Diamante constan de 4 fases, Descubrir, Definir, Desarrollar, Evaluar. Los ciclos de iteración y los bucles de retroalimentación continua y la constante validación del usuario son parte estructural de esta metodología.

El primer diamante conjuga las 2 fases iniciales de esta metodología. Descubrir y definir, en estas fases se busca comprender el problema, investigar, hablar con personas y con esta información se busca identificar insights y se formula un problema y los objetivos de este (Design Council, s.f.).

En la fase 1 la documentación, observación, entrevistas y el acercamiento a la temática, son el eje que conduce esta etapa con el objetivo de esta fase es obtener una comprensión empática y completa de los comportamientos digitales del usuario, las

vulnerabilidades y los conocimientos o los conceptos que no tienen muy claros o que directamente no saben con respecto a la ciberseguridad.

Para la fase 2, se procesa, organiza y clasifica la información de la fase anterior, esto para identificar los hallazgos y transfórmalos en objetivos claros y medibles

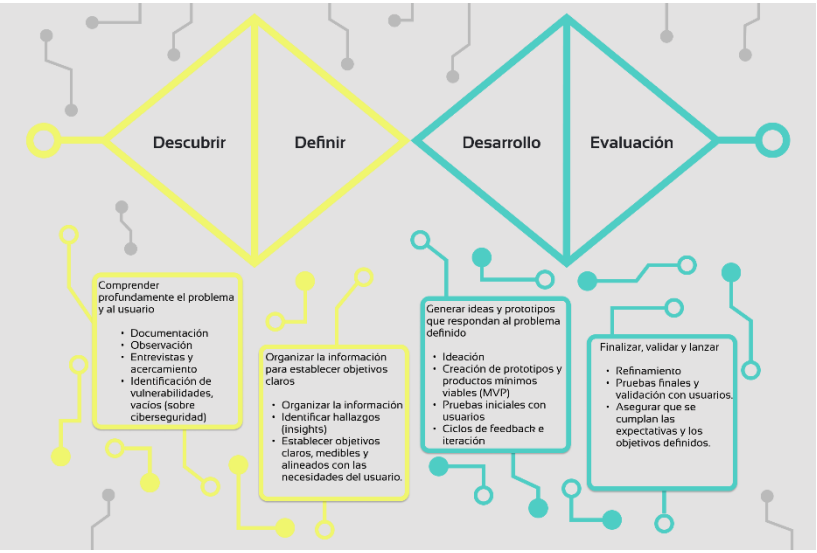
En la metodología de doble diamante el proceso de iteración con los usuarios en todo el proceso es muy importante, sobre todo en la transición del diamante 1, donde se encuentra la investigación y planteamiento del problema y el diamante 2 donde se lleva a cabo el desarrollo más técnico.

En la fase 3, con base en toda la investigación y filtración de las fases anteriores se entra en la etapa de ideación y prototipado, en esta fase, son útiles herramientas como el Brainstorming para las ideas iniciales y el producto mínimo viable para hacer pequeños prototipos que se puedan testear con los usuarios en búsqueda de un feedback que aporte al desarrollo de un producto útil y relevante. Esto es un ciclo donde cada prototipo, cada prueba y cada validación con usuarios aportan a una siguiente versión que considere la interacción de los usuarios.

Como ultima parte, la fase 4, evaluación, aquí se refina, se prueba y se valida la solución a la que llego posterior a las diferentes fases de prototipado, testeos y pruebas con usuarios. En esta fase se busca llegar a una calidad optima que de solución al problema y que

cumpla con las expectativas de los usuarios y acorde con los objetivos planteados (Figura 2)

**Figura 2** Planteamiento metodológico




*Fuente:* Elaboración propia

Esta metodología permite explorar la complejidad del tema de la educación en ciberseguridad, donde estos conocimientos deben convertirse en acciones en el ciberespacio. Además, se prioriza al usuario, lo cual hace que el producto tenga relevancia. El diseño debe centrarse en la prevención y en el fomento de la adquisición y apropiación de conceptos de ciberseguridad. El éxito del producto se encontrará en el trabajo interdisciplinar, de la mano del usuario.

## 1.7 Alcances y limitaciones

### *1.7.1 Alcances*

El proyecto se enfocará en el desarrollo de una herramienta interactiva dirigida a adolescentes de 14 a 18 años, esto con el objetivo de mejorar y facilitar la identificación de amenazas digitales, particularmente la prevención de ataques de phishing. La herramienta deberá incorporar elementos dinámicos y de gamificación, para mejorar la comprensión y retención de la información sobre ciberseguridad.

Inicialmente se centrará en el phishing y otros modos de ingeniería social, pero no se descarta la posibilidad de ampliar los alcances del producto a otros temas de ciberseguridad, para que este proyecto evolucione de acuerdo con los intereses de los usuarios, ya que debe estar actualizado en estos temas, y el entorno virtual evoluciona de manera constante.

### *1.7.2 Limitaciones*

La ciberseguridad es un tema muy amplio que abordarlo todo sería francamente ambicioso y exagerado, presenta limitaciones en beneficio de un trabajo pulido. Otra limitación presente es el acceso al público objetivo, adolescentes de 14 a 18 años, esto requiere lógicamente unas normativas y seguir un protocolo, lo cual puede diezmar la participación y limitar la diversidad de perfiles considerados en la validación del producto.

La siguiente limitación presente es el tiempo destinado para

llevar a cabo el proyecto, Además, dado que el phishing es una amenaza en constante evolución, el producto digital a desarrollar tiene que contemplar actualizaciones constantes para mantenerse al día con las nuevas tácticas utilizadas por los ciberdelincuentes.

# 2. Base teórica del proyecto

## 2.1 Marco referencial

Este apartado establece una estructura teórica y contextual para indagar y abordar el tema del phishing como una amenaza central dentro de la ciberseguridad. A través de marcos teóricos uno específicamente para la temática contextual, y el otro para lo que se refiera a lo disciplinar, marcos conceptuales, institucionales y legales, con esto se establece una base sólida para comprender la problemática y su impacto en jóvenes usuarios digitales. También se incluye un análisis del estado del arte, que permite identificar soluciones previas, otras propuestas ya existentes y tendencias en el abordaje del phishing, así como una caracterización del usuario que fundamenta el enfoque del proyecto. Todo esto orienta el desarrollo de un producto de diseño digital enfocado en la prevención y educación frente al phishing.

### *2.1.1 Antecedentes*

Para comprender el problema de investigación se realizó una revisión literaria y contextualización histórica. La ciberseguridad es el tema del cual parte la idea inicial, dentro de esta temática se encuentran las

ciberamenazas y para propósitos de este proyecto se abordará la ingeniería social y particularmente el phishing, esto y la adopción de estos conceptos en los adolescentes. Este grupo ya que según estadísticas pasan más tiempo en línea lo cual, sin la suficiente precaución los deja expuestos a ciberdelincuentes, la revisión aborda antecedentes históricos y disciplinares relevantes para este proyecto.

Cuando se habla de ciberseguridad, se habla de uno de los pilares más importantes para la protección de la información en la era digital contemporánea. Con la sofisticación de las ciberamenazas en aumento, el phishing se destaca por su persistencia y adaptabilidad y esto lo podemos analizar con ayuda de la historia de este ataque y con las medidas que han tomado para mitigar su impacto que ha evolucionado con el tiempo.

La ciberseguridad, entendida como la protección de la información digital, tiene sus raíces en medio de la Segunda Guerra Mundial, cuando máquinas como Enigma y ENIAC fueron las protagonistas de los primeros intentos por encriptar y proteger comunicaciones sensibles (Keepnet, 2024). Posteriormente en la Guerra Fría, la creación de la Agencia de Seguridad Nacional (NSA) en Estados Unidos evidenció la creciente preocupación por salvaguardar información estratégica y el desarrollo de sistemas de autenticación más robustos (Nason, 2024).

Los primeros hackers surgieron con la conexión de computadores mediante ARPANET, que si bien trajo un avance importante en la facilitación de intercambio de información a distancia,

las vulnerabilidades en los sistemas se abrieron paso. Estos primeros hackers se centran principalmente en obtener acceso a ciertos sistemas, como las pruebas realizadas por IBM a estudiantes para identificar vulnerabilidades en sus nuevas computadoras (Nason, 2024). Cuando la ciberseguridad se establece como hoy en día fue en la década de 1970, con el gusano informático “Creeper” dentro de ARPANET y con el primer antivirus para eliminar los “Creeper”, “Reaper” (Ricardo, 2024).

El phishing como técnica específica de ataque apareció en la década de los 90, cuando ciberdelincuentes suplantaron empleados de America Online (AOL) para obtener contraseñas y datos de tarjetas de crédito (Waltz, 2024). Durante los años 2000, esta práctica se sofisticó y extendió a servicios como eBay y PayPal, apalancada por el crecimiento del comercio electrónico.

A partir de 2010, el phishing dejó de limitarse al correo electrónico para expandirse a redes sociales, apps de mensajería, SMS e incluso llamadas telefónicas. Actualmente, se combina con el uso de inteligencia artificial y técnicas avanzadas de ingeniería social, lo que permite ataques más dirigidos, convincentes y difíciles de detectar. Además, se ha convertido en uno de los métodos principales de distribución de ransomware, que afecta tanto a usuarios individuales como a grandes organizaciones.

