Ensayo: Ciencias del aprendizaje, Gamificación, aprendizaje personalizado (IA) y Seguridad en el SPEI: Una Propuesta de Inclusión Financiera Digital

1. Introducción y problemática detectada

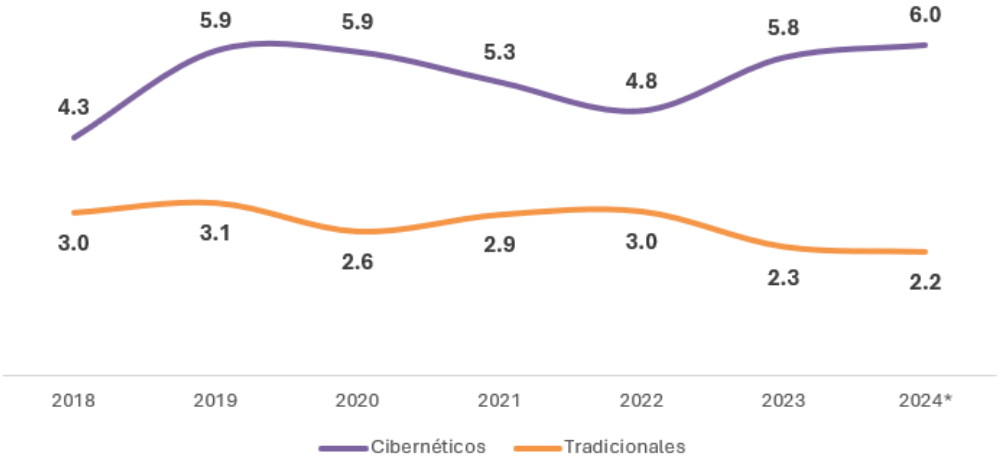
En la vida digital actual, la seguridad informática se ha convertido en una prioridad, principalmente para la población adulta. Los ataques basados en técnicas de ingeniería social, que manipulan a las personas para obtener información confidencial, son cada vez más sofisticados. Tradicionalmente, la capacitación en seguridad se ha centrado en métodos teóricos que a menudo resultan ineficaces para adultos con diferentes niveles de conocimiento tecnológico y estilos de aprendizaje.

Esto en una propuesta innovadora y altamente efectiva para abordar esta problemática de ciberseguridad. El objetivo principal es crear una herramienta que nos ayude a medir el nivel de peligro que puede llegar a correr una persona y no solo transmite información, sino que también transforma el comportamiento y fortalece la capacidad de los adultos para protegerse contra los ciberataques.

En México los fraudes cibernéticos relacionados con el phishing y otras formas de ingeniería social representan una de las principales amenazas para las personas.

De acuerdo a cifras de “The Competitive Intelligence Unit” (The CIU) aproximadamente 13.5 millones de personas mexicanas han sido víctimas de phishing durante el año 2024, lo cual equivale al 13.5% de la población conectada a internet.

Esto indica que en 2024 se registraron alrededor de 6 millones de fraudes cibernéticos, cifra que representa un aumento del 40% respecto a 2018. En contraste, los fraudes tradicionales sumaron 2.2 millones, lo que demuestra que los ciberdelitos se concentran cada vez más en la banca en línea y las operaciones digitales.

