PROTOTIPO WEB PARA FOMENTAR BUENAS PRÁCTICAS EN CIBERSEGURIDAD CON GAMIFICACIÓN PARA LA UNIVERSIDAD DE CUNDINAMARCA

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

PAULA CAROLINA BARRERA CAMARGO

SALOMON FORERO CASTAÑEDA

UNIVERSIDAD DE CUNDINAMARCA EXTENSIÓN CHIA

PROGRAMA DE INGENIERÍA DE SISTEMAS

FACULTAD DE INGENIERÍA

2024

PROTOTIPO WEB PARA FOMENTAR BUENAS PRÁCTICAS EN CIBERSEGURIDAD CON GAMIFICACIÓN PARA LA UNIVERSIDAD DE CUNDINAMARCA

PAULA CAROLINA BARRERA CAMARGO

561220102

SALOMON FORERO CASTAÑEDA

561220119

DIRECTOR

MAGISTER JORGE PARAMO

UNIVERSIDAD DE CUNDINAMARCA EXTENSIÓN CHIA

PROGRAMA DE INGENIERÍA DE SISTEMAS

FACULTAD DE INGENIERÍA

2024

**AGRADECIMIENTOS**

Queremos expresar nuestro más sincero agradecimiento a todas las personas que contribuyeron de manera significativa a la realización de este proyecto de grado.

En primer lugar, agradecer a nuestro director de proyecto, Jorge Paramo, por su orientación, su paciencia y sus valiosas sugerencias que han enriquecido enormemente este trabajo. Su dedicación y apoyo fueron fundamentales para alcanzar los objetivos planteados.

Agradecemos a los profesores y compañeros de clase por su inspiración, intercambio de ideas y contribuciones que han moldeado nuestro enfoque hacia el tema de investigación, a amigos y familiares, gracias por su constante ánimo y apoyo emocional durante este viaje académico. Su comprensión y aliento fueron fundamentales en los momentos desafiantes.

Finalmente, les damos gracias a todos aquellos que directa o indirectamente contribuyeron a este proyecto, su influencia ha dejado una marca significativa en nuestro desarrollo académico y personal.

**RESUMEN**

Este proyecto va centrado en la elaboración de un prototipo web que emplea la gamificación como estrategia para fomentar e instruir en prácticas seguras de ciberseguridad a los alumnos de la Universidad de Cundinamarca Extensión Chía. Así mismo el propósito fundamental de esta propuesta es concienciar acerca de los peligros vinculados con la gestión de información en línea suministrando herramientas y saberes para reducir estos riesgos mediante el manejo adecuado de los datos.

Para alcanzar este propósito, se llevará a cabo un proceso de desarrollo que comprenderá la creación de una base de datos que contendrá la información esencial para el funcionamiento del prototipo, la elaboración de diagramas como orientación para el diseño e implementación del sistema, la inclusión de elementos de gamificación para hacer la experiencia más atractiva y motivadora para los usuarios, y pruebas exhaustivas para asegurar la calidad y eficacia del software elaborado.

Finalmente, se espera que este prototipo no solo proporcione conocimientos teóricos sobre ciberseguridad, sino que también estimule a los estudiantes a participar activamente mediante actividades interactivas, desafíos y recompensas, generando así un entorno universitario más seguro y consciente de los riesgos cibernéticos.

**Palabras clave:** concienciación; ciberseguridad; gamificación; comunidad estudiantil; prototipo web.

**ABSTRACT**

This project focuses on developing a web prototype utilizing gamification as a strategy to promote and instruct students at the University of Cundinamarca Extension Chía in safe cybersecurity practices. The primary objective of this proposal is to raise awareness about the dangers associated with online information management by providing tools and knowledge to mitigate these risks through proper data handling.

To achieve this goal, a development process will be undertaken, involving the creation of a database containing essential information for the prototype's operation, the creation of diagrams to guide the design and implementation of the system, the integration of gamification elements to enhance user engagement, and rigorous testing to ensure the quality and effectiveness of the developed software.

Ultimately, it is anticipated that this prototype will not only provide theoretical knowledge about cybersecurity but also encourage active student participation through interactive activities, challenges, and rewards. This approach aims to create a safer and more cyber-conscious university environment.

**Keywords:** awareness; cybersecurity; gamification; student community; web prototype.

**TABLA DE CONTENIDO**

[**CAPÍTULO 1** 10](#_Toc164022937)

[**INTRODUCCIÓN** 10](#_Toc164022938)

[**1.** **PROBLEMA** 10](#_Toc164022939)

[**1.1.** **Planteamiento del problema** 10](#_Toc164022940)

[**1.2.** **Formulación del problema** 12](#_Toc164022941)

[**2.** **OBJETIVOS** 12](#_Toc164022942)

[**2.1.** **Objetivo General** 12](#_Toc164022943)

[**2.2.** **Objetivos específicos** 12](#_Toc164022944)

[**3.** **ALCANCES Y LIMITACIONES** 13](#_Toc164022945)

[**4.** **JUSTIFICACIÓN** 14](#_Toc164022946)

[**5.** **LÍNEA DE INVESTIGACIÓN** 17](#_Toc164022957)

[**CAPITULO 2** 17](#_Toc164022958)

[**6.** **MARCO TEÓRICO** 17](#_Toc164022959)

[**6.1.** **Marco Referencial** 17](#_Toc164022960)

[**6.2.** **Marco Conceptual** 20](#_Toc164022961)

[**6.3.** **Marco Ingenieril** 24](#_Toc164022962)

[**CAPITULO 3** 26](#_Toc164022963)

[**7.** **METODOLOGÍA** 26](#_Toc164022964)

[**7.1.** **Metodología de Investigación** 26](#_Toc164022965)

[**7.2.** **Metodología de Desarrollo** 28](#_Toc164022966)

[**8.** **DESARROLLO DEL PROYECTO** 30](#_Toc164022968)

[**8.1.** **Desarrollo de la Metodología** 30](#_Toc164022969)

[**8.1.1 Metodología de Investigación** 30](#_Toc164022970)

[**8.1.2 Metodología de Desarrollo** 43](#_Toc164022972)

[**8.2.** **Costo del proyecto** 80](#_Toc164023011)

[**9.** **TESTER** 81](#_Toc164023013)

[**CAPITULO 4** 82](#_Toc164023014)

[**10.** **CONCLUSIONES** 82](#_Toc164023015)

[**11.** **RECOMENDACIONES** 82](#_Toc164023016)

[**PROYECCIONES** 83](#_Toc164023017)

[**REFERENCIAS BIBLIOGRÁFICAS** 83](#_Toc164023018)

**LISTA DE TABLAS**

[Tabla 1. Etapas de la metodología RUP. (Jorge Paramo, 2024). 29](#_Toc164090425)

[Tabla 2. Características del usuario administrador. 46](#_Toc164090426)

[Tabla 3. Características de un usuario. 46](#_Toc164090427)

[Tabla 4. Funcionalidad 01. 46](#_Toc164090428)

[Tabla 5. Funcionalidad 02. 46](#_Toc164090429)

[Tabla 6. Funcionalidad 03. 47](#_Toc164090430)

[Tabla 7. Funcionalidad 04. 47](#_Toc164090431)

[Tabla 8. Funcionalidad 05. 47](#_Toc164090432)

[Tabla 9. Funcionalidad 06. 48](#_Toc164090433)

[Tabla 10. Funcionalidad 07. 48](#_Toc164090434)

[Tabla 11. Funcionalidad 08. 48](#_Toc164090435)

[Tabla 12. Matriz del análisis de riesgo. 53](#_Toc164090436)

[Tabla 13. Matriz de control de pruebas de caja blanca y caja negra. 74](#_Toc164090437)

[Tabla 14. Recursos financieros 81](#_Toc164090438)

# **LISTA DE FIGURAS**

[Figura 1. Formula de Cochran para poblaciones finitas. (Herrera, M. s. f.) 30](#_Toc164090458)

[Figura 2. Respuestas de los alumnos encuestados a la pregunta 1 de la encuesta. 32](#_Toc164090459)

[Figura 3. Respuestas de los alumnos encuestados a la pregunta 2 de la encuesta. 33](#_Toc164090460)

[Figura 4. Respuestas de los alumnos encuestados a la pregunta 3 de la encuesta. 34](#_Toc164090461)

[Figura 5. Respuestas de los alumnos encuestados a la pregunta 4 de la encuesta. 35](#_Toc164090462)

[Figura 6. Respuestas de los alumnos encuestados a la pregunta 5 de la encuesta. 36](#_Toc164090463)

[Figura 7. Respuestas de los alumnos encuestados a la pregunta 6 de la encuesta. 37](#_Toc164090464)

[Figura 8. Respuestas de los alumnos encuestados a la pregunta 7 de la encuesta. 38](#_Toc164090465)

[Figura 9. Respuestas de los alumnos encuestados a la pregunta 8 de la encuesta. 39](#_Toc164090466)

[Figura 10. Respuestas de los alumnos encuestados a la pregunta 9 de la encuesta. 40](#_Toc164090467)

[Figura 11. Respuestas de los alumnos encuestados a la pregunta 10 de la encuesta. 41](#_Toc164090468)

[Figura 12. Diagrama de requisitos funcioanles. 49](#_Toc164090469)

[Figura 13. Diagrama de reglas de negocio del software. 50](#_Toc164090470)

[Figura 14. Diagrama de perfiles de usuario. 51](#_Toc164090471)

[Figura 15. Diagrama de requerimientos. 52](#_Toc164090472)

[Figura 16. Diagrama de restricciones. 52](#_Toc164090473)

[Figura 17. Caso de uso 01: Crear Usuario 56](#_Toc164090474)

[Figura 18. Caso de uso 02: Modificar Usuario 57](#_Toc164090475)

[Figura 19. Caso de uso 03: Mostrar Usuario 58](#_Toc164090476)

[Figura 20. Caso de uso 04: Listar usuarios 59](#_Toc164090477)

[Figura 21. Caso de uso 05: Crear estadística. 60](#_Toc164090478)

[Figura 22. Caso de uso 06: Modificar estadística. 61](#_Toc164090479)

[Figura 23. Caso de uso 07: Mostrar estadística. 62](#_Toc164090480)

[Figura 24. Caso de uso 08: Listar estadísticas. 63](#_Toc164090481)

[Figura 25. Diagrama del Sistema parte I. 64](#_Toc164090482)

[Figura 26. Diagrama del sistema parte II 64](#_Toc164090483)

[Figura 27. Colección Usuario 66](#_Toc164090484)

[Figura 28. Colección de estadísticas. 66](#_Toc164090485)

[Figura 29. Diagrama de actividades. 68](#_Toc164090486)

[Figura 30. Flujo de navegación. 68](#_Toc164090487)

[Figura 31. Wireframe de la página Índex. 69](#_Toc164090488)

[Figura 32. Wireframe de los formularios de la página web 69](#_Toc164090489)

[Figura 33. Wireframe de la página de contacto. 69](#_Toc164090490)

[Figura 34. Wireframe de la página del juego. 70](#_Toc164090491)

[Figura 35. Wireframe de selección de respuestas en el juego. 71](#_Toc164090492)

[Figura 36. Wireframe de consulta sobre información sobre temas de ciberseguridad. 72](#_Toc164090493)

[Figura 37. Wireframe del perfil de usuario. 73](#_Toc164090494)

# **CAPÍTULO 1**

# **INTRODUCCIÓN**

# **PROBLEMA**

## **Planteamiento del problema**

Desde la llegada del entorno digital, la seguridad informática se ha convertido en una preocupación importante. Debido al deseo de las personas por la conectividad y el consumo de servicios, o para los recursos del entorno de red, la seguridad suele ocupar un lugar secundario. Es en esta ignorancia y falta de interés que Los ciberdelincuentes buscan un lugar abierto para llevar a cabo sus delitos.

