



Empoderando a la Nueva Generación: Diseño de Software para Fomentar la Seguridad

Informática en Niños y Adolescentes de Bogotá

Elaborado por:

Julián Enrique Alfonso León

William Andrés Parada Antonio

Jairo Andrés Castiblanco Briceño

Universidad EAN

Facultad de Ingeniería

Proyecto de Grado de Pregrado

Bogotá, 2025



Tabla de contenido

Introducción	5
Objetivos	6
Objetivo general	6
Objetivos específicos	6
Problema de Investigación	6
Justificación	8
Marco Teórico	10
Exposición Digital y Riesgos en Niños y Adolescentes	11
Importancia de la ciberseguridad en los niños	11
Contexto legal en Colombia	12
Inteligencia Artificial y Ciberseguridad: Oportunidades y Amenazas	13
Educación Digital y Enfoques Pedagógicos	14
El diseño de un software	15
Análisis de Requerimientos	16
Análisis de Restricciones	17
Restricciones Políticas	17
Restricciones Económicas	18
Restricciones Sociales	19
Restricciones Tecnológicas	20
Restricciones Ecológicas	21
Restricciones Legales	22
Metodología	23
Análisis Costos	26
Resultados	27
Resultados para el objetivo 1	27
Resultados para el objetivo 2	31
Resultados para el objetivo 3	36
Requerimientos Funcionales	36
Requerimientos No Funcionales	37



Diseño del juego 1: Cofee Security	45
Diseño del juego 2: Detectores de peligro	48
Diseño del juego 3: Gu@rdianes de cl@ves	50
Diseño del juego 4: Hunting	52
Evaluación del prototipo	54
Prototipo #2	56
Conclusiones	59
Bibliografía	61

Lista de figuras

Figura 1 Pantalla principal del prototipo “SafeWeb”	40
Figura 2 Pantalla de Login	41
Figura 3 Pantalla de Registro	42
Figura 4 Pantalla de la "racha"	43
Figura 5 Pagina Inicial juegos	44
Figura 6 Pantalla de confirmación.	45
Figura 7 Pantalla principal del juego Cofee Security.	46
Figura 8 Pagina web Maliciosa	47
Figura 9 Decisión correcta	48
Figura 10 Decisión incorrecta	48
Figura 11 Historial de navegación en Safe Web.	49
Figura 12 Retroalimentación visual.	50
Figura 13 Presentacion pregunta y opciones.	51
Figura 14 Retroalimentación de la actividad Contraseñas	51
Figura 15 Página principal Juego "Hunting"	52
Figura 16 Pantalla Victoria anticipada	53
Figura 17 Pantalla de demora en identificación de mensajes	54
Figura 18 Correcta identificación de mensajes	54
Figura 19 Index.html	57
Figura 20 Prototipo COFFEE SECURITY	58
Figura 21 COFFEE SECURITY EN JUEGO	59



Resumen

El eje principal de esta investigación es reconocer que el nivel educativo es seguridad cibernética de los niños y adolescentes en Bogotá es muy bajo en comparación a la gran relación que los jóvenes tienen con la tecnología, la cual todos los días crece aun más de manera exponencial. A partir de esto, se busca diseñar una solución moderna, interactiva y eficaz de generar un impacto en esa brecha de conocimiento sobre el uso responsable de las tecnologías inteligentes, mediante la implementación de software, abarcando conceptos y métodos relacionados como lo son las principales pautas para tener en cuenta en el diseño de un software y demás herramientas relacionadas, y verificar que tan viable seria este proyecto y si el impacto generado seria satisfactorio para este mismo.



Introducción

Los conocimientos sobre ciberseguridad, tras el aumento de nuestra dependencia los dispositivos inteligentes, se vuelve cada vez más necesario, el uso de dispositivos electrónicos se está volviendo, no solo un hábito de uso, sino una necesidad para el desarrollo de muchas actividades en el diario vivir, con respecto a la conexión a internet específicamente, pues, es una herramienta fundamental tanto en entornos profesionales, educativos y, actualmente, en espacios personales como para la interacción social, y uno de los periodos en los que es más importante abarcarlo es desde la niñez y juventud de las personas (García D, 2022), debido principalmente a la gran cantidad de amenazas que están ya presentes y de las que emergen todos los días con diversas características y métodos de detección.

Aunque claramente, no es necesario inculcar conceptos y metodologías tan complejas a una edad tan temprana, ya sea por la capacidad de comprender factores de la seguridad informática, o por el hecho de mantener la atención e interés de los jóvenes en la materia, para ello es necesario encontrar el foco en el que los más jóvenes pueden reforzar sus habilidades



como una práctica que mejora su capacidad de acción frente a cualquier situación en el contexto cibernético (Gutiérrez, J. A et al., 2024). Para ello, se debe tener en cuenta que tan vulnerables se encuentran hoy en día los niños y adolescentes, con diferentes análisis centrados en la población Bogotana, cuáles son los principales peligros a los que se enfrentan y así mismo, comprender desde su postura y capacidades, como pueden actuar ante estas amenazas virtuales, de esta manera, desarrollar un software que ayude a la población a catalizar sus métodos de protección.

Objetivos

Objetivo general

- Diseñar un software educativo que funcione como herramienta contra el desconocimiento en seguridad informática en los más jóvenes en Bogotá.

Objetivos específicos

1. Analizar los principales riesgos de seguridad informática a los que están expuestos los jóvenes en Bogotá, identificando sus conocimientos y hábitos digitales.
2. Diseñar actividades interactivas con las que los jóvenes puedan aprender lúdicamente sobre ciberseguridad.
3. Prototipar los requerimientos fundamentales del software para evaluarlo en alcance, integridad y escalabilidad.

Problema de Investigación

La constante implementación de tecnologías inteligentes conlleva el ir generando una sobre exposición de la información personal de los usuarios, especialmente en los niños, quienes difícilmente pueden medir que tan confidencial debe ser su información personal. Por ejemplo, en un artículo sobre la adicción al internet de la revista Científica de Edu-comunicación señala



que Cuando los adolescentes empiezan a compartir fotografías en sus redes sociales se comienza a generar ciertos conflictos de privacidad, relacionados con la protección de la imagen del menor (Hinojo-Lucena et al., 2020), al referirse a conflictos de privacidad también, se da idea a las diversas vulnerabilidades que se pueden llegar a presentar en el ambiente cibernético pues en el contexto cibernético, los niños son un foco de vulnerabilidad, pues incluso elementos como inteligencias artificiales permiten su implementación legal desde los 14 años sin consentimiento parental (EFE News Services, 2023).

Estas vulnerabilidades pueden comprometer la seguridad de la información de los niños y sucesivamente la de sus padres, como datos bancarios. A pesar de ello, sabiendo que estas amenazas siempre están presentes en los ambientes informáticos, los niños y adolescentes no cuentan con espacios de aprendizaje en los cuidados que se deben tener al conectarse en la red, estrategias que disminuirían considerablemente las brechas de seguridad que su pueden llegar a generar inconscientemente, esto no solo se refiere desde las escuelas, sino también a herramientas virtuales.

Con base a esto, surge la pregunta principal con la que se realiza la investigación, el descifrar, ¿Cómo el diseño de un software puede funcionar como una herramienta que pueda contribuir en el desconocimiento sobre seguridad informática en niños y adolescentes en Bogotá?

Un estudio realizado por la empresa privada Tigo, en asociación con la Universidad de los Andes y Aulas en Paz, encuestando una cantidad de 5718 estudiantes de las diferentes regiones colombianas en 58 colegios distintos, buscando caracterizar las experiencias digitales de los niños y adolescentes después de la pandemia del COVID-19 en Colombia, en donde para términos más precisos “El estudio contó con 5.718 niñas, niños y adolescentes participantes de



los cuales el 51,2% eran mujeres y el 44,7% eran hombres. Más de un 64% tenía 13 años o más y en su gran mayoría provenían de zonas urbanas.” (p. 8).

Obteniendo resultados tales como que el 38% de los niños y adolescentes no usan métodos de seguridad tales como bloqueo de usuarios, reporte de contenido y/o usuarios, asimismo se reportó que:

El 62% respondió que en el último año solo unas pocas veces han sentido que algo en internet que les haya molestado o que los haya hecho sentir molestos, incómodos o asustados. Sin embargo, un 14% reporta haberlo sentido al menos una vez al mes y un 8.6% al menos una vez a la semana. (Universidad de los Andes. Et al., 2024)

Estos resultados reflejan la situación a nivel Colombia, lo cual, es importante para, abarcar ahora el cómo se vive esta situación específicamente en Bogotá, la cual, al ser la capital del país, y asimismo ser una ciudad que para el 2022 tiene un porcentaje de 80,7% de hogares poseen un acceso a internet (García D, 2022), debido a esto el riesgo en niños y adolescentes de manera informática también aumenta.

Profundizando en esta situación se encontró que se realizó una investigación “con la participación de 22 estudiantes (14 niñas-8 niños) que oscilan entre los 7 y 10 años, los cuales fueron escogidos por conveniencia representado el 25% de la población” (Lizarazo, S. J. Et Al., 2021), acerca del uso de las TIC, estos estudiantes ubicados en la localidad 6 de Bogotá, con resultados tales como que el 90.9% de los encuestados tienen redes sociales dedicando aproximadamente de 5 a 6 horas al día.

Justificación



Gracias a los datos estadísticos recopilados y la problemática vista, surge la realización de este diseño, fortaleciendo el conocimiento de seguridad informática en niños y adolescentes, buscando no solo concientizar sobre los diversos riesgos informáticos, sino proporcionar estrategias y herramientas de navegación seguras. Creando una cultura de prevención y protección de uso y manejo de las tecnologías. Crear e implementar un software educativo puede traer consigo beneficios durante el aprendizaje, como exponen en la recopilación de ensayos “Utilización de tecnologías educativas en el proceso de enseñanza-aprendizaje de asignaturas en ciencias. Estudio de caso: software educativo Exploración de la Efectividad de los Recursos Educativos Abiertos” se exponen dos puntos de vista muy importantes “Los recursos educativos de software mejoran la accesibilidad y flexibilidad en la enseñanza de ciencias. Estas tecnologías representan una herramienta valiosa, pero requieren adaptación según el contexto y el nivel educativos del usuario, acompañado de soporte y formación continua.” (Román Aguilar et al., 2023) o como expone Antonieta Figueroa “Se requiere incluir en su diseño criterios que favorezcan la comprensión del contenido por parte del alumno; es decir, deben apoyarse en bases psicopedagógicas sobre el aprendizaje, así como en los principios básicos de la ingeniería de software que permitan concretar el desarrollo de la aplicación en forma exitosa” (Figueroa A. A., 2009). Todas estas cuestiones confirman como el objetivo principal de este proyecto, mientras se mantenga en un margen de efectividad y calidad puede llegar a soportar el alcance que se le quiere dar como herramienta de software.

Dentro de los proyectos propuestos por miembros de la facultad de la Universidad EAN, se encuentra el proyecto “Propuesta De Formación En Lenguajes De Programación En La tecnología Virtual De Análisis Y Desarrollo De Software Del Sena” desarrollado por Margarita Claudia Correa Villar y Liliana Patricia Vargas Escobar en donde es su análisis de resultados se



puede identificar la efectividad de las herramientas tecnológicas en el contexto educativo, en el que “se identifica gran aceptación de los usuarios a estas metodologías, avances tecnológicos que hacen que estos espacios virtuales sean innovadores y realmente útiles, aunque también se identificó falta de acompañamiento y complejidad de entender algunos contenidos” (Correa V. & Vargas Escobar L., 2024), con las que se consiguen conceptos de metodologías activas, niveladas y de fácil acceso, que crean herramientas de software que pueden ser muy útiles para el aprendizaje de cualquier temática, como puede ser la ciberseguridad dentro del contexto de este proyecto.

Marco Teórico

El siguiente marco teórico tiene como propósito proporcionar al lector los conceptos clave sobre el diseño de software que reduzca el desconocimiento en ciberseguridad en niños y adolescentes. Para ello, se analizan estudios previos que permiten identificar enfoques útiles y brechas existentes, con el fin de construir una base sólida para la propuesta.

El primer estudio revisado, “Desarrollo de una guía de ciberseguridad para la protección de estudiantes adolescentes en la institución educativa San Luis”, resalta cómo la falta de educación en ciberseguridad expone a los jóvenes a riesgos como el phishing, grooming y ciberacoso. Se concluye que una guía adaptada al contexto escolar mejora significativamente su capacidad de protección digital (Gutiérrez, J. A. et al., 2025), lo cual resulta útil como base para el diseño de un software educativo con componentes interactivos y adecuados a su edad.

El segundo estudio, “Estrategias para alfabetización de adolescentes en Colombia dentro del ecosistema digital”, identifica la vulnerabilidad de los adolescentes frente a amenazas digitales debido a su alta exposición en redes sociales y al bajo nivel de educación en seguridad



informática. Propone programas formativos y medidas legales para reforzar la protección de datos (Quintero R. & Cristancho D., 2024), aportando así elementos clave para promover una cultura digital responsable desde el diseño del software.

Exposición Digital y Riesgos en Niños y Adolescentes

La creciente digitalización ha transformado la interacción social, educativa y personal de niños y adolescentes, generando nuevas vulnerabilidades. Como señala Hinojo-Lucena (2020) en ReMedCom, el uso de redes sociales y la publicación de contenido personal (como fotografías) exponen a los menores a conflictos de privacidad, grooming y ciberacoso. (Hinojo-Lucena et al., 2020) Este estudio destaca que, aunque los adolescentes son usuarios activos de plataformas digitales, carecen de conciencia crítica sobre los riesgos asociados a la sobreexposición de su información personal.

