Montevideo, 31 de octubre del 2025

Herramienta de entrenamiento y capacitación para evitar fraudes a través de Ingeniería Social.

Integrantes

Diego Balbis - dbalbis8@gmail.com

Dayron Muñiz - munizdayron@gmail.com

Tutor

Pablo Martres - pmartres@gmail.com

Resumen

El presente proyecto se ejecutó con la finalidad de brindar una herramienta que contribuya a la prevención de fraudes digitales llevados a cabo a través de la ingeniería social, un tema de gran relevancia en estos tiempos que afecta tanto a usuarios particulares como a organizaciones. Estos ataques no se apoyan en fallas técnicas, sino en la manipulación emocional de las personas, el uso de la confianza, lo que hace importante estar capacitados y preparados en ciberseguridad.

La propuesta desarrollada consiste en una plataforma web educativa integrada por diferentes módulos y etapas, cuyo contenido puede ser modificado siempre que sea necesario sin necesidad de tocar una línea de código. Su diseño busca fomentar el aprendizaje dinámico mediante ejercicios interactivos y contenidos claros que ayudan a identificar los distintos tipos de engaño digital.

El desarrollo de este proyecto representó para los integrantes una oportunidad para consolidar conocimientos técnicos adquiridos a lo largo de la carrera, así como de gestión e ingeniería de software. Constituye el último peldaño en la aspiración de graduarnos.

Como resultado final, se obtuvo una aplicación funcional, moderna y fácil de usar, orientada a generar conciencia y promover una cultura de seguridad digital responsable.

Introducción

Los ciberataques a través de la ingeniería social en la actualidad son más comunes de lo que podemos imaginar, a diferencia de los ataques puramente técnicos, estos no buscan vulnerar directamente los sistemas informáticos, sino que se aprovechan del factor humano, haciendo uso de la confianza y de las emociones de las personas para obtener información sensible o acceso no autorizado.

Es por ello que aunque se han destinado importantes recursos a reforzar la infraestructura tecnológica, persiste una problemática en la capacitación de los usuarios en estos temas.

No son pocas las ocasiones en que los atacantes logran su cometido no por fallas técnicas, sino por desconocimiento o falta de entrenamiento frente a técnicas de manipulación.

Con este proyecto nos proponemos realizar una herramienta educativa que posibilite disminuir la vulnerabilidad humana ante los diferentes tipos de ataques basados en ingeniería social.

Antecedentes

A lo largo de la fase de investigación se revisaron distintas herramientas y programas de capacitación en ciberseguridad, observándose que no son pocas en las que se requiere que los usuarios posean cierto nivel técnico o experiencia previa en el tema. El sistema desarrollado busca ofrecer una alternativa que acompañe al usuario desde los conceptos más básicos, facilitando la comprensión de las principales modalidades de ciberataques mediante el uso de la ingeniería social.

La plataforma se estructura en módulos y etapas que pueden editarse y adaptarse por el usuario administrador sin necesidad de modificar el código fuente, lo que permite actualizar contenidos o ajustarlos. Más que reemplazar otras soluciones existentes, CAPFIS procura ser una herramienta práctica y flexible que contribuya a la formación inicial en seguridad digital, promoviendo el aprendizaje progresivo y la actualización constante frente a nuevas modalidades de fraude.

Pruebas Realizadas

El proceso de testing se planificó de acuerdo con el Plan de Testing documentado en el proyecto. La estrategia de pruebas se basó en lo siguiente:

Pruebas unitarias: revisión del código en Visual Studio.

Pruebas de integración: comprobación del sistema, verificando la correcta comunicación de sus capas.

Pruebas funcionales: validación de todos los requerimientos definidos en el análisis.

Pruebas de regresión: validación de la aplicación ante cada actualización ya fuera debido a correcciones o mejoras.

Pruebas de aceptación: validación final del sistema por parte del equipo y tutor académico.

Las mismas contemplaron siempre las principales funcionalidades como registro de usuarios, inicio de sesión, administración de módulos y registro del progreso de aprendizaje.