En un mundo donde nuestra identidad digital está intrínsecamente ligada a nuestra personalidad, es esencial entender cómo esta identidad puede ser vulnerada y cuáles son los riesgos predominantes en los ciberataques en Colombia. Según la investigación del Dr. Santiago Acurio Del Pino en 2022, titulada "Delitos Informáticos: Generalidades", se señalan diversas formas y métodos mediante los cuales los delincuentes pueden obtener información de las víctimas. Entre estos métodos se destacan los datos falsos o engañosos (data diddling), la manipulación de programas o "caballos de troya" (troya horses), la técnica del salami (salami technique/rounching down), las falsificaciones informáticas, la manipulación de los datos de salida y el phishing (Acurio Del Pino, S. 2020, pp. 22-24). Estos métodos de ataque son comunes en la metodología de robo de información. Además, la Escuela de Inteligencia y Contrainteligencia (ESICI) publicó en mayo de 2022 un boletín titulado "EL RIESGO DE LOS CIBERATAQUES PARA COLOMBIA", donde se analiza la falta de seguridad informática en el país en el contexto actual.

Gracias a la pandemia por el Covid-19 ha aumentado la virtualización de la vida y el trabajo, lo que ha resultado en un incremento de la ciberdelincuencia como lo indica un estudio realizado por INTERPOL sobre el impacto de la pandemia de COVID-19 en la seguridad informática en el año 2020. Donde las entidades más afectadas por estos ataques solían ser individuos y pequeñas empresas; sin embargo, en la actualidad, se ha registrado un desplazamiento hacia grandes corporaciones, entidades gubernamentales y sistemas de infraestructura crítica. (INTERPOL, 2020)

Según el boletín, "han incrementado el uso de páginas falsas, textos desinformativos, mensajes con virus adjuntos y llamadas engañosas para apropiarse tanto de datos personales como de datos bancarios" (ESICI, 2022, pág. 1). Además, el boletín hace referencia a que cerca del 43% de las compañías en Colombia no están debidamente equipadas para hacer frente a posibles ciberataques.

La Universidad de Cundinamarca, al igual que muchas otras instituciones educativas, se enfrenta a desafíos significativos en lo que respecta a la concienciación y formación en ciberseguridad entre su comunidad estudiantil. Aunque la Universidad de Cundinamarca cuenta con jornadas de seguridad y privacidad en la información, cursos y canales digitales, muchos estudiantes no están informados, no muestran interés en el tema o encuentran que es poco efectivo, lo que puede perjudicar tanto a los sistemas como al entorno universitario, e incluso al bienestar de un estudiante fuera de la entidad educativa.

Ante la problemática expuesta, surge la idea de este proyecto: proporcionar a los estudiantes una herramienta que les permita comprender los riesgos asociados con la información en internet y cómo reducirlos mediante buenas prácticas de almacenamiento de información personal, identificación de posibles amenazas en la web, consejos para la exposición de información en redes sociales y planes de contingencia para enfrentar cualquier riesgo que se presente.

## **Formulación del problema**

¿Cómo desarrollar un prototipo web que pueda fomentar buenas prácticas en ciberseguridad para los estudiantes de la Universidad de Cundinamarca extensión Chía?

# **OBJETIVOS**

## **Objetivo General**

Desarrollar un prototipo web el cual ayude a fomentar buenas prácticas en ciberseguridad por medio de gamificación para los estudiantes de la Universidad de Cundinamarca extensión Chía.

## **Objetivos específicos**

* Sintetizar los requisitos funcionales y no funcionales esenciales para el prototipo.
* Diseñar el conjunto de diagramas para el desarrollo del prototipo.
* Desarrollar el software completo a partir del estudio y evaluación del modelo propuesto.
* Verificar la calidad del software mediante la ejecución de pruebas de caja blanca y caja negra.

# **ALCANCES Y LIMITACIONES**

* 1. **Alcances**

Los alcances del aplicativo son:

* Se busca desarrollar un aplicativo web que pueda integrarse en el sistema de la Universidad de Cundinamarca, con el propósito de brindar formación en ciberseguridad a los estudiantes que forman parte de esta institución.
* El entorno web desarrollado pretende ser usado por los estudiantes como recurso de consulta y revisión de conocimientos para minimizar futuros errores que se cometan a la hora de interactuar con información relacionada a la ciberseguridad.
* La plataforma puede rastrear el progreso de los usuarios de manera precisa. Esto va a permitir a los administradores y profesores hacer un seguimiento de la participación y el rendimiento de cada estudiante, identificar áreas de mejora.
* Promover la interacción activa de los estudiantes a través de ejercicios, casos prácticos y cuestionarios, integrando elementos de gamificación como recompensas, desafíos y seguimiento del progreso.
* La plataforma web se diseñará para ser compatible con diferentes dispositivos y navegadores, asegurando su accesibilidad para todos los estudiantes.
* El aplicativo puede fomentar la colaboración entre estudiantes y profesores en proyectos relacionados con la ciberseguridad, lo que puede enriquecer aún más la experiencia de aprendizaje y promover la investigación en este campo.
  1. **Limitaciones**

Las limitaciones del aplicativo son :

* Es posible que algunos estudiantes y usuarios no puedan acceder a las aplicaciones web debido a la falta de dispositivos o conexiones confiables a Internet. Esta situación podría reducir la posibilidad de participación y, en última instancia, dejar fuera a aquellos con recursos limitados.
* Disponibilidad exclusiva para los estudiantes de la Universidad de Cundinamarca, Extensión Chía. Implementar un sistema de autenticación que requiera que los usuarios ingresen con sus credenciales de la Universidad de Cundinamarca junto con un sistema de auditoría y monitoreo constante para detectar y abordar posibles accesos no autorizados.
* Para conservar una plataforma de formación útil, es fundamental actualizar su contenido periódicamente con las tendencias más actuales y los mejores métodos. Mantener el contenido actualizado y relevante puede ser un desafío constante.
* No abordará aspectos más avanzados de ciberseguridad.

# **JUSTIFICACIÓN**

Los sistemas de información están cada vez más arraigados a nuestra cultura, ya sea para la comunicación con otras personas, adquisición de productos o servicios, plataformas educativas, etcétera. Estos sistemas sólo pueden obtener datos si los usuarios los suministran, es aquí el punto de toda la problemática, estos mismos usuarios no saben distinguir entre software legítimo y alguna copia que esté diseñada para captar estos datos que pueden ser sensibles o de carácter no divulgativo, esto para ser utilizada con fines ilícitos, ya sea robo de identidad, datos sensibles, cuentas bancarias, entre otros. Y son los propios usuarios los que entregan esa información por desconocimiento, por eso es importante que se concienticen sobre ciberseguridad.

Para comprender el nivel de conocimiento sobre los temas que se tratan en el proyecto y si éste sí es aplicable para resolver la problemática dentro de la institución Universidad de Cundinamarca extensión Chía se realizó una encuesta con estudiantes de primer a tercer semestre del programa Ingeniería de Sistemas en el primer periodo académico de 2024, la encuesta se realizó con base en la idea de comprender si los estudiantes tienen conocimientos sobre los riesgos a los que están expuestos, conceptos sobre ciberseguridad, capacidad de detectar elementos sospechosos que se les envían y si han visto información relacionada a los temas tratados en el proyecto como Ingeniería Social, Spam o Phishing por distintos medios de comunicación, incluyendo los portales de la Universidad de Cundinamarca extensión Chía. Los resultados de la encuesta están en el punto 8.1.2 titulado Metodología de Investigación.

Gracias a las conclusiones de la encuesta realizada a los alumnos se pudo extraer que aproximadamente un tercio de los participantes en la encuesta exhibe niveles más bajos de conciencia y prácticas en ciberseguridad. La carencia en la verificación de autenticidad, revisión de enlaces y actualización de conocimientos resalta áreas críticas que requieren mejoras significativas. Es fundamental que la Universidad de Cundinamarca Extensión Chía aborde de manera efectiva la escasez de información sobre ciberseguridad, especialmente considerando que un 67.5% de los encuestados perciben que la información disponible es poco accesible.

La concepción y perspectiva del prototipo web tiene como objetivo concientizar a los usuarios de las plataformas y espacios virtuales de la Universidad de Cundinamarca en Chía sobre los riesgos inherentes a la navegación en internet. Su propósito es equipar a los usuarios con las herramientas necesarias para identificar estos peligros, prevenirlos activamente y conocer las acciones adecuadas a tomar en caso de enfrentar cualquier problema relacionado con la ciberseguridad. De esta manera, se pretende crear una herramienta que contribuya a aumentar el porcentaje de estudiantes que tengan acceso a información sobre ciberseguridad en la Universidad de Cundinamarca extensión Chía.

Una estrategia pedagógica esencial en este proyecto es la gamificación, ya que proporciona una experiencia de aprendizaje dinámica y participativa, motivando a los estudiantes a instruirse con conocimientos esenciales en ciberseguridad. Además del compromiso, la gamificación ayuda a los usuarios a adquirir las habilidades que necesitan para mantenerse seguros en línea en un mundo cada vez más digital y conectado.

La universidad tiene el reto de transformar al estudiante y buscar la forma de que trascienda el conocimiento de las aulas. La gamificación es un método ideal para lograr ese objetivo dentro del ámbito educativo universitario puesto que los estudiantes valoran positivamente la metodología de aprendizaje de manera activa y colaborativa según lo remarca el proyecto Torres Toukoumidis, A. y Romero Rodríguez, L. en el 2018 titulado “Gamificación en Iberoamérica: Experiencias desde la comunicación y la educación” para la facultad de Comunicación en la Universidad Politécnica Salesiana, Quito, Ecuador. Aunque se debe tener un balance entre los retos y la capacidad de los alumnos evitando que tengan sentimientos de frustración al no cumplir con la meta o aburrimiento al ser demasiado fácil. En las instituciones educativas surgen problemáticas con el concepto de gamificación y cómo puede ser aplicado para enseñar sobre buenas prácticas de seguridad informática, puesto que el rol del profesor cambia cuando la gamificación entra como metodología de enseñanza, sus formas de impartir conocimiento pasan a ser simples guías para los alumnos, estos últimos adoptan un papel más protagónico porque son los que generan el conocimiento al interactuar con la actividad (Torres Toukoumidis, A. y Romero Rodríguez, L. 2018, pg. 246). Este enfoque educativo en el campo de los sistemas dentro del entorno universitario facilita la interacción entre el alumno y el software. Este último actúa como un docente al guiar a los estudiantes y estimular su interés en adquirir conocimientos en ciberseguridad, ofreciendo así una experiencia de aprendizaje interactiva y efectiva.

# **LÍNEA DE INVESTIGACIÓN**

SOFTWARE, SISTEMA EMERGENTES Y NUEVAS TECNOLOGÍAS

# **CAPITULO 2**

# **MARCO TEÓRICO**

## **Marco Referencial**

El marco teórico se fundamenta en proyectos previos de distintas instituciones que guardan relación con nuestro enfoque, ya sea por compartir una línea de investigación afín o por presentar resultados similares a los que esperamos obtener en este desarrollo.