En línea con esto, Cristancho & Quintero (2024) enfatizan que, en Colombia, la falta de conocimiento respecto al ambiente digital en adolescentes los hace vulnerables a amenazas como el robo de identidad y fraudes (Quintero R. & Cristancho D., 2024). Su investigación revela que, a pesar del alto tiempo invertido en internet (5-6 horas diarias, según Lizarazo, 2021), los jóvenes no aplican medidas básicas de seguridad, como el bloqueo de usuarios o el reporte de contenido inapropiado (Lizarazo Sindy Johanna et al., 2021).

Importancia de la ciberseguridad en los niños

Según el autor, Gutiérrez Pineda et al. (2025) señalan que las tecnologías que antes eran un espacio abierto y fascinantes, se ha transformado en un campo plagado de peligrosos riesgos cibernéticos que exponen amenazas que podrían poner en jaque su privacidad, su seguridad personal y su salud emocional. por lo que en actualmente es muy importante la educación en seguridad informática, principalmente por la salud e integridad de los más jóvenes.



Bajo el concepto de la seguridad cibernética se puede reforzar esta idea, como expone Vincent Pons Gamón (2017), el ciberespacio es un espacio virtual complementado por redes eléctricas y medios físicos que, si reciben alguna interferencia externa, se presentan consecuencias graves sobre la seguridad de la información, surgiendo así desde el nacimiento del internet términos de cibercrímenes como actividades ilícitas que se cometen en el ciberespacio, con un desarrollo tan fácil, en cuestión a requerimientos de recursos y espacios físicos, para la ejecución de estas actividades. (Pons Gamón, 2017).

Moviéndose al contexto moderno sin duda alguna, el internet de las cosas, pone en juego ambientes virtuales desde los cuales actividades que ponen aún más en riesgo la seguridad informática consiguiendo del mismo modo, un mayor campo de acción para comprometer los diferentes dispositivos y a los usuarios mediante una mayor interconexión con el entorno físico, y sin la necesidad de tener altos como conocimientos en informática, acciones como el fraude, el chantaje, la falsificación no requieren de mucha habilidad con las nuevas tecnologías. Por otro lado, como resalta Babilonia Ospina et al. (2023) Este concepto expone nuevas tendencias en diversos campos en los que abarca espacios en los que antes no se visualizaba a la tecnología, como el desarrollo de ideas de negocio, servicios, industria e igualmente mejoras en los métodos de ciberseguridad. Es decir, que del mismo modo en que las nuevas tecnologías comprometen la seguridad de las personas, estas también son un pilar para reforzar los sistemas informáticos de prevención de ataques y vulnerabilidades en la web. (Babilonia Ospina et al., 2023).

Contexto legal en Colombia

Cabe destacar, el enfoque que se tiene a nivel legal y gubernamental en Colombia, la Ley 1273 de 2009, específicamente resalta los delitos informáticos como el acceso no autorizado a cualquier sistema de información, daño o sabotaje de este o inyección de cualquier software



considerado malicioso con multas de hasta 1500 SMMLV (LEY 1273, 2009). Del mismo modo la ley 1620 de 2013, define desde los derechos de protección de los más jóvenes, específicamente de los estudiantes, determina ciertas prácticas como el ciberbullying o el ciberacoso, como vulnerabilidades a las que se exponen los niños en los ambientes virtuales (Ley 1620, 2013) . De la mano de estas leyes, establecido el decreto 338 de 2022, se establece ya el cómo se responde desde un modelo de gobernanza con el que actuar bajo el avance digital presente desde la pandemia (Decreto 338, 2022). Todas estas hacen parte del modelo cultural que se debe abordar para el conocimiento de la población.

Las leyes establecen sanciones para delitos informáticos y promueven la gobernanza digital. Sin embargo, como critica Beltrán Muñoz (2024), las leyes no tienen efecto si no hay una cultura de prevención (Muñoz, 2024). La investigación de Global Public Health (2022) vincula esta problemática con la salud mental, mostrando que el ciberacoso afecta emocionalmente al 14% de los adolescentes bogotanos, según los datos del informe. (González et al., 2022).

Inteligencia Artificial y Ciberseguridad: Oportunidades y Amenazas

Las tendencias en inteligencia artificial determinan un gran impacto en la protección y vulnerabilidad de los datos, funcionando como un arma de doble filo. Mark Coeckelbergh (2021) expone que “la disponibilidad de grandes conjuntos de datos, la IA, y especialmente el aprendizaje automático, ha logrado avances significativos. Este hecho ha permitido a los algoritmos hacerse cargo de muchas de nuestras actividades, incluyendo la planificación, el habla, el reconocimiento facial y la toma de decisiones.” Si bien estas innovaciones optimizan herramientas educativas y actividades cotidianas, también facilitan métodos de irrupción en la privacidad web, empleados por los denominados “ciberdelincuentes” (Coeckelbergh, 2021).



En este sentido, la IA ha permitido que plataformas digitales registren menores de edad sin supervisión parental, exponiéndolos a la recolección no consentida de datos (EFE News Services, 2023). Esto refuerza la necesidad de fortalecer la cultura y el conocimiento de los usuarios en la implementación de nuevas tecnologías para la protección de su privacidad. Alberto Beltrán Muñoz (2024) señala que “dichos conocimientos aportan una capacitación que permite a los individuos defenderse, sin embargo, esa carencia encontrada desde la investigación les deja en una situación de mayor vulnerabilidad en los medios.” (Muñoz, 2024). Este desafío es especialmente relevante en el uso popular de redes sociales y otros entornos digitales atractivos para los jóvenes.

No obstante, la inteligencia artificial también puede ser un aliado en la prevención de estos riesgos. Babilonia Ospina et al. (2023) proponen su uso para diseñar sistemas adaptativos que enseñen ciberseguridad mediante simulaciones interactivas, una estrategia clave para el software propuesto en esta investigación. (Babilonia Ospina et al., 2023)

Educación Digital y Enfoques Pedagógicos

Educar sobre los ambientes digitales es fundamental para reducir brechas de seguridad. El artículo de Revista Ocnos analiza cómo los programas educativos tradicionales fallan en abordar las dinámicas del ecosistema digital, sugiriendo metodologías basadas en:

Gamificación: Uso de desafíos y recompensas, motivando el aprendizaje (ejemplo: módulos interactivos con retroalimentación inmediata).

Enfoque situado: Escenarios realistas que simulen amenazas como phishing o grooming (Andrea et al., 2023)

El estudio de Universidad de los Andes et al. (2024) refuerza esta necesidad: el 38% de los adolescentes colombianos no usa herramientas de protección, evidenciando la urgencia de



usos de tecnología para enseñar métodos de protección y prevención (Universidad de los Andes, 2024)

El análisis de Vincent Pons Gamón (2017) sobre el ciberespacio subraya que la facilidad para cometer ciberdelitos está relacionada con la falta de conocimiento de ciberseguridad. Esto se corrobora con los hallazgos de Tigo y Aulas en Paz (2024): el 62% de los jóvenes ha sentido incomodidad en línea, pero pocos actúan.

El software que se propone tiene como objetivo disminuir la falta de conocimiento en seguridad informática mediante metodologías activas que han demostrado ser efectivas en el aprendizaje digital. Estrategias como la gamificación y los escenarios situados permitirán que los niños y adolescentes adquieran hábitos seguros en internet de una manera interactiva y adaptada a su entorno.

Al incorporar estas estrategias de aprendizaje en el diseño del software, se busca promover una educación digital efectiva que no solo ofrezca conocimientos teóricos, sino que también desarrolle habilidades prácticas para navegar de forma segura en internet. Así, esperamos que los niños y adolescentes adopten buenas prácticas de ciberseguridad y disminuyan su vulnerabilidad en el mundo digital (Pons Gamón, 2017).

El diseño de un software

El desarrollo de software es un proceso complejo que abarca la creación, diseño, implementación y soporte de software, implicando una serie de actividades informáticas destinadas a producir sistemas que satisfagan necesidades específicas de los usuarios. En este campo, la elección de las herramientas adecuadas es crucial, pues, como se menciona en Indeed (2024), existen al menos 10 herramientas de desarrollo de software que deben conocerse para ser



competitivos en el mercado, ya que no solo facilitan el proceso de desarrollo, sino que también permiten una mayor eficiencia y productividad (Equipo editorial de Indeed, 2024).

En el aprendizaje del desarrollo de software, resulta evidente la importancia de las metodologías, siendo las metodologías ágiles fundamentales para estructurar y planificar el proceso, asegurando un enfoque sistemático y eficiente. Según la Universidad Católica Argentina (2010), estas metodologías permiten una mayor flexibilidad y colaboración con el cliente, lo cual es esencial en proyectos dinámicos. Además, la elección de proveedores confiables es crucial para el éxito en el desarrollo de software.

El conocimiento en desarrollo de software también requiere mantenerse actualizado con las últimas tendencias, ya que la inteligencia artificial y el aprendizaje automático están revolucionando el proceso de desarrollo, mejorando la calidad y velocidad del software. Asimismo, el desarrollo de baja codificación y sin codificación permite a personas sin experiencia en programación crear aplicaciones, reduciendo la barrera de entrada al mundo del desarrollo. Herramientas que se lanzan a menudo pueden facilitar esta tarea al ofrecer soluciones más accesibles y eficientes, lo que refleja cómo el desarrollo de software está evolucionando para ser más inclusivo y accesible (Jimenezb, 2025).

Análisis de Requerimientos

A partir de los conceptos abordados y de los objetivos planteados para el correcto proceso metodológico del proyecto se plantean la siguiente lista de requisitos pertinente para todas las tareas a realizarse. Se establecen de manera enumerada, así durante la sección de la metodología se indicará numéricamente, cuales de estos requerimientos soportan las actividades planteadas.



- 1) Computadores con sistema Windows 10/11 con disposición de Visual Studio para realizar la codificación del prototipo del software.
- 2) Aplicación Teams como espacio de comunicación y socialización virtual entre los miembros del proyecto.
- 3) Bases de datos: Mc Graw Hill, Scopus, Taylor & Francis e IBM como principales fuentes de información.
- 4) Inteligencias artificiales: Chat GPT, DeepSeek y Perplexity como soporte y solidificación de conceptos investigativos y de prototipado.
- 5) Sistema de Host y diseño estable con moderada accesibilidad y soporte de una densidad de usuarios aceptable, con soporte de diseño de todas las funciones.
- 6) Sistema Word como procesador de textos para documentar el proyecto y los avances relacionados a este.

Análisis de Restricciones

Para identificar cualquier clase de restricciones externas que se deban tener en cuenta durante el desarrollo de alguno de los objetivos planteados, se evaluarán dichas restricciones mediante un análisis PESTEL para entender que puntos hay que incluir en cualquier fase dentro de los niveles pertinentes: Político, Económico, Social, Tecnológico, Ecológico y Legal dentro del contexto de Colombia y la ciudad de Bogotá y, a su vez, identificar las potenciales Amenazas y Oportunidades y como priorizar estos descubrimientos.



Restricciones Políticas

La evaluación de políticas que afectan directamente al proyecto a través de decretos, regulaciones, políticas fiscales y la estabilidad del gobierno pueden crear factores y parámetros para tener en cuenta en el desarrollo del proyecto en cualquiera de sus fases.

Dentro de este marco en el contexto colombiano, el proyecto se presenta mediante iniciativas nacionales como el Plan Nacional de Desarrollo 2022-2026 “Colombia, Potencia Mundial de la Vida” y la Política Nacional de Confianza y Seguridad Digital. Estas promueven la ciberseguridad y concientización en ámbitos de seguridad como pilares para la transformación digital del país. Sin embargo, la restricción principal se presentaría en el cambio de prioridades en las políticas educativas a nivel distrital y nacional.

Un cambio de gobierno o de enfoque en la Secretaría de Educación de Bogotá podría afectar la viabilidad de implementar el software en colegios públicos, ya que podría verse beneficiado el desarrollo en la alineación con los programas oficiales y la disponibilidad de recursos asignados por el estado (Departamento nacional de planeación, 2023). Además, se pueden perder oportunidades al no alinear el proyecto con otros ya establecidos como el programa “Escuela Digital” de MinTIC, ya que estos pueden ofrecer financiación y apoyo en desarrollo.

Restricciones Económicas

Los factores económicos, tanto internos como el presupuesto disponible, como externos, como el crecimiento del PIB, la inflación y las tasas de interés, son fundamentales para la planificación de un proyecto. Un entorno económico favorable puede impulsar la demanda y facilitar la inversión, mientras que condiciones desfavorables pueden restringir las oportunidades y afectar la rentabilidad o la calidad de los resultados.



Dentro de la investigación planteada, el índice de brecha digital y los costos asociados a la tecnología educativa son aspectos especialmente sensibles en el contexto de la educación pública, donde la infraestructura y el acceso a dispositivos adecuados aún representan retos significativos, según el MinTIC. Entre los años 2018 y 2023, Colombia registró una disminución del 11,3% en la brecha digital, indicador que mide las diferencias en el acceso y uso de las tecnologías de la información y la comunicación entre distintos grupos poblacionales.

En 2023, las dimensiones que más contribuyeron a la brecha digital a nivel nacional fueron las Habilidades Digitales (35,1%), seguidas por el Acceso Material (31,7%), el Aprovechamiento de las TIC (29,9%) y, en último lugar, la Motivación (3,3%) Colombia TIC, 2024).