Resultados

De los casos de pruebas definidos y adjuntos en el anexo obtuvimos como resultado que un 90% fueron exitosos corrigiendo así los que dieron error o decidimos que se podían mejorar la funcionalidad probada, para lograr un resultado del 100%. No obstante no es posible garantizar que el producto se encuentre libre de errores.

Asimismo, las pruebas de regresión demostraron que las nuevas implementaciones no afectaron el comportamiento de las funcionalidades previas, y las pruebas de aceptación validaron que el producto final cumpliera con los criterios establecidos junto al tutor académico.

Conclusiones

Este proyecto nos permitió consolidar los conocimientos adquiridos a lo largo de la carrera, integrando aspectos técnicos, metodológicos y humanos en un producto funcional y con propósito social.

Las métricas aplicadas confirmaron un código con alta mantenibilidad, bajo acoplamiento y complejidad controlada, reflejando un desarrollo concordante con los principios de la ingeniería de software moderna.

En el plano metodológico, la aplicación del marco ágil Scrum permitió un trabajo iterativo, con entregas parciales verificables, reuniones de seguimiento constantes y adaptación a los cambios. Esta metodología fomentó la colaboración, la organización del trabajo y la autogestión del equipo, asegurando el cumplimiento de los plazos establecidos.

En cuanto al proceso formativo, la experiencia de planificación, desarrollo, testing y documentación ofreció un aprendizaje integral, fortaleciendo competencias técnicas, comunicacionales y de gestión. CAPFIS se constituye, por tanto, en un producto académico completo que evidencia la capacidad del equipo para analizar, diseñar, implementar y evaluar soluciones tecnológicas aplicadas a un problema real.

Finalmente, el proyecto no solo cumple con los objetivos propuestos, sino que aporta un valor educativo y social, al contribuir a la formación de usuarios más conscientes y preparados frente a las amenazas de la ingeniería social.

Referencias

[1] C. Hadnagy, Ingeniería social: El arte del hacking humano (2ª ed.) [Edición en español]. Wiley, 2011.

[2] K. D. Mitnick y W. L. Simon, El arte de la intrusión: Las historias reales detrás de los exploits de hackers. McGraw-Hill, 2011.

[3] Ley N.º 18.331 — Protección de Datos Personales y Acción de Habeas Data, Uruguay, 2008.

[4] IBM, Ingeniería social. [En línea]. Disponible en: https://www.ibm.com/es-es/topics/social-engineering . Consultado: 14 de abril de 2025.

[5] Instituto Nacional de Ciberseguridad (INCIBE), Técnicas de ingeniería social [Infografía]. [En línea]. Disponible en: https://www.incibe.es/ciudadania/formacion/infografias/tecnicas-ingenieria-social . Consultado: 16 de abril de 2025.

[6] Kaspersky, ¿Qué es la ingeniería social? [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering . Consultado: 18 de abril de 2025.

[7] Microsoft, Documentación de .NET. Microsoft Learn. [En línea]. Disponible en: https://learn.microsoft.com/es-mx/dotnet/ . Consultado: 24 de abril de 2025.

[8] Microsoft, C# – Lenguaje de programación. Microsoft Learn. [En línea]. Disponible en: https://learn.microsoft.com/es-mx/dotnet/csharp/ . Consultado: 24 de abril de 2025.

[9] I. Sommerville, Ingeniería del software (9.ª ed.) [PDF]. [En línea]. Disponible en: https://gc.scalahed.com/recursos/files/r161r/w25469w/ingdelsoftwarelibro9_compressed.pdf . Consultado: 24 de abril de 2025.

[10] L. Solís Fajardo, “Ciberseguridad y amenazas informáticas: el rol de la ingeniería social,” Religación. Revista de Ciencias Sociales y Humanidades, vol. 7, no. 34, pp. 104–117, 2025. [En línea]. Disponible en: https://revista.religacion.com/index.php/religacion/article/view/1310/1661 . Consultado: 18 de abril de 2025.

[11] M. Susatama, La ingeniería social como herramienta de los ciberdelincuentes: análisis de técnicas y contramedidas [Trabajo de grado, Universidad Piloto de Colombia]. Repositorio Institucional UNIPILOTO. [En línea]. Disponible en: https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/12497/articulo%20Marcela%20susatama.cleaned.pdf . Consultado: 19 de abril de 2025.