Hoy en día el phishing es una de las principales formas de vulneración, se estima que por lo menos el 75% de los ciberataques comienzan con un correo malicioso (Traynor, 2025) y el uso de IA

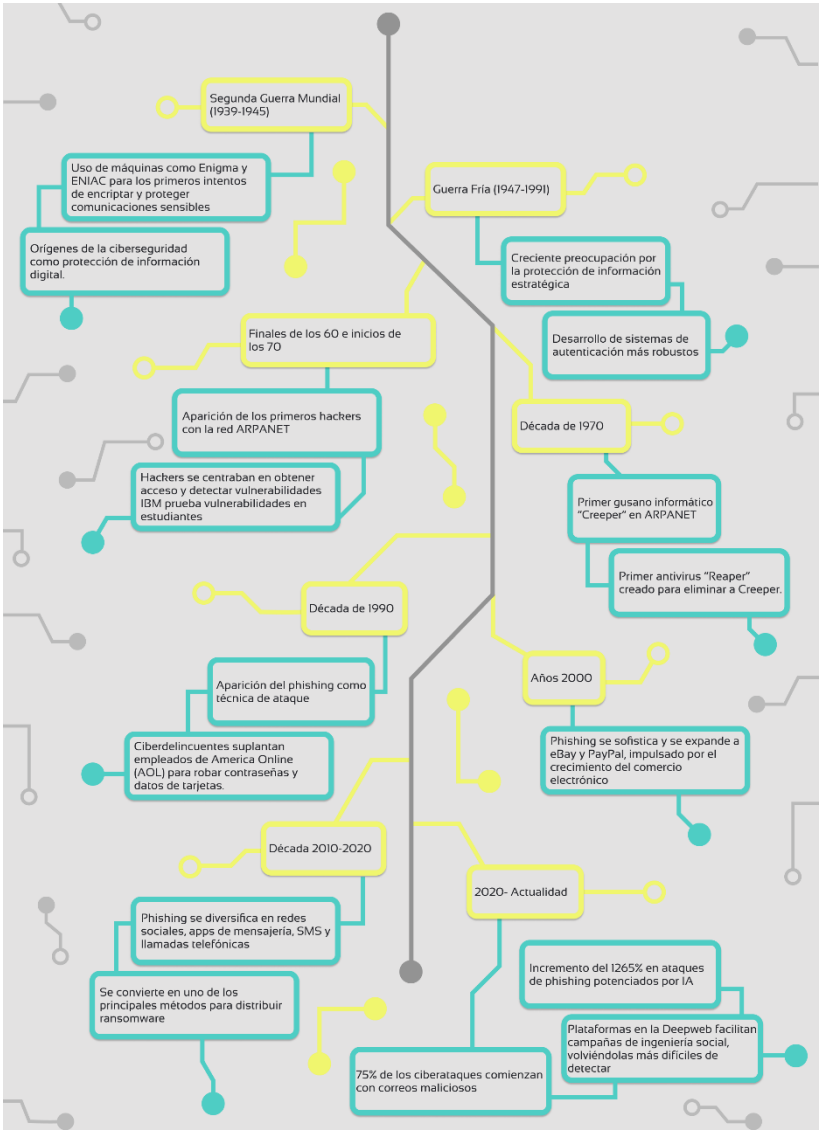
para potenciar este tipo de ataques también es algo que se ha visto un aumento, desde noviembre del 2022 se ha visto un incremento del 1265% (Michalowski, 2025).

La inteligencia artificial ha transformado la forma en la que la ingeniería social ataca, esto mediante formas más sofisticadas y difíciles de detectar, plataformas como FraudGPT o WormGPT en la deepweb fueron identificadas por La Revista Internacional de Investigación Científica en Ciencias de la Computación, Ingeniería y Tecnologías de la Información (IJSR CSEIT) han facilitado las campañas de ingeniería social y las han convertido en herramientas más útiles para aumentar la vulnerabilidad de los usuarios.

**2.1.1.1 Línea del tiempo.** La línea del tiempo (figura 3) presenta el panorama de la ciberseguridad desde un punto de vista histórico y como ha evolucionado hasta el panorama actual, como esta descrito en el apartado anterior.

**Figura 3**

*Línea del tiempo*




*Fuente.* Elaboración propia

### *2.1.2 Marco teórico contextual*

En esta sección se delimitan algunos conceptos necesarios para la comprensión de las problemáticas relacionadas a la ciberseguridad e importantes para el contexto del proyecto. La conceptualización del espacio donde se desarrollan las dinámicas digitales, y cómo progresivamente se va adentrando al tema principal, que es el phishing bajo el término paraguas Ingeniería Social, son la base del producto propuesto.

**2.1.2.1 Concepto de ciberespacio.** La RAE da una definición al ciberespacio como un “espacio imaginario en el que se establecen las comunicaciones de una red informática, especialmente de internet”  le debe poner un título a cada tema y este reemplaza el texto“ (s.f.). Este breve acercamiento al concepto nos brinda un abrebocas al tema, en tanto nos introduce al término como un espacio imaginario, es decir, inmaterial e intangible que se halla en el entorno virtual y le proporciona una función comunicativa, y aunque en esta definición se da la posibilidad de ampliar su uso más allá del internet, destaca su conexión con ella. Pero se es aún muy vago como concepto.

En Colombia, mediante la Resolución 2258 de 2009 de la Comisión de Regulación de Comunicaciones (CRC), también se brinda una descripción del ciberespacio un poco más técnica: “Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado

para la interacción entre usuarios.” (2009). Se consideran los aspectos físicos, como la infraestructura tecnológica, y los virtuales que más allá del internet es donde se señalan los datos e información, se reconoce que debe haber un medio material para que exista el ciberespacio. A diferencia de la RAE, que apunta a un espacio imaginario, en el concepto que adopta esta resolución se tiene en cuenta la infraestructura que permite la existencia del ciberespacio. Este enfoque lo delimita como un sistema funcional para la conectividad y el intercambio de información entre usuarios, sin abordar de manera expresa los posibles vínculos y las dinámicas sociales que en ella se puedan generar.

Si bien estas definiciones dan una apertura al concepto de ciberespacio, aún son cortas para abordar la complejidad que este puede tener. Santana-Soriano y Báez Vizcaíno proponen un concepto con un enfoque un poco diferente, desde el materialismo sistémico. Lo definen “como un espacio artificial y ficcional emergente en el que tienen lugar relaciones sociales entre personas, organizaciones y máquinas, y que no tiene existencia independiente del conjunto de equipos y programas informáticos que le posibilitan.” (2022, pág. 49). Hablamos de lo técnico e incorpora lo social; más allá de la infraestructura necesaria, se señala como importantes las dinámicas entre las personas, organizaciones y máquinas que allí ocurren. Además, este lugar “artificial y ficcional” no tiene existencia autónoma sin la suma de las partes. El ciberespacio no es algo fijo y tiene un carácter mutable, que se le atribuye a los componentes que lo

conforman, y así pueden surgir nuevos ciberespacios que dependen de los cambios tecnológicos, sociales y culturales.

**2.1.2.2 Alcances de la ciberseguridad.** Actualmente, la ciberseguridad va más allá de la protección en el sentido técnico; debe ser un campo integral en el que se garantice la confianza y protección de las interacciones que se generan en los entornos digitales. Es por ello que, desde una perspectiva más institucional, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) describe la ciberseguridad como un conjunto de recursos, políticas, prácticas, tecnologías y acciones que tienen como propósito proteger los recursos digitales y a las personas dentro del ciberespacio (s.f.). El objetivo es asegurar condiciones como la integridad, la confidencialidad, la autenticación y el no repudio de la información, lo cual abarca procesos como la gestión, formación y actualización constante.

Una perspectiva más académica, dada por Craigen, Diakun-Thibault y Purse (2014), entiende a la ciberseguridad como la organización de recursos, procesos y estructuras para proteger el ciberespacio y los sistemas que lo habilitan frente a eventos que afectan el pleno goce de los derechos legales y de facto. Con esta definición se pone sobre la mesa otro aspecto: los derechos digitales, que muchas veces se ven vulnerados o comprometidos.

La ciberseguridad se refiere a todas las tecnologías, prácticas y políticas para prevenir los ciberataques o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas

informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra el ransomware y otros malware, las estafas de phishing, el robo de datos y otras ciberamenazas.

Por otra parte, Lindemulder y Kosinski (2024), para IBM, definen la ciberseguridad desde una perspectiva operacional y funcional:

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

Esta perspectiva resalta la necesidad de adaptabilidad a los diferentes tipos de amenazas, las cuales evolucionan y cada vez son más sofisticadas.

Con estas perspectivas se puede desarrollar un concepto amplio sobre la ciberseguridad, donde los aspectos van desde el conocimiento, la conciencia, las prácticas hasta la comprensión técnica, y adquiere especial importancia en usuarios altamente expuestos a entornos digitales.

**2.1.2.3 Fenómeno de los ciberataques.** El ciberespacio enfrenta amenazas que van en constante aumento, y estas se consolidan en ciberataques que son acciones deliberadas que usan

los ciberatacantes para “robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital” (IBM Corporation, 2025). Las motivaciones detrás de estos ataques son diversas y con objetivos distintos, desde el robo de información hasta espionaje o interrupción de sistemas.

Como mencioné anteriormente, las motivaciones y objetivos son variados, lo que refleja la pluralidad de estos ataques. Entre ellas se encuentran el lucro económico que probablemente es el factor más común, el robo de datos para su posterior venta en redes ocultas como la deep web o la dark web, y los ataques en contextos bélicos, cuyo fin es desestabilizar infraestructuras críticas u organizaciones gubernamentales, entre otras motivaciones presentes en el ámbito del ciberespacio (Proofpoint, s.f.).

Los tipos de ciberataques también son amplios, variados y responden al objetivo del atacante. De manera amplia, se halla el malware, que no es más que software malicioso; lo que hace depende del tipo, entre ellos están los troyanos, los virus, los gusanos, etc., en general, su objetivo es tener acceso absoluto a las redes o dispositivos para robar datos o causar daños. Otro, bastante común, son los ataques por ransomware, este es un malware que “secuestra” los datos y pide una tarifa de rescate para restaurarlos. Los ataques de denegación de servicios (DoS), donde colapsan páginas web, redes o sistemas con alto tráfico o solicitudes. La suplantación de identidad (phishing) engaña a usuarios para robar datos mediante

correos o sitios falsos, se usa enlaces o archivos maliciosos, que pueden ser masivos o dirigidos. Los ataques MITM interceptan datos entre el usuario y un servicio, como en redes Wi-Fi falsas que roban credenciales (Fortinet, s.f.), entre muchos otros que existen y responden a un modo diferente de vulnerabilidad.

**2.1.2.4 Ingeniería social y phishing como una amenaza emergente.** Los humanos respondemos a estímulos como la curiosidad, el sentimiento de urgencia, la ambición, la confianza o la simple ignorancia. De esto es de lo que se aprovechan los ciberdelincuentes para entrar a los sistemas: solo se necesita un pequeño error para poner todos los datos y redes privadas en manos de los hackers. Esto se logra a través de engañar al eslabón más débil de cualquier entorno digital: el usuario; esto, mediante diferentes tipos de artimañas y trampas con el fin de ganarse la confianza del usuario o del personal de empresas (Borghello, 2009, pág. 2).