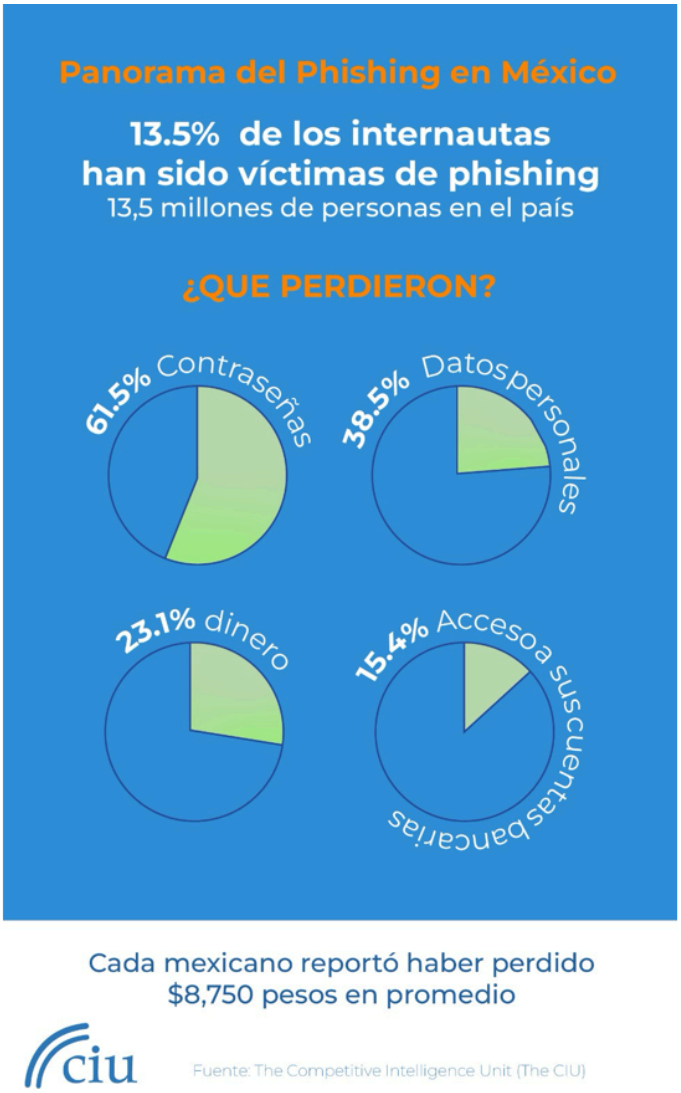


*Cifra estimada

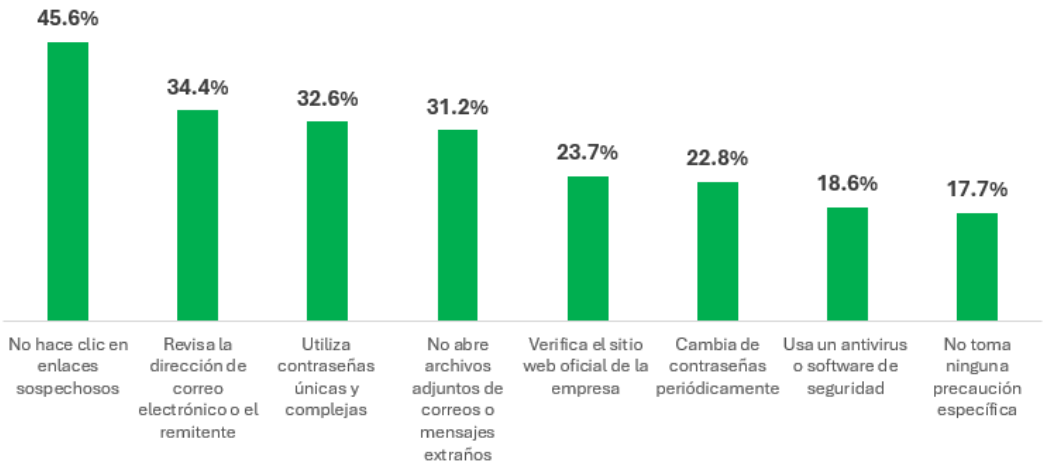
Fuente: The Competitive Intelligence Unit con información de Secretaría de Hacienda

El monto total reclamado por estos incidentes superó los 20 mil millones de pesos. En promedio cada víctima de phishing perdió cerca de $8,750, mientras que considerando todos los tipos de fraudes cibernéticos, el costo promedio por incidente se ubicó en $3,525.

En cuanto a la información comprometida, el 61.5% de las víctimas perdieron sus contraseñas, el 38.5% vio expuestos otros datos personales (dirección, fotográficas o teléfonos), el 23.1% tuvo pérdidas económicas directas y el 15.4% perdió el acceso a sus cuentas bancarias.



Respecto a las medidas de defensa contra el phishing, el 45.6% de las personas evita hacer clic en enlaces sospechosos, el 34.4% revisa la autenticidad de correos o números de contacto, el 32.6% utiliza contraseñas complejas, el 31.2% no abre archivos adjuntos y el 18.6% cuenta con algún software de seguridad. Sin embargo, el 17.7% reconoció no tomar ninguna precaución específica. Además 1 de cada 3 personas se siente poco o nada seguro de reconocer un intento de phishing, lo que representa a más de 30 millones de mexicanos vulnerables a este tipo de ciberataques



Fuente: The Competitive Intelligence Unit

El Enfoque Integral: Ciencias del Aprendizaje, Gamificación y Aprendizaje Personalizado

Ciencias del Aprendizaje: La capacitación se hará siguiendo principios neurocientíficos y psicológicos para la retención a largo plazo. Se utilizarán técnicas como la repetición espaciada, el aprendizaje basado en problemas y la retroalimentación inmediata, adaptadas a la forma en que el cerebro adulto procesa y consolida nueva información.

Gamificación: Para aumentar el compromiso y la motivación, se aplicarán elementos de juego a la experiencia de aprendizaje. Esto incluirá desafíos, puntos, insignias y un sistema de progresión que haga el proceso divertido e interactivo. La gamificación no sólo motivará a los usuarios a completar la formación, sino que también les permitirá aplicar los conceptos de seguridad en un entorno sin riesgos. en donde la gamificación motiva a los participantes, siendo la retroalimentación y los niveles elementos bien percibidos.