Estos resultados evidencian que, aunque en Bogotá la infraestructura y el acceso a dispositivos se encuentran relativamente garantizados, persiste el desafío en la capacidad de utilizar efectivamente estas tecnologías con fines educativos, laborales y personales. Esto subraya la necesidad de implementar políticas y programas enfocados en fortalecer las habilidades digitales y en promover un uso consciente y productivo de las TIC.

En el ámbito de los costos y presupuestos asociados a la tecnología educativa, se evidencia que la inversión no se limita a la compra inicial de dispositivos y plataformas digitales, en donde el verdadero gasto incluye componentes recurrentes como licencias de software, tarifas de suscripción, mantenimiento, actualizaciones y la capacitación docente para garantizar un uso adecuado de las herramientas. Una planeación presupuestaria efectiva debe contemplar todos estos factores, priorizando las necesidades de la institución y asegurando que las soluciones sean escalables y adaptables a los cambios futuros (FasterCapital, 2025).



Esto implica planificar con visión de sostenibilidad, considerando no solo la adquisición de equipos y plataformas, sino también la integración con los sistemas ya existentes, el soporte técnico continuo y la protección de los datos de los estudiantes.

Restricciones Sociales

En cuanto a los factores sociales, estos incluyen cambios demográficos y tendencias culturales y educativas que influyen en el comportamiento y en las decisiones que se deben tomar en el proyecto. Entender las preferencias y valores de la población es clave para diseñar productos y estrategias que conecten con el público objetivo y aseguren la aceptación del proyecto dentro del alcance establecido.

En cuestiones más específicas la brecha digital en Colombia no se limita al acceso a dispositivos y conectividad, sino que también se refleja en la desigualdad en el desarrollo de habilidades digitales y en el uso pedagógico de las TIC, disparidades que están estrechamente ligadas a las condiciones socioeconómicas y que generan exclusión en comunidades vulnerables y zonas rurales, afectando la calidad y equidad del proceso educativo (Escobar M. W., 2024).

Asimismo, la resiliencia digital se ha convertido en un factor social fundamental para abordar los riesgos asociados al uso de las TIC en niños, niñas y adolescentes, entendida como la capacidad de afrontar de manera positiva los desafíos del entorno digital, tales como la exposición a contenidos inadecuados, el ciberacoso o la pérdida de privacidad. Según González-Díaz y otros (2023). Fortalecer la resiliencia digital implica no solo proveer acceso a tecnologías, sino también desarrollar competencias emocionales, sociales y cognitivas que permitan a los estudiantes utilizar internet de forma segura y responsable.

Tanto la brecha digital como la resiliencia digital evidencian que el acceso a dispositivos y conectividad, aunque necesario, no es suficiente para garantizar un uso efectivo y seguro de las



TIC en el ámbito educativo. La persistencia de desigualdades limita las oportunidades de aprendizaje, mientras que la falta de competencias digitales y de estrategias de afrontamiento frente a los riesgos del entorno virtual aumenta la vulnerabilidad de niños, niñas y adolescentes.

Restricciones Tecnológicas

La tecnología juega un papel crucial en la innovación y la eficiencia operativa del proyecto, especialmente si se trata del diseño o desarrollo de software que necesariamente debe ser accesible a través de dispositivos. Adaptarse a las nuevas tecnologías puede optimizar procesos y mejorar la propuesta final, lo cual es esencial para mantenerse relevante en un entorno en constante evolución.

Dentro de los objetivos del proyecto, una restricción tecnológica significativa es la brecha de infraestructura y conectividad dentro de la ciudad de Bogotá. Aunque la ciudad tiene una alta tasa de conectividad, la misma no es consistente entre los distintos sectores. El software, al ser una herramienta digital, requiere acceso a internet. Según el estudio más reciente realizado por el DANE (2023), el 80.7% de los hogares bogotanos tiene internet, siendo de los porcentajes más altos, departamentos periféricos como la Amazonía, el Caquetá o la Guainía presentan porcentajes de acceso a internet por debajo del 62% (DANE, 2023). El software debe ser desarrollado para funcionar en una amplia gama de dispositivos (computadores, smartphones) y sistemas operativos (Windows, Android, iOS), incluyendo versiones no tan recientes, para asegurar la máxima accesibilidad. Esto limita el uso de tecnologías más complejas en el desarrollo que podrían no ser soportadas por hardware antiguo, muy común en estratos socioeconómicos más bajos.



Restricciones Ecológicas

Los factores ecológicos están cobrando cada vez más importancia debido a la creciente preocupación por la sostenibilidad y el cambio climático, especialmente considerando el enfoque que debemos dar a cualquier solución propuesta como profesionales. Cumplir con las regulaciones ambientales y adoptar prácticas sostenibles no solo es necesario, sino que también puede realzar la imagen del proyecto.

La principal restricción ecológica para un proyecto de software es su huella de carbono digital indirecta. Al usar nuevos dispositivos, generamos más residuos, por lo que fomentar el uso de software en dispositivos antiguos puede extender su vida útil, reduciendo la basura electrónica. (Freitag et al., 2021)

Restricciones Legales

Por último, los factores legales abarcan todas las normativas que impactan la operación del proyecto, como la legislación laboral, de seguridad y de propiedad intelectual. Cumplir con estas leyes es vital para evitar sanciones y proteger los intereses del proyecto, asegurando así su viabilidad.

La Ley 603 de 2000 regula los derechos de autor en Colombia, es clave para el desarrollo y diseño del software, ya que establece las normas para proteger cualquier tipo de producto o información desarrollada por alguien esto incluye programas de computadora. Esta ley asegura que los desarrolladores de software conserven los derechos sobre sus creaciones, lo que significa que cualquier código, diseño o documentación generada durante el proceso de desarrollo está protegida contra el uso no autorizado. Por lo tanto, es vital asegurarse de que el software creado cumpla con las disposiciones de esta ley, registrando adecuadamente los derechos de autor y evitando infringir los derechos de terceros.



De igual forma, el artículo 47 de la Ley 222 de 1995 aborda la responsabilidad de los administradores de sociedades, es decir de empresas legalmente estructuradas y su obligación de actuar con diligencia y lealtad hacia dicha empresa, en el contexto del desarrollo de un software, esto significa que los miembros del proyecto deben actuar de manera responsable y ética en todas las decisiones y procesos relacionados con el proyecto. Esto también implica cumplir con las normativas de protección de datos y privacidad, garantizando que el software respete la confidencialidad de la información de los usuarios y se adhiera a las regulaciones pertinentes (El Congreso de Colombia, 1995).

Con respecto a la protección de los datos y de la información, se debe mantener el artículo 1273 de 2009 en el que se especifican los que son atentados contra la confidencialidad, la integridad y disponibilidad, como acceso abusivo, obstaculización, interceptación, violación o cualquier vulnerabilidad hacia los datos de cualquier usuario.

Metodología

Para el cumplimiento de los objetivos planteados, se establecen una serie de tareas por las cuales darle resolución a cada uno de estos.

Inicialmente, para dar cumplimiento al objetivo número uno, “Analizar los principales riesgos de seguridad informática a los que están expuestos los jóvenes en Bogotá, identificando sus conocimientos y hábitos digitales”, se propone la siguiente metodología:

- Revisión documental en bases de datos especializadas: Se realizará una búsqueda académica en las bases de datos disponibles en la Universidad EAN, priorizando Scopus,



ScienceDirect, Google Scholar y Redalyc, empleando combinaciones de palabras clave como “ciberseguridad en jóvenes”, “riesgos digitales en Bogotá”, “hábitos de navegación en adolescentes” y “ciberacoso escolar”. Esta búsqueda permitirá obtener investigaciones y reportes técnicos actualizados que brinden información confiable sobre las amenazas más comunes y las conductas digitales de la población juvenil.

- **Análisis temático y categorización de riesgos:** La información recopilada se analizará de forma crítica, identificando y clasificando los tipos de amenazas según su naturaleza (phishing, malware, ingeniería social, grooming, ciberbullying, suplantación de identidad, etc.) y evaluando su frecuencia e impacto. Este análisis permitirá construir un panorama detallado de los riesgos que enfrentan los jóvenes y detectar vacíos de conocimiento en sus prácticas de seguridad digital.
- **Sistematización y priorización de resultados:** Los hallazgos se organizarán para poder relacionar la probabilidad de ocurrencia e impacto, lo que facilitará priorizar las amenazas más críticas. Esta información se establecerá para el documento en forma de informe analítico, con el cual servirá como base para orientar el diseño de las actividades lúdicas y los contenidos educativos del software, asegurando que respondan a los riesgos más relevantes en Bogotá.

Seguidamente, para el cumplimiento del segundo objetivo específico planteado, “Diseñar actividades interactivas con las que los jóvenes puedan aprender lúdicamente sobre ciberseguridad”, se plantean las siguientes acciones:

- Clasificar las amenazas identificadas en la fase anterior y adaptarlas al contexto juvenil, por ejemplo, transformar un caso de phishing empresarial en un mensaje fraudulento en



redes sociales o en una supuesta promoción de videojuegos, de manera que el riesgo sea cercano y comprensible para los estudiantes.

- Diseñar actividades interactivas que permitan a los jóvenes aprender de forma práctica y entretenida, como simuladores de chat para reconocer estafas, juegos de construcción de contraseñas seguras, trivias con puntajes acumulativos o retos tipo “escape room” digital donde deban identificar prácticas seguras para avanzar.
- Definir indicadores de evaluación concretos para medir la efectividad de las dinámicas, tales como: porcentaje de aciertos en la resolución de los ejercicios, tiempo promedio de respuesta frente a una amenaza simulada, nivel de participación (cantidad de estudiantes que finalizan la actividad), y una breve autoevaluación de satisfacción en la que los jóvenes valoren la claridad y utilidad de lo aprendido. Estos indicadores permitirán tanto validar la comprensión de los conceptos como la motivación generada por la actividad.
- Crear tutoriales de apoyo que acompañen cada actividad, en diferentes formatos para asegurar accesibilidad y comprensión. Por ejemplo, guías escritas con pasos breves y esquemáticos para quienes prefieran texto, videos animados cortos (2-3 minutos) que expliquen la dinámica de forma visual y atractiva, e incluso pequeños ejemplos interactivos previos a la actividad principal, a modo de práctica guiada. De esta manera, se garantiza que tanto niños como adolescentes con distintos niveles de familiaridad tecnológica puedan realizar los ejercicios sin dificultad.

Finalmente, para el desarrollo del tercer objetivo, “Prototipar los requerimientos fundamentales del software para evaluarlo en alcance, integridad y escalabilidad”, se plantean las siguientes acciones:



- En primera instancia se plantea la definición de los requerimientos funcionales y no funcionales que servirán como base para la construcción del prototipo, considerando en los primeros aspectos como el acceso a las actividades, la generación de resultados, los mecanismos de retroalimentación y la interacción del usuario dentro de la plataforma, mientras que en los no funcionales se priorizan elementos como la velocidad de carga, la compatibilidad con distintos dispositivos y la facilidad de uso, tomando como referencia las buenas prácticas de desarrollo de software educativo y los objetivos del proyecto.
- Luego se trabaja en la estructura visual del prototipo y en la organización de sus componentes principales, utilizando Canva para crear los primeros modelos gráficos o mockups de las pantallas, buscando que el diseño sea claro, coherente y atractivo. En esta etapa se incluyen elementos como la pantalla de inicio, el apartado de actividades interactivas, los menús de navegación y las zonas de retroalimentación, procurando que la interfaz sea intuitiva y comprensible para los jóvenes que interactuarán con el software.
- Más adelante se establecen los requerimientos y alcances específicos para la versión inicial del prototipo, seleccionando una parte funcional del sistema que represente la esencia del proyecto, en este caso una de las actividades interactivas propuestas, lo que permitirá validar la viabilidad técnica, demostrar su funcionalidad y proyectar la escalabilidad hacia futuras versiones más completas del software.
- Finalmente, el desarrollo del prototipo se lleva a cabo mediante el uso de Visual Studio Code como entorno de programación, empleando tecnologías web como HTML y JavaScript para la construcción de la interfaz y las funcionalidades del aplicativo. Dentro del sistema se integran herramientas que permitan registrar el número de aciertos en las actividades, medir los tiempos de reacción en simulaciones y generar un pequeño informe



automático al finalizar cada sesión, promoviendo una experiencia interactiva que combine aprendizaje, evaluación y retroalimentación en un mismo entorno digital.

