****

**UNIVERSIDAD DE LA EMPRESA**

# **FACULTAD DE INGENIERÍA**

## **TÉCNICO EN INFORMÁTICA Y ANALISTA EN TECNOLOGÍA INFORMÁTICA**

**PROYECTO INTEGRADOR**

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

**Integrantes:**

Diego Balbis — C.I. 4.451.623-5  
Dayron Muñiz — C.I. 6.295.606-3

**Tutor:**  
Ing. Pablo Martres

**Año:**  
2025

**Sigla: CAPFIS**

**ÍNDICE**

DESCRIPCIÓN DEL PROBLEMA………………………………………………………………….3

[OBJETIVOS…………………………………………………………………………………………...3](#_heading=h.qai28p8wk6jf)

[OBJETIVO GENERAL………………………………………………………………………3](#_heading=h.sbyggzdlnl2a)

[OBJETIVOS ESPECÍFICOS……………………………………………………………….3](#_heading=h.z8sia7d9mr75)

[ALCANCE……………………………………………………………………………………………..4](#_heading=h.980h4lxqefzk)

[PRODUCTOS Y FUNCIONALIDADES……………………………………………………4](#_heading=h.aoar7pyohhoh)

ARQUITECTURA………………………………………………………………………..…..5

TECNOLOGÍA Y VERSIONES…………………………...………………………………...5

DOCUMENTACIÓN……………………………………………...…………………………..6

METODOLOGÍA DE TRABAJO…………………………………………………….....…..6

[IMPORTANCIA DEL PROYECTO](#_heading=h.cau6fq3bthnx)………………………………………………………………….6

CRONOGRAMA………………………………………………………………………………………7

BIBLIOGRAFÍA……………………………………………………………………………………….8

**DESCRIPCIÓN DEL PROBLEMA**

Hoy en día los fraudes basados en Ingeniería Social constituyen una amenaza crítica dentro del ámbito digital, ya que explotan el factor humano mediante el engaño, la manipulación emocional y la confianza. [[1]](#footnote-0)

A diferencia de los ataques técnicos, estos métodos no requieren esencialmente vulnerar sistemas. Un ataque de Ingeniería Social tiene una base psicológica, pero los medios tecnológicos pueden potenciar dicho ataque o influir directamente sobre las decisiones del usuario. Aunque muchas organizaciones invierten en infraestructura tecnológica, la formación de los usuarios en buenas prácticas sigue siendo insuficiente, especialmente en entornos educativos y laborales. Las estrategias actuales de capacitación no logran preparar adecuadamente a las personas para reconocer y responder ante situaciones reales de riesgo. [[2]](#footnote-1)

Ante esta problemática, se identifica la necesidad de desarrollar una herramienta interactiva que combine simulación, práctica y retroalimentación, promoviendo hábitos digitales seguros y fortaleciendo la capacidad individual para enfrentar este tipo de amenazas.

## 

## **OBJETIVOS**

### **OBJETIVO GENERAL**

Desarrollar una herramienta interactiva de entrenamiento en ciberseguridad orientada a prevenir fraudes por ingeniería social, mediante la simulación de escenarios reales, la generación de contenidos educativos accesibles y juegos didácticos para fomentar las buenas prácticas.

### **OBJETIVOS ESPECÍFICOS**

* Fortalecer competencias en análisis de vulnerabilidades que explotan la psicología induciendo a comportamientos de riesgo.
* Desarrollar una herramienta que impacte positivamente en la formación de otros usuarios y cree conciencia de la importancia de la ciberseguridad en la era digital.
* Con el desarrollo de la aplicación lograr culminar satisfactoriamente la Carrera y poder obtener el título de Técnico en Informática y Analista en Tecnología Informática

### 

### **ALCANCE**

La herramienta estará destinada a todos los usuarios interesados en esta problemática, con un especial énfasis hacia estudiantes y empresas. Se centrará únicamente en fraudes digitales que dependen de la persuasión más que de la ingeniería tecnológica.