Aprendizaje Personalizado: Se reconocerá que cada persona tiene un punto de partida diferente en cuanto a su conocimiento de seguridad (ciberseguridad). El sistema adaptará el contenido y la dificultad de los desafíos (tests) en función del desempeño y el progreso de cada individuo. Esto asegura que el aprendizaje sea relevante, desafiante y nunca abrumador.

Acompañamiento con IA: En nuestra aplicación integramos a **Baxi**, un asistente virtual impulsado por inteligencia artificial que acompaña al usuario en cada paso de su experiencia. Baxi no solo responde dudas sobre los test, servicios y productos disponibles de Banxico, sino que también actúa como una guía interactiva que facilita el aprendizaje y la toma de decisiones. Su diseño busca ser accesible para todas las edades, ofreciendo información clara, confiable y siempre al alcance, lo que convierte a la app en una herramienta moderna, educativa y cercana para identificar y comprender los riesgos que enfrenta cada usuario.

El Proceso de Onboarding:

Test de habilidades cibernéticas y asignarle el nivel de riesgo o una certificación de usuario digital.

Inspirado en el modelo del examen para obtener la licencia de conducir en la Ciudad de México, se propone un test de conocimientos como medida de seguridad para la apertura de una cuenta bancaria digital. Este test servirá como un punto de partida para el aprendizaje personalizado, para ver los temas que tenemos que profundizar más.

Estructura del Test: El test evaluará conceptos básicos de ciberseguridad, como la detección de phishing, la creación de contraseñas robustas y la identificación de sitios web fraudulentos. Contendrá una combinación de preguntas de opción múltiple escenarios interactivos donde el usuario deberá identificar riesgos potenciales.

Retroalimentación y Aprendizaje: El resultado del test indicará el nivel de riesgo en el que se encuentra la persona evaluada frente ataques de esta índole. Con esta información, daremos tips e infografías para reforzar las áreas donde necesita mejorar. Una vez completado el ejercicio, el usuario podrá volver a realizar el examen. Este enfoque asegura que la apertura de la cuenta bancaria esté vinculada a la adquisición de conocimientos de seguridad.

Este enfoque complementa las técnicas de ingeniería social con la inteligencia artificial para crear un método de concientización proactivo y efectivo que prepara a los adultos para enfrentar las amenazas cibernéticas de la vida real.

2. Descripción resumida de la solución tecnológica propuesta

Proponemos el desarrollo de una plataforma de educación digital innovadora, que se apalanque en las ciencias del aprendizaje, la gamificación y el aprendizaje personalizado para abordar la problemática detectada. La solución consiste en una aplicación móvil, diseñada para medir el nivel de conocimiento en ciberseguridad de los usuarios en el uso correcto y seguro del SPEI y otros sistemas de pago complementarios como CoDi®. Nuestra aplicación busca medir de manera proactiva el nivel de riesgo al que se enfrentan los usuarios, al tiempo que ofrece una experiencia de aprendizaje diseñada para transformar su comportamiento y fortalecerlos contra ciberataques. Con este enfoque dual, no solo se fomenta la confianza en las herramientas tecnológicas que brinda el sistema financiero, sino que también se dota a los adultos de conocimientos prácticos y estrategias efectivas para mitigar el riesgo de ser víctimas de fraudes.

Con esta sinergia entre IA, educación y confianza, nuestra aplicación se convierte en un puente entre la innovación tecnológica y la seguridad del usuario, asegurando que cada persona tenga las herramientas necesarias para reconocer, prevenir y enfrentar riesgos digitales en el sistema financiero.