En el proyecto titulado "Campaña de sensibilización y buenas prácticas de ciberseguridad" realizado por los estudiantes Ahumada Ortiz y Teresa Paulina en 2020, se destaca la importancia de la educación en ciberseguridad para los empleados. Esta investigación subraya que la formación en ciberseguridad es esencial para prevenir riesgos y proteger la información vital de la empresa. Se concluye que, a pesar de contar con políticas de seguridad respaldadas por estándares internacionales, las empresas a menudo descuidan la vulnerabilidad de sus empleados, constituyendo el punto más débil de la organización en términos de ciberseguridad. Esto refuerza la necesidad de realizar campañas de concienciación en ciberseguridad para mitigar estos riesgos.

En el proyecto "Guía de buenas prácticas para reducir riesgos de engaños a menores entre 13 a 15 años en redes sociales" llevado a cabo por Peña Sandoval, Mayra Alejandra Sánchez Rodríguez y Diana Marcela en 2022, se resalta la importancia de abordar la ciberseguridad en el contexto de las redes sociales, especialmente para la población juvenil. Se evidencian los riesgos que enfrentan los menores en las plataformas digitales y la necesidad imperante de guiarlos hacia prácticas seguras en línea.

El proyecto realizado por el estudiante Álvarez Oria, Luis en 2021, titulado "Desarrollo de una herramienta para plan de concienciación en ciberseguridad basada en gamificación", expone cómo la universalización del uso de tecnologías de comunicación y el acceso generalizado a Internet brindan una oportunidad relevante para diseñar software destinado a concienciar sobre ciberseguridad. Este proyecto busca proporcionar formación básica en ciberseguridad para el usuario promedio de Internet que carece de conocimientos específicos en este campo. Se reconoce la existencia de talleres y kits de concienciación en ciberseguridad que facilitan la adquisición de conocimientos básicos.

Además, el estudio de Weitl-Harms, Sherri; Spanier, Adam; Hastings, John; & Rokusek, Matthew en 2023, titulado "A Systematic Mapping Study on Gamification Applications for Undergraduate Cybersecurity Education", enfatiza las ventajas de la gamificación en la educación, especialmente para mejorar la participación de los estudiantes en temas complejos como las Operaciones de Ciberseguridad (CSO). Aunque se reconoce el potencial de la gamificación, se subraya la falta de investigaciones exhaustivas sobre su efectividad en la educación de las OSC (Operaciones de Ciberseguridad). Este estudio llena este vacío de conocimiento al examinar 74 artículos relevantes que analizan 80 estrategias de gamificación empleadas en la educación de las OSC. Los resultados recopilados brindan información esencial sobre estas estrategias y su impacto en el compromiso de los estudiantes, estableciendo así una base valiosa para futuras investigaciones en este ámbito.

Con este marco de referencia, subrayamos la crucial importancia de la educación en ciberseguridad para mitigar riesgos y salvaguardar información, focalizándose especialmente en estudiantes como puntos vulnerables. Considerando la probada efectividad de la gamificación en la enseñanza de ciberseguridad, respaldada por investigaciones anteriores, generamos nuestra estrategia de emplearla para potenciar la formación en ciberseguridad y fomentar buenas prácticas en entornos educativos. Además, la necesidad de orientar a los usuarios, particularmente a los jóvenes, hacia prácticas seguras en redes sociales se alinea perfectamente con nuestro propósito de generar conciencia y fomentar un uso seguro de la tecnología a través de nuestro proyecto.

## **Marco Conceptual**

El marco conceptual de este proyecto abarca la concepción de los elementos utilizados en el mismo, desde el desarrollo de la interfaz de usuario hasta la gestión de datos y la recopilación de información a través de encuestas. Conceptos clave como la gamificación, la seguridad de la información y la documentación del proyecto son fundamentales para crear un entorno educativo interactivo, motivador y seguro, con el objetivo de fortalecer la conciencia y las habilidades en ciberseguridad en la comunidad estudiantil, generando así un impacto positivo en la seguridad digital.

* Ciberseguridad:

Según Cisco (2024, párrafo 1), la ciberseguridad se define como "la práctica de proteger sistemas, redes y programas de ataques digitales", lo que implica la implementación de prácticas y medidas destinadas a salvaguardar la integridad, confidencialidad y disponibilidad de la información en entornos digitales.

* Gamificación:

Torres Toukoumidis, A. y Romero Rodríguez, L. (2018, pág. 11) definen la gamificación como "la aplicación de elementos de juego en contextos no lúdicos con el fin de motivar cambios de comportamiento hacia una dirección específica". Esto implica el uso de recompensas, competiciones y desafíos para aumentar la participación y retención de información en experiencias educativas o laborales.

* Front-End

Según Bautista Garcia (2021), el Front-End se refiere a la parte frontal de una página web, que abarca el diseño de la estructura del sitio hasta los estilos de los colores, fondos, tamaños, animaciones y efectos. Esta definición resalta que el Front-End es la parte de la interfaz con la que los usuarios finales interactúan directamente cuando utilizan una aplicación o navegan por un sitio web. Involucra aspectos visuales y de diseño, así como la experiencia del usuario en términos de navegación y usabilidad utilizando tecnologías como HTML, CSS y JavaScript.

* Back-End:

La definición de Bautista Garcia (2021) nos dice que el Back-End es la capa de acceso a los datos de un software. Se refiere a la lógica tecnológica que hace que una página web funcione, y queda oculta a ojos del visitante. Esta definición resalta que el Back-End es responsable del procesamiento de datos y la lógica de la aplicación, incluyendo el manejo de servidores, bases de datos y la implementación de algoritmos. Es la parte no visible de la aplicación que permite que funcione de manera eficiente y segura.

* Modelo Cliente-Servidor:

Según Know How (2023), un principio cliente-servidor es un modelo de comunicación que permite la distribución de tareas dentro de una red de ordenadores. Esto implica que los clientes, que son las interfaces de usuario, realizan solicitudes al servidor, que es donde reside la lógica y el almacenamiento de los recursos. El servidor responde a estas solicitudes proporcionando los recursos solicitados. Esta arquitectura de red permite una distribución eficiente de tareas y recursos dentro de una red, facilitando la interacción entre los usuarios y los sistemas.

* Bases de Datos:

Según Oracle (2024), una base de datos es una recopilación organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema informático. Esta definición resalta que las bases de datos son sistemas organizados para almacenar, gestionar y recuperar información de manera estructurada. Utilizan tablas, registros y campos para organizar datos, permitiendo la gestión eficiente de grandes cantidades de información.

* Concepto de Metodología de Desarrollo:

La metodología de desarrollo es un enfoque sistemático y estructurado para planificar, ejecutar y controlar el proceso de construcción de un sistema, aplicación o proyecto. En este proyecto, se adoptará una metodología ágil, caracterizada por su enfoque iterativo e incremental. Este enfoque permite una respuesta ágil a los cambios, una mayor colaboración entre equipos y una entrega continua de funcionalidades mejoradas. La metodología de desarrollo guiará la planificación de tareas, la asignación de recursos y la implementación eficiente, asegurando la alineación del proyecto con los objetivos y adaptándose de manera flexible a medida que evolucionan los requisitos y desafíos.

* Informes en Gráficas:

Según MicroStrategy (2021), un informe gráfico consiste en una representación de datos en un formato visual que ayuda a ver las tendencias generales con facilidad, a identificar medianas y excepciones, entre otros. Los informes en gráficas se refieren a la presentación visual de datos a través de gráficos y visualizaciones. Estos informes facilitan la comprensión rápida de tendencias, patrones y relaciones en los datos, proporcionando una representación visual clara y efectiva.

* Encuestas:

Las encuestas son instrumentos de recopilación de datos que utilizan preguntas estructuradas para obtener información específica de un grupo de participantes. Son herramientas valiosas para la obtención de opiniones, percepciones y datos cuantitativos o cualitativos sobre un tema determinado.

* Documentación del Proyecto:

Según Sinnaps (2024), la documentación del proyecto comprende la creación y mantenimiento de registros escritos y visuales que describen todos los aspectos del proyecto. Incluye detalles sobre el diseño, desarrollo, pruebas, implementación y gestión, proporcionando una referencia integral para todos los involucrados en el proyecto. La documentación del proyecto es fundamental para garantizar la comprensión, la colaboración y la continuidad del proyecto a lo largo de su ciclo de vida. Los documentos que se realizan para la descripción del prototipo incluyen:

* Requerimientos funcionales.
* Reglas de negocio.
* Perfiles de usuarios.
* Requisitos.
* Restricciones.
* Casos de uso
* Diagrama de actividades
* Wireframe

## **Marco Ingenieril**

En este marco se explican las herramientas que se usan dentro del proyecto y cuál es la función que cumplen dentro del mismo:

* Herramientas para Front-End:
  + HTML (Hypertext Markup Language): Utilizado para definir la estructura básica y los elementos de la interfaz de usuario. Permite organizar y presentar contenido de manera semántica.
  + CSS (Cascading Style Sheets): Responsable de la presentación y diseño visual. Se utiliza para dar estilo a los elementos HTML, mejorando la estética y la experiencia del usuario.
  + JavaScript (JS): Lenguaje de programación que se destina en el Front-End a la interactividad y dinamismo a la interfaz. Se utiliza para manipular el contenido de la página en tiempo real, responder a acciones del usuario y mejorar la experiencia de navegación.
  + Google Charts: Biblioteca que ofrece una variedad de gráficos y visualizaciones interactivas. Se utilizará para presentar de manera clara y comprensible los informes visuales generados a partir de los datos recopilados.
* Herramientas para Back-End:
  + Node.js: Plataforma basada en JavaScript que permite ejecutar código del lado del servidor. Se utiliza para gestionar la lógica de negocio, manejar las solicitudes del cliente y conectar con la base de datos.
* Gestión de Bases de datos:
  + MongoDB: Base de datos NoSQL que almacena datos en formato JSON. Se emplea para almacenar de manera eficiente la información del proyecto y facilitar su consulta y actualización.
* Gestión de Líneas de Tiempo:
  + Gantt Project: Herramienta especializada en la planificación y gestión de proyectos mediante diagramas de Gantt. Facilita la representación visual de tareas, hitos y plazos, mejorando la organización y seguimiento del proyecto.
* Realización de Encuestas:
  + Google Forms: Plataforma para crear encuestas personalizadas y recopilar respuestas de manera eficiente. Ofrece una interfaz fácil de usar para diseñar encuestas y analizar los resultados.
* Documentación del Proyecto:
  + Enterprise Architect: Utilizado para crear diagramas y casos de uso que representa la arquitectura y la interacción de los componentes del proyecto.
  + Microsoft 365: Herramienta para la redacción y almacenamiento de documentos formales relacionados con el proyecto, como informes, manuales y especificaciones.
  + Figma: Plataforma colaborativa para diseñar wireframes y prototipos de interfaz de usuario. Facilita la visualización y comprensión del diseño del proyecto antes de la implementación.

# **CAPITULO 3**

# **METODOLOGÍA**

## **Metodología de Investigación**

Para abordar los desafíos de la ciberseguridad entre los estudiantes, se optó por implementar una metodología mixta que combina técnicas de investigación cuantitativa y cualitativa. Esta elección se fundamenta en la capacidad de este enfoque para proporcionar una comprensión integral y detallada de las percepciones y experiencias de los usuarios.

En primer lugar, se llevaron a cabo encuestas aleatorias a 40 estudiantes de primer a tercer semestre para obtener datos cuantitativos sobre sus conocimientos, actitudes y prácticas en materia de ciberseguridad. Este enfoque cuantitativo permite obtener información de manera eficiente y generalizable sobre las tendencias y patrones en la seguridad en línea entre la población estudiantil.