La ingeniería social tiene dos grandes tipos según la ejecución: la basada en humanos y la basada en computadores y algoritmos (software). En la ingeniería basada en humanos, el atacante interactúa directamente con la víctima. En la basada en el software, el atacante usa programas o plataformas como correos electrónicos, páginas web o herramientas automáticas. También hay una clasificación según el enfoque, como lo es el acercamiento físico. Este se basa en que el atacante se acerca de manera física y “hurga en la basura” (dumpster diving) en busca de información valiosa de primera mano. El acercamiento social es aquel en el que se crean

estas relaciones de confianza falsas. Dentro de esta clasificación también se encuentran los acercamientos técnicos; estos son puramente digitales y se usa la información en internet y redes sociales para atacar a un usuario. Los ataques y aproximaciones más efectivas son las que combinan varios de los enfoques, cuando se une lo técnico con lo social, por ejemplo, la curiosidad con un malware (Koyun & Al Janabi, 2017, pág. 7534)

Dentro de los diversos tipos de ataques, el principal es el *phishing*. En este, el atacante se hace pasar por un destinatario de confianza con el objetivo de que las personas entreguen información sensible o realicen acciones que afecten su seguridad digital. Existe el *phishing* por correos electrónicos masivos, en el que usualmente se hacen pasar por empresas legítimas; el *spear phishing*, que es un ataque dirigido a CEOs o personas reconocidas dentro de las empresas u organizaciones; el *vishing*, que se realiza por medio de llamadas; y el *smishing*, que es el *phishing* mediante mensajes de texto. También se encuentra la suplantación de páginas en motores de búsqueda y el *Angler phishing*, que consiste en la suplantación de identidad de los equipos de ayuda en redes sociales (Kosinski, 2024).

La ingeniería social funciona porque dentro de toda la gama de amenazas cibernéticas, esta se dirige principalmente en quienes son incautos y tienden a ser más susceptibles al engaño. Una trampa bien diseñada puede evadir los controles establecidos por los antivirus o incluso por sistemas computacionales especializados en ciberseguridad. Es por ello que, es cuestión de comportamiento y

conciencia, y en la falta de esto radica la verdadera amenaza ya que la eficacia de esto no radica en los factores técnicos sino en el factor humano.

### *2.1.3 Marco teórico disciplinar*

El marco teórico disciplinar consolida los fundamentos que desde el diseño orientan el desarrollo del proyecto. La gamificación como puente entre la pedagogía y las dinámicas de juego y el diseño centrado en el usuario para asegurar que el producto cumpla con la pertinencia y usabilidad que requiere el usuario. Estos enfoques articulados son la base en la que se apoya el proyecto para su desarrollo.

**2.1.3.1 Aprendizaje gamificado.** La gamificación, tal como la define Karl Kapp en *The Gamification of Learning and Instruction* (2012), es la implementación de elementos que se consideran de "juego" en la enseñanza y el aprendizaje. Su planteamiento va más allá de recompensas y puntos: habla de la necesidad de abordarlo de manera integral, con fusión de la motivación intrínseca, que nace del mero interés y curiosidad, y la motivación extrínseca, que es la que surge por los estímulos que provoca el storytelling, la estética, las recompensas, los castigos y demás elementos, los cuales deben ser incorporados de manera "inteligente y cautelosa" (Kapp, 2012, pág. 22).

La gamificación permite la adopción de temas complejos de manera más sencilla. Esto, de hecho, es uno de los fundamentos de

la gamificación que Kapp nombra en su libro: la abstracción de los temas complejos, no la trivialización de estos. Se trata de presentar los temas de manera más concreta y clara, sin distracciones ni información irrelevante que pueda confundir. Esta forma de aprendizaje se articula con el modelo del aprendizaje experiencial de David Kolb, donde la experiencia y la reflexión de esta son la base sobre la que se construye un aprendizaje efectivo. Dicho modelo consta de cuatro etapas: la experiencia concreta, la observación reflexiva, la conceptualización abstracta y la experimentación activa. Este ciclo se ve potenciado por la gamificación, ya que el usuario participa en una abstracción de modelos basados en la vida real, lo que le permite vivir experiencias para el aprendizaje (Kapp, 2012, pág. 26).

La gamificación interseca diferentes puntos necesarios para un diseño con un fin educativo óptimo: la narrativa, el factor estético, las dinámicas y mecánicas de juego, además del factor motivacional. Es por ello que resulta importante para este proyecto, dirigido al desarrollo de un producto digital para la enseñanza de buenas prácticas de ciberseguridad y, particularmente, la prevención del phishing.

**2.1.3.2 Diseño centrado en el usuario.** Donald Norman desarrolló el diseño centrado en el usuario como un enfoque en el que “los productos se basan en una comprensión explícita de los usuarios, las tareas y los entornos” (Interaction Design Foundation - IxDF, 2016). Es decir, hay que analizar las necesidades y limitaciones de

los usuarios, y no únicamente diseñar con base en la lógica del diseñador. Este enfoque comienza con una investigación profunda para comprender el comportamiento y el contexto del usuario. Dicha comprensión es la base de cada decisión de diseño, y con ello se garantiza un producto que será relevante y útil para quien está destinado.

El diseño centrado en el usuario es un proceso iterativo con el fin de satisfacer las necesidades del usuario. La investigación con usuario incluye entrevistas, encuestas, observación, etc., además de la evaluación constante mediante pruebas y testeos. Es aquí donde Jakob Nielsen aporta las “heurísticas de usabilidad”, que sirven para evaluar los productos bajo criterios como la visibilidad, correspondencia, control, coherencia, prevención, reconocimiento, estética, mensajes de error y ayuda al usuario (Nielsen, 1994) . Esto se usa para identificar problemas que existen en el diseño y buscar la mejora de la experiencia que tendrá el usuario al interactuar con el producto.

Para el desarrollo de un producto gamificado, su utilidad es de gran trascendencia, ya que su efectividad se basa en la interacción con el usuario. El DCU de Norman y las heurísticas de Nielsen permiten lograr un producto atractivo, intuitivo y que cumpla con los criterios técnicos para alcanzar el objetivo principal del proyecto.

### *2.1.4 Marco conceptual*

**Tabla 1**

*Marco conceptual*

| | |
|---|---|
| **Ciberespacio** (Santana-Soriano & Báez Vizcaíno, 2022) | El ciberespacio como un espacio artificial y ficcional emergente en el que se desarrollan relaciones sociales entre personas, organizaciones y máquinas. Este no existe de manera independiente, sino que depende de los equipos, programas y sistemas informáticos que lo posibilitan, y debe entenderse como una entidad emergente que evoluciona conforme cambian sus componentes. |
| **Ciberseguridad** (Lindemulder & Kosinski, ¿Qué es la ciberseguridad?, 2024) (Kaspersky, s.f.) | La ciberseguridad es un conjunto de tecnologías, prácticas y políticas diseñadas para proteger los sistemas informáticos contra ataques maliciosos, accesos no autorizados o daños potenciales. Su objetivo es salvaguardar la confidencialidad, integridad y disponibilidad de la información, prevenir ciberataques como el ransomware, malware y phishing, y |

| | |
|---|---|
| | mitigar sus posibles efectos. La ciberseguridad abarca áreas que van desde la protección de infraestructuras tecnológicas en empresas hasta la seguridad de dispositivos personales, promoviendo la defensa continua frente a las crecientes amenazas digitales |
| **Ingeniería Social** (Salahdine & Kaabouch, 2019) | La ingeniería social hace referencia a las técnicas que usan los ciberdelincuentes para manipular o engañar a las personas y así obtener vulnerar la información y los datos, la Ingeniería Social se aprovecha del eslabón más débil que es el humano, para la prevención de este tipo de ataque no basta tener sistemas robustos sino que dependen de las personas para reconocer ye evitar estas manipulaciones |
| **Phishing** (National Institute of Standards and Technology [NIST], s.f.) | Phishing es una técnica que busca obtener datos sensibles, mediante una solicitud fraudulenta por correo electrónico o sitio web en la que el atacante se presenta como una entidad legítima. También se describe como "una forma de ingeniería social que |

| | |
|---|---|
| | hace que los usuarios accedan a sitios falsos y revelen información personal" |
| **Gamificación** (Kapp, 2012, pág. 10) | “La gamificación es el uso de mecánicas basadas en juegos, estética y pensamiento de juego para involucrar a las personas, motivar la acción, promover el aprendizaje y resolver problemas” |

*Nota.* En la tabla se da definición a algunos conceptos a tratar en el documento y en el proyecto. Fuente: Santana-Soriano & Báez Vizcaíno, 2022; Lindemulder & Kosinski, ¿Qué es la ciberseguridad?, 2024, Kaspersky, s.f.; Salahdine & Kaabouch, 2019; National Institute of Standards and Technology [NIST], s.f.; Kapp, 2012.

### *2.1.5 Marco institucional*

**2. 1. 5. 1. Colegio Gimnasio Santa Rocío.** El caso de estudio se desarrolla en el colegio Gimnasio Santa Rocío una institución educativa de carácter privado ubicado en el barrio Villa del Rio en la localidad de Bosa, tiene mas de 750 estudiantes de primaria y bachillerato.

El colegio se centra en la formación integral de los estudiantes haciendo especial énfasis en el pensamiento crítico, resolución de conflictos y espíritu investigativo, características que

orientan los procesos de convivencia y formación ciudadana en la comunidad.

Cuentan con un curso curricular de Robótica, aquí los estudiantes pueden fortalecer sus competencias en ciencia, tecnología e innovación, este espacio está diseñado para que los estudiantes se familiaricen con herramientas tecnológicas, este curso es reflejo del interés que tiene la institución con esa área. En este marco, resulta como buen caso de estudio, ya que el colegio tiene un interés en formar estudiantes en el área de las tecnologías y los estudiantes están expuestos a los entornos virtuales , y aún existen los desafíos con relación a la ciberseguridad, como lo es la ingeniería social y el phishing.

Por esto, el desarrollo el producto gamificado para la promoción de buenas prácticas digitales se articula con la misión institucional y puede complementar el proceso de innovación en el área de la tecnología que ya tiene el colegio.

**2.1.5.2. Uqbar.** El grupo estudiantil de Seguridad Informática Uqbar, de la Universidad Nacional, funciona como un aliado y referente para este proyecto. Su experticia en el fomento y divulgación de la ciberseguridad permite tener un producto a la vanguardia por el contexto en el que ellos se desarrollan. Uqbar funciona como respaldo contextual y temático que ayuda a garantizar que la temática este abordada de manera correcta y de relevante en el campo de la ciberseguridad.