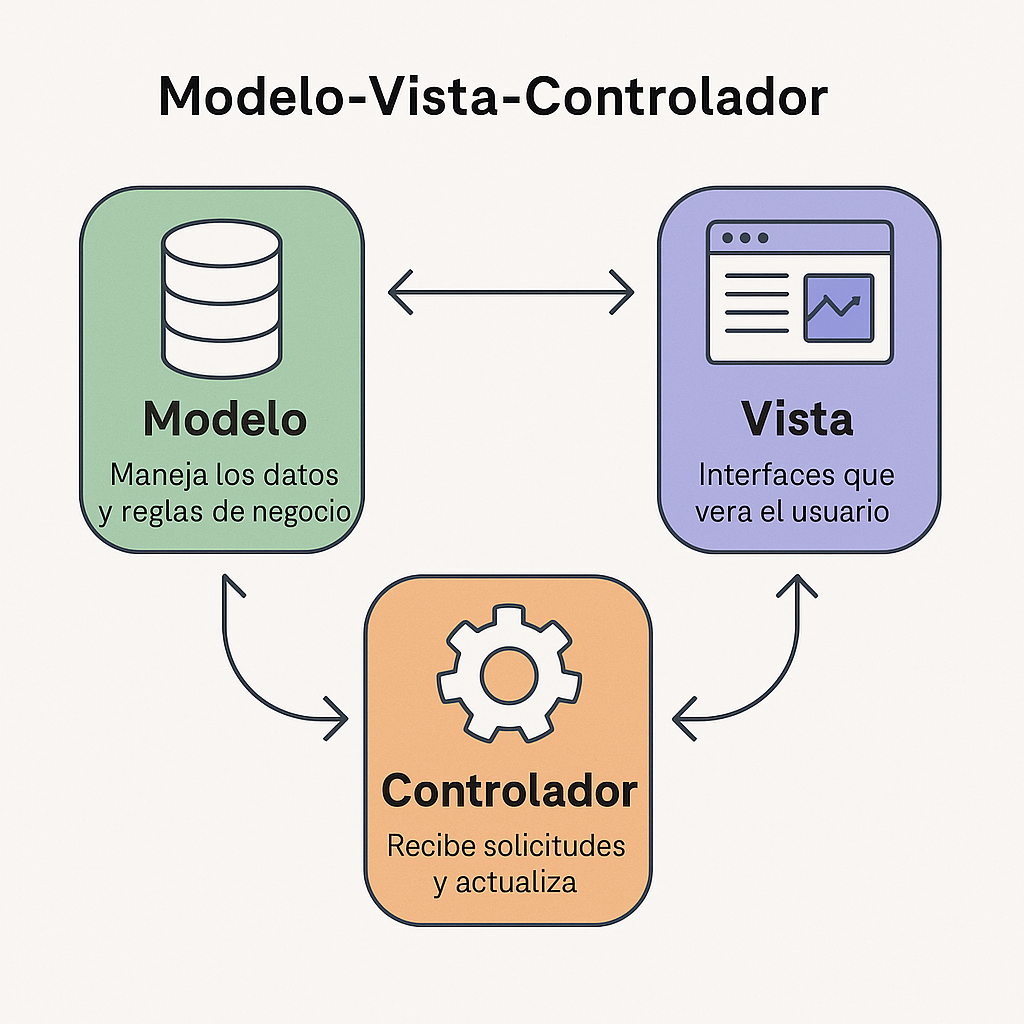
### **PRODUCTOS Y FUNCIONALIDADES**

* Plataforma web interactiva
* Registro e inicio de sesión: Los usuarios podrán crearse una cuenta e iniciar sesión para acceder a sus módulos, simulaciones y estadísticas personalizadas.
* Secciones con diferentes tipos de ataque (phishing, smishing, vishing, redes sociales)
* Módulos educativos con tips, videos cortos y preguntas frecuentes
* Cuestionarios
* Juegos
* Historias de Casos reales

**ARQUITECTURA**

Se desarrollará como una aplicación web basada en el modelo cliente-servidor, una estructura que permite dividir las responsabilidades entre el navegador del usuario (cliente) y el servidor donde se procesa la lógica de la aplicación. Esta elección responde a la necesidad de ofrecer una solución accesible desde cualquier dispositivo con conexión a internet, sin necesidad de instalaciones adicionales.

Además, se implementará el patrón de diseño Modelo-Vista-Controlador (MVC) tal como refleja el siguiente diagrama:



Esta arquitectura permite que cada componente se desarrolle y mantenga de manera independiente, lo cual es clave para un proyecto que puede ir creciendo con el tiempo. También simplifica las tareas de prueba y depuración, ya que cada parte cumple una función bien definida.

.