3. Detalle de la solución

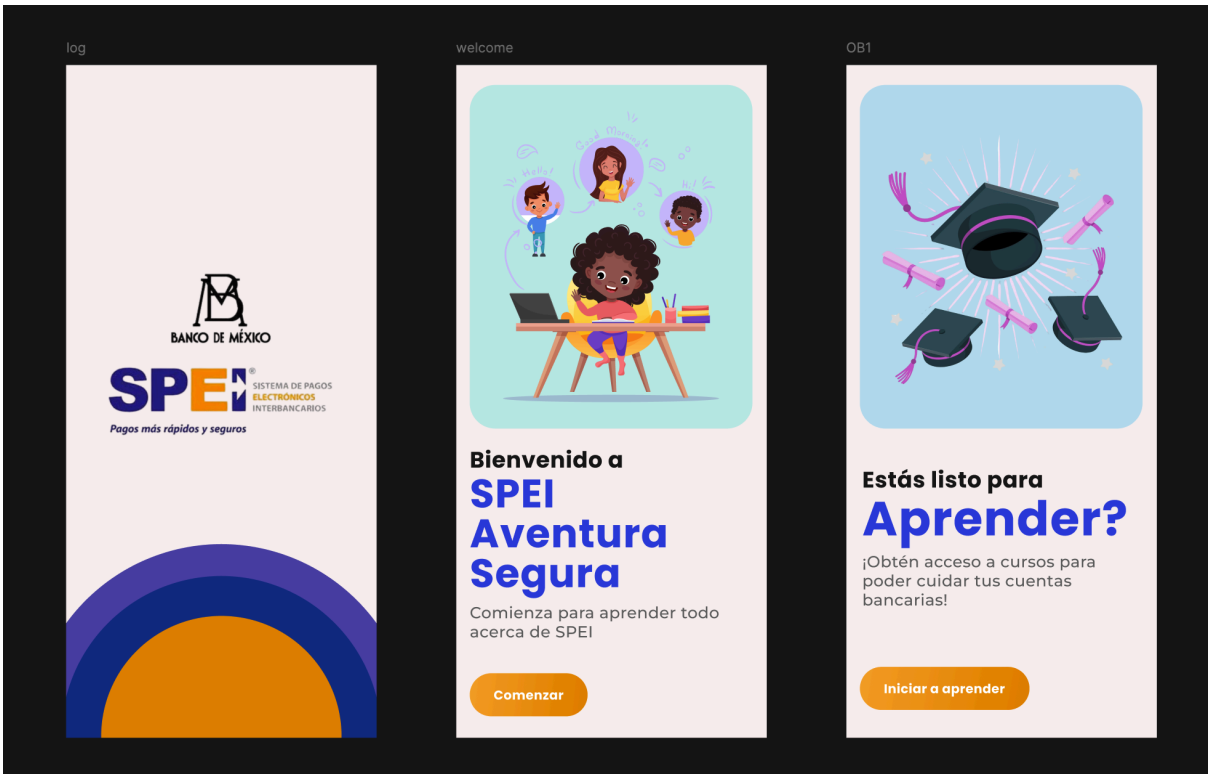
a. Análisis de factibilidad

La viabilidad de "SPEI Aventura Segura" es alta, tanto a nivel técnico como económico. Desde el punto de vista técnico, la aplicación se puede construir utilizando tecnologías modernas de desarrollo multiplataforma (como React Native o Flutter), lo que permite su despliegue en iOS y Android con una sola base de código. La personalización del aprendizaje se puede lograr mediante el uso de Inteligencia Artificial (IA) para un chatbot y un sistema de evaluación adaptativa. Estos sistemas se pueden implementar mediante la integración con APIs de modelos de lenguaje existentes, lo que reduce la complejidad y el costo de desarrollo.

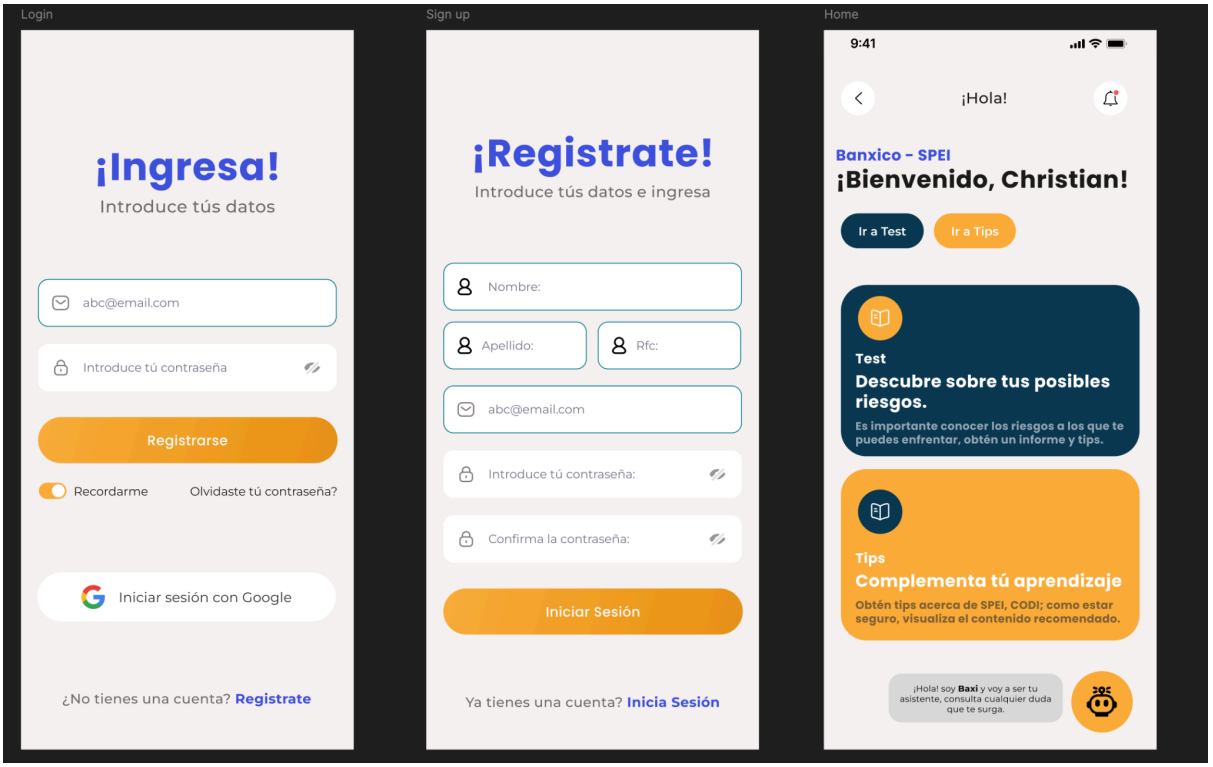
Desde el punto de vista económico y operativo, la solución es escalable y sostenible. La infraestructura en la nube (como Google Cloud o Firebase) permite un