### *2.1.6 Marco legal*

En Colombia la seguridad digital ha estado en la mesa de dialogo desde hace mas de 15 años de manera activa, reconociendo como delitos la intromisión de manera abusiva e ilegitima a los sistemas informáticos, la violación de privacidad, la distribución de software malicioso con intención de daño informático además de reconocer los derechos que tienen las personas en el ciberespacio y otra serie de regulaciones de las TIC.

**2.1. 6.1. Ley 1273 de 2009.** Reformo el código penal para crear la “protección de la información y de los datos” y estableció un marco legal contra delitos informáticos, esta normal busca garantizar los principios de confidencialidad, integridad y disponibilidad de datos y sistemas que usan TIC, sanciona multas y penas de prisión a quienes incurran en actos ilícitos en el entorno virtual.

**2. 1. 6. 2. Decreto 338 de 2022.** Modifica el marco de la gobernanza de la seguridad digital, aplicable a sectores críticos para proteger la infraestructura y servicios esenciales e información en el ciberespacio.

**2. 1. 6. 3. CONPES 3995.** Política nacional de confianza y seguridad digital que esta orientada a reforzar la seguridad digital de los ciudadanos y de los sectores públicos y privados promoviendo la adopción de modelos y estándares internacionales, con énfasis en nuevas tecnologías para mayor inclusión y competitividad

## 2.2 Estado del arte

Hay proyectos, diseño y herramientas existentes que funcionan como referentes, ya sean por sus características narrativas, interactivas o funcionales.

**2. 2. 1. Google Interland.** Este es un juego online de aventuras para aprender sobre seguridad y ciudadanía digital, en el jugador debe tener practicas positivas y combatir contra el mal comportamiento de los hackers. Este juego consta de diferentes mundos en los que los niños pueden aprender de manera didáctica como desenvolverse correctamente en la red, hace parte de “se genial en internet” iniciativa también de Google para que los niños desarrollen habilidades responsables en línea.

**Figura 4** Interland - Google

*Fuente. Be internet awesome – Google*

**2. 2. 2. Space Shelter** Un juego desarrollado por Google para Euroconsumers y con apoyo de TechSoup, en el se introduce al jugador en una aventura espacial mientras se cumplen misiones que introducen al jugador a conceptos de seguridad digital, como lo puede ser la autenticación en dos pasos, o la contraseña segura. Al final se entrega un reconocimiento, es un juego intuitivo, limpio, con dinámicas suaves.

**Figura 5** Space shelter


*Fuente. Gamindo – Space Shelter*

**2. 2. 3. Duolingo.** La plataforma mas famosa de aprendizaje en línea cuenta con una estructura gamificada que tiene gran éxito por su forma, desde las medallas al terminar cada lección hasta las notificaciones para volver a la aplicación, otro aspecto llamativo es

las pausas entre lecciones, las mini historias entre nivel y nivel y la competencia que hay por puntos, haciendo que el usuario quiera superar a los otros pasando mas tiempo en la plataforma.

**Figura 6** Logo Duolingo


*Fuente. Duolingo*

### 2.3 Caracterización de usuario

Inicialmente se realizo una indagación meramente académica en la que se concluyó que las personas altamente en línea eran quienes estaban mas vulnerables a ataques de phishing e ingeniería social, dentro de este perfil llamo la atención los usuarios entre 15 y 17 años que aunque pasan gran parte del tiempo en internet, especialmente en redes sociales y videojuegos en línea, aun no se encuentran inmersos en las dinámicas digitales de personas un poco mayores, como lo puede ser el uso de aplicaciones bancarias con montos considerables de dinero o el uso constante de correo electrónico (es importante aclarar que aunque si usan aplicaciones bancarias y correo electrónico no es en la misma media que una persona con un

poco más de responsabilidades), esto es lo que hace a este grupo interesante, pues se les puede educar en la prevención del phishing antes de que se enfrenten a entornos reales donde el riesgo traiga consecuencias reales. Es por eso que la idea de fortalecer habilidades en ciberseguridad de manera temprana ayuda que en el futuro puedan desenvolverse en entornos digitales con mayor criterio.

Durante el ejercicio de acercamiento al usuario el primer grupo focal ya tenía cierto conocimiento previo en ciberseguridad, lo cual hizo que generara cierto rechazo al tema, lo considero “aburrido” o que “ya lo sabía”, esto contrasta con el segundo grupo focal quienes mostraron gran interés en el tema pues, aunque sabían la importancia de la ciberseguridad, afirmaron que carecían de herramientas que los ayudaran a identificar amenazas como el phishing.

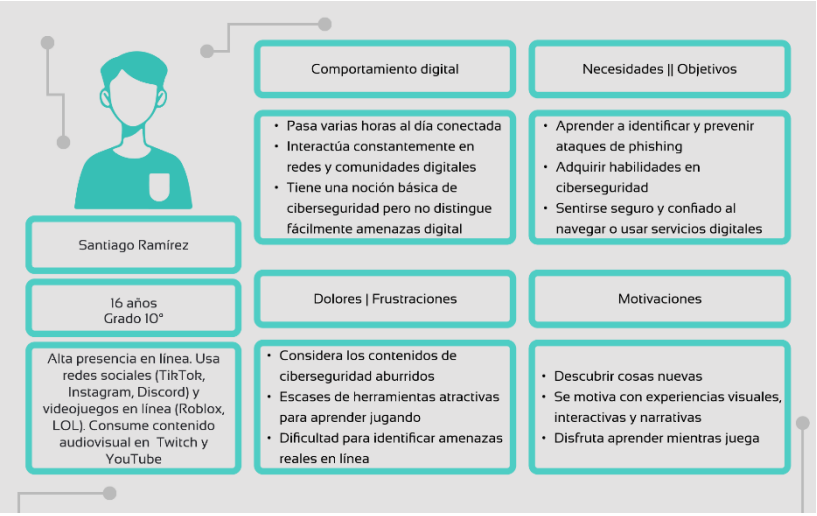
El usuario para este proyecto son estudiantes entre 15 y 17 años que pasen mucho tiempo en línea, además que sean activos en redes sociales, participen de videojuegos en línea y consuman contenido audiovisual en plataformas digitales. Y aunque su vida este mediada por la tecnología su relación con la ciberseguridad sea meramente superficial y básica, también es importante que reconozcan la importancia del tema, pero no tenga las herramientas o los conocimientos necesarios para poder identificar y prevenir amenazas como lo es el phishing.

Este usuario aún no está inmiscuido en las dinámicas de un mundo digital un poco más adulto como por ejemplo el manejo de cuentas o los correos electrónicos de manera constante y masiva,

pero se encuentra pronto asumir estas nuevas estas responsabilidades.

Este usuario busca experiencias de aprendizaje que sean dinámicas y entretenidas dado su interés y su forma de usar la tecnología, además buscan herramientas donde la interactividad y la narrativa funcionen como motivadores ya que las actividades resultan aburridas si son muy teóricas o repetitivas por esa razón las herramientas gamificadas se ajustan a su forma de aprender y sirven para mantener su interés, lo cual propicia adquisición del conocimiento y el fortalecimiento de las habilidades en ciberseguridad que adquieran.

**Figura 7** Caracterización de usuario




*Fuente:* Elaboración propia

# 3. Desarrollo de la metodología, análisis y presentación de resultados

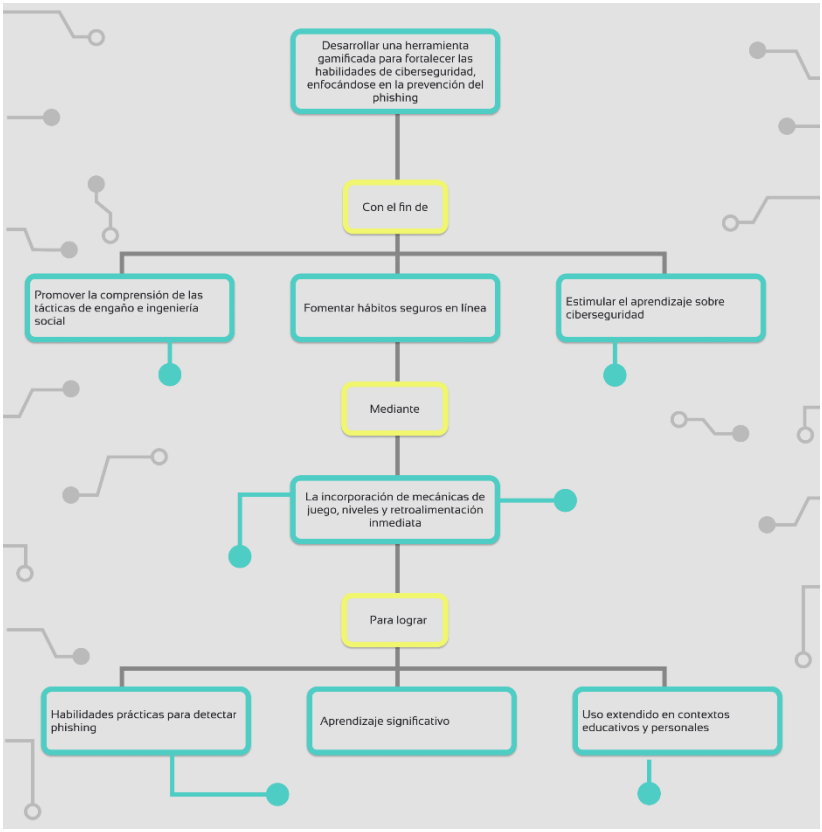
## 3.1 Criterios de diseño

Como se identifico en el apartado anterior el usuario son adolescentes de 15 a 17 años que, aunque sepan la importancia de la ciberseguridad no tengan amplio conocimiento del tema, como caso de estudio se tomo el colegio Gimnasio Santa Rocío de la ciudad de Bogotá con estudiantes de los grados noveno, decimo y once. La propuesta que inicialmente se presento como un videojuego educativo que busca que el usuario pueda fortalecer sus habilidades digitales en ciberseguridad mediante simulaciones y narrativas que hacen que sea llamativo y genere que ellos mismos desarrollen un pensamiento critico frente a las posibles amenazas digitales.

El problema de los ciberataques es algo que va en aumento y es importante que desde que empecemos a tener presencia en línea tengamos conocimientos de los riesgos y de las amenazas existentes, y que tengamos también el criterio para poder actuar en caso de un ataque real.