**TECNOLOGÍAS Y VERSIONES**

● .NET 9.0.4   
  
● C# 13

● Razor Views  
  
● Bootstrap 5.3.3  
  
● MySQL Community Server 9.3.0 / Microsoft SQL Server 2022

● Entity Framework Core 9.0.0

● Pomelo.EntityFrameworkCore.MySql 8.0.3

● ASP.NET Core Identity 9.0.4   
  
● GitHub   
  
● Google Drive  
  
● GanttProject 3.3.3316

**DOCUMENTACIÓN**

* Informe Final
* Resumen Gerencial
* Presentación de Defensa del Proyecto
* Copia del Código

### **METODOLOGÍA DE TRABAJO**

Para la gestión y desarrollo del proyecto se utilizará la metodología ágil Scrum. Esta elección permite adaptar el proyecto a posibles cambios, promover la colaboración entre el equipo y garantizar entregas funcionales en cortos períodos de tiempo. El proyecto se dividirá en Sprints, con una duración de cuatro semanas. Esta metodología mantiene al equipo enfocado, permitiendo responder rápidamente a cambios en los requerimientos o en la planificación del proyecto.

### 

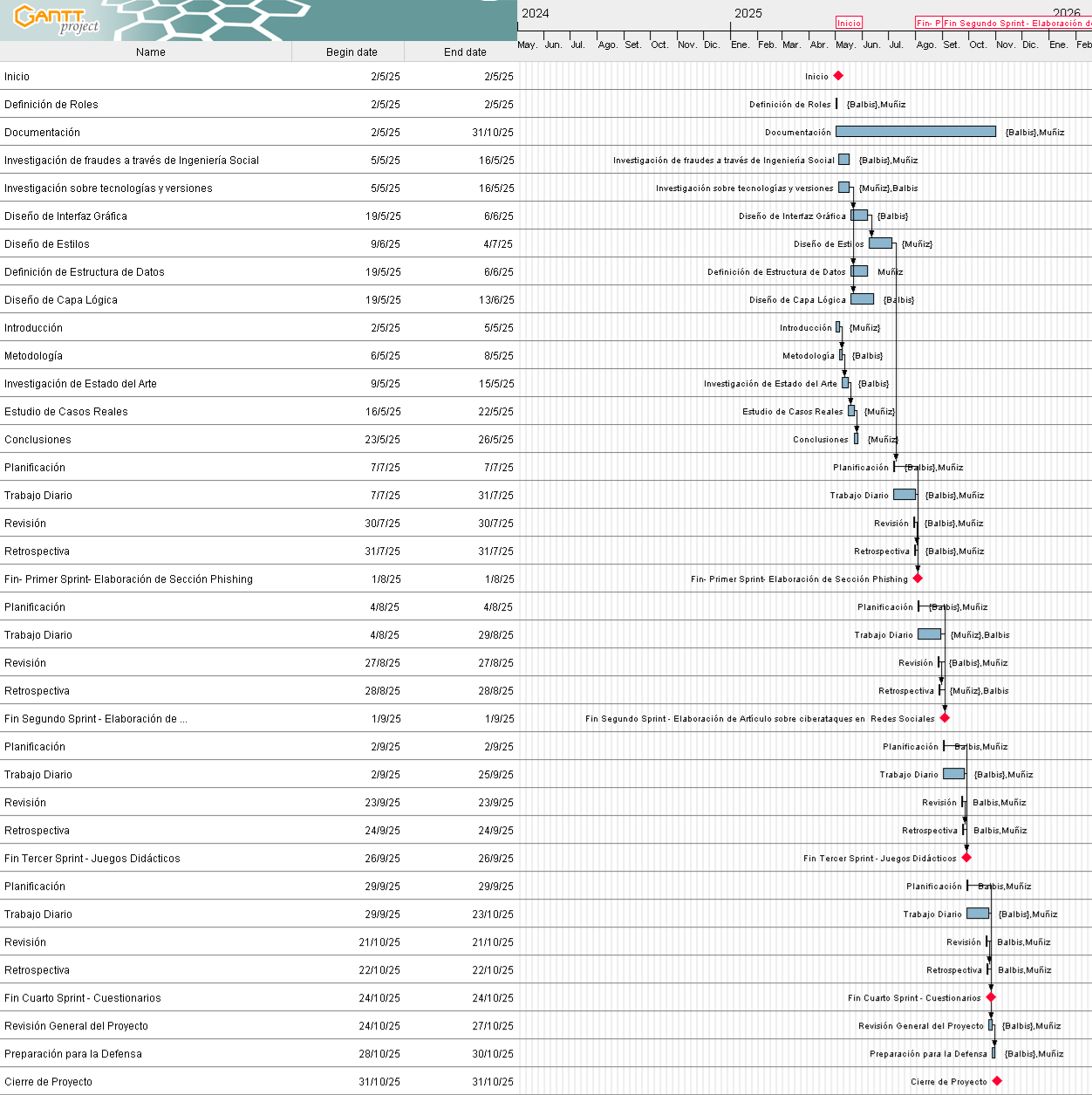
### **IMPORTANCIA DEL PROYECTO**

Este proyecto tiene especial relevancia al centrarse en uno de los aspectos más críticos, pero a menudo subestimados, de la seguridad digital: el factor humano. En la mayoría de los casos, los ataques no se dirigen directamente a sistemas tecnológicos complejos, sino a las personas, explotando emociones y estados como la confianza, el apuro, la desinformación, la autoridad y el miedo. Estos elementos son aprovechados sistemáticamente por los delincuentes para manipular a sus víctimas. En este contexto, CAPFIS surge como una herramienta clave que apuesta por la formación práctica de los usuarios, permitiéndoles identificar y reaccionar ante intentos de manipulación que simulan situaciones cotidianas.

Lo que distingue a esta iniciativa es su enfoque dinámico. En lugar de limitarse a brindar solamente información teórica, propone una experiencia educativa que conecta con la realidad. De esta manera, se busca generar un cambio en la forma en que las personas enfrentan su día a día en entornos digitales.

El impacto esperado apunta a fortalecer la capacidad de cada individuo para detectar y evitar engaños, no solo en el ámbito personal, sino también en los espacios que habitamos diariamente, como instituciones educativas, organizaciones laborales y el hogar. En definitiva, este proyecto no solo mejora la seguridad individual, sino que también promueve una cultura de prevención y conciencia frente a los riesgos crecientes de la Ingeniería Social.