despliegue global con costos ajustables al crecimiento de usuarios. La integración con los bancos a través de APIs para la verificación de certificados de capacitación sería un proceso de bajo costo y alta eficiencia. Adicionalmente, el proyecto se alinea con las competencias del Hackathon SPEI, promoviendo la **inclusión financiera** y la **innovación tecnológica**, al tiempo que fomenta la **seguridad** y la **accesibilidad** (Hackathon SPEI BANXICO, 2025).

b. Pantallas o maquetas (mockups)



En esta sección se presenta el diseño corporativo de la aplicación “SPEI Aventura Segura”, definiendo la identidad visual a través de la selección de colores principales aplicados en títulos, contenido, botones e imágenes. Asimismo, se desarrollaron pantallas de carga que enriquecen la experiencia del usuario.



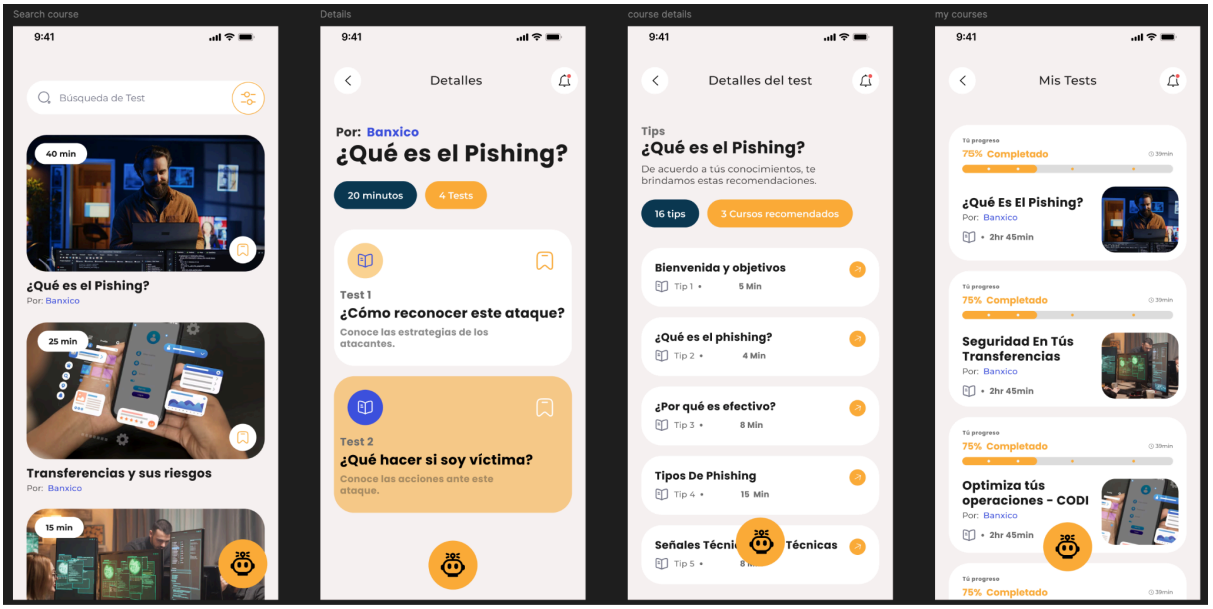
La primera figura muestra la vista de inicio de sesión, la cual permite el acceso mediante correo y contraseña, o bien con una cuenta de Google. También se diseñó el flujo de registro, donde se solicitan datos clave para nuestro modelo de negocio: nombre, apellido, RFC, correo electrónico y contraseña.