Además, se recurrió a enfoques cualitativos, como el análisis de contenido mediante herramientas de análisis de datos como Google Analytics, para profundizar en las percepciones y experiencias de los usuarios. Este análisis cualitativo proporciona una comprensión más rica y detallada de los factores subyacentes que influyen en el comportamiento y las actitudes de los estudiantes hacia la ciberseguridad.

El proyecto se basa en un enfoque metodológico deductivo, partiendo de premisas generales sobre ciberseguridad para llegar a conclusiones aplicables a la realidad estudiantil. Este proceso implica la recolección y análisis de información descriptiva para identificar necesidades y áreas de mejora en las prácticas de seguridad en línea de los estudiantes.

A través de este enfoque deductivo, se formularon hipótesis sobre el impacto del prototipo web en la formación de buenas prácticas en ciberseguridad. Esto permitirá evaluar mejor la efectividad del prototipo y su influencia en la concienciación y capacitación en ciberseguridad, proporcionando así una base sólida para la toma de decisiones y la implementación de medidas de mejora.

## **Metodología de Desarrollo**

Para garantizar el correcto desarrollo del aplicativo web, se ha optado por hacer uso de la metodología ágil Rational Unified Process (RUP), la cual ofrece una estructura flexible y adaptable para el desarrollo de proyectos de software.

Según el trabajo de Fabio Orlando Cruz (2022) titulado "Análisis de la metodología RUP en el desarrollo de software académico mediante la herramienta DJANGO", los desarrollos aplicados con la metodología RUP deben seguir un enfoque por fases, que incluye etapas de Inicio, Elaboración, Construcción y Transición. Esta estructura por fases permite una planificación clara y una gestión eficiente del proyecto, asegurando un progreso ordenado y controlado a lo largo del ciclo de vida del desarrollo.

La metodología RUP fue creada por Rational Software en 1998 bajo el liderazgo de Grady Booch, Ivar Jacobson y James Rumbaugh. Surgió como una actualización de la metodología ROP (Rational Objectory Process) y ha sido ampliamente utilizada en la industria del software debido a su enfoque pragmático y su capacidad para adaptarse a diferentes contextos y necesidades de desarrollo. La tabla de la metodología RUP, que se muestra en la tabla 1 titulada "Etapas de la metodología RUP", es una herramienta para guiar y estructurar el proceso de desarrollo en nuestro proyecto, y ha sido una contribución del director del proyecto.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TAREAS DEL PROCESO** | **INICIO** | **ELABORACIÓN** | **COSTRUCCIÓN** | **TRANSISIÓN** |
| MODELADO DEL NEGOCIO | Hablar con el cliente | Borrador de la propuesta | Propuesta | Lista y diagrama de Funcionalidades, Reglas de Negocio, Perfiles de usuario, requisitos y restricciones. |
| REQUISITOS | Evaluación y aceptación de los requisitos por parte del cliente, el jefe del proyecto y el arquitecto de software | Análisis del riesgo. | Casos de Uso en formato extendido. | Documento con los casos de uso en formato extendido. |
| ANALISIS Y DISEÑO | Estudio de los casos de uso en formato extendido y pasarlo al modelo general. | Estructura de la BD. | Diagramas de actividades, flujo de navegación, diagramas de presentación y diseños de wireframe. | Modelo completo y corregido. |
| IMPLEMENTACIÓN  DESARROLLO | Estudio y evaluación del modelo por parte de los desarrolladores y codificadores | Generación de la BD. | Desarrollo de los formularios y subida de registros para pruebas. | Software completo |
| PRUEBAS | Matriz de comportamiento de caja blanca como de caja negra. | Ejecución de pruebas de caja blanca. | Ejecución de pruebas de caja negra. | Certificado de carencia de defectos. |

1. Etapas de la metodología RUP. (Jorge Paramo, 2024).

# **DESARROLLO DEL PROYECTO**

## **Desarrollo de la Metodología**

8.1.1 Metodología de Investigación

Para abordar los desafíos de la ciberseguridad entre los estudiantes, se optó por implementar una metodología mixta que combina técnicas de investigación cuantitativa y deductiva. Esta elección se fundamenta en la capacidad de este enfoque para proporcionar una comprensión integral y detallada de las percepciones y experiencias de los usuarios.

Dado que el proyecto se enfoca en la totalidad de los estudiantes de primer a tercer semestre de Ingeniería de Sistemas de la Universidad de Cundinamarca Sede Chía, durante el primer periodo académico de 2024, se llevó a cabo una muestra aleatoria simple de 40 individuos para determinar los participantes de la encuesta. El tamaño de la muestra se determinó utilizando la fórmula de Cochran, dado que la población es finita.

1. Formula de Cochran para poblaciones finitas. (Herrera, M. s. f.)

Considerando que *n* representa el tamaño de la muestra necesario, *N* denota el total de la población, que en este caso comprende 240 estudiantes de Ingeniería de Sistemas en la universidad, incluyendo cursos diurnos y nocturnos. *Z* representa el valor crítico de la distribución normal estándar para un nivel de confianza específico, utilizando un 90% de confianza en la investigación. *p* indica la proporción estimada de la población con la característica de interés, fijada en un 5% para el estudio, mientras que *q* representa 1-*p*. *d* representa la precisión, establecida en un 5% para la investigación. Aplicando estos datos a la fórmula, el resultado indica que deberíamos tener una muestra de 39.8154 individuos, aunque se redondeó a 40 para obtener un número entero para toma de la muestra. La encuesta comprende 10 preguntas que exploran la conciencia en ciberseguridad, abordando los conocimientos, prácticas y actitudes de los estudiantes frente a situaciones de riesgo como la vulneración de datos, enlaces maliciosos, robo de identidad, entre otros. Este enfoque cuantitativo facilita la obtención eficiente y generalizable de información sobre las tendencias y patrones en seguridad en línea dentro de la población estudiantil.

Además, se empleó Google Analytics para generar gráficos basados en las respuestas de las encuestas, lo cual facilitó la comprensión de los datos y la extracción de información relevante relacionada con la conciencia en ciberseguridad, mejorando así la interpretación de la información recolectada.

Y en cuanto al enfoque metodológico deductivo, partiendo de premisas generales sobre la conciencia en ciberseguridad para llegar a conclusiones aplicables a la realidad estudiantil. A través de este enfoque deductivo, se formuló la hipótesis sobre el impacto del prototipo web en la formación de buenas prácticas en ciberseguridad. Esto permitirá una evaluación más precisa de la efectividad del prototipo y su influencia en la concientización y capacitación en ciberseguridad, proporcionando así una base sólida para la toma de decisiones y la implementación de medidas de mejora para los alumnos.

Estos son los resultados de la encuesta, la cual consta de diez preguntas, fueron cuarenta estudiantes de manera anónima entre primer y tercer semestre del programa de Ingeniería de Sistemas de la Universidad de Cundinamarca extensión Chía quienes contestaron la encuesta.

1. Respuestas de los alumnos encuestados a la pregunta 1 de la encuesta.

En la Figura 2 se presentan las respuestas de los alumnos a la pregunta 1, dirigida a entender la frecuencia con la que utilizan redes sociales, correos electrónicos y otros medios para compartir información en línea. Quince (15) estudiantes siempre emplean estos medios, diecinueve (19) lo hacen normalmente, cinco (5) no lo hacen regularmente, y solo un encuestado casi nunca los utiliza.

1. Respuestas de los alumnos encuestados a la pregunta 2 de la encuesta.

En la Figura 3 se evidencian las respuestas de los alumnos a la pregunta 2, que busca entender la facilidad con la que comparten información personal cuando se les solicita en medios en línea. Cuatro (4) estudiantes siempre comparten esta información, doce (12) lo hacen normalmente, quince (15) no lo hacen regularmente, seis (6) casi nunca, y tres (3) nunca comparten la información solicitada.

1. Respuestas de los alumnos encuestados a la pregunta 3 de la encuesta.

En la Figura 4 se presentan las respuestas de los estudiantes a la pregunta 3, la cual busca entender la frecuencia con la que verifican la autenticidad de la información en las páginas web que visitan, incluyendo certificados SSL y firmas de dominio. Los resultados indican que nueve (9) estudiantes siempre realizan esta verificación, once (11) lo hacen normalmente, siete (7) no lo hacen regularmente, diez (10) casi nunca lo hacen, y dos (2) nunca lo hacen.

1. Respuestas de los alumnos encuestados a la pregunta 4 de la encuesta.

En la Figura 5 se muestran las respuestas de los estudiantes a la pregunta 4, que busca conocer si revisan los enlaces de las páginas web antes de abrirlos. Doce (12) estudiantes siempre llevan a cabo esta revisión, trece (13) lo hacen normalmente, seis (6) no lo hacen regularmente, seis (6) casi nunca lo hacen, y dos (2) nunca lo hacen.

1. Respuestas de los alumnos encuestados a la pregunta 5 de la encuesta.

En la Figura 6 se destacan las respuestas de los estudiantes a la pregunta 5, la cual indaga sobre si verifican la procedencia de los mensajes que reciben a través de redes sociales, correo o mensajes de texto antes de abrirlos. Dieciséis (16) estudiantes siempre realizan esta verificación, diez (10) lo hacen normalmente, seis (6) no lo hacen regularmente, seis (6) casi nunca lo hacen, y uno (1) nunca lo hace.

1. Respuestas de los alumnos encuestados a la pregunta 6 de la encuesta.

La Figura 7 presenta las respuestas de los estudiantes a la pregunta 6, la cual explora si mantienen actualizados sus conocimientos sobre temas como ingeniería social, spam y phishing mediante noticias, foros o videos en línea. Cinco (5) estudiantes siempre se mantienen actualizados, dieciocho (18) lo hacen normalmente, ocho (8) no lo hacen regularmente, seis (6) casi nunca lo hacen, y dos (2) nunca lo hacen.

1. Respuestas de los alumnos encuestados a la pregunta 7 de la encuesta.

En la Figura 8 se ilustran las respuestas de los estudiantes a la pregunta 7, que busca determinar si utilizan medidas de protección para prevenir spam y phishing en sus actividades en línea. Diez (10) estudiantes siempre utilizan estas medidas, catorce (14) lo hacen normalmente, siete (7) no lo hacen regularmente, seis (6) casi nunca lo hacen, y dos (2) nunca lo hacen.

1. Respuestas de los alumnos encuestados a la pregunta 8 de la encuesta.

La Figura 9 muestra las respuestas de los estudiantes a la pregunta 8, la cual indaga sobre si suelen tener precauciones respecto a la información que comparten en internet, incluyendo fotos, datos personales o rutinas. Diecisiete (17) estudiantes siempre tienen precauciones, quince (15) lo hacen normalmente, cuatro (4) no lo hacen regularmente, tres (3) casi nunca lo hacen, y ninguno (0) nunca lo hace.

1. Respuestas de los alumnos encuestados a la pregunta 9 de la encuesta.

En la Figura 10 se exponen las respuestas de los estudiantes a la pregunta 9, que busca determinar si han encontrado información sobre ciberseguridad en la Universidad de Cundinamarca extensión Chía, relacionada con temas como ingeniería social, phishing o spam. Solo uno (1) de los encuestados siempre ha encontrado esta información, once (11) lo hacen normalmente, diez (10) no lo hacen regularmente, nueve (9) casi nunca lo hacen, y ocho (8) nunca lo hacen.

1. Respuestas de los alumnos encuestados a la pregunta 10 de la encuesta.

La Figura 11 presenta las respuestas de los estudiantes a la pregunta 10, la cual investiga si reportan de manera regular mensajes sospechosos de spam o phishing en sus cuentas de redes sociales, correo electrónico o celular. Siete (7) estudiantes siempre reportan estos mensajes, trece (13) lo hacen normalmente, siete (7) no lo hacen regularmente, seis (6) casi nunca lo hacen, y seis (6) nunca lo hacen.