Análisis Costos

Teniendo en cuenta las implicaciones económicas que generar el proyecto conlleva, se desglosa una serie de gastos y costos que se deben tener en cuenta para que el diseño del software que se llegara hacer de una forma adecuada, representado mediante la siguiente tabla:

Tabla 1

Análisis de costos para la solución de ingeniería

Categoría	Descripción del ítem	cantidad	Unidad	Costo unitario	Costo total	Tipo de costo
Recursos humanos	Horas de trabajo del desarrollador 1	60	horas	\$ 25.000	\$ 1.500.000	Variable
Recursos humanos	Horas de trabajo del desarrollador 2	60	horas	\$ 25.000	\$ 1.500.000	Variable
Recursos humanos	Horas de trabajo del diseñador de interfaz	60	horas	\$ 25.000	\$ 1.500.000	Variable
Infraestructura	Computadores personales	3	unidad	\$ 2.000.000	\$ 6.000.000	Fijo
Software y licencias	Licencias varias		licencia	\$ 100.000	\$ 100.000	Fijo
Servicios	Conexión a internet	4	meses	\$ 100.000	\$ 400.000	Fijo
Servicios	Energía eléctrica	4	meses	\$ 50.000	\$ 200.000	Variable
Logística	Transporte a reuniones presenciales	6	trayecto	\$ 20.000	\$ 120.000	Gasto
Logística	Papelería e impresión	1	lote	\$ 50.000	\$ 50.000	Gasto
Otros	Refrigerios en jornadas largas	5	jornadas	\$ 30.000	\$ 150.000	Gasto
TOTAL					\$ 11.520.000	

Nota. Esta tabla muestra cómo se debe desarrollar económicamente el proyecto



Resultados

Resultados para el objetivo 1

Teniendo en cuenta el objetivo número 1 y la metodología planteada y anteriormente se desglosa la siguiente información como resultado de la investigación desarrollada: Primero, se debe aclarar la base de la actividad del proyecto, pues los conocimientos que se buscan aportar se basan tanto en los daños físicos que se pueden presentar frente a un ataque cibernético, como pueden ser el robo de datos o vulneración de la privacidad, y de igual forma sobre los daños psicosociales que también se pueden dar en un espacio virtual, como el ciberacoso o el chantaje. Igualmente, se establece que los principales riesgos cibernéticos a los que los niños y adolescentes son más vulnerables se toman en cuenta en diversos contextos, puesto que son muchos los espacios virtuales en los que los más jóvenes pueden verse expuestos. Inicialmente se tienen los juegos en línea, un área donde claramente la mayor cantidad de sus usuarios son menores de edad y que sirve como buena base de inicio para extraer todos los riesgos posibles, se pueden presentar ataques de diversas formas, según el artículo “Las amenazas cibernéticas” de Daniel Reyna Ramos, “Los principales riesgos en este entorno son el phishing y el ciberacoso, esto de forma generalizada pero a partir de estos dos aspectos se van de la mano muchos otros riesgos tanto físicos como mentales para los más jóvenes”(Reyna R. & Olviera G., 2016). Con respecto al phishing siendo una táctica “popular” entre los ciberdelincuentes se entiende en el envío de correos falsos que dirigen a una página web fraudulenta donde te incitan a meter tus datos personales o de jugador donde llegan a usurpar las cuentas de los usuarios esta técnica se amplía a espacios como las redes sociales o falsificación de datos que se van a detallar más adelante, por el lado del ciberacoso se entrelaza las actitudes de Ciberbullying generadas por los



videojuegos por momentos que generar odio y discusión entre los usuarios siendo un gran influenciador en riesgos psicológicos para las personas.

Desde el mismo campo de los videojuegos pero ahora generalizándolo a un apartado más global, se encuentran los riesgos de descargar malware, abarcándolo más al contexto de los niños se trata tanto de la piratería, aspecto en el que se descarga de forma ilícita y muy por lo general gratuita programas que en la mayoría de ocasiones cuentan con archivos ilícitos que pueden robar información personal, entre esta información están contraseñas, cookies (información que muestra nuestra forma de actuar en el internet) o programas que en segundo plano pueden minar criptomonedas, lo que afecta al rendimiento del dispositivo. Sin embargo, estos problemas de archivos con malware 1) no solo se presentan en computadoras y 2) no se encuentran exclusivamente en páginas no oficiales.

Las aplicaciones con malware han llegado a escabullirse en páginas oficiales como la play store para los dispositivos Android y en Steam plataforma de videojuegos totalmente legal para las computadoras. Según un artículo en 3D Juegos solo desde febrero de 2025 “ya se han presentado 3 ocasiones en las que en Steam se había introducido un juego que tenía alguna clase de malware en sus archivos y que para la actualidad al menos dos juegos diarios deben ser retirados por tener archivos maliciosos escondidos” (Giacconi Brenda, 2025) lo que muestra que para los jóvenes no es suficiente guiarse solo por la página que usan, ni siquiera es de seguridad el pagar por estos videojuegos cuando ni las mismas webs oficiales pueden controlarlo. Volviendo al entorno de Bogotá se vuelve un dato muy importante puesto que aproximadamente de los 132 millones de usuarios globales, más o menos 2 millones de cuentas se pueden encontrar registradas por menores de edad en la ciudad de Bogotá.



Moviéndose al segundo entorno fundamental del ciberespacio para los niños y adolescentes, las redes sociales, se puede recapitular al phishing como técnica de robo de información. Sin embargo, un campo de mayor impacto en la población es el ciberacoso donde además de las cuestiones de Ciberbullying ya planteadas, se tienen casos también de grooming o ciberacoso, momento en el que no se busca solo insultar a un usuario, sino que también, pueden presentarse palabras vulgares o incitación a actos inapropiados a contenido que suben las personas a sus redes sociales.

De igual forma, se ven casos de lo que se conoce como ingeniería social, según el artículo “Social Engineering: ¡Hacking the Wetware!” de la revista “Information Security Journal: A Global Perspective”, “La ingeniería social es el uso de la manipulación psicológica para engañar a las personas y obtener información confidencial, dinero o acceso a sistemas. Los ciberdelincuentes explotan la confianza y la emoción humana” (Scott D. Applegate, 2009). Donda así pie modalidades de estafas entre las que se destaca como la principal amenaza para los jóvenes, el sexting, modalidad en la que logran incitar a los jóvenes, tanto hombres como mujeres, al envío de contenido en el que muestren sus partes íntimas o se muestren de manera provocativa, procediendo igual que otras estafas a olas de chantaje y extorsión. De igual forma, dentro de estas modalidades de suplantación mediante inteligencia artificial, métodos de estafa que han tenido un auge en la época actual y con las que mucha gente, en su mayoría adolescentes cae en transferencias económicas o vulnerabilidades de esta clase.

Finalmente, recopilando las principales amenazas cibernéticas a los que son vulnerables los niños y jóvenes, y que son el enfoque de las actividades y juegos a desarrollar se mencionan:

- El robo de información:
 - El phishing



- Modalidades de piratería y software malicioso (malware)
- Estafas y falsificación:
 - ingeniería social: sexting, estafas, chantaje
 - suplantación de identidad incluyendo la implementación de IA
- Ciberacoso
 - Cyberbullying
 - Grooming o ciberacoso
 - Influencia en riesgos psicosociales y emocionales

Por otra parte, el cómo se establecen los conocimientos previos que tienen los jóvenes sobre mecánicas de ciberseguridad en Bogotá muestra en segmentos como el ministerio MISTIC, siendo esta la iniciativa pública en tecnologías y comunicaciones, que no son de gran enfoque en los avances de ciberseguridad, debido a que su marco estratégico se encarga principalmente del envío, inversión y desarrollo de tecnologías en todo el país, principalmente para los sectores de negocios y de industria, claramente no dejan de lado el enfoque educativo, de hecho, tienen estrategias como Talento TECH o Avanza TEC donde se hacen cursos y campañas sobre temas relacionados a la seguridad informática con intenciones de ampliarlo al sector escolar, pero la concientización en este conocimiento no ha alcanzado este nivel, es decir, no hay obligación de ninguna escuela o delegación e instruir sobre ciberseguridad.

Tiene sentido, pues muchas partes de Colombia no tienen las capacidades para incorporar las tecnologías como en puede ser en Bogotá, sin embargo, por lo mismo Bogotá, en contexto al país, esta a la vanguardia de tecnologías y es importante en la



población más joven educarse sobre protocolos y conceptos clave sobre la seguridad informática.

Resultados para el objetivo 2

Teniendo en cuenta los estudios e investigación obtenidos en el primer objetivo, se procedió con el diseño conceptual y funcional de las actividades interactivas que se representarán para integrar los conceptos de ciberseguridad dentro de experiencias dinámicas, con las cuales se busca transformar los principales riesgos identificados, tales como el robo de información, el ciberacoso y las estafas digitales. Promoviendo el pensamiento crítico de los jóvenes frente a su comportamiento en la época digital, se plantea el diseño de estas actividades a partir de experiencias propias y ajenas, buscando generar interés y atractivo tanto visual como de razonamiento, evitando que se conviertan en juegos meramente teóricos o repetitivos y ajenos a situaciones reales del entorno digital, permitiendo así que los jóvenes reconozcan amenazas, evalúen consecuencias y adopten prácticas seguras mediante medios interactivos que, en este caso, se representan a través de los juegos.

A partir de los lineamientos establecidos, se diseñaron diferentes actividades basadas en metodologías lúdicas y participativas, cada una enfocada en diversos riesgos específicos del entorno digital y en el desarrollo de competencias en ciberseguridad, la primera de ellas se titula “*Coffe Security*”, la cual se centra en que el jugador asume el rol de dueño de un cibercafé durante una jornada de ocho horas, manteniendo la rentabilidad económica mediante una supervisión activa de los usuarios, dentro de esta dinámica se utiliza una interfaz que simula una pantalla de computador donde se pueden observar los diferentes equipos disponibles en el establecimiento, permitiendo revisar las actividades que



se realizan en cada uno, recibir alertas sobre posibles sitios maliciosos y controlar el tiempo de uso solicitado y el realmente utilizado, de esta forma se puede identificar cuándo un usuario está por agotar su tiempo y aplicar los cobros correspondientes, al inicio de la partida el jugador dispone de un patrimonio base de \$2.000.000 que se verá afectado según las decisiones tomadas, cobrando por ejemplo \$20.000 por cada segundo excedido en el uso de los equipos y aplicando multas entre \$100.000 y \$500.000 en caso de no bloquear un virus o permitir el acceso a una página maliciosa. De esta manera, el jugador debe mantener una gestión equilibrada entre la supervisión técnica y la administración económica del negocio.

Además, se incluye una amplia variedad de sitios web simulados, entre los que se encuentran servicios de mensajería electrónica como Gmail, Outlook y Yahoo, redes sociales como Facebook, Instagram, Twitter y TikTok, plataformas de streaming como Netflix, YouTube, Spotify y Twitch, y servicios de videojuegos legales como Steam y Epic Games, junto a sitios de riesgo que representan páginas de streaming pirata o descargas de software ilícito, tanto de juegos como de otras aplicaciones que exponen al jugador a riesgos cibernéticos, asimismo se implementan conexiones de riesgo que pueden provenir de enlaces en redes sociales, correos o anuncios que redirigen a sitios web maliciosos o fraudulentos, generando así un entorno realista que exige al jugador mantener la vigilancia constante para evitar pérdidas económicas y proteger la seguridad del ciberespacio que administra.

El segundo juego web que se plantea se titula “*Hunting*”, el cual se enfoca en la identificación y documentación de conductas inapropiadas dentro de los entornos de comunicación digital, buscando que el jugador reconozca las diferentes señales de acoso en



conversaciones cotidianas y desarrolle una postura crítica frente a las interacciones que se presentan en las redes sociales, en esta actividad el jugador asume el papel de un amigo o acompañante de la víctima, observando en tiempo real una conversación que se desarrolla durante un periodo aproximado de diez minutos, donde progresivamente se manifiestan mensajes con intenciones maliciosas o manipuladoras, introduciendo momentos clave en los que las decisiones del jugador determinan el desarrollo y desenlace de la situación, como idea adicional se plantea que a partir del minuto siete el jugador deba intentar persuadir a la víctima para que abandone la conversación o denuncie lo ocurrido, buscando que actúe a tiempo, ya que de no hacerlo se presentará una acción irreversible que evidencia las consecuencias de la inacción frente al ciberacoso. De esta manera, el juego genera un ambiente de tensión y reflexión que representa con realismo la forma en que se desarrollan este tipo de situaciones en el entorno digital.

De esta forma, “*Hunting*” busca sensibilizar al jugador sobre las conductas inapropiadas que pueden presentarse virtualmente, promoviendo la reflexión sobre la responsabilidad individual y colectiva dentro de los espacios digitales, además de fortalecer habilidades como la comunicación asertiva, la empatía y la toma de decisiones ante situaciones de riesgo, convirtiéndose en una herramienta educativa que trasciende el entretenimiento al fomentar la conciencia, la prevención y la reacción adecuada frente a los casos de acoso digital.

Para el tercer juego, titulado “*Detectores de Peligro*”, se propone una dinámica orientada al análisis de historiales de navegación con el fin de identificar sitios web potencialmente peligrosos, en donde el jugador deberá reconocer los distintos tipos de riesgos digitales a través de la observación detallada de los comportamientos y



características de las páginas visitadas, presentando historiales compuestos por hasta veinte enlaces que mezclan sitios legítimos con sitios maliciosos, en este escenario el jugador debe evaluarlos en un tiempo limitado, aplicando criterios como los permisos solicitados, las políticas de cookies, la reputación del dominio y la autenticidad de las direcciones URL, buscando desarrollar una mirada analítica frente a los elementos que permiten detectar amenazas digitales.

El sistema de puntuación se establece con base en la precisión de los reportes, otorgando aproximadamente ocho puntos por cada identificación correcta y un bono adicional de cuatro puntos si el formulario es completado de manera precisa, mientras que los errores restarán seis puntos del puntaje total, de esta forma se pretende fortalecer la capacidad de discernimiento ante los múltiples entornos digitales que aparentan confiabilidad pero esconden riesgos de seguridad, incentivando la atención al detalle y el pensamiento crítico frente a la navegación cotidiana.