Posteriormente, se desarrolló la página de inicio, que ofrece un saludo personalizado y accesos rápidos a funciones principales como el test inicial que ayuda a tener un punto de partida en las recomendaciones de contenido, tips y puntos a mejorar y/o tener en cuenta que mejoraran la experiencia y conocimientos de los usuarios.

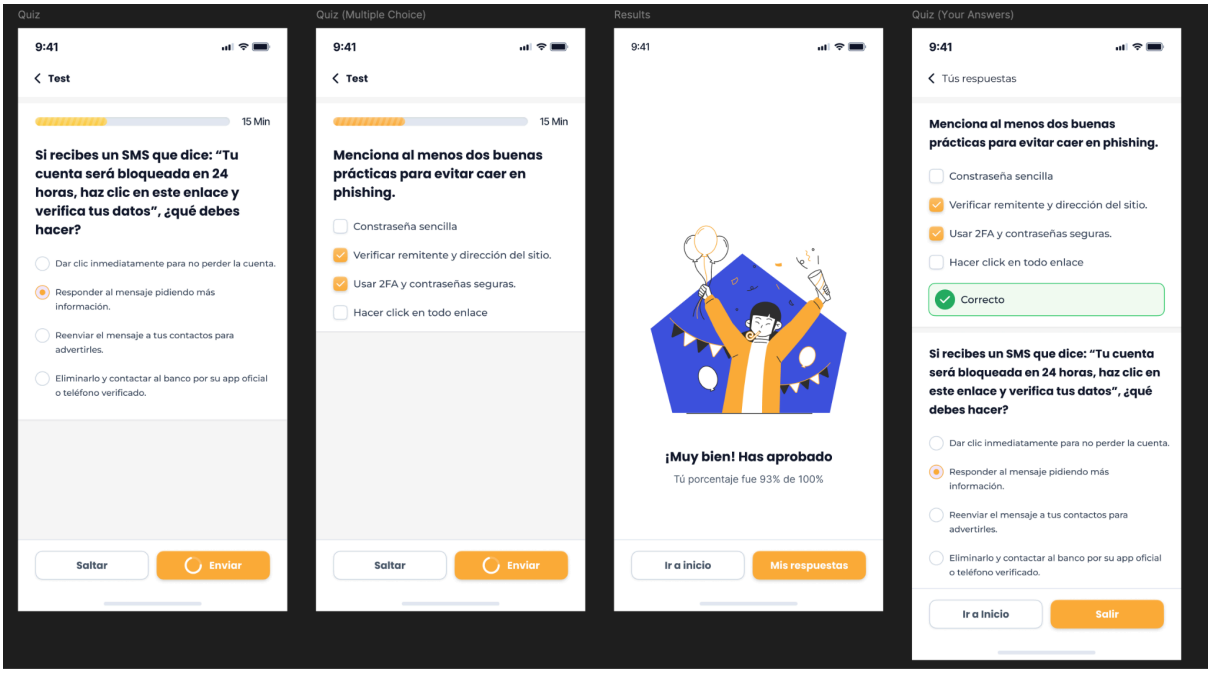
Por otro lado, se incluye una sección que dirige a los distintos tests disponibles, con el objetivo de que el usuario tome conciencia de los riesgos a los que está expuesto y pueda contrarrestarlos mediante el conocimiento, contenido, tips que la aplicación le proporciona.

En esta sección aparece por primera vez nuestro agente virtual Baxi, una IA que apoya al usuario, un agente virtual impulsado por inteligencia artificial, diseñado para acompañar al usuario durante todo su proceso de aprendizaje. Su función principal es resolver dudas en tiempo real sobre técnicas, certificaciones y

procedimientos relacionados con la ciberseguridad. Además, actúa como una guía interactiva y accesible.