### *3.1.1 Árbol de objetivos de diseño*

**Figura 8** Árbol de Objetivos de diseño




Nota: Este es el esquema del árbol de objetivos de diseño, como objetivo general se encuentra: Desarrollar una herramienta gamificada para fortalecer las habilidades de ciberseguridad, enfocándose en phishing. *Elaboración propia*

### *3.1.2 Requerimientos y determinantes de diseño*

Con el análisis del usuario y la caracterización definidas, se

identifican las necesidades y los requerimientos necesarios para un videojuego para el fortalecimiento de habilidades en ciberseguridad, además de la comprensión de contenidos y la motivación para interactuar con ellos. Estos requerimientos de diseño que se presentan nacen del problema y de la experiencia de aprendizaje, las posibilidades que ofrece el diseño digital y multimedia y la gamificación en la implementación de conocimiento son valiosas y permiten aplicar el aprendizaje experiencial basado en simulaciones abstraídas de la realidad.

Durante la investigación, en el acercamiento del usuario se pudo identificar algunos puntos ayudaron a la definición de estos requerimientos, como lo fue el desinterés frente a contenidos técnicos o monótonos, dificultad para comprender terminología especializada, la frustración ante los errores y la falta de conexión con lo que estén aprendiendo. Con estos hallazgos se organizaron en requerimientos de modo que cada uno pueda responder a algún aspecto dentro del videojuego.

**Tabla 2 Tabla de requerimientos y determinantes**

| Dimensión del diseño (categoría) | Factor de diseño (condición específica) | Subproblema identificado | Requerimiento de diseño | Parámetro(s) de diseño (valor o rango propuesto) | Criterio de validación |
|---|---|---|---|---|---|
| **Narrativa** | Historia que le sea llamativa al usuario | Falta de conexión con los contenidos más técnicos sobre ciberseguridad | Diseñar una trama gamificada que permita la participación activa en un entorno donde se aborden temas de ciberseguridad como el phishing | Historia dividida en misiones y metas claras | Testeo que muestre cuántos participantes completan la historia |
| **Mecánicas de juego** | Retos, recompensas e interacciones | Baja motivación para aprender términos técnicos y protocolos | Implementar misiones, desbloqueos y medallas virtuales | Simulaciones de ataques, recompensas coherentes a la narrativa y feedback constante | Evaluación de retención de conceptos |
| **Feedback** | Feedback inmediato y contextualizado | Aprendizaje pasivo y sin corrección de errores inmediata, lo que genera miedo a equivocarse | Dar mensajes y pistas en el momento del error o acierto | Mensajes breves y señales que no abrumen al usuario | Observación de la respuesta de los usuarios ante los feedback |
| **Repetición** | Poder volver a iniciar cuantas veces sea necesario sin penalizaciones | Frustración por no poder volver a intentarlo | Permitir que se puedan repetir misiones o niveles sin consecuencias negativas | Botón u opción de reiniciar niveles | Testear cuántas veces repiten un nivel |
| **Usabilidad** | Facilidad de comprensión y navegación | Dificultad para entender las instrucciones o la interfaz | Diseñar una interfaz clara, con iconos intuitivos y lenguaje cercano al público adolescente | Instrucciones visuales, íconos reconocibles y lenguaje informal pero claro | Pruebas de usabilidad con usuarios reales |
| **Motivación y engagement** | Conexión emocional con la experiencia de juego | Desinterés o desmotivación frente a contenidos educativos | Incluir recompensas emocionales (mensajes positivos, insignias personalizadas) que refuercen la autoestima y la curiosidad | Retroalimentación positiva y personalizada | Evaluación de tiempo promedio de uso y retorno voluntario a la app |
| **Identidad visual** | Estética y estilo visual afín al público | Desconexión entre la apariencia del entorno digital y los gustos de los adolescentes | Desarrollar un sistema visual coherente, con colores, tipografía y personajes que representen el universo digital juvenil | Paleta cromática vibrante, personajes tipo avatar o ilustrados | Test de preferencia visual con usuarios |
| **Cognitiva (educativa)** | Nivel de complejidad de los contenidos | Exceso de tecnicismos o lenguaje muy formal | Adaptar el lenguaje y la progresión del contenido al nivel cognitivo y vocabulario de adolescentes de 15–17 años | Frases cortas, ejemplos visuales, glosario de términos | Evaluación de comprensión del contenido en pruebas piloto |

Nota: en esta tabla se encuentran los requerimientos y determinantes del videojuego bajo los factores: narrativos, mecánicas de juego y funcionamiento. *Elaboración propia*

### 3.2 Hipótesis de producto

Durante del proceso de diseño y validación, se formularon varias hipótesis con el uso de la gamificación y los elementos interactivos para el aprendizaje sobre ciberseguridad y particularmente el phishing, cada una de ellas permitió orientar el prototipo y definir varias ventajas y limitaciones con los componentes del videojuego.
La primera hipótesis establece que si se utiliza la gamificación con una narrativa interactiva, los usuarios mostrarán mayor interés en aprender sobre ciberseguridad, lo malo es que existía el riesgo de que el usuario centrará su intención en la jugabilidad más que en los conceptos.

La segunda hipótesis plantea que sí se dan recompensas, se incrementar la retención de los conocimientos sobre phishing, el prototipo responde la idea de una plataforma gamificada con sistema de puntos insignias y simulaciones de ataques, además de usar esfuerzo y la persistencia para percibir el progreso, la desventaja identificada puede ser que sí no son muy visibles el usuario pierde el interés.

Una tercera hipótesis sugiere que tener feedback inmediato, así que el usuario quiere aprender de manera autónoma y le pierda

miedo a equivocarse para eso se puede implementar elementos visuales y sonoros que respondan a ciertos elementos, lo que podría ser negativo para que se distraiga del mensaje si no está bien estructurado

Cuarta hipótesis, si el lenguaje y el nivel se adaptan al perfil cognitivo del usuario, se mejora la comprensión del contenido. Lo malo es que se puede caer en la ultra simplificación de los conceptos y cuesta equilibrar lo lúdico de lo que verdaderamente es lo importante que es la adquisición del conocimiento

Por último, quinta hipótesis, si se desarrolla una identidad visual coherente se aumenta en impacto, el proyecto no obstante se reconoce que si no es algo con lo que los usuarios puedan conectar no ha resultar llamativo para el público objetivo

**Tabla 3** Matriz de hipótesis de producto

| Hipótesis | Prototipo | Ventajas (+) | Desventajas (–) |
|---|---|---|---|
| Si se utiliza la gamificación con narrativa interactiva, los adolescentes mostrarán mayor interés en aprender sobre ciberseguridad | Prototipo de videojuego narrativo sobre casos de phishing y seguridad digital | • Incrementa la motivación y la participación<br>• Favorece el aprendizaje activo<br>• Facilita la conexión emocional con el contenido | • Riesgo de que el usuario se enfoque más en el juego que en los conceptos<br>• Puede requerir altos recursos de diseño y tiempo |
| Si se integran recompensas, logros y simulaciones, se incrementará la retención de conocimientos sobre prevención de phishing | Plataforma gamificada con sistema de puntos, insignias y simulaciones de ataques | • Refuerza la persistencia y la práctica constante<br>• Permite medir progreso fácilmente | • Posible pérdida de interés si las recompensas no son significativas |
| Si se emplea feedback inmediato y contextualizado, los adolescentes aprenderán de manera más autónoma y sin miedo al error | Sistema de retroalimentación visual y sonora que responde a aciertos o errores en tiempo real | • Promueve la autorregulación<br>• Reduce la frustración<br>• Facilita la comprensión de conceptos difíciles | • Puede distraer si los mensajes no están estrategicamente puestos<br>• Exige un diseño iterativo de pruebas y varias pruebas con usuario |
| Si se adapta el lenguaje y el nivel de complejidad al perfil cognitivo del usuario, se mejorará la comprensión del contenido | Interfaz educativa con lenguaje juvenil, ejemplos visuales y glosario interactivo | • Incrementa la accesibilidad cognitiva<br>• Favorece la inclusión de usuarios con distintos niveles de conocimiento<br>• Mejora la percepción del contenido educativo | • Riesgo de simplificación excesiva<br>• Dificultad para equilibrar lo lúdico con lo académico sin que se difumine ninguno de los dos |
| Si se desarrolla una identidad visual coherente, aumentará el sentido de pertenencia y el impacto | Diseño visual con estética que vaya en concordancia con el perfil de los usuarios | • Genera reconocimiento<br>• Potencia la recordación de lo aprendido en el videojuego | • Puede volverse obsoleta con tendencias visuales cambiantes<br>• Riesgo de no se llamativo a parte del público objetivo |

Nota: En esta tabla se desarrolla las diferentes hipótesis alrededor del

producto. *Fuente:* Elaboración propia

### 3.3 Etapa Descubrir

Para comenzar, se busca entender el tema atendiendo a la documentación, conferencias, guías, los informes que hay en la web, además de contar con el apoyo en la parte teórica de Uqbar , con ello se busca entender primero cómo está el panorama de la ciberseguridad, sí es un tema qué merezca la pena ser abordado, qué consideraciones tiene este tema y cómo afecta a las personas de manera particular y de manera más global. Con esto se pudo determinar el phishing es la forma de ataque más efectivo y qué menos barreras técnicas debe enfrentar, ya que afecta directamente a la confianza del usuario, es por eso que el tema de ciberseguridad es tan relevante, todos estamos en el entorno digital y el phishing es tan importante, todos estamos vulnerables ante esta amenaza.

#### 3.3.4 Etapa Definir

Con una base académica se hizo el perfil de varios posibles usuarios y el más llamativo fueron los adolescentes de 15 17 años ya que muchos aún no estaban inmersos en dinámicas en las que estos riesgos puedan traducirse en consecuencias reales y graves. Se hizo un acercamiento a un grupo focal con estudiantes entre estas edades con un nivel medio de ciberseguridad y posteriormente se hizo otro grupo focal con estudiantes del mismo rango de edad con conocimientos bajos o básicos quiénes fueron los que mostraron

mayor interés en el proyecto y especialmente en la temática, pues ellos mismos reconocieron que aunque saben de la importancia de la ciberseguridad, no tienen las herramientas para hacerle frente a amenazas, esto, de hecho, estaba en concordancia con algunos estudios que afirman cosas similares.

La información tanto académica junto con el acercamiento al usuario marca una ruta en el proseguir del proyecto, donde hay metas mas claras, objetivos más concretos y necesidades más definidas.