Finalmente, para el cuarto y último juego propuesto, titulado *“Gu@rdianes de Cl@ves”*, se plantea una dinámica orientada a la evaluación de la seguridad en las contraseñas digitales mediante diferentes métodos de identificación asociados con datos personales, en esta actividad el jugador deberá analizar diversas combinaciones de contraseñas y determinar qué tan vulnerables resultan según la información que estas revelan, considerando elementos como nombres de familiares, fechas importantes, gustos personales o referencias laborales y académicas, la mecánica principal del juego se basa en asociar fragmentos de una contraseña con los posibles datos personales proporcionados en un contexto específico, presentando cuatro opciones de las cuales solo una será correcta, definida por la cantidad de asociaciones acertadas que logre el jugador.



El propósito central de “*Gu@rdianes de Cl@ves*” es que el jugador comprenda cómo los patrones predecibles o el uso de información personal pueden comprometer la seguridad de sus datos, promoviendo la creación de contraseñas más seguras y conscientes, y fomentando al mismo tiempo la reflexión sobre la importancia de mantener la privacidad y la protección de la identidad digital en los diferentes entornos en línea.

En conclusión, el desarrollo de las cuatro experiencias interactivas permitirá integrar de manera dinámica y pedagógica los principales conceptos de la ciberseguridad, logrando que los jugadores adquirieran conocimientos prácticos sobre la identificación de riesgos digitales, la prevención de amenazas y la adopción de comportamientos responsables en los entornos virtuales, cada uno de los juegos abordó problemáticas específicas como el robo de información, el ciberacoso, la navegación insegura y la debilidad en las contraseñas, transformando estos riesgos en oportunidades de aprendizaje a través de la participación activa, la toma de decisiones y la reflexión crítica, de esta forma se consolidó una propuesta lúdica que no solo busca entretener, sino también sensibilizar y formar usuarios más conscientes, capaces de desenvolverse con responsabilidad y criterio en la era digital.

Resultados para el objetivo 3

Como parte del desarrollo del tercer objetivo del proyecto, orientado a prototipar los requerimientos fundamentales del software para su evaluación en términos de alcance, integridad y escalabilidad, se llevó a cabo la construcción de un prototipo web que materializa las ideas, dinámicas y funcionalidades definidas en las fases previas del diseño conceptual, este proceso permitió integrar de manera práctica los elementos teóricos, técnicos y pedagógicos relacionados con la ciberseguridad, facilitando la validación de la



propuesta dentro de un entorno interactivo y visualmente coherente con la identidad del proyecto.

A partir del análisis de los objetivos previos y de las necesidades detectadas en el público objetivo, se establecieron los requerimientos fundamentales que orientan el diseño y desarrollo del prototipo, dividiéndose en funcionales y no funcionales, definiendo tanto las acciones específicas que el sistema debe ejecutar como las características de calidad que garantizarán su desempeño, seguridad y escalabilidad.

Requerimientos Funcionales

- Módulos de Aprendizaje Interactivo:

El prototipo presenta la estructura de módulos educativos orientados a explicar conceptos fundamentales de ciberseguridad, tales como la creación de contraseñas seguras, la privacidad en redes sociales y la identificación de riesgos digitales, buscando adaptar el contenido de acuerdo con la edad y nivel de comprensión del usuario.

- Simulaciones y Escenarios Prácticos:

El diseño contempla espacios donde se integrarán las actividades interactivas y juegos educativos desarrollados, permitiendo al usuario tomar decisiones ante situaciones simuladas, los cuales se ilustran en el prototipo mediante pantallas, rutas de navegación y ejemplos de interacción que representan su funcionalidad.

- Panel de Control para Padres o Docentes:

Se proyecta un espacio administrativo donde se podrá visualizar el progreso y desempeño de los estudiantes, función que se deja representada de manera conceptual en el prototipo, indicando su futura integración dentro del sistema final.



- Gamificación y Motivación:

El prototipo incluye elementos visuales y conceptuales que simulan técnicas de motivación, como la implementación de niveles y un sistema de rachas, con el propósito de incentivar la participación del usuario y promover una experiencia de aprendizaje más dinámica e interactiva.

Requerimientos No Funcionales

- Usabilidad:

El prototipo fue diseñado con un enfoque en la facilidad de uso, priorizando la navegación intuitiva, la disposición clara de los elementos, el lenguaje visual comprensible y una estructura adaptada al público infantil y juvenil.

- Seguridad:

Aunque el prototipo no gestiona datos reales, su diseño considera principios de seguridad y privacidad digital, representando prácticas seguras en el uso de la información personal y promoviendo la concientización sobre la protección de datos.

- Accesibilidad:

El prototipo fue estructurado para visualizarse de forma adecuada en diferentes dispositivos (computadores, tabletas y teléfonos), simulando un entorno adaptable y accesible a distintos contextos educativos.

- Rendimiento y Escalabilidad:

La organización modular del contenido y la estructura del sitio permiten proyectar un desarrollo escalable, que podría alojar nuevos módulos, actividades o actualizaciones sin afectar la estabilidad general del sistema.

- Mantenibilidad y Actualización:



El diseño conceptual se elaboró con base en la reutilización de componentes visuales y secciones independientes, lo que facilita la actualización del contenido o la incorporación de nuevas temáticas sin alterar la coherencia estructural del software.

Seguidamente se desarrolló un prototipo de forma visual y funcional los requerimientos definidos previamente, integrando los aspectos pedagógicos, técnicos y de usabilidad planteados en el proyecto. Este prototipo busca evidenciar la estructura general del software educativo orientado a la formación en ciberseguridad, mostrando la distribución de contenidos, las rutas de navegación y los elementos interactivos que guiarán al usuario a través de los distintos módulos de aprendizaje.

Para la elaboración del prototipo interactivo se utilizó la plataforma Canva Web, una herramienta digital que permite la creación de sitios web funcionales de manera visual, rápida y accesible, la cual fue seleccionada debido a su capacidad para integrar elementos multimedia, animaciones, vínculos interactivos y diseños adaptativos, lo que facilita la representación del flujo de navegación y la disposición visual de los módulos educativos.

El diseño general del prototipo se estructuró con base en la organización de los módulos educativos definidos en los requerimientos funcionales, buscando reflejar una experiencia de navegación fluida, atractiva y coherente con los objetivos pedagógicos del proyecto, en la cual su interfaz principal se compone de una página de inicio que presenta la identidad visual del software, su propósito educativo y un acceso directo a las actividades y juegos diseñados, representando de forma clara la temática de la ciberseguridad.

Figura 1 Pantalla principal del prototipo “SafeWeb”



Figura 1. En la pantalla de inicio se muestra la identidad visual del software y el acceso directo a las actividades educativas. *Elaboración propia (2025).*

Como se observa en la Figura 1, la pantalla de inicio combina elementos visuales llamativos con un lenguaje accesible para el público joven, integrando colores contrastantes, tipografía moderna y un menú interactivo que facilita el acceso a las diferentes secciones. Además, se resalta el mensaje principal “Desarrolla tus habilidades digitales”, acompañado de un llamado a la acción que invita al usuario a practicar mediante actividades lúdicas



relacionadas con la ciberseguridad, buscando captar la atención del usuario desde el primer momento y orientar su navegación de manera intuitiva dentro del entorno educativo digital.

Asimismo, se evidencia la opción de iniciar sesión o registrarse, lo que permitirá en futuras fases del desarrollo vincular los avances del usuario con un perfil individual, posibilitando un seguimiento personalizado del progreso dentro de la plataforma. También se incorpora una llama en la parte superior, que representa el registro de actividades o “racha”, funcionando como un elemento de motivación lúdica orientado a incentivar la constancia y participación continua del usuario en las distintas actividades educativas, fortaleciendo su compromiso con el aprendizaje y el desarrollo de competencias digitales seguras.

La pantalla de inicio de sesión fue diseñada con un enfoque minimalista y funcional, priorizando la claridad en los campos de ingreso y la facilidad de uso, permitiendo que el usuario introduzca sus credenciales de manera rápida y sencilla, con opciones visibles para recuperar la contraseña o acceder al registro en caso de no contar con una cuenta (ver Figura 2).

Figura 2 Pantalla de Login



Figura 2. Pantalla de inicio de sesión del prototipo SAFE WEB. elaboración propia, (2025).

Por su parte, la pantalla de registro incorpora campos básicos como nombre de usuario, edad, correo electrónico y contraseña, permitiendo la creación de un perfil personalizado dentro de la plataforma, reforzando el objetivo pedagógico del prototipo al ofrecer una experiencia clara y orientada a un público joven, donde se prioriza la simplicidad en el proceso de registro y la coherencia con la estética general del sitio (ver Figura 3).

Figura 3 Pantalla de Registro

Figura 3. Pantalla de registro del prototipo SAFE WEB. elaboración propia (2025).

En la pantalla de progreso y motivación se incorpora un elemento visual distintivo representado por una llama acompañada de un contador numérico, el cual simboliza la racha de participación del usuario, es decir, el número de días consecutivos en los que el jugador ha ingresado y completado actividades dentro de la plataforma. Este componente cumple una doble función, ya que además de servir como registro visual del compromiso del

usuario, actúa como un mecanismo de gamificación que incentiva la constancia y la interacción continua con los contenidos educativos (ver figura 4).

Figura 4 Pantalla de la "racha"



Figura 4. Pantalla de progreso con racha del prototipo SAFE WEB. elaboración propia (2025).

Como se observa en la figura 4, este diseño integra un calendario dinámico en el cual se resaltan los días activos mediante el ícono de la llama, reforzando la idea de progreso y logro personal, lo cual contribuye a mantener la motivación del usuario frente al proceso de aprendizaje digital.

Las actividades interactivas del prototipo SAFE WEB constituyen el eje central del aprendizaje, ya que permiten que los usuarios fortalezcan sus conocimientos sobre ciberseguridad mediante dinámicas lúdicas y entornos simulados, orientados al desarrollo del pensamiento crítico y la toma de decisiones frente a situaciones digitales cotidianas.

Estas actividades se organizan en cuatro juegos principales, cada uno diseñado para abordar

temáticas específicas relacionadas con la protección en línea, la privacidad, la seguridad de la información y la conducta responsable en entornos virtuales, promoviendo una experiencia educativa más participativa y significativa.

Figura 5 Pagina Inicial juegos



Figura 5. Pantalla de inicio para la entrada a los juegos. elaboración propia (2025).

Como se observa en la figura 5, el menú principal presenta los accesos directos a cada una de las actividades diseñadas, destacando los juegos “Coffe Security”, “Detectores de Peligro”, “Hunting” y “Gu@rdianes de Cl@ves”, los cuales se encuentran organizados de manera visualmente equilibrada, facilitando la navegación y fomentando la exploración del usuario a través de un entorno colorido, claro y coherente con la identidad gráfica del proyecto.

Asimismo, se tiene que en la figura 6 se ve la pantalla de confirmación al juego seleccionado el cual se da para convalidar la decisión del usuario y de ahí si continua al juego seleccionado.

Figura 6 Pantalla de confirmación.

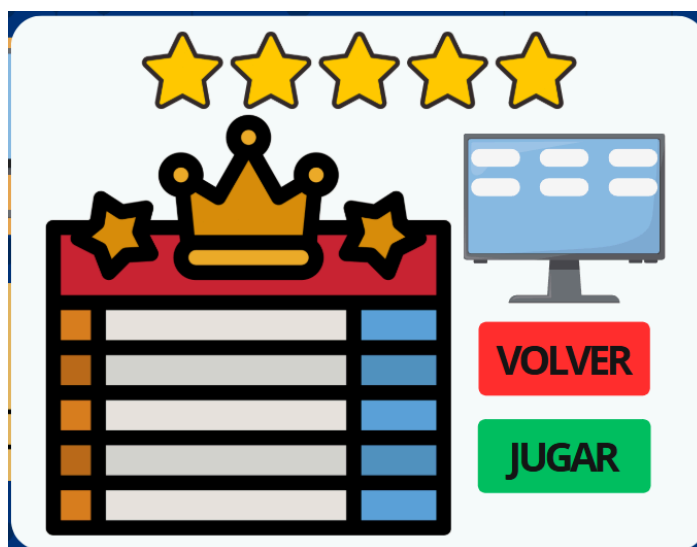


Figura 6. Pantalla de confirmación a la selección de juego. elaboración propia (2025).

Diseño del juego 1: Cofee Security

El primer juego, denominado *Cofee Security*, está diseñado con el propósito de fortalecer las habilidades de los usuarios en la identificación de amenazas digitales y la toma de decisiones seguras en entornos virtuales, donde el jugador asume el rol de un administrador encargado de supervisar varios equipos informáticos, decidiendo si permitir o bloquear el acceso a páginas web sospechosas.

En la Figura 6 se presenta la pantalla principal del juego, donde se observa el entorno de trabajo del usuario compuesto por varios equipos conectados en red, introduciendo al jugador al contexto del reto y mostrando la interfaz general que simula un entorno informático real.

Figura 7 Pantalla principal del juego Cofee Security.



Figura 7. Pantalla de inicio juego Cofee Security. elaboración propia (2025).

La Figura 8 presenta un ejemplo de página sospechosa, en la cual el jugador debe determinar si se trata de un sitio legítimo o de una amenaza potencial. Para ello, aplica sus conocimientos sobre ciberseguridad, identificando señales de alerta como direcciones URL irregulares, ventanas emergentes o mensajes engañosos.

Figura 8 Pagina web Maliciosa



Figura 8. Pantalla de web maliciosa dentro del juego. elaboración propia (2025).

En la Figura 9 y 10 se ilustra la retroalimentación inmediata que el sistema ofrece tras una decisión correcta o incorrecta respectivamente, mostrando mensajes motivacionales y un incremento en la puntuación si se realizó la decisión correcta, sin embargo, si se escogió la respuesta errónea hay una disminución en la puntuación.