**CRONOGRAMA**



**BIBLIOGRAFÍA**

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

IBM. (sf). *Ingeniería social*. Consultado: 14 de abril del 2025

<https://www.ibm.com/es-es/topics/social-engineering>

Instituto Nacional de Ciberseguridad (INCIBE). *Técnicas de ingeniería social* [Infografía]. Consultado: 16 de abril del 2025

<https://www.incibe.es/ciudadania/formacion/infografias/tecnicas-ingenieria-social>

Kaspersky. *¿Qué es la ingeniería social?* [Consultado: 18 de abril del 2025](https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering)

<https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering>

Microsoft. *Documentación de .NET*. Microsoft Learn. Consultado: 24 de abril de 2025

<https://learn.microsoft.com/es-mx/dotnet/>

Microsoft. *C# - Lenguaje de programación*. Microsoft Learn. Consultado: 24 de abril de 2025

<https://learn.microsoft.com/es-mx/dotnet/csharp/>

Mitnick, K. D., & Simon, W. L. (2011). *El arte de la intrusión: Las historias reales detrás de los exploits de hackers*. McGraw-Hill.

Sommerville. *Ingeniería del software* (9.ª ed.) [PDF]. Consultado: 24 de abril de 2025

<https://gc.scalahed.com/recursos/files/r161r/w25469w/ingdelsoftwarelibro9_compressed.pdf>

Solís Fajardo, L. Ciberseguridad y amenazas informáticas: el rol de la ingeniería social. *Religación. Revista de Ciencias Sociales y Humanidades, 7*(34), 104–117. [Consultado: 18 de abril del 2025](https://revista.religacion.com/index.php/religacion/article/view/1310/1661)

<https://revista.religacion.com/index.php/religacion/article/view/1310/1661>

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

<https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/12497/articulo%20Marcela%20susatama.cleaned.pdf>

1. Salvador Llaro, E. P., Roncal Sánchez, G. A., & Mendoza De Los Santos, A. C. (2022). Técnicas de la ingeniería social más usadas que amenazan tu privacidad digital. *Revista de Investigación Multidisciplinaria CTSCAFE*, 6(17), 12. Recuperado de <https://www.ctscafe.pe/index.php/ctscafe/article/view/174/202> [↑](#footnote-ref-0)
2. López, R. (2024, diciembre 8). La clave es mentalizar al equipo contra el 'phishing'. *El País*. Recuperado de <https://elpais.com/extra/eventos/2024-12-08/la-clave-es-mentalizar-al-equipo-contra-el-phising.html> [↑](#footnote-ref-1)