### 3.3.5 Etapa Desarrollo

Con base en las investigaciones de las anteriores fases, se generaron ideas orientadas del diseño de una herramienta digital gamificada, un videojuego, que fortalezca habilidades en ciberseguridad y en prevención del phishing En la propuesta inicial el jugador debía moverse por un escenario en el que va a explorar diferentes partes de este y debía estar alerta a las a las posibles amenazas de phishing y de ingeniería social.

En este ciclo se realizaron testeos para evaluar narrativa y la mecánica de estructura general del juego. El primero de estos testeos fue realizado en papel con el público objetivo, se determinaron aciertos y áreas de mejora. Y el segundo testeo, fue con un grupo de estudiantes de pertenecientes a Uqbar quienes aportaron observaciones técnicas sobre en el desarrollo de la temática y algunas cosas y con respecto al desarrollo del juego

Los resultados de estos testeos se enfocan en buscar en

hacer que el usuario disfrute esta herramienta, aprenda y fortalezca las habilidades en ciberseguridad

## 3.6 Desarrollo y análisis Etapa Evaluación

En esta última etapa se busca comprobar y determinar que la propuesta que se desarrolló cumple con los objetivos definidos y satisface las necesidades de los usuarios. El proceso de evaluación debe ser con el usuario objetivo en búsqueda de las últimas retroalimentaciones, teniendo en cuenta que con anterioridad ya se les pidió lo mismo. A su vez de manera paralela se busca una opinión de los expertos de Uqbar con respecto a la viabilidad técnica y la solidez del de desarrollo y por último la implementación simulada de ciberataques de phishing.

Estos resultados permitan una última ronda de ajustes para asegurar que si se cumpla con los requisitos que se han planteado a lo largo del desarrollo de este proyecto.

## 3.7 Resultados de los testeos

### *3.7.1 Primer testeo*

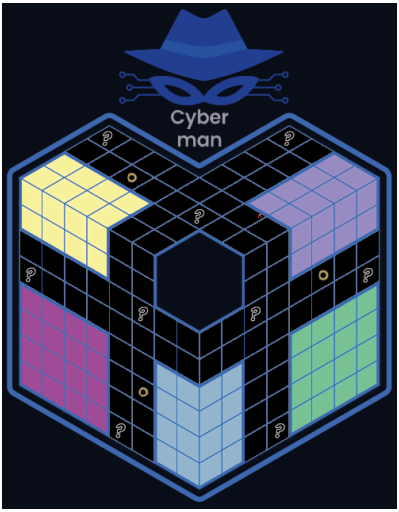
**3.7.1.1 Evidencias (Prototipo, testeo y proceso de iteración).** El primer testo se realizo en el colegio Gimnasio Santa Rocío en la ciudad de Bogotá, el objetivo de este testeo era evaluar el primer prototipo del juego, un prototipo en papel que contaba de un escenario, de cartas con los ataques de phishing, cartas de narrativa

y cartas de taque global, un sistema de puntos basado en el concepto de credenciales. Para esta sesión de testeo se seleccionaron 6 participantes con edades comprendidas entre 15 y 17 años que es el rango de edad del usuario objetivo.

Antes de iniciar si realiza una bebé conversación entrevista no estructurada en la que afirmaron que sabían la importancia de la ciberseguridad pero que no tenían y los conocimientos algunos dijeron que no se los habían impartido en el colegio y otros que probablemente sí se los hayan enseñado pero que no lo recordaba. Algo en lo que todos estuvieron de acuerdo, fue que su entendimiento en su seguridad se basaba en la lógica, no abrir enlaces sospechosos o tener contraseñas medianamente seguras, esto permitió confirmar la pertinencia del tema de ciberseguridad y prevención del phishing desde un enfoque gamificado basado en el aprendizaje experiencial mediante entornos simulados y abstraídos.

En el prototipo, el jugador podía moverse por todo el tablero de manera libre y en algunas casillas estaban marcadas distintos tipos de eventos narrativa ataques o el ataque phishing. La dinámica general consistía en avanzar por el tablero, acumulando o perdiendo credenciales.

**Figura 9** Tablero prototipo




*Fuente:* Elaboración propia

Los jugadores perdían cuando perdían todas las credenciales y ganaban cuando pasaban por los 5 espacios donde había ataques phishing. En las casillas de narrativa se centraba en la figura antagónica denominada "Cyberman" que era quien había puesto los ataques phishing a lo largo del tablero.

**3.7.1.2 Evidencias (Percepción del usuario).** Durante la partida y posterior a ella, los participantes manifestaron que el sistema de credenciales es atractivo y motivador, aparte que entendieron qué credenciales hacen son su identidad en internet y que pierden cuando se pierden ese tipo de credenciales. También les resultó interesante identificar con ejemplos concretos los ataques phishing, sin embargo, a lo largo de la sesión de testeo surgieron cosas que son áreas de

mejora, como, por ejemplo, el tablero, resultó confuso y demasiado abierto sin orden específico y carecía de sentido de avance, además, las mecánicas relacionadas al tablero se sentían complejas y enredadas, lo cual hizo que olvidaran parte de las reglas. Otro aspecto que salió dentro de la ronda de retroalimentación fue la extensión de las partidas, esto derivado al mal tablero, generaba que las partidas fueran largas y los jugadores perdieran interés. También propusieron incluir un glosario con términos técnicos relacionados a la ciberseguridad.

Esta sesión de prueba con usuario permitió conocer la disposición y el interés del usuario, además dejo lecciones valiosísimas que deben ser implementadas para mejorar la experiencia del usuario.

**Figura 10** Testeo 1

*Fuente:* Fotografía propia

### *3.7.2 Segundo testeo*

**3.7.2.1 Evidencias (Prototipo, testeo y proceso de iteración).** El segundo testeo se realizó de la mano del grupo estudiantil de la Universidad Nacional, Uqbar que se enfoca en el estudio y el fomento de la seguridad digital. El propósito de este testeo era obtener una. evaluación en la técnica del prototipo ya llevado a un espacio virtual, se presentó una versión de prototipo presentado en el anterior testeo con algunas mejoras llevado a un entorno virtual en 3D en la plataforma unity, este mantenía la estructura narrativa, el sistema

La retroalimentación se basó principalmente en la optimización del entorno 3D, lo cual para ellos no es una elección técnicamente eficiente, esto por la alta demanda de recursos para que se procesen de manera correcta los elementos, además de la mano con eso necesitaba reforzar el código hacerlo mucho más sólido, también recomendaron hacer las simulaciones de phishing más realistas, sugirieron que representarán situaciones un poco más cercanas a lo que es la realidad del usuario.

**Figura 11** Testeo 2

*Fuente:* Fotografía propia

**3.7.2.2 Evidencias (Percepción del usuario).** En general la percepción fue positiva destacando el enfoque educativo y la

intención qué hay de sensibilizar a este grupo de público joven sobre las amenazas del phishing y la ciberseguridad, y reconocieron que el concepto de las credenciales como recompensas y motivadores del juego funciona en términos pedagógicos, sin embargo, fueron enfáticos en que la estructura fuera clara, y que debe evitar complejidades innecesarias, en ese sentido recomendaron mejorar la estructura de los eventos de seguridad para que el jugador tenga un impacto más directo y evidente.

La sesión de testeo con Uqbar fue importante para orientar el proyecto a una solución más funcional, más realista y técnicamente sostenible, sin comprometer la experiencia del usuario .

## 3.8 Prestaciones del producto

El producto desarrollado, denominado “Cyberman en la red”, es un videojuego que se busca fortalecer las habilidades en ciberseguridad, particularmente que el usuario caiga en estafas de ingeniería social y phishing. La idea es que reconozcan los riesgos y actúen con criterio frente a las ciber amenazas y desarrollen habilidades útiles en entornos digitales.

### *3.8.1 Aspectos morfológicos*

El juego desarrolla una vista 2D top-down para facilitar la comprensión espacial del usuario y así pueda reconocer el mapa y moverse de manera más intuitiva. Este tipo de desarrollo permite optimizar la jugabilidad en distintos dispositivos porque no requiere tantos recursos técnicos como lo pudieran necesitar otro tipo de

estructuras visuales.

Los escenarios están conectados como cuartos que representan diferentes sitios del ciberespacio o hacen una referencia a ellos. Esto, además de una narrativa que se va construyendo poco a poco, genera un entorno llamativo, el cual genera interés en seguir conociendo.

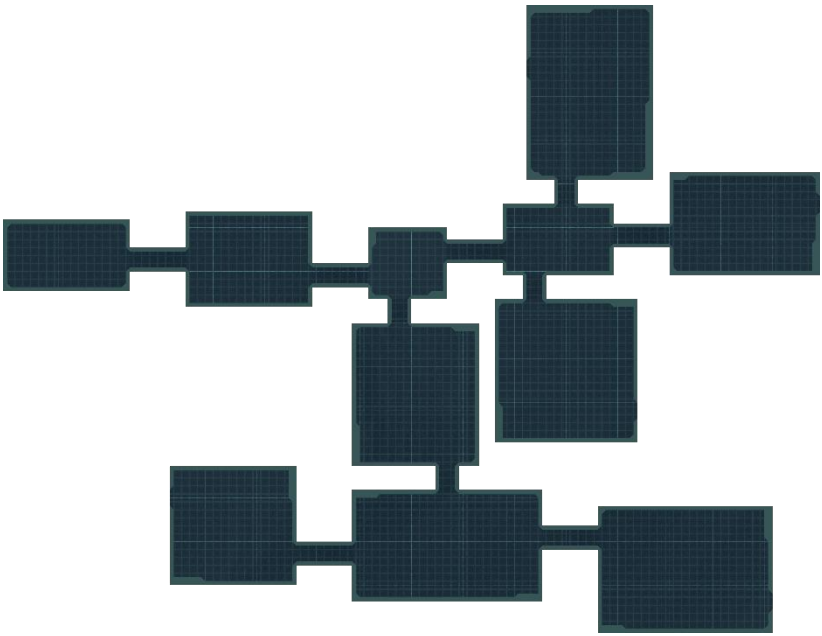
La historia sigue a un protagonista que viaja por la web, que es el mapa del juego, y tiene que enfrentarse a diferentes ataques que pone Cyberman alrededor del mismo, él es antagonista del juego, que simboliza las amenazas digitales y los hackers y quienes quieren aprovechar de las credenciales, es decir, de la información de las personas. A medida que el jugador avanza, descubre fragmentos de la trama y la historia de Cyberman, sus motivaciones y su objetivo final, que es filtrar la mayor cantidad de credenciales posible.