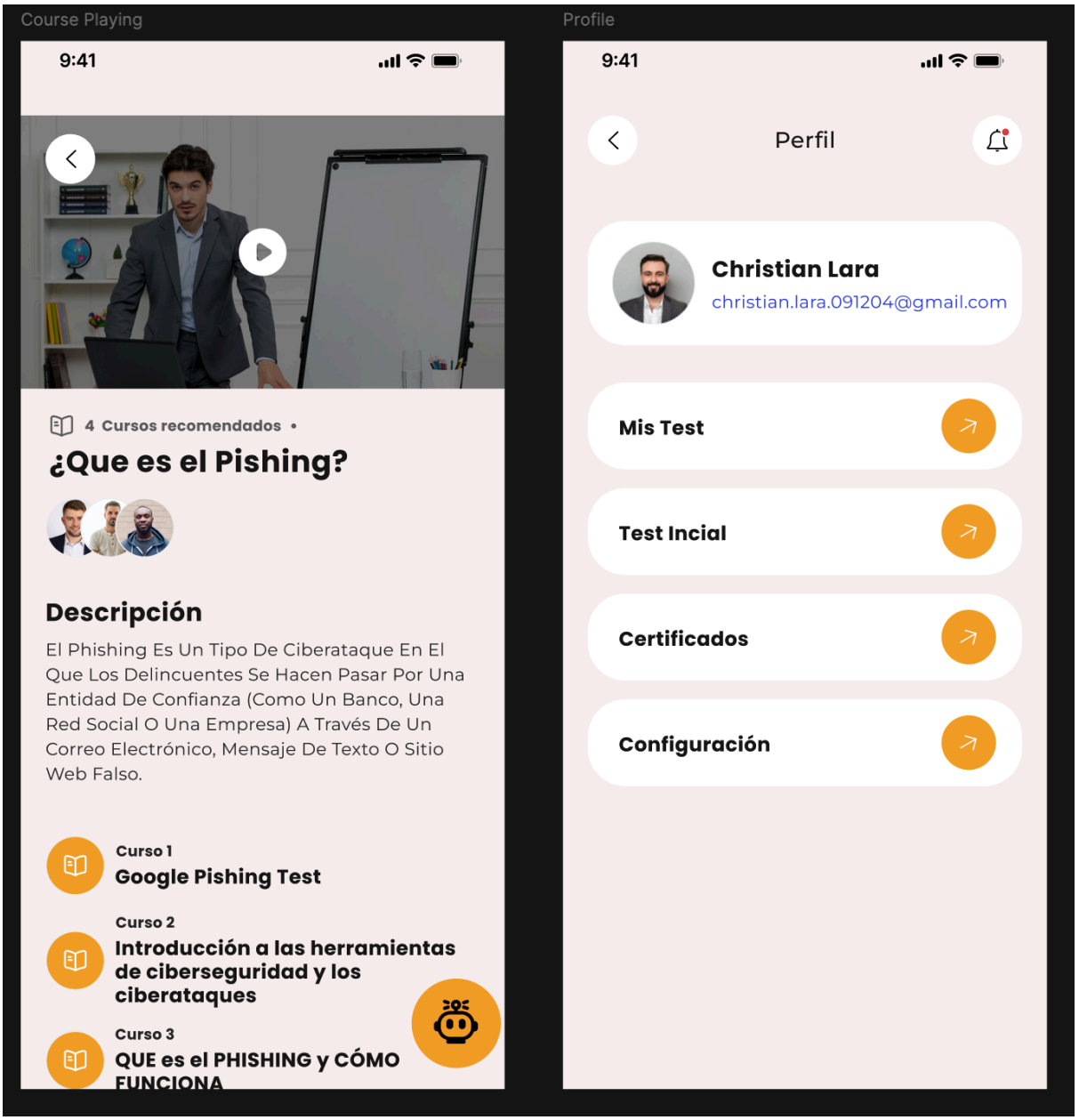


El catálogo de tests se diseñó para ser claro y accesible. Al seleccionar una infografía y sus conceptos clave, el usuario accede a detalles como la duración estimada, el número de tips y los contenidos específicos. Este proceso se complementa con la integración de elementos de gamificación para potenciar la motivación y el aprendizaje.



El test se ha diseñado para que el usuario identifique claramente los riesgos a los que está expuesto, las áreas que debe mejorar y lo que puede seguir intentando. Para garantizar la autenticidad de los resultados, se limita el acceso a la IA durante la prueba.

Las preguntas se presentan de manera progresiva en distintos formatos y temáticas. Al finalizar, el usuario recibe retroalimentación inmediata junto con su calificación, además de contenido, tips y recomendaciones específicas de la aplicación, alineadas con su nivel actual de desempeño.



Finalmente, se incluye un ejemplo de pantalla de tips, que introduce el tema de forma breve y concisa para mantener el interés del usuario, posterior en base a sus resultados se le proporcionan una serie de recursos (cursos, tips, juegos, apps, etc.) que pueden ayudar a mejorar sus conocimiento acerca del tema.

Además, se diseñó la vista de perfil, que centraliza la información personal, las configuraciones generales y los ajustes de la cuenta, asegurando un acceso ágil y ordenado a todas las funciones de la aplicación.

c. Arquitectura general de la solución

La arquitectura de la solución se plantea como un modelo modular, escalable y adaptable a futuras necesidades.