Figura 9 Decisión correcta



Figura 9. Pantalla de cuando se realiza una decisión correcta. elaboración propia (2025).

Figura 10 Decisión incorrecta



Figura 10. Pantalla de cuando se escoge la opción incorrecta. elaboración propia (2025).

Diseño del juego 2: Detectores de peligro

El siguiente juego se llama “Detectores de peligro” el cual permite al usuario analizar una lista de sitios web que simula un historial de navegación, en la que debe determinar cuáles páginas son seguras y cuáles representan un posible riesgo. Esta dinámica

busca fortalecer la capacidad de los estudiantes para identificar enlaces sospechosos o direcciones que no cumplen con los estándares de seguridad digital, fomentando la atención al detalle y el pensamiento crítico frente a posibles ataques de phishing. (ver figura 11)

Figura 11 Historial de navegación en Safe Web.

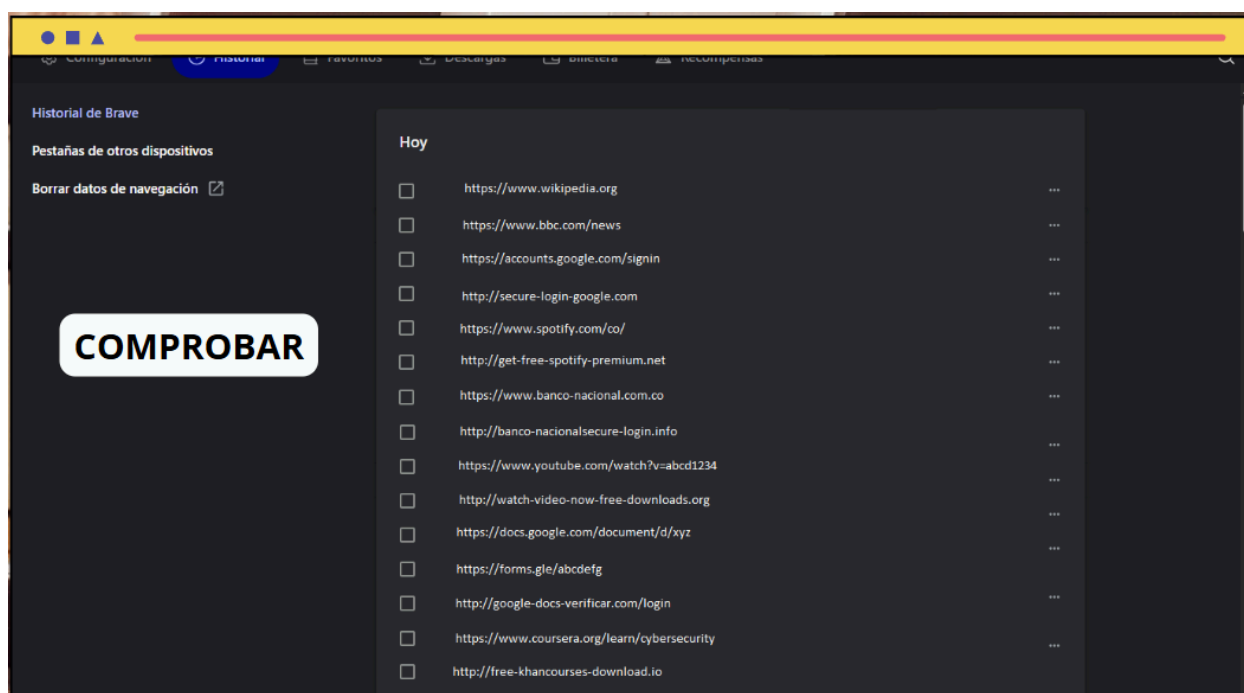


Figura 11. Pantalla del historial de búsqueda. elaboración propia (2025).

En la Figura 12 se muestra la misma actividad después de que el usuario ha realizado la comprobación, destacando las páginas marcadas como inseguras con un ícono distintivo. Este diseño proporciona retroalimentación visual inmediata, permitiendo al participante contrastar sus respuestas y aprender de los errores cometidos, reforzando su criterio frente a la navegación segura.

Figura 12 Retroalimentación visual.

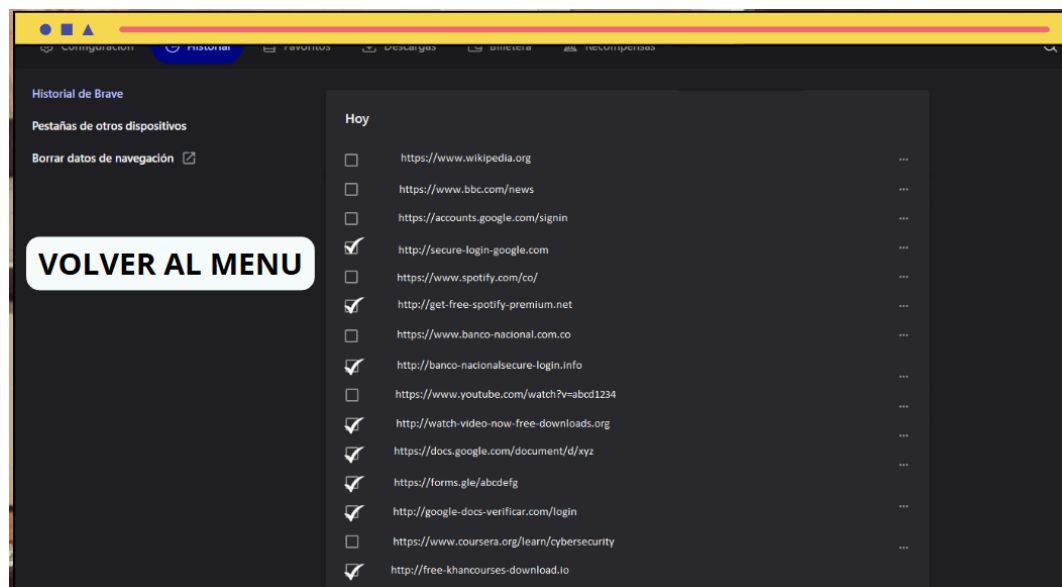


Figura 12. Pantalla de cuando da la retroalimentación de páginas maliciosas. elaboración propia (2025).

Diseño del juego 3: Gu@rdianes de cl@ves

Para esta actividad, el participante debe analizar un caso en el que se presenta información personal y laboral de una persona, con el fin de elegir, entre varias opciones, la contraseña que resulte más segura, fomentando la reflexión sobre los riesgos de utilizar datos fácilmente identificables, como nombres, gustos o fechas importantes, asimismo con una cantidad de cinco rondas en las cuales el contexto varia, disponiendo también de un tiempo de 30 segundos por ronda. (figura 13)

Figura 13 Presentacion pregunta y opciones.

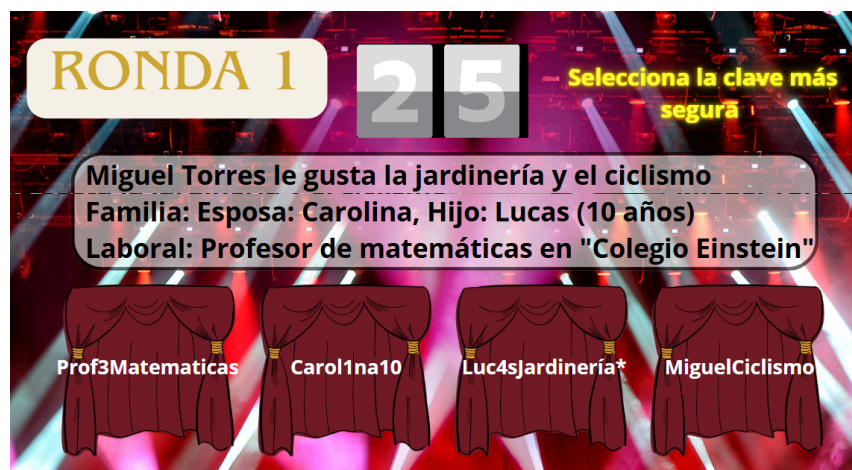


Figura 13. En esta actividad, el participante debe identificar cuál de las contraseñas presentadas es la más segura según las buenas prácticas de ciberseguridad. elaboración propia (2025).

En esta sección se muestra la retroalimentación de la actividad, indicando si la selección realizada fue correcta o incorrecta, lo que permite al participante identificar los errores cometidos, comprender con mayor claridad los criterios que hacen que una contraseña sea segura y reforzar el aprendizaje práctico, fortaleciendo la capacidad de aplicar estos conocimientos en situaciones reales antes de avanzar a la siguiente ronda.

Figura 14 Retroalimentación de la actividad Contraseñas

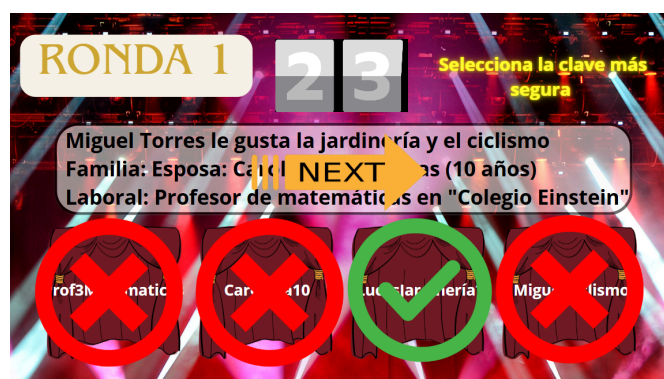


Figura 14. Se muestra la respuesta correcta y el botón para la siguiente ronda. elaboración propia (2025).

Diseño del juego 4: Hunting

Esta actividad coloca al usuario en un escenario interactivo en el que recibe un mensaje de una persona desconocida, simulando una situación frecuente en redes sociales o aplicaciones de mensajería. El participante debe analizar el contexto del mensaje y tomar una decisión responsable entre dos opciones: continuar la conversación o reportar el chat. De este modo, se busca fomentar la conciencia sobre los riesgos de compartir información personal con desconocidos, reforzando la precaución, la desconfianza ante contactos no identificados y la capacidad de reconocer señales de posible acoso o fraude digital. (ver figura 15)

Figura 15 Página principal Juego "Hunting"

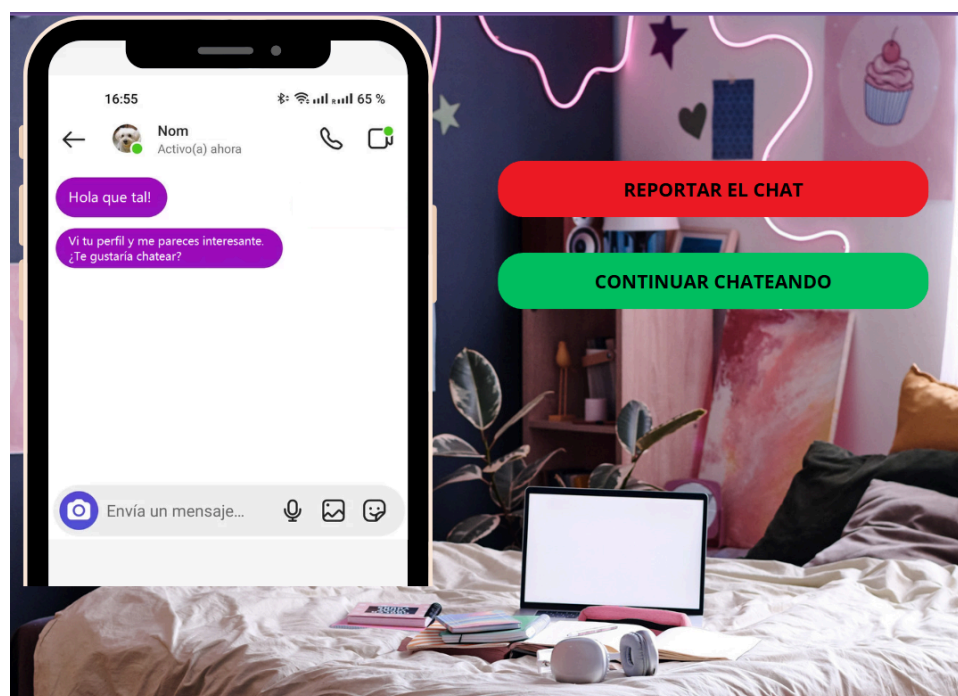


Figura 15. Pantalla principal “hunting”, inicio del chat. elaboración propia (2025).

A continuación, se presentan dos pantallas diferentes, cada una correspondiente a una posible decisión del usuario dentro de la actividad. La primera pantalla muestra el caso

en el que el chat de la persona desconocida es reportado de forma anticipada (Figura 16), destacando los elementos visuales que indican que la acción se realizó correctamente, como mensajes de confirmación y señales que refuerzan la conducta responsable dentro del entorno simulado.

Figura 16 Pantalla Victoria anticipada



Figura 16. Pantalla Victoria anticipada. elaboración propia (2025).

Por otro lado, la segunda pantalla refleja la situación en la que el usuario no logra identificar los mensajes maliciosos, mostrando los indicadores de alerta y la retroalimentación visual que señala que el objetivo no se alcanzó.

Figura 17 Pantalla de demora en identificación de mensajes



Figura 17. Pantalla de pérdida del juego. elaboración propia (2025).