De las tablas con la cantidad de respuestas podemos concluir lo siguiente:

* Un 15% de los encuestados no utiliza regularmente estos medios para compartir información en línea, indicando una posible falta de conciencia en prácticas de seguridad.
* Un preocupante 37.5% de los encuestados no muestra una resistencia consistente a compartir información solicitada en línea, sugiriendo una vulnerabilidad potencial a riesgos de seguridad.
* Un alto 45% no verifica la autenticidad de la información en las páginas web de manera regular, indicando una brecha en la conciencia de seguridad en línea.
* El 35% no revisa los enlaces de las páginas web antes de abrirlos con regularidad, lo que podría aumentar el riesgo de exposición a amenazas en línea.
* Un 32.5% no verifica la procedencia de mensajes en línea antes de abrirlos, lo que podría ponerlos en riesgo de ataques de phishing u otras amenazas.
* Un alto 40% de los encuestados no mantiene sus conocimientos actualizados sobre amenazas de ingeniería social, spam y phishing de manera regular, señalando una posible falta de conciencia continua.
* Un 40% no utiliza medidas de protección contra spam y phishing de manera regular, indicando una posible falta de implementación de medidas de seguridad activas.
* Solo el 17.5% de los encuestados no toma precauciones en línea, lo que sugiere una conciencia generalmente alta en cuanto a la información compartida.
* Un 67.5% de los encuestados encuentra información sobre ciberseguridad de manera irregular o nunca, lo que sugiere una necesidad urgente de mejorar la disponibilidad de información en la universidad.
* Un 32.5% no reporta mensajes sospechosos regularmente, indicando una oportunidad para fomentar una cultura de denuncia.

8.1.2 Metodología de Desarrollo

Teniendo en cuenta la Tabla 1 y los conceptos del trabajo de grado de Fabio Orlando, la metodología RUP se desarrolla en nuestro proyecto de la siguiente manera:

* **MODELADO DEL NEGOCIO:**
* **Inicio:**
  + Reunión inicial con el director del proyecto para el planteamiento del prototipo web, elaborando el anteproyecto.
* **Elaboración** 
  + El borrador de la propuesta fue la entrega del anteproyecto, con los ítems de Línea de investigación, el problema que consta del planteamiento del problema y formulación del problema, la justificación, los objetivos los cuales son el objetivo general y los específicos, alcances y limitaciones del proyecto, marco de referencia, la aproximación metodológica, recursos, resultados esperados, el cronograma del proyecto y las referencias bibliográficas.
* **Construcción** 
  + Definición de casos de uso para las funcionalidades del prototipo web.

Nuestro prototipo consta de un actor el cual puede ser un usuario o un administrador, el usuario tiene privilegios básicos mientras que el administrador tiene acceso a todas las funcionalidades del software. Otra de las entidades en el proyecto son las estadísticas que hay por cada usuario y se generan interactuando con el videojuego del aplicativo, Las funcionalidades están dadas por cada entidad y son las siguientes:

* Entidad Usuario:
  + Crear usuario (F 01).
  + Mostrar usuario (F 02).
* Listar usuarios (F 03).
* Editar usuario (F 04).
* Entidad Estadísticas
* Generar estadística (F 05).
* Mostrar estadística (F 06).
* Listar estadísticas (F 07).
* Dentro del proyecto se establecieron las reglas del negocio y son las siguientes:
  + - * Usuario no duplicado (RN 01): No puede haber usuarios duplicados.
      * Nombres y apellidos (RN 02): Se debe registrar al menos un nombre y un apellido.
      * Correo (RN 03): Se debe registrar al menos un correo institucional.
      * Fecha de nacimiento (RN 04): A los usuarios sin fecha de nacimiento se les registrará el 1 de enero de 1900.
      * Mayoría de catorce (14) años para los usuarios (RN 05): Los usuarios deben ser mayores de catorce (14) años.
      * Estadísticas no duplicadas (RN 06): No debe haber estadísticas duplicadas.
      * Estadísticas asignadas (RN 07): Cada usuario debe tener asignado una estadística.
      * Registro completo (RN 08): Se debe registrar usuario y estadística.
* Los perfiles de usuarios dentro del proyecto son aquellos que interactúan con el prototipo, hay dos perfiles los cuales son:
  + - * Administrador (PU 01), el cual tiene el control y manejo del sistema en general, permitiendo listar las listas de todos los usuarios y las estadísticas de cada uno.
      * Usuario (PU 02), el cual puede comprobar los datos de sí mismo y revisar sus estadísticas.
* Los requerimientos del software son:
* Requerimiento 01: Un sistema operativo compatible con un Navegador Web y los requisitos de este.
* Requerimiento 02: Una conexión a internet mínima de 10 Mb.
* Requerimiento 03: Un motor de conexión a base de datos compatible con MongoDB. Es necesario el motor de conexión para almacenar, acceder, modificar y mostrar los datos en el software.
* Requerimiento 04: Lenguaje de programación JavaScript. Es necesario el lenguaje de programación porque por medio de este se dan las instrucciones para que los usuarios puedan usar el programa web.
* Las restricciones del prototipo son:
* Restricción 01: No pueden acceder más de 30 usuarios al mismo tiempo, para no sobrecargar la página web.
* Restricción 02: No se puede hacer una interfaz compleja para evitar inconvenientes en dispositivos móviles.
* **Transición** 
  + Lista y diagrama de requisitos:

Características de los usuarios:

1. Características del usuario administrador.

|  |  |
| --- | --- |
| Tipo de usuario | Administrador |
| Actividades | Control y manejo del sistema en general |

1. Características de un usuario.

|  |  |
| --- | --- |
| Tipo de usuario | Usuario |
| Actividades | Comprobar las estadísticas que tiene. |

Funcionalidades:

1. Funcionalidad 01.

|  |  |
| --- | --- |
| Identificación de la función | F01 |
| Nombre del requerimiento | **Crear usuario** |
| Descripción | Opción para registrar un nuevo usuario. |

1. Funcionalidad 02.

|  |  |
| --- | --- |
| Identificación de la función | F02 |
| Nombre del requerimiento | **Modificar usuario** |
| Descripción | Opción para editar los datos del usuario. |

1. Funcionalidad 03.

|  |  |
| --- | --- |
| Identificación de la función | F3 |
| Nombre del requerimiento | **Mostrar usuario** |
| Descripción | Visualiza los detalles del usuario sin posibilidad de edición. |

1. Funcionalidad 04.

|  |  |
| --- | --- |
| Identificación de la función | F04 |
| Nombre del requerimiento | **Listar usuarios** |
| Descripción | Muestra todos los usuarios registrados. |

1. Funcionalidad 05.

|  |  |
| --- | --- |
| Identificación de la función | F05 |
| Nombre del requerimiento | **Crear estadística** |
| Descripción | Crear un nuevo registro estadístico. |

1. Funcionalidad 06.

|  |  |
| --- | --- |
| Identificación de la función | F06 |
| Nombre del requerimiento | **Modificar estadística** |
| Descripción | Visualiza las estadísticas de un usuario en particular. |

1. Funcionalidad 07.

|  |  |
| --- | --- |
| Identificación de la función | F07 |
| Nombre del requerimiento | **Mostrar estadística** |
| Descripción | Muestra los detalles de una estadística sin opción de modificación. |

1. Funcionalidad 08.

|  |  |
| --- | --- |
| Identificación de la función | F07 |
| Nombre del requerimiento | **Listar estadísticas** |
| Descripción | Muestra todas las estadísticas registradas. |

1. Diagrama de requisitos funcioanles.



En la figura 12 se puede observar el diagrama de las funcionalidades del proyecto, con los actores que acceden a ellas.

1. Diagrama de reglas de negocio del software.



En la Figura 12 se pueden evidenciar el diagrama de las reglas de negocio impuestas para este proyecto, junto a las funcionalidades a las que aplica, las cuales están determinadas según cada aplicabilidad de la regla a la funcionalidad.

1. Diagrama de perfiles de usuario.



En la Figura 14 se pueden evidenciar el diagrama de los perfiles de usuario dados en este prototipo, junto a las funcionalidades a las que aplica cada perfil, en el caso del perfil de usuario administrador se le aplican todas las funcionalidades del software, mientas que al perfil usuario sólo se le aplican las funcionalidades F01, F02, F03, F05 y F06 las cuales corresponden a las funcionalidades que no tienen que ver con listar usuarios ni estadísticas.

1. Diagrama de requerimientos.



En la Figura 15 se pueden evidenciar el diagrama de los requerimientos del software, los cuales están dados por las necesidades para poder usar el prototipo.

1. Diagrama de restricciones.



En la Figura 16 se pueden evidenciar el diagrama de restricciones del software.

Con estos ítems, los cuales están fundamentados en lo proyectado anteriormente por el cliente y la revisión de los estudiantes que desarrollaron el software, se culmina la primera etapa de la metodología que consta de las listas y diagramas de funcionalidades, reglas de negocio, perfiles de usuario, requerimientos y restricciones.

* **Requisitos**
* **Inicio:**

Los requisitos fueron evaluados y aprobados por el director del proyecto Jorge Paramo y por los arquitectos del software los cuales son los autores del proyecto.

* **Elaboración:**

En esta etapa se generó el análisis del riesgo relacionado al desarrollo del software, estos son evidenciados en la Tabla # con cada uno de los riesgos con sus impactos y medidas de mitigación que se pueden presentar dentro de la creación del prototipo.

1. Matriz del análisis de riesgo.

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo** | Amenaza | Impacto | Medidas de mitigación |
| **Falta de seguridad en el sistema** | Hackeo de la plataforma, robo de datos de usuarios. | Pérdida de confianza de los usuarios, daño a la reputación de la institución. | Implementación de medidas de seguridad robustas, como encriptación de datos, autenticación de dos factores. |
| **Errores en la lógica del juego** | Bugs o fallos en los juegos de gamificación. | Reducción de la efectividad de la plataforma como herramienta educativa. | Pruebas exhaustivas de los juegos, incluyendo pruebas de usuario, para identificar y corregir posibles errores. |
| **Problemas de rendimiento del sistema** | Sobrecarga del servidor debido a un alto número de usuarios. | Tiempos de carga lentos, experiencia de usuario deficiente. | Pruebas de carga y rendimiento para identificar y optimizar el sistema, y la escalabilidad adecuada del servidor. |
| **Falta de compatibilidad con navegadores y dispositivos** | Problemas de visualización y funcionamiento en diferentes navegadores y dispositivos. | Exclusión de ciertos segmentos de usuarios. | Pruebas exhaustivas de compatibilidad en una variedad de navegadores y dispositivos durante el desarrollo y antes del lanzamiento. |
| **Incumplimiento de los requisitos de seguridad de la información** | Falta de cumplimiento de las regulaciones de protección de datos. | Sanciones legales, multas. | Garantizar el cumplimiento de las normativas de privacidad de datos, y mantenerse actualizado con las mejores prácticas de seguridad de la información. |
| **Falta de participación de los usuarios** | Falta de interés o participación de los estudiantes en las actividades de gamificación | Reducción del impacto educativo y la efectividad de la plataforma. | Obtener retroalimentación de los usuarios durante todo el proceso de desarrollo, ajustar y mejorar la plataforma según sus necesidades y preferencias. |

* **Construcción:**

La construcción del proyecto está dada por la creación de los casos de uso, en este apartado se muestran los casos de uso del proyecto:

* Caso 01: Crear Usuario, se crea el usuario, se guarda el registro y se muestra en pantalla.
* Caso 02: Modificar Usuario, se necesita que haya creado un usuario, se filtra el registro, se guarda el registro modificado y se imprime en pantalla.
* Caso 03: Mostrar usuario, se filtra el registro de usuarios, se imprime en pantalla.
* Caso 04: Listar Usuarios, se seleccionan todos los registros de los usuarios y se muestran en pantalla.
* Caso 05: Crear estadística, se crea la estadística del usuario, se guarda el registro y se muestra en pantalla.
* Caso 06: Modificar estadística, se filtra el registro de estadísticas, se guarda el registro, se imprime en pantalla.
* Caso 07: Mostrar estadística, se filtra el registro de estadísticas, se imprime en pantalla.
* Caso 08: Listar estadísticas, se seleccionan todos los registros de las estadísticas y se muestran en pantalla.
* **Transición:**

La transición de los casos de uso viene dada con la aplicación los casos de uso con su formato extendido:

1. Caso de uso 01: Crear Usuario



|  |  |
| --- | --- |
| Nombre | CU01 Crear Usuario |
| Descripción | Crea un usuario |
| Actores | Administrador, Usuario |
| Entradas | Nombre, apellido, contraseña, correo, fecha de nacimiento. |
| Salidas | Registro creado (mensaje de éxito o fracaso) |
| Precondiciones | Que no exista ese usuario, que ningún campo debe estar vacío. |
| Postcondiciones | N/A |
| Precedentes | N/A |
| Usan o extienden | Usan CU 05 |

1. Caso de uso 02: Modificar Usuario



|  |  |
| --- | --- |
| Nombre | CU02 Modificar Usuario |
| Descripción | Modifica un usuario |
| Actores | Administrador, Usuario |
| Entradas | Nombre, apellido, contraseña, correo, fecha de nacimiento. |
| Salidas | Registro creado (mensaje de éxito o fracaso) |
| Precondiciones | Que ningún campo debe estar vacío. |
| Postcondiciones | N/A |
| Precedentes | N/A |
| Usan o extienden | Usan CU 01 |

1. Caso de uso 03: Mostrar Usuario



|  |  |
| --- | --- |
| Nombre | CU03 Mostrar Usuario |
| Descripción | Crea un usuario |
| Actores | Administrador, Usuario |
| Entradas | N/A |
| Salidas | Impresión en pantalla del usuario. |
| Precondiciones | Que exista el usuario. |
| Postcondiciones | N/A |
| Precedentes | N/A |
| Usan o extienden | Usan CU 01 |

1. Caso de uso 04: Listar usuarios



|  |  |
| --- | --- |
| Nombre | CU04 Listar Usuarios |
| Descripción | Listar a los usuarios registrados. |
| Actores | Administrador |
| Entradas | N/A |
| Salidas | Impresión de todos los registros de usuarios. |
| Precondiciones | Que existan registros de usuarios. |
| Postcondiciones | N/A |
| Precedentes | N/A |
| Usan o extienden | Usan CU 01 |

1. Caso de uso 05: Crear estadística.



|  |  |
| --- | --- |
| Nombre | CU05 Crear estadística. |
| Descripción | Crea una estadística. |
| Actores | Administrador, usuario. |
| Entradas | N/A |
| Salidas | Registro de la estadística. |
| Precondiciones | Que exista creación de usuarios. |
| Postcondiciones | N/A |
| Precedentes | N/A |
| Usan o extienden | Usan CU 01 |

1. Caso de uso 06: Modificar estadística.



|  |  |
| --- | --- |
| Nombre | CU06 Modificar estadística. |
| Descripción | Mostrar una estadística. |
| Actores | Administrador, usuario. |
| Entradas | ID del usuario. |
| Salidas | Impresión en pantalla (Éxito o fracaso) |
| Precondiciones | Que existan registros de estadísticas. |
| Postcondiciones | N/A |
| Precedentes | N/A |
| Usan o extienden | Usan CU 05 |

1. Caso de uso 07: Mostrar estadística.



|  |  |
| --- | --- |
| Nombre | CU07 Mostrar estadística. |
| Descripción | Mostrar una estadística. |
| Actores | Administrador, usuario. |
| Entradas | ID del usuario. |
| Salidas | Impresión de la estadística. |
| Precondiciones | Que existan registros de estadísticas. |
| Postcondiciones | N/A |
| Precedentes | N/A |
| Usan o extienden | Usan CU 05 |

1. Caso de uso 08: Listar estadísticas.

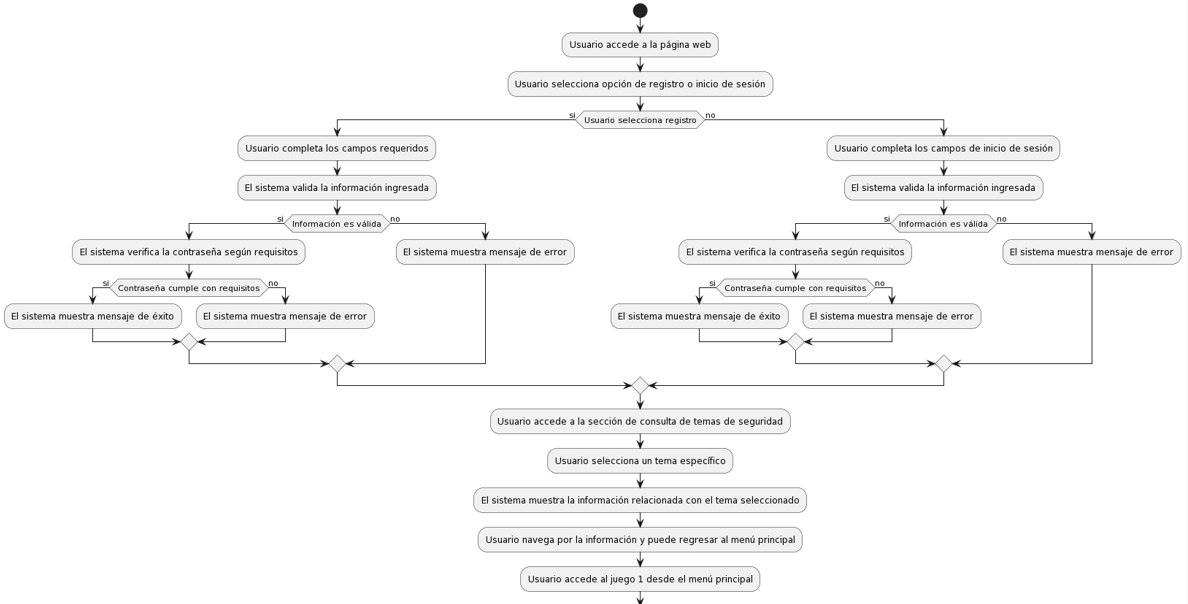


|  |  |
| --- | --- |
| Nombre | CU08 Listar estadísticas. |
| Descripción | Mostrar todo el registro de estadísticas. |
| Actores | Administrador, usuario. |
| Entradas | N/A |
| Salidas | Impresión de los registros de todas las estadísticas. |
| Precondiciones | Que existan registros de estadísticas. |
| Postcondiciones | N/A |
| Precedentes | N/A |
| Usan o extienden | Usan CU 05 |

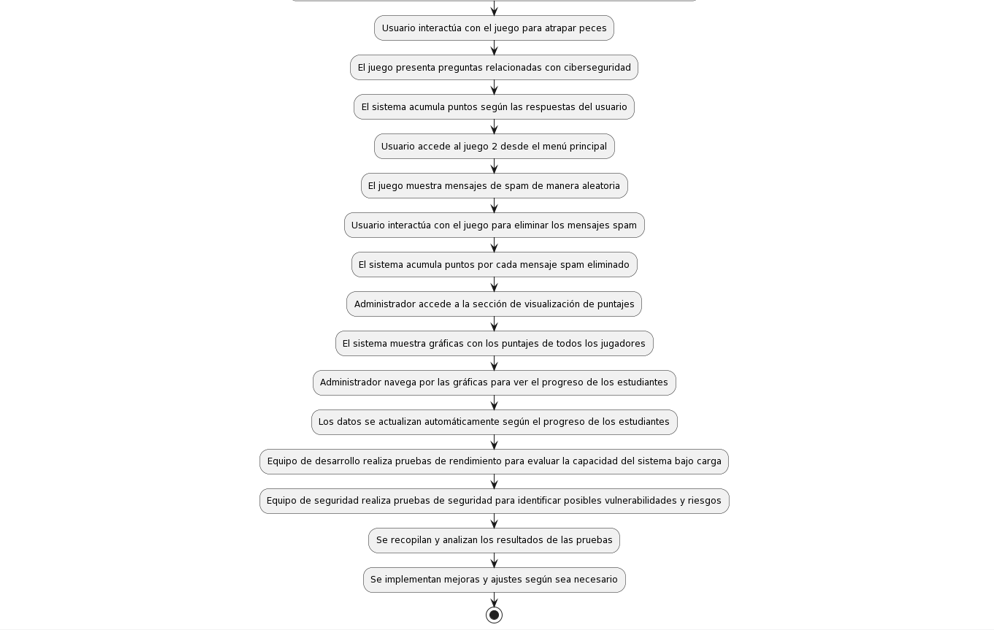
* **Análisis y Diseño**
* **Inicio:**

El estudio de los casos de uso en formato extendido desarrollado abarca el funcionamiento dentro del sistema, para este se ha generado un Diagrama del Sistema.

1. Diagrama del Sistema parte I.



1. Diagrama del sistema parte II



* **Elaboración:**

La estructura de la base de datos del sistema está dada por las entidades del proyecto, las cuales son los usuarios y las estadísticas, por otra parte, la base de datos al estar desarrollada con un motor de base de datos No SQL como lo es MongoDB no tiene un diagrama de entidad relación, por lo cual su representación es con el formato en el que se envían los documentos JSON al programa, estas se llaman colecciones, las cuales contienen los datos de campos de los datos que tiene cada entidad dentro de la base de datos. Las colecciones con sus campos son:

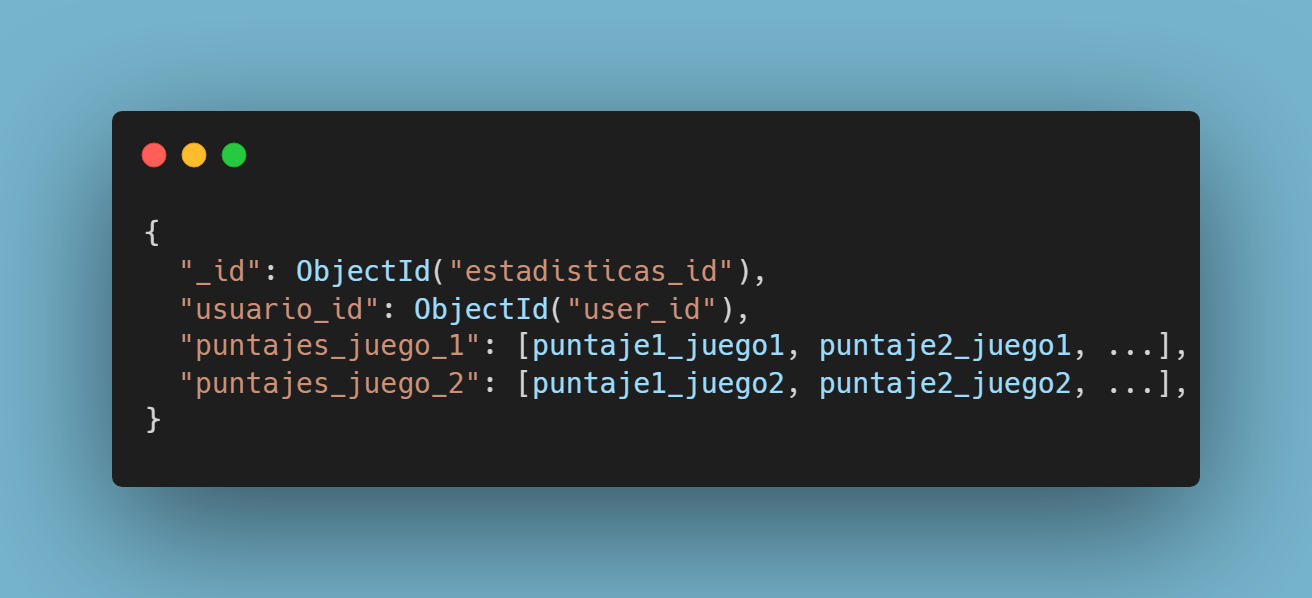
* Colección de Usuarios:
  + Id: El ID único del usuario dentro de la colección.
  + nombre y apellido: Almacenar el nombre y apellido del usuario.
  + contraseña: Almacenar la contraseña de forma segura y encriptada para garantizar la seguridad de los usuarios.
  + rol: (Usuario o Administrador) para gestionar diferentes niveles de acceso y funcionalidades en la aplicación.
  + fecha de nacimiento: Edad del usuario.
  + correo: Almacenar el correo electrónico institucional del usuario.
* Colección de Estadísticas:
  + Id: El ID único de la estadística dentro de la colección.
  + usuario\_id: Vincular las estadísticas al ID del usuario permite un fácil acceso y consulta de las estadísticas específicas de cada usuario.
  + puntajes\_juego\_1 y puntajes\_juego\_2: Almacenar los puntajes de los juegos permite realizar un seguimiento del progreso individual de cada usuario en los juegos enfocados a la concientización en ciberseguridad.

1. Colección Usuario



En la figura 26, se puede evidenciar la estructura de la colección de la base de datos No SQL de los Usuarios.

1. Colección de estadísticas.



En la figura 27, se puede evidenciar la estructura de la colección de la base de datos No SQL de las Estadísticas.

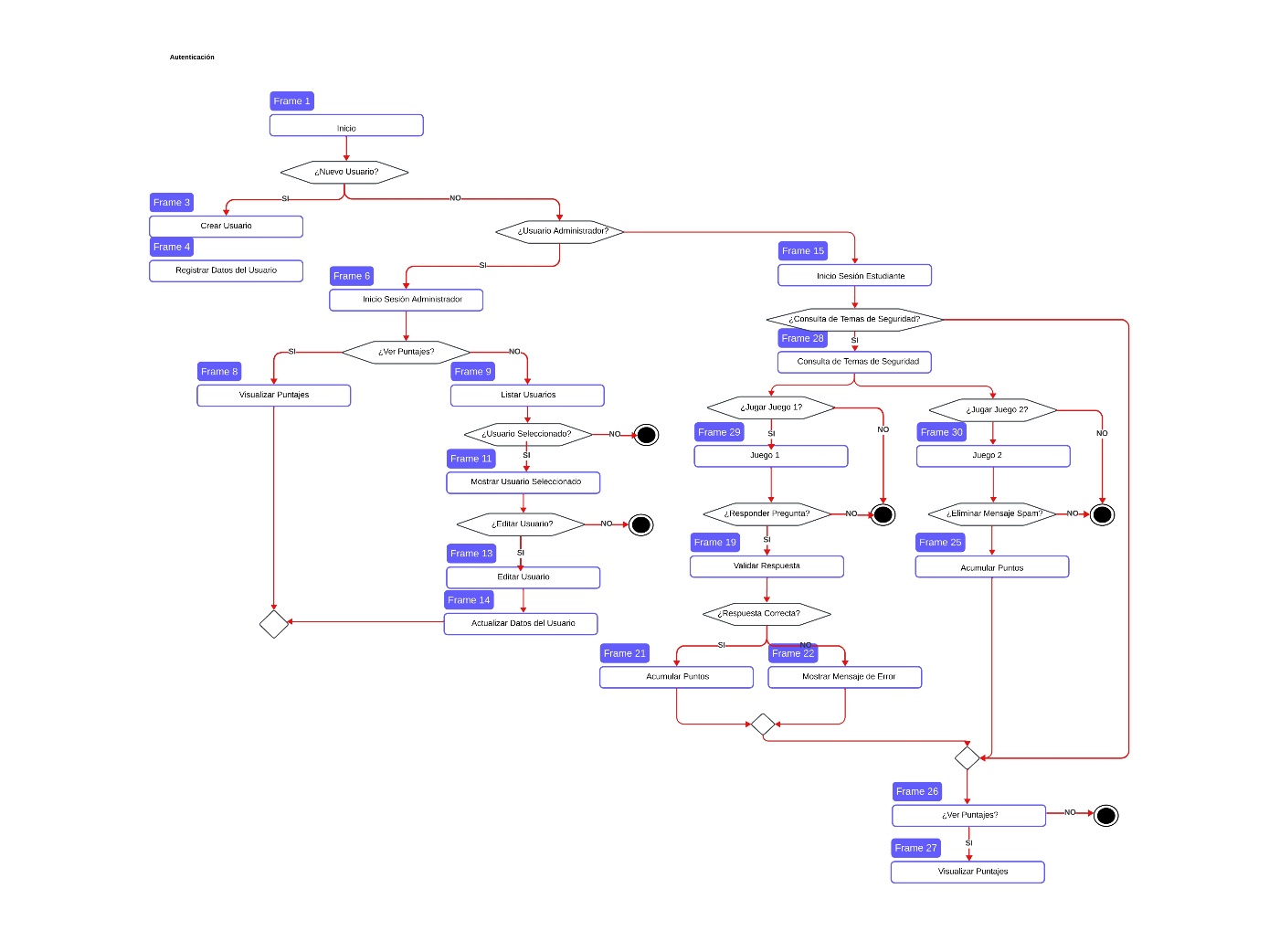
* **Construcción:**

Dentro de la construcción del proyecto están el diagrama de actividades, el flujo de navegación dentro del software y el diseño de wireframe del proyecto.

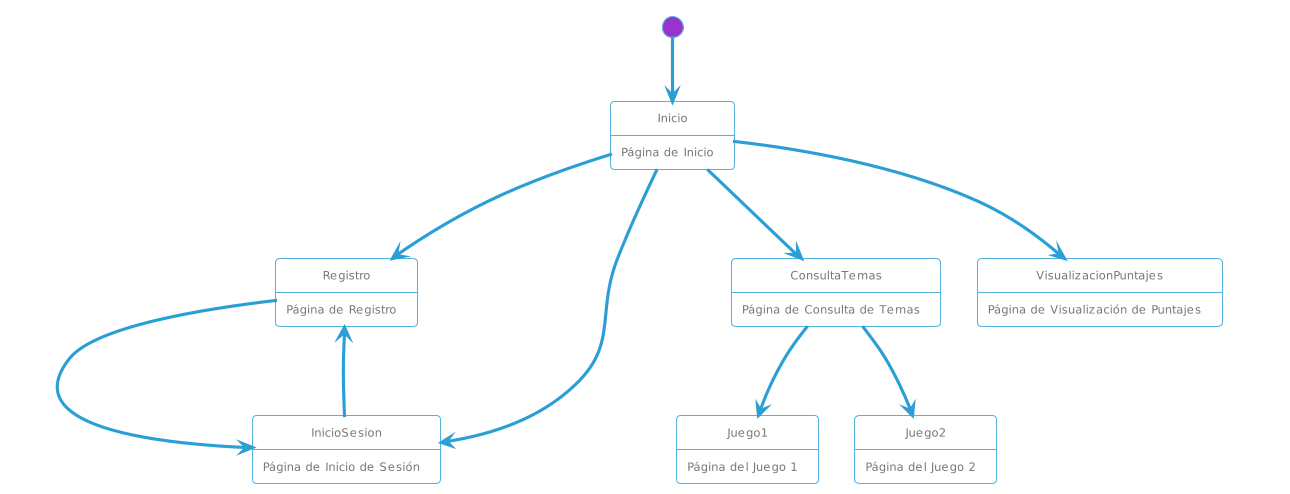
* Diagrama de actividades:
* Flujo de navegación: Dentro del flujo de navegación están los ítems por los cuales se puede navegar dentro del prototipo, esto se ve reflejado en la Figura 28.
* Diseño del wireframe: El diseño del wireframe del proyecto se desarrolla con base en las ideas que se tienen sobre cómo se generará la interfaz de usuario para la interacción de botones, véase las figuras 30, 31, 32, 33, 34, 35 y 36.
* **Transición:**

En esta etapa se generaron las figuras para la representación de cada elemento de la construcción del proyecto.

1. Diagrama de actividades.

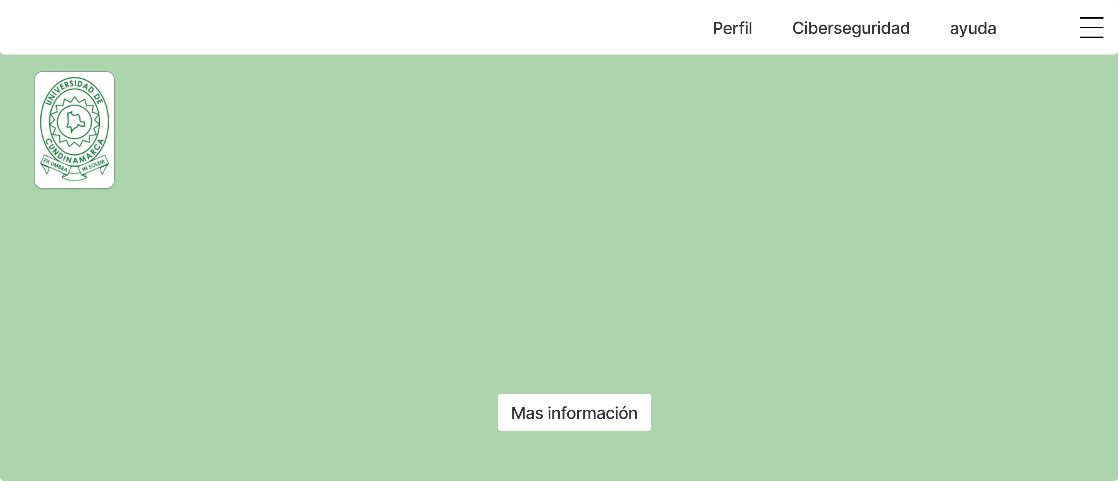


La Figura 28 es el diagrama de actividades del prototipo.

1. Flujo de navegación.

En la Figura 29 se puede evidenciar el flujo del sistema, como se puede navegar dentro del mismo y como se fluye a través de este por sus apartados.