1. **Frontend (Interfaz de Usuario):** La aplicación móvil será desarrollada en React Native, partiendo de una maquetación previa en Figma, lo que permite definir una identidad corporativa sólida y coherente. El diseño estará orientado a mejorar la accesibilidad y ofrecer una experiencia visual atractiva y amigable para el usuario. Esta capa será responsable de la presentación gráfica, la interacción con el usuario y la integración de la lógica de gamificación (niveles, puntos e insignias) que motiva la participación activa.
2. **Backend (Lógica del Servidor):** Gestiona la autenticación de usuarios, el progreso del curso, la validación del examen y la generación de certificados. Nuestro backend estará desarrollado en Node.js con TypeScript y NestJS, garantizando comunicación ágil, bajo costo y escalabilidad. Para el almacenamiento usaremos Firestore en el MVP, con posibilidad de migrar a PostgreSQL y Redis en un futuro, tomando en cuenta la escalabilidad.
3. **Base de Datos:** Se utilizará una base de datos en la nube (como Firestore) para almacenar los datos de los usuarios, su historial de aprendizaje, los resultados de los exámenes y los certificados digitales.
4. **Servicios de IA (Chatbot y Examen Adaptativo):** La integración se realizará mediante una API conectada a un modelo de lenguaje, lo que permitirá implementar tanto el chatbot como la lógica de un examen dinámico. Este examen adaptará la dificultad de las preguntas en función del desempeño del usuario, garantizando una experiencia personalizada.

Además, se desarrollará Baxi, un agente de inteligencia artificial basado en modelos de lenguaje pre entrenados (LLM) y técnicas de RAGs. Su implementación se facilitará gracias a la documentación, información y estadísticas disponibles por parte de Banxico. Para optimizar su desempeño, Baxi se entrenará mediante Fine-Tuning y Chunking, lo que permitirá una integración más eficiente y una experiencia de usuario más confiable.

5. **API de Verificación:** Un servicio externo que permitiría a las instituciones financieras validar el certificado digital de un usuario antes de otorgar un producto financiero, cumpliendo con la necesidad de certificar a los usuarios en un nivel básico de educación financiera digital.
6. **Módulo Analítico:** Un tablero de control basado en IA para bancos y Banxico, que ofrecería estadísticas sobre el nivel de capacitación de los usuarios, errores comunes y el impacto en la reducción de fraudes.

4. Referencias consultadas para la elaboración del ensayo

- [1] F. Vargas, “Phishing en México: Amenaza creciente y llamado a la acción,” The CIU, https://www.theciu.com/publicaciones-2/2025/6/16/phishing-en-mxico-amenaza-creciente-y-llamado-a-la-accin (accessed Sep. 29, 2025).
- [2] Informe anual sobre las infraestructuras de los mercados ..., https://www.banxico.org.mx/publicaciones-y-prensa/informe-anual-sobre-las-infraestructuras-de-los-me/%7BE0085475-B1D7-DED0-60AF-05ED88153BDC%7D.pdf (accessed Sep. 30, 2025).
- [3] A. D. de León Carillo, CODI®: La Nueva Forma de Pagar en México, https://www.banxico.org.mx/publicaciones-y-prensa/presentaciones/%7B1CA33D18-A38C-EE29-41BF-6302A641D617%7D.pdf (accessed Sep. 30, 2025).
- [4] D. Lerís and M. L. Sein-Echaluce, “La Personalización del Aprendizaje: Un Objetivo del Paradigma educativo centrado en el aprendizaje,” Arbor, https://arbor.revistas.csic.es/index.php/arbor/article/view/1417 (accessed Sep. 29, 2025).
- [5] R. S. Contreras Espinosa, Experiencias de Gamificación en Aulas , https://ddd.uab.cat/pub/llibres/2018/188188/ebook15.pdf (accessed Sep. 30, 2025).

- [6] C. C. Monares Marin, LA SEGURIDAD INFORMÁTICA EN LA VIDA COTIDIANA DE LAS PERSONAS(INGENIERÍA SOCIAL) CASO CREZCAMOS S.A, https://repository.unad.edu.co/bitstream/handle/10596/36487/cmonares.pdf?sequence=1&isAllowed=y (accessed Sep. 30, 2025).
- [7] J. C. Malagon Lara, ANÁLISIS DE LAS TÉCNICAS DE INGENIERÍA SOCIAL QUE AMENAZAN LA SEGURIDAD INFORMÁTICA DE USUARIOS DE ENTIDADES FINANCIERAS, https://repository.unad.edu.co/bitstream/handle/10596/55080/jcmalagonl-.pdf?sequence=3 (accessed Sep. 30, 2025).
- [8] Banxico SPEI hackathon, https://www.banxico.org.mx/hackathonspei/d/HS2025_bases.pdf (accessed Sep. 14, 2025).