### *3.8.2 Aspectos técnico-funcionales*

Actualmente el juego está siendo desarrollado en Unity2D, con una arquitectura modular que facilita la incorporación de nuevos niveles o temáticas para futuros tópicos que se quieran abordar acerca de ciberseguridad, es decir, que permite las expansiones.

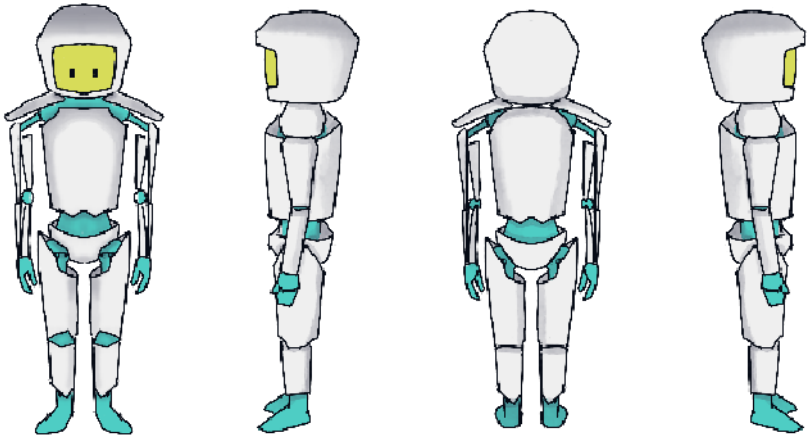
El mapa en general del juego está conformado por cuartos interconectados donde el personaje se mueve libremente y llega a 5 minijuegos donde se abordan diferentes formas de ciberataques relacionados a la ingeniería social y phishing.

**Figura 12** Mapa del juego



Fuente: Elaboración propia

**Figura 13** Avatar



Fuente: ilustración propia

Cada jugador inicia con 5 credenciales que simbolizan su identidad digital y funcionan como vidas. El sistema base se rige por decisiones del jugador frente a eventos interactivos: Si abre un elemento que es un ataque, pierde credenciales. Si identifica correctamente un elemento legítimo, gana credenciales. Si ignora o rechaza la interacción, mantiene su puntaje igual.

Los minijuegos abordan aspectos como las páginas falsas donde el jugador debe elegir el enlace real dentro de las opciones; correos electrónicos que pueden ser reales o falsos o la identificación de perfiles reales o falsos, si el minijuego se termina de completa de manera positiva se le dará al jugador herramientas de protección digital, al completar estas herramientas, el jugador pasa a tener una batalla con el enemigo mayor, Cyberman y si el jugador le gana, ha ganado el juego. El jugador pierde si este se queda sin credenciales, estas se pierden en los minijuegos que están en el mapa, o en ataques aleatorios que aparecen en medio del juego.

El juego está pensado para que se pueda ejecutar en diferentes computadores y se busca que en futuro se pueda incorporar algún espacio para el seguimiento de docentes, padres o tutores.

### *3.8.3 Aspectos de usabilidad*

El diseño del videojuego se fundamenta con la heurística de Nielsen, que prioriza la claridad, la coherencia y la retroalimentación inmediata. La vista top-down 2D ayuda a que el jugador esté orientado, cosa que simplifica la navegación, sin que se pierda la curiosidad innata ni la sensación de exploración.

Con los testeos se pudieron pulir las dinámicas y la distribución de los recorridos y la estructuración del mapa. También se hizo hincapié en la incorporación de ayudas visuales y de hacer un entorno mucho más inmersivo con ayuda de estímulos sonoros.

En el feedback se priorizó que las decisiones erróneas no sean penalizadas fuertemente penalizadas, sino que por el contrario se conviertan en oportunidades de aprendizaje. Este aprendizaje también va de la mano de las recompensas que es el acumulo de las credenciales y el desbloqueo de las herramientas, además de mensajes de logro que estimula y propicia la curiosidad del jugador y el esfuerzo que pueda poner en el juego.

El videojuego debe agrupar factores y elementos que lo hagan visualmente atractivo, técnicamente viable y enfocado en las necesidades y requerimientos del usuario.

# 4. Conclusiones

## 4.1 Conclusiones

El proyecto “cyberman en la red” representa y da como un resultado todo un proceso de investigación creación en la que se articuló el análisis del usuario mediante identificación de características requerimientos y la materialización de un producto digital como lo es en este caso el videojuego. Para responder a una problemática que es la ciberseguridad, especialmente los ataques de ingeniería social y el phishing. Tras la identificación del problema y usuario, los adolescentes entre 15 y 17 años que son usuarios del entorno digital carecen de herramientas y habilidades prácticas para reconocer amenazas cibernéticas y cómo responder ante ellas. Con esto se propuso diseñar una experiencia que fuera atractiva interesante y sobre todo relevante.

El proceso permitió entender que la educación en ciberseguridad tiene que ser más allá de solo lo técnico y se tiene que dejar a un lado el miedo al riesgo sí se quiere tener una conexión con el usuario. Según Kolb, el aprendizaje es más efectivo cuando se vive de manera experiencial, en ese sentido y basándonos en la teoría de Kapp, el videojuego se convierte en un espacio seguro para explorar las consecuencias de decisiones digitales sin enfrentarse un daño real, es decir, jugar se transforma en la manera de aprender.

Lo importante era un transformar un tema complejo, como es la ciberseguridad en una narrativa sencilla y llamativa, se buscaba que el usuario comprendiera el impacto su identidad digital, esto, más allá de lo técnico, además, el objetivo principal que era fortalecer habilidades de ciberseguridad permite reflexionar sobre la confianza y responsabilidad en los entornos digitales.

Desde el diseño digital y multimedia, el proyecto reafirmo la importancia de la información, el usuario y al diseñador como puente entre ambos. Transformar una información técnica en algunos casos un poco densa y convertirla en una experiencia lúdica comprensible es un ejercicio donde el diseño más allá de comunicar, tiene un propósito que es educar y transformar, para allá de la repercusión inmediata el proyecto deja una enseñanza importante, la ciberseguridad no es sólo una cuestión técnica sino también humana.

### 4.2 Estrategia de mercado

Para este proyecto, el enfoque de viabilidad se analiza desde la lógica del mínimo producto viable (MVP) para el producto gamificado “Cyberman en la red”, que concentra las funcionalidades esenciales para cumplir con su propósito, que se basa en la enseñanza de ciberseguridad y, particularmente, el phishing a adolescentes de 15 a 17 años, con interés en el ciberespacio, pero sin el conocimiento real de las amenazas en los distintos entornos digitales.

El producto mínimo vital se debe hacer con una perspectiva realista; es por ello que se usan ciertas herramientas para este

propósito, además de jerarquizar y priorizar aspectos y decisiones importantes para el desarrollo de este. La matriz de construcción del mvp y el triángulo ágil establecen esta guía, que prioriza los elementos y que define los márgenes de negociación del proyecto. Con ellas, la viabilidad se ve como la garantía que hay para la presentación de un producto útil, pertinente y con objetivos claros, dentro del tiempo y recursos establecidos.

### *4.2.1 Segmentos de cliente*

Aunque el tema de ciberseguridad nos atraviesa a todos quienes estamos constantemente en línea, para este proyecto hay una serie de actores y usuarios que representan el segmento de cliente; esto incluye tanto al usuario final como a quien le ve el valor pedagógico del proyecto.

Los adolescentes de 15 a 17 años, con interés en la ciberseguridad, sin mucho conocimiento de las formas de ciberataque ni de formas de protegerse, se catalogan como usuario final, quien comprobará la jugabilidad y la narrativa, además del aprendizaje en Phishing. Los docentes y padres funcionan como tutores y son quienes confirman la pertinencia del producto desde el exterior; además, son quienes invierten en él como personas con poder adquisitivo.

### *4.2.2 Propuesta de valor*

Cada propuesta debe tener un valor diferenciador, y es por ello que la propuesta de valor cobra tal relevancia. Para este proyecto, es

importante brindar una experiencia gamificada en la que se puede aplicar el aprendizaje experiencial. Si bien es cierto que existen juegos de ciberseguridad que ya existen en el mercado, el factor diferenciador se basa en combinar narrativa lo suficientemente profunda para sostener una experiencia lúdica con enfoque gamificado experiencial, que hace que los jugadores comprendan el riesgo del phishing y la importancia de la ciberseguridad en contextos simulados, abstraídos de entornos reales.

### *4.2.3 Canales*

La relación con los clientes siempre es fundamental porque define la interacción de los usuarios y se vincula con la experiencia de ellos. En este proyecto, la relación se constituye a través del feedback visual que el jugador opera como respuestas inmediatas a sus propias decisiones dentro del juego. Esto, dentro del entorno de aprendizaje experiencial, es muy importante, ya que el usuario determina mediante sus acciones qué es lo correcto y qué no. Además, eso va de la mano con el uso autónomo, que le da la autonomía de explorar y aprender al tiempo que se equivoca o acierta.

### *4.2.4 Relaciones con los clientes*

La relación con los clientes siempre es fundamental porque define la interacción de los usuarios y se vincula con la experiencia de ellos. En este proyecto, la relación se constituye a través del feedback visual que el jugador opera como respuestas inmediatas a sus propias decisiones dentro del juego. Esto, dentro del entorno de aprendizaje

experiencial, es muy importante, ya que el usuario determina mediante sus acciones qué es lo correcto y qué no. Además, eso va de la mano con el uso autónomo, que le da la autonomía de explorar y aprender al tiempo que se equivoca o acierta.

### *4.2.5 Fuentes de ingresos*

Uno de los elementos más importantes dentro de la viabilidad del proyecto son las fuentes de ingreso. Es por ello que, en primer lugar, está el capital inicial, que se constituye a base de recursos propios y préstamos adquiridos, los cuales son la base financiera inicial para el desarrollo del MVP. Posteriormente, se añaden los ingresos operativos, que incluirían ventas dentro del juego, incorporación de publicidad y la posibilidad de contenido adicional o expansiones, que garantiza el desarrollo a mediano o largo plazo. También existen oportunidades de financiación externa, como la convocatoria Crea Digital, con aporte significativo, aunque su acceso es más complejo; por ende, no hay que contar con ello de primera, por su alta competitividad entre los postulados. Es importante tener ingresos diversificados para el desarrollo de este proyecto.

## 4.3 Consideraciones

El desarrollo de Cyberman en la red permitió reconocer la importancia del diseño más allá de lo visual y lo funcional meramente, el diseño puede verse como transformador o como elemento que incentive la reflexión en este caso, el entorno digital. El videojuego busca responder la necesidad concreta de educación en

ciberseguridad, fomentar la conciencia la curiosidad y la reflexión sobre la red.