La última pantalla visible en este juego corresponde a la correcta identificación de los mensajes maliciosos, como se muestra en la Figura 18, evidenciando que el usuario ha logrado reconocer las señales de riesgo y ha tomado la decisión adecuada dentro del escenario simulado

Figura 18 Correcta identificación de mensajes



Figura 18. Pantalla de Identificación precisa de mensajes maliciosos. elaboración propia (2025).



Evaluación del prototipo

El prototipo cumple con los objetivos planteados, integrando de manera práctica los conceptos de ciberseguridad definidos en la fase de diseño conceptual, abarcando temáticas como contraseñas seguras, navegación segura y detección de amenazas digitales, y permitiendo que el público objetivo, compuesto por niños y adolescentes, interactúe con los contenidos mediante actividades lúdicas y simulaciones que refuerzan el aprendizaje de forma significativa, además, su estructura modular facilita la incorporación de nuevos juegos o contenidos adicionales, asegurando un alcance escalable y la posibilidad de expansión en futuras implementaciones.

Asimismo, demuestra coherencia entre sus componentes visuales, textuales y pedagógicos, combinando elementos gráficos atractivos, tipografía clara y menús interactivos que facilitan la navegación, de manera que la experiencia del usuario se mantiene uniforme, con transiciones fluidas entre pantallas de inicio, login, registro, progreso, selección de juegos y actividades educativas.

Finalmente, el prototipo fue desarrollado de forma modular, lo que permite su migración futura a otras plataformas como HTML o React, así como la incorporación de nuevos módulos y contenidos sin afectar la estabilidad general del sistema, además, la representación visual y funcional de la navegación y los elementos interactivos mediante Canva Web garantiza que el prototipo se adapte a distintos dispositivos y contextos educativos.

El prototipo SAFE WEB logró materializar de manera efectiva los requerimientos fundamentales definidos en el proyecto, integrando de forma coherente elementos pedagógicos, técnicos y de usabilidad, lo que permite evaluar su alcance, integridad y escalabilidad, además, la evaluación evidenció que el prototipo proporciona una experiencia de aprendizaje interactiva y



motivadora, refuerza el pensamiento crítico frente a la ciberseguridad y constituye una base sólida para futuras implementaciones, de esta manera, los resultados confirman que el prototipo constituye un punto de partida confiable para el desarrollo de un software educativo funcional, escalable y adaptable a distintos contextos y plataformas.

Prototipo #2

Con base en el diseño conceptual previamente planteado, se procedió a la construcción técnica del prototipo web SAFE WEB, materializando las ideas funcionales y pedagógicas del proyecto en un entorno navegable e interactivo. Esta etapa tuvo como propósito representar de manera práctica las funcionalidades esenciales del software, evidenciando su estructura, flujo de navegación y comportamiento general ante las acciones del usuario, permitiendo así evaluar el alcance y la viabilidad del sistema propuesto. El desarrollo se centró en la implementación de interfaces intuitivas, componentes dinámicos y simulaciones que reflejan los escenarios educativos diseñados, integrando la teoría de la ciberseguridad con una experiencia digital que facilita la comprensión de los riesgos y prácticas seguras en línea.

El desarrollo del prototipo SAFE WEB se realizó utilizando principalmente los lenguajes de programación HTML, CSS y JavaScript, seleccionados por su accesibilidad, compatibilidad multiplataforma y facilidad de integración en entornos web educativos. HTML permitió estructurar de manera clara los contenidos y elementos visuales del sitio, garantizando una disposición ordenada de los módulos y actividades.

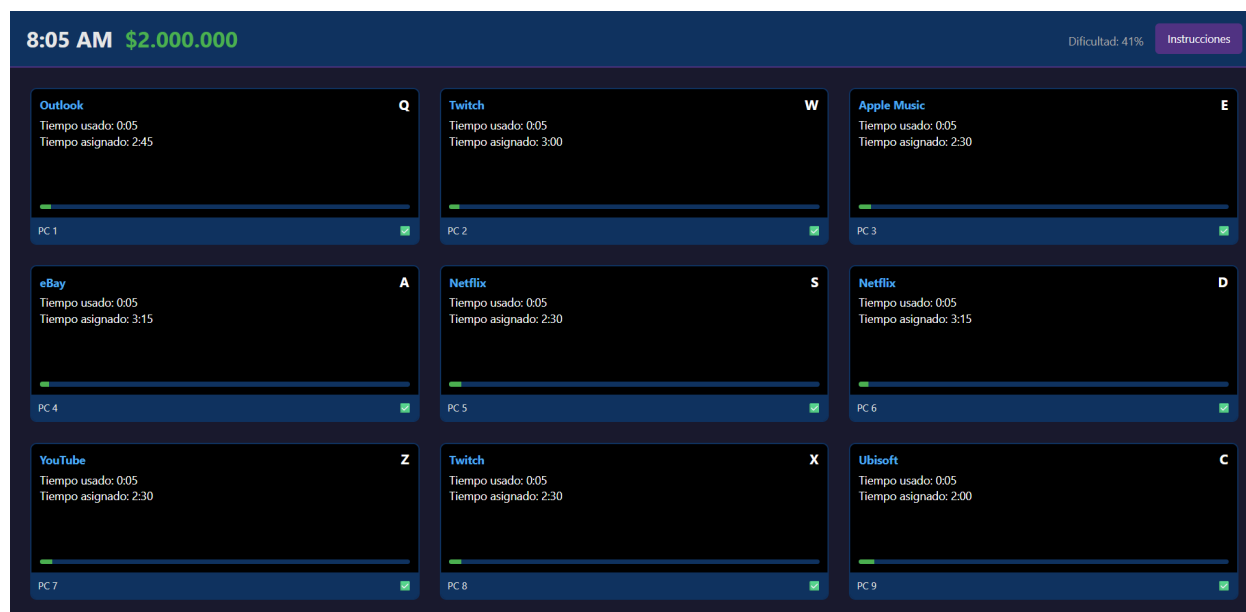
Figura 19 Index.html



Como se observa en la figura 19, la página principal del prototipo SAFE WEB muestra la identidad visual del sistema, organizada en un entorno digital pensado para captar la atención de un público infantil y adolescente, donde predominan los colores azul y amarillo que simbolizan confianza y dinamismo. En esta pantalla se presenta el mensaje “Desarrolla tus habilidades digitales”, que introduce al usuario a las actividades prácticas de ciberseguridad, acompañadas de imágenes ilustrativas que refuerzan el componente educativo del proyecto.

Asimismo, esta interfaz sirve como punto de acceso a los diferentes módulos de práctica, integrando un diseño adaptable, limpio y accesible que promueve una experiencia de navegación clara y amigable, en coherencia con los principios de usabilidad definidos en los requerimientos funcionales y no funcionales.

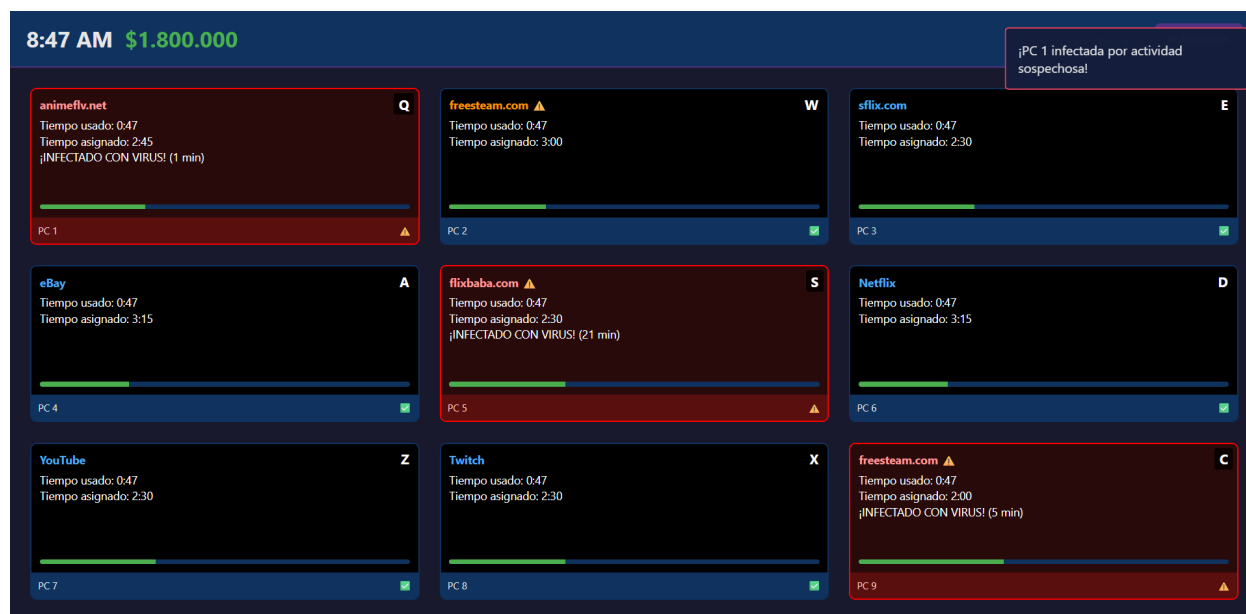
Figura 20 Prototipo COFFEE SECURITY



En la figura 20 se observa el entorno interactivo del juego “Coffee Security”, diseñado como una simulación en la que el usuario asume el rol de un encargado de seguridad digital en un entorno de oficina. En este escenario, se visualizan diferentes equipos informáticos representados por cuadros o paneles que contienen información de servicios y plataformas, tales como correos electrónicos o aplicaciones en línea, junto con indicadores de tiempo y progreso.

El propósito de esta actividad es fomentar la identificación rápida de amenazas y la toma de decisiones ante eventos de riesgo, permitiendo al jugador comprender la importancia del monitoreo constante de la seguridad informática. Además, el diseño de la interfaz se basa en principios de claridad visual, contraste de colores y retroalimentación inmediata, con el fin de mantener la atención del usuario y favorecer el aprendizaje a través de la acción.

Figura 21 COFFEE SECURITY EN JUEGO



La figura 3 representa el momento en que el sistema detecta amenazas dentro del entorno del juego, destacando visualmente los equipos comprometidos mediante el uso de colores de alerta, mensajes emergentes y cambios en el estado de los paneles., este interfaz visual busca reproducir situaciones reales en las que el usuario debe identificar comportamientos sospechosos o infecciones de malware, reforzando así la toma de decisiones en contextos digitales simulados. De esta manera, el juego no solo promueve el reconocimiento de señales de riesgo, sino que también estimula la reflexión sobre las consecuencias de la navegación insegura y el uso irresponsable de los recursos tecnológicos.

Para la visualización del código fuente y la estructura completa del prototipo SAFE WEB, se dispuso un repositorio en la plataforma GitHub, donde se encuentran los archivos desarrollados y su organización interna, permitiendo revisar el funcionamiento técnico, la lógica de programación y los componentes visuales implementados en el proyecto, el cual puede



consultarse a través del siguiente enlace:

<https://github.com/JulianAlfonso3845/SecurityWeb---Prototype>

Conclusiones

Las amenazas cibernéticas son prácticamente imposibles de evitar al cien por ciento, la única forma sería tener dispositivos que estén completamente fuera de línea, por ello identificar las amenazas más puntuales que pueden tratar de vulnerar a la población de niños y adolescentes, es esencial en un mundo cada vez más metido y dependiente del sector tecnológico.

Igualmente, el empleo de mecánicas educativas como la planteada para este proyecto, puede que no mitigue en su totalidad las lagunas de información sobre ciberseguridad en los más jóvenes, sin embargo, al igual que otras aplicaciones similares que educan en diversos temas, como Duolingo orientado a los idiomas, logran disminuir el desconocimiento, en el caso de la aplicación diseñada muestra conocimientos básicos en mecánicas y tácticas básicas de seguridad que reducen, así sea en una pequeña medida, la probabilidad de sufrir un ataque cibernético serio y puede motivar a los más jóvenes a indagar más en estos temas.

Se hizo un trabajo de diseño y un breve trabajo de desarrollo, aunque este último no se presenta con el avance completo, a fin de cuentas, hubo un centro de atención en un diseño más claro, entre el diseño y el desarrollo del software presentados son suficientes para mostrar el alcance y, a su vez, como un desarrollo completo podría generar el impacto esperado y postulado.

Bibliografía

- Acevedo-Rincón Jenny Patricia, & Flórez Pabón Campo Elías. (2022). Children's lives in times of pandemic: experiences from Colombia. *Children's Geographies*, 20, 404–411.
<https://doi.org/10.1080/14733285.2022.2078655>
- Alvites-Huamaní, C. G., Stanziola, M., & Rojas-Montero, J. A. (2024). Knowing Me: Web Application for Mood Screening in Childhood and Adolescence. *Lecture Notes in Educational Technology*, 356–365.
<https://www-scopus-com.bdbiblioteca.universidadean.edu.co/record/display.uri?eid=2-s2.0-85201952076&origin=resultslist&sort=plf-f&src=s&sot=b&sdt=b&s=TITLE-ABS-KEY%28colombia+AND+technology+AND+children%29&sessionSearchId=d619211505ea56fa1d23d6597ebc0c30&relpos=11>
- Andrea, J., Pineda, G., Ríos Hernández, G., Andrés, M., Bonilla, T., & Barreto Florez, L. (2024). *Desarrollo de una Guía de Ciberseguridad para la Protección de Estudiantes*.
<https://repository.universidadean.edu.co/items/1973c8fd-e0be-45eb-9b5e-4811b47fea63>
- Ávalos Mariano, & Borba Domingo. (2023). *Inteligencia artificial en ámbitos educativos: propuestas para el trabajo en el aula* (1a edición.). Buenos Aires: Bonus Books.
- Babilonia Ospina, A., Fernando Garcés-Giraldo, L., Valencia-Arias, A., Camila Bermeo-Giraldo, M., Gómez-Bayona, L., Camilo Patiño-Vanegas, J., & Bao García, R. (2023). *Tendencias investigativas en ciberseguridad del Internet de las Cosas (IoT)*.
<https://www-proquest-com.bdbiblioteca.universidadean.edu.co/docview/2880949498/fulltextPDF/5D65961B26EC49A8PQ/1?accountid=34925&sourcetype=Scholarly%20Journals>
- Belkhir L. (218 C.E.). Assessing ICT global emissions footprint: Trends to 2040 & recommendations. *Clear Production*, 177, 448–463.
<https://www.sciencedirect.com/science/article/abs/pii/S095965261733233X>
- Coeckelbergh, M. (2021). *Ética de la inteligencia artificial* (Difusora Larousse, Vol. 1).
<https://elibro-net.bdbiblioteca.universidadean.edu.co/es/ereader/bibliotecaean/216546>
- Correa Villar, M. C., & Vargas Escobar Liliana Patricia. (2024). PROPUESTA DE FORMACIÓN EN LENGUAJES DE PROGRAMACIÓN EN LA TECNOLOGIA VIRTUAL DE ANÁLISIS Y DESARROLLO DE SOFTWARE DEL SENA. *Universidad EAN*.
<https://repository.universidadean.edu.co/entities/publication/0416887d-b55e-40ee-8598-b6c2c343ec3c>
- Danah M. Boyd, & Nicole B. Ellison. (2001). Social Network Sites: Definition, History, and Scholarship. *Oxford Academic*, 13(1).
<https://academic.oup.com/jcmc/article/13/1/210/4583062>



- Dane. (2023). *Indicadores básicos de TIC en Hogares*. Indicadores Básicos de TIC En Hogares. <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>
- De Zan, Tommaso., & Di Franco, Fabio. (2019). *Cybersecurity skills development in the EU : the certification of cybersecurity degrees and ENISA's Higher Education Database*. ENISA. <https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union>
- Decreto 338 de 2022 (2022). <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866>
- Departamento nacional de planeación. (2022). *Plan Nacional de Desarrollo 2022-2026*. Plan Nacional de Desarrollo 2022-2026. <https://www.dnp.gov.co/plan-nacional-desarrollo/pnd-2022-2026>
- EFE News Services. (2023). Un 43 % de niños latinoamericanos está expuesto a riesgos digitales, alertan los expertos: LATINOAMÉRICA CIBERSEGURIDAD. *EFE News Services, Inc.*, 2886623652, 1–2. <https://login.bdbiblioteca.universidadean.edu.co/login?url=https://www-proquest-com.bdbiblioteca.universidadean.edu.co/wire-feeds/un-43-de-niños-latinoamericanos-está-expuesto/docview/2886623652/se-2>
- El Congreso de Colombia. (1995). *Ley 222 de 1995*. Ley 222 de 1995. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6739>
- El Congreso de Colombia. (2000). *Ley 603 de 2000*. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=13960>
- Equipo editorial de Indeed. (2024, June 28). *10 herramientas de desarrollo de software preferidas por los desarrolladores*. Indeed. <https://es.indeed.com/orientacion-laboral/desarrollo-profesional/herramientas-desarrollo-software>
- Escobar M. W. (2024). *Análisis a la Brecha Digital en la Educación Colombiana*.
- FasterCapital. (2025, May 14). *Costo y presupuesto para gastos de tecnología educativa El verdadero costo de la tecnología educativa una guía completa*. Costo y Presupuesto Para Gastos de Tecnología Educativa El Verdadero Costo de La Tecnología Educativa Una Guía Completa. <https://fastercapital.com/es/contenido/Costo-y-presupuesto-para-gastos-de-tecnologia-educativa--El-verdadero-costo-de-la-tecnologia-educativa--una-guia-completa.html>
- Figuerola A. A. (2009). *MeISE: Metodología de Ingeniería de Software Educativo*.
- Freitag, C., Berners-Lee, M., Widdicks, K., Knowles, B., Blair, G. S., & Friday, A. (2021). The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations. *Cell Press*, 2(9). <https://www.sciencedirect.com/science/article/pii/S2666389921001884>
- Fujita, Hamido., & Zualkernan, Imran. (2008). *New trends in software methodologies, tools and techniques*. IOS Press.
- Gabriel Pacienza, E., & Pacienza, J. (2015). *METODOLOGIAS DE DESARROLLO DE SOFTWARE*. <https://repositorio.uca.edu.ar/bitstream/123456789/522/1/metodologias-desarrollo-software.pdf>
- García D. (2022, July 1). *Bogotá registra aumento histórico en conexión a Internet y disminución en pobreza rural multidimensional*. Secretaria de Planeación de Bogotá.

- <https://www.sdp.gov.co/noticias/bogota-registra-aumento-historico-conexion-a-internet-y-disminucion-pobreza-rural-multidimensional>
- Giacconi Brenda. (2025). *Un juego de Steam ha estado infectando los PC de los jugadores con malware. Valve ya lo ha eliminado, pero los que jugaron a PirateFi deben seguir unos consejos*.
<https://www.3djuegos.com/pc/noticias/juego-steam-ha-estado-infectando-pc-jugadores-malware-valve-ha-eliminado-que-jugaron-a-piratefi-deben-seguir-unos-consejos>
- González, S. A., Rubio, M. A., Triana, C. A., King, A. C., Banchoff, A. W., & Sarmiento, O. L. (2022). Building healthy schools through technology-enabled citizen science: The case of the our voice participatory action model in schools from Bogotá, Colombia. *Global Public Health*, 17(3), 403–419.
- Hinojo-Lucena, F. J., Aznar-Díaz, I., Cáceres-Reche, M. P., Trujillo-Torres, J. M., & Romero-Rodríguez, J. M. (2020). Sharenting: Internet addiction, self-control and online photos of underage children. *Comunicar*, 28(64), 93–103.
<https://doi.org/10.3916/C64-2020-09>
- Hofstede, G. (2011). Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture*, 2(1). <https://doi.org/10.9707/2307-0919.1014>
- Hoyos-Cifuentes John D., Fernández-Otoya, F. A., Rodríguez-Gómez, W. F., & Bernal-Torres, C. A. (2024). Emotional intelligence, human values, creation and dissemination of content on social networks by girls in countries with emerging economies. *International Journal of Adolescence and Youth*, 29. <https://doi.org/10.1080/02673843.2024.2306886>
- Itu. (2020). *Global Cybersecurity Index 2020 Measuring commitment to cybersecurity Acknowledgements*. <https://www.itu.int/pub/D-STR-GCI.01-2021>
- Jimenezb, I. (2025). 11 herramientas de desarrollo de software que te harán más productivo. *Ubiquum*.
<https://ubiquum.com/11-herramientas-de-desarrollo-de-software-que-te-haran-mas-productivo/>
- Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 53(1), 59–68.
<https://doi.org/10.1016/j.bushor.2009.09.003>
- Lenis Trujillo, D. F. (2024). Generation of guidelines for a public policy proposal to guide advertising aimed at children between 2 and 10 years of age as its target market for the prevention of harmful effects on them. *Estudios de Derecho*, 81(177), 72–93.
<https://doi.org/10.17533/udea.esde.v81n177a4>
- LEY 1273 DE 2009 (2009).
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492>
- Ley 1620 de 2013 (2013).
<https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1685356>
- LIZARAZO SINDY JOHANNA, TÉLLEZ BURGOS DEICY MARCELA, & TÉLLEZ BURGOS PAOLA ANDREA. (2021). LAS CAUSAS DEL USO EXCESIVO DE LAS TIC EN LOS NIÑOS Y LAS NIÑAS . *CORPORACIÓN UNIVERSITARIA IBEROAMERICANA*, 1.
<https://repositorio.iberu.edu.co/server/api/core/bitstreams/ef238b4b-09d4-4cd6-8349-a59d3305c660/content>
- López-Gil, K. S., & Franco-Chávez, F.-P. (2021). Promoting children's literature online: Practices of a booktuber girl. *OCNOS*, 20(1), 50–64.

- <https://www-scopus-com.bdbiblioteca.universidadean.edu.co/record/display.uri?eid=2-s2.0-85109733514&origin=resultslist&sort=plf-f&src=s&sot=b&sdt=b&s=TITLE-ABS-KEY%28colombia+AND+technology+AND+children%29&sessionSearchId=d619211505ea56fa1d23d6597ebc0c30&relpos=63>
- López-Ordosgoitia, R., Piracón-Fajardo, J.-A., Arias, V., & Giraldo-Cadavid, D.-A. (2025). Parental Mediation in Children's Use of Mobile Devices: A Comparative Study Between Argentina and Colombia. *Revista Mediterranea de Comunicacion*, 16(1).
<https://www-scopus-com.bdbiblioteca.universidadean.edu.co/record/display.uri?eid=2-s2.0-85214094602&origin=resultslist&sort=plf-f&src=s&sot=b&sdt=b&s=TITLE-ABS-KEY%28colombia+AND+technology+AND+children%29&sessionSearchId=d619211505ea56fa1d23d6597ebc0c30&relpos=2>
- Martínez B. M. (2016). *INTERACCIONES INFLUIDAS POR EL USO DE TICS, EN FAMILIAS CON HIJOS ADOLESCENTES EN LA CIUDAD DE BOGOTÁ*.
- Ministerio las TIC. (2024). *Índice de Brecha Digital 2023*.
https://colombiatic.mintic.gov.co/679/articles-238353_recurso_4.pdf
- Montes, P. A. T., Morales, V. T., & Duque-Méndez, N. D. (2024). Esmeralda: Support for Early Detection and Initial Intervention of Dyslexia in First-Grade Students Through the Development of Digital Educational Resources. *Communications in Computer and Information Science*, 2209, 228–244.
<https://www-scopus-com.bdbiblioteca.universidadean.edu.co/record/display.uri?eid=2-s2.0-85214019467&origin=resultslist&sort=plf-f&src=s&sot=b&sdt=b&s=TITLE-ABS-KEY%28colombia+AND+technology+AND+children%29&sessionSearchId=d619211505ea56fa1d23d6597ebc0c30&relpos=7>
- Muñoz, A. B. (2024). Educate and protect: analysis of cybersecurity education to combat cybercrime. *Revista de Educacion y Derecho*, 30.
<https://doi.org/10.1344/REYD2024.30.44082>
- National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. <https://doi.org/10.6028/NIST.CSWP.04162018>
- Patricia, E., & Gallo, P. (2024). *Actas Iberoamericanas en Ciencias Sociales Volumen 2 (I) enero-diciembre 2024*. <https://plagcis.com/journal/index.php/aicis/article/view/28>
- Pons Gamon, V. (2017). Internet, la nueva era del delito: cibercrimo, ciberterrorismo, legislación y ciberseguridad/ Internet, the new age of crime: cybercrime, cyberterrorism, legislation and cybersecurity. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, 20, 80.
<https://doi.org/10.17141/urvio.20.2017.2563>
- Quintero R., J., & Cristancho D., F. (2024). *Estrategias para alfabetización de adolescentes en Colombia dentro del ecosistema digital*.
<https://repository.universidadean.edu.co/bitstream/handle/10882/13851/QuinteroJeizon2024.pdf?sequence=1>
- Reyna Ramos, D., & Olviera Gómez, D. A. (2016). *Las amenazas cibernéticas*.
<https://universita.ux.edu.mx/universita-ciencia/article/view/220>
- Román Aguilar, M. M., Jumbo Castillo, E. M., Cunalata, M. Á., Tusa Jumbo, F. E., & Maza Cordova, J. (2023). Utilización de tecnologías educativas en el proceso de enseñanza-aprendizaje de asignaturas en ciencias. Estudio de caso: software educativo Exploración de la Efectividad de los Recursos Educativos Abiertos. *Ciencia Latina Revista Científica Multidisciplinar*, 7(4), 3436–3453. https://doi.org/10.37811/cl_rcm.v7i4.7195



- Ronald W. Rogers. (2010). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology* , 91(1).
<https://www.tandfonline.com/doi/abs/10.1080/00223980.1975.9915803>
- Scott D. Applegate. (2009). Social Engineering: Hacking the Wetware! *Information Security Journal: A Global Perspective*, 18(1), 40–46.
<https://www-tandfonline-com.bdbiblioteca.universidadean.edu.co/doi/full/10.1080/19393550802623214#abstract>
- Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly: Management Information Systems*, 34(SPEC. ISSUE 3), 487–502. <https://doi.org/10.2307/25750688>
- Slovic Paul. (1987). Perception of Risk. *Science*, 236(4799), 280–285.
<https://www.science.org/doi/10.1126/science.3563507>
- Universidad de los Andes. (2024). *Riesgos y Oportunidades del Uso de Internet para Niñas, Niños y Adolescentes en Colombia*.
<https://www.contigoconectados.com/wp-content/uploads/2024/03/RIESGOS-Y-OPORTUNIDADES-DEL-USO-DE-INTERNET-PARA-NNA-EN-COLOMBIA-RESUMEN-DE-RESULTADOS-V-FINAL.pdf>
- Whitman Michael, & Mattord Herbert. (2022). *Principles of Information Security* (7th ed., Vol. 1). Cengage.
<https://www.cengage.com/c/principles-of-information-security-7e-whitman-mattord/9780357506431/>