Además del proceso de investigación creación, en lo personal, me mostró el valor del error y la iteración, cada comentario retroalimentación, cada ajuste fueron partes importantes para analizar cómo los usuarios percibían el entorno, el producto, cuestión fundamental para un proyecto relevante.

Finalmente, el diseño digital y multimedia tiene un rol muy importante en la educación tiempos más actuales. El modo como se generan estas relaciones, el modo como las personas se conectan con la información también es muy importante, este proyecto queda como invitación a seguir explorando, inspirando y tal vez protegiendo los entornos virtuales.

## Referencias

Borghello, C. (2009). El arma infalible: la Ingeniería Social. *Eset Latinoamérica*.

Comisión de regulación de comunicaciones. (23 de Diciembre de 2009). RESOLUCION 2258 DE 2009. Bogotá.

Comisión de Regulación de Comunicaciones. (18 de Mayo de 2021). *En 2020 conexiones de Internet móvil en Colombia llegaron a 32,5 millones*. Comisión de Regulación de Comunicaciones: https://crcom.gov.co/es/noticias/comunicado-prensa/en-2020-conexiones-internet-movil-en-colombia-llegaron-325-millones

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review, 4*, 13-21. https://doi.org/10.22215/timreview/835

Cyberpeace Tech. (19 de Febrero de 2025). *Ciberataques en 2024: crecimiento alarmante del 14%*. Cyberpeace: https://www.cyberpeace.tech/post/ciberataques-en-2024-crecimiento-alarmante-del-14

Departamento Administrativo Nacional de Estadística [DANE]. (2023). *Indicadores básicos de TIC en Hogares*. DANE: https://www.dane.gov.co/index.php/estadisticas-por-tema/tecnologia-e-innovacion/tecnologias-de-la-informacion-y-las-comunicaciones-tic/indicadores-basicos-de-tic-en-hogares

Design Council. (s.f.). *Framework for Innovation*. Design Council: https://www.designcouncil.org.uk/our-resources/framework-for-innovation/

Deterding, S., Khaled, R., Nacke, L., & Dixon, D. (2011). *Gamification: Toward a definition*. https://www.researchgate.net/publication/273947177_Gamifi

cation_Toward_a_definition/citations

Durán Becerra, T., Ortiz Rubio, J., Villada, J. D., Castañeda, J. G., Méndez, A. F., Hernández Vásquez, L. J., . . . González Gil, N. (2024). *Jóvenes en línea.* Civix Colombia: https://civixcolombia.org/jovenesenlinea/

FBI. (2 de Noviembre de 2018). *The Morris Worm*. FBI: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

Fortinet. (s.f.). *¿Qué es un ciberataque?* Fortinet: https://www.fortinet.com/lat/resources/cyberglossary/what-is-cyber-attack

Hernández, P. (Febrero de 2024). El juego de guerra como instrumento fundamental para la educación militar profesional y el entrenamiento de líderes. *Military review*. https://www.armyupress.army.mil/Journals/Edicion-Hispanoamericana/Archivo-de-articulos-exclusivos-en-linea/Hispanoamericana-On-line-2024/Hern%C3%A1ndez-SPA-Feb-2024/#:~:text=Para%20obtener%20los%20beneficios%20educativos,antes%20de%20comenzar%20el%20juego

IBM Corporation. (2024). *X-Force Threat Intelligence Index 2024.* IBM Corporation.

IBM Corporation. (2025). *¿Qué es un ciberataque?* IBM: https://www.ibm.com/es-es/topics/cyber-attack

IBM Corporation. (2025). *IBM X-Force 2025 Threat Intelligence Index .* IBM Corporation.

Interaction Design Foundation - IxDF. (05 de Junio de 2016). *What is User Centered Design (UCD)?* Interaction Design Foundation - IxDF: https://www.interaction-design.org/literature/topics/user-centered-design

Interaction Design Foundation. (s.f.). *Interaction Design (IxD)*. Interaction Design Foundation: https://www.interaction-design.org/literature/topics/interaction-design?srsltid=AfmBOoqpfL0G39UAE0yqfMzu4jZKfG6ogAwCCgMgbrk0j-uqZN3ik2Wf#what_is_interaction_design_(ixd)?-0

Kapp, K. M. (2012). *The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education.* Pfeiffer.

Kaspersky. (s.f.). *¿Qué es la ciberseguridad?* Kaspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security?srsltid=AfmBOorB9rjwgZePCl2ZS_8ZeTAlP3z-gOdNQds7dcavX5tEbYpRBHa8

Keepnet. (25 de Enero de 2024). *History of Cybersecurity: An Overview From Past to Day - Keepnet*. Keepnet Labs: https://keepnetlabs.com/blog/cybersecurity-breaches-lessons-from-history

Kemp, S. (3 de Marzo de 2025). *Digital 2025: Colombia*. Datareportal: https://datareportal.com/reports/digital-2025-colombia

Kosinski, M. (17 de Mayo de 2024). *¿Qué es el phishing?* IBM: https://www.ibm.com/es-es/topics/phishing

Koyun, A., & Al Janabi, E. (2017). Social Engineering Attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST), 4*(6), 7533-7538. https://doi.org/https://www.jmest.org/wp-content/uploads/JMESTN42352270.pdf

Lindemulder, G., & Kosinski, M. (12 de Agosto de 2024). *¿Qué es la ciberseguridad?* IBM: https://www.ibm.com/es-es/topics/cybersecurity

Lindemulder, G., & Kosinski, M. (12 de Agosto de 2024). *¿Qué es la ciberseguridad?* IBM: https://www.ibm.com/es-es/topics/cybersecurity

Michalowski, M. (8 de Julio de 2025). *Top 54 Phishing Attack Statistics & Latest Trends for 2025*. Spacelift: https://spacelift.io/blog/phishing-statistics

Ministerio de Tecnologías de la Información y Comunicaciones de Colombia [MinTIC]. (2023). *Estrategia nacional digital de Colombia 2023-2026.* Ministerio de Tecnologías de la Información y Comunicaciones de Colombia [MinTIC].

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTic]. (s.f.). *Ciberseguridad*. Ministerio de Tecnologías de la Información y las Comunicaciones: https://mintic.gov.co/portal/inicio/18723:Ciberseguridad

Nason, A. (25 de Abril de 2024). *A History Of Cybersecurity And Cyber Threats*. Coro.net: https://www.coro.net/blog/history-of-cybersecurity-and-cyber-threats

National Cyber Security Centre. (12 de Febrero de 2024). *Understanding vulnerabilities - NCSC.GOV.UK*. National Cyber Security Centre: https://www.ncsc.gov.uk/collection/vulnerability-management/understanding-vulnerabilities

National Institute of Standards and Technology [NIST]. (s.f.). *phishing*. National Institute of Standards and Technology U.S. Department of Commerce: https://csrc.nist.gov/glossary/term/phishing?utm_source=chatgpt.com#

Nielsen, J. (24 de Abril de 1994). *10 Usability Heuristics for User Interface Design*. Nielsen Norman Group: https://www.nngroup.com/articles/ten-usability-heuristics/

Proofpoint. (s.f.). *What Is a Cyber-Attack? - Definition, Statistics & More*. Proofpoint: https://www.proofpoint.com/us/threat-reference/cyber-attack

Real Academia Española [RAE]. (s.f.). *ciberespacio*. Real Academia Española [RAE]: https://www.rae.es/diccionario-estudiante/ciberespacio

Red PaPaz. (23 de Noviembre de 2021). *Riesgos en línea - Blog RedPapaz*. Red Papaz: https://www.redpapaz.org/blog/riesgos-en-linea/147/

Regalado, P. (24 de Octubre de 2024). *Cybersecurity Threats: What They Are & How They Work Today*. Splunk: https://www.splunk.com/en_us/blog/learn/cybersecurity-threats.html

Ricardo, R. (7 de Abril de 2024). *Historia de la Ciberseguridad, definición y cronología*. Estudyando: https://estudyando.com/historia-de-la-ciberseguridad-definicion-y-cronologia/

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet, 11*(89). https://doi.org/doi:10.3390/fi11040089

Santana-Soriano, E., & Báez Vizcaíno, K. (2022). Ciberespacio y cibermundo: delimitaciones conceptuales desde el materialismo sistémico. *Ciencia Y Sociedad, 47*, 45-57. https://doi.org/https://doi.org/10.22206/cys.2022.v47i1.pp45-57

Statista. (12 de Septiembre de 2024). *¿Cuántas horas al día pasamos conectados a internet?* Statista: https://es.statista.com/grafico/22701/tiempo-medio-de-uso-diario-de-internet/

StudySmarter. (s.f.). *Diseño Interactivo*. StudySmarter:

https://www.studysmarter.es/resumenes/estudios-de-arquitectura/arquitectura-parametrica/diseno-interactivo/

Traynor, O. (20 de Febrero de 2025). *AI-Powered Phishing is on the Rise [What to Do?]*. CyberAngel: https://cybelangel.com/rise-ai-phishing/

Waltz, B. (2024). Phishing Emails: An Evolving Cyberattack. *Cybersecurity Undergraduate Research Showcase, 2*, 14. https://doi.org/10.25776/scrt-kp76

We Are Social; Meltwater. (2025). *Digital 2025: Global Overview Report.* https://datareportal.com/reports/digital-2025-global-overview-report

## Anexos

**Anexo A.** Portafolio

https://www.behance.net/gallery/228520971/Portafolio-by-Valeria-2025

**Anexo B.** Entrevista Uqbar

https://drive.google.com/file/d/1yIOGUrHnDonFxiJeUKQpIGfHctH60Qbg/view?usp=drive_link

**Anexo C** Árbol de problemas

https://www.figma.com/design/qwl4QJicQHue14cwl0NPDO/%C3%81rbol-de-problemas?node-id=1-2&t=m9RrC7dHj1uYhwpO-1

**Anexo D** Mapa de Objetivos

https://www.figma.com/design/tKae399Vt1yQuw44rdGwnA/Mapa-de-Objetivos?node-id=0-1&t=L0Y3rW4myL3qJhOt-1

**Anexo E** Tabla de inversiones

https://docs.google.com/spreadsheets/d/1R7rYxrIMcgNkc5L6kRlrCiPq6eC46qb7yL6hQdH-fo0/edit?usp=sharing