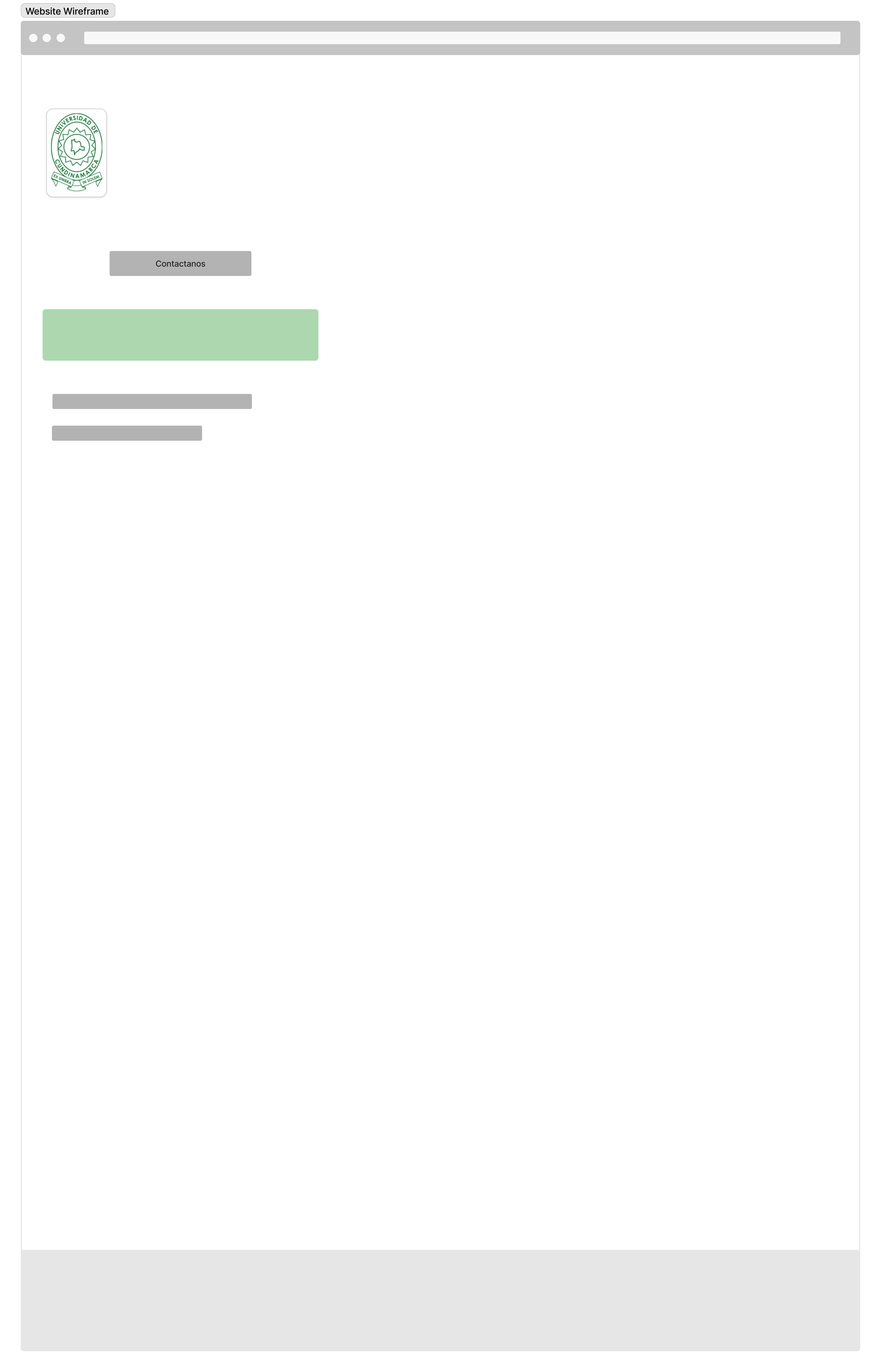
1. Wireframe de la página Índex.



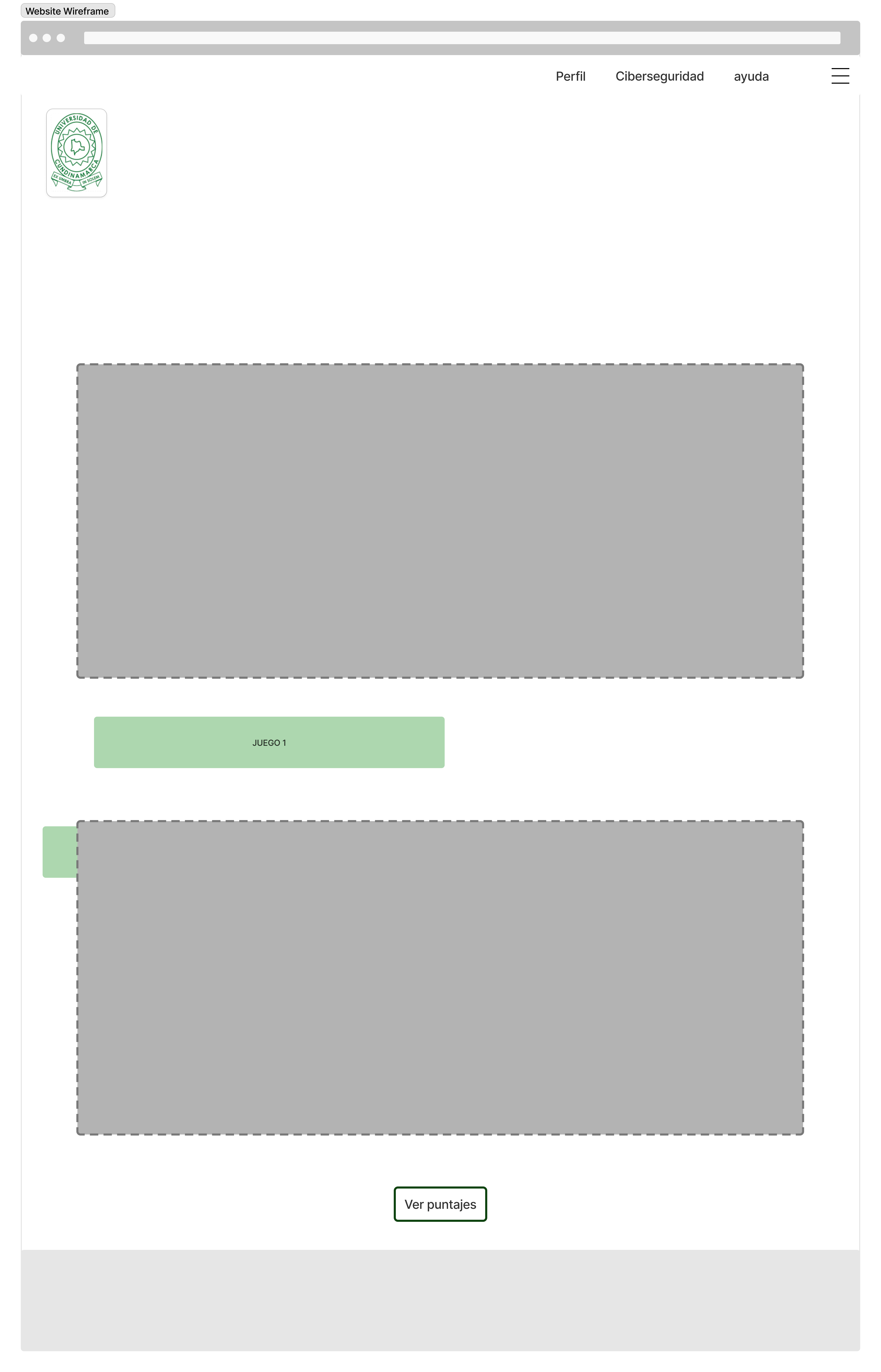
1. Wireframe de los formularios de la página web



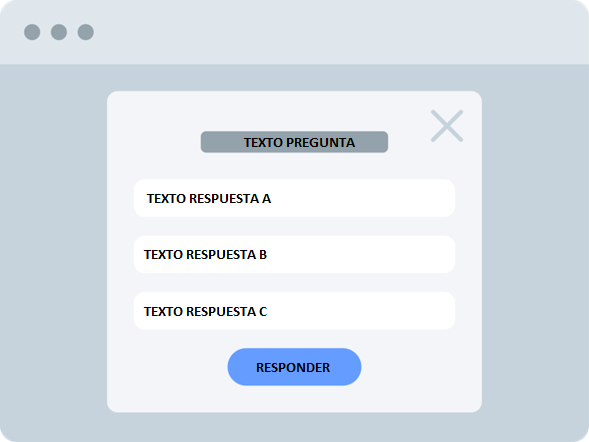
1. Wireframe de la página de contacto.



1. Wireframe de la página del juego.



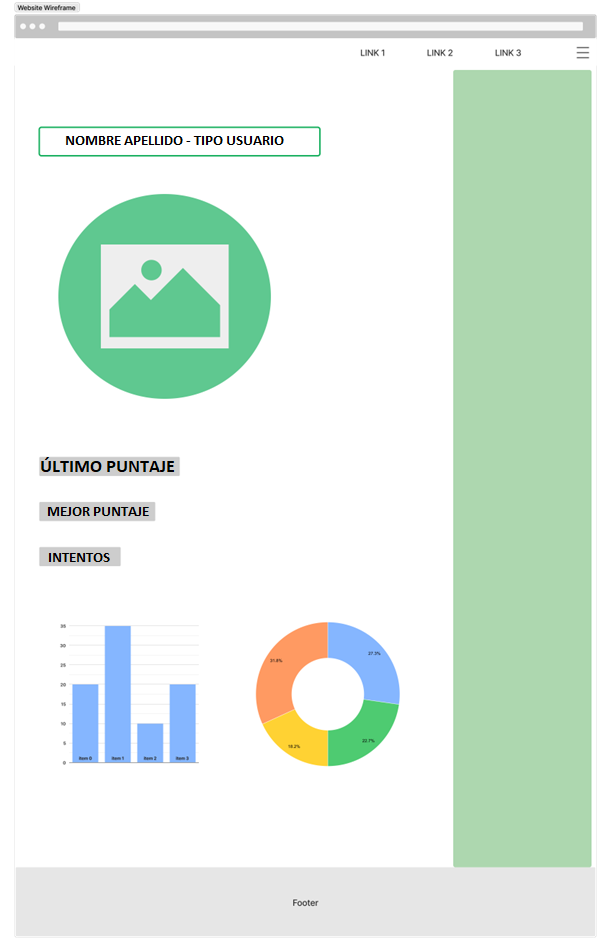
1. Wireframe de selección de respuestas en el juego.



1. Wireframe de consulta sobre información sobre temas de ciberseguridad.



1. Wireframe del perfil de usuario.



* **Implementación Desarrollo**
* **Inicio:**
  + Estudio y evaluación del modelo presentado.
* **Elaboración:**
  + Generación de la Base de Datos.
* **Construcción:**
  + Pulida de clases, desarrollo de los formularios y subida de registros de prueba.
* **Transición:**
  + Software completo.
* **Pruebas**
* **Inicio:**

Dentro de las pruebas realizadas al proyecto

1. Matriz de control de pruebas de caja blanca y caja negra.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tipo de Prueba** | **Funcionalidad Probada** | **Encargado** | **Proceso** | **Resultado obtenido** |
| Caja Blanca | Iniciar sesión con usuario Administrador | Salomón Forero | Se verifica si un usuario válido puede iniciar sesión correctamente utilizando credenciales válidas. | CORRECTO |
| Caja Blanca | Iniciar sesión con un usuario sin privilegios de administrador. | Paula Barrera | Se verifica si un usuario sin privilegios de administrador puede iniciar sesión correctamente y si tiene acceso limitado a las funciones de administrador. Se utilizan diferentes combinaciones de usuarios y contraseñas para probar esta funcionalidad. | CORRECTO |
| Caja Blanca | Iniciar sesión con un usuario que no exista | Salomón Forero | Se verifica si el sistema maneja adecuadamente el inicio de sesión con un usuario que no existe en la base de datos. Se intenta iniciar sesión con un usuario que no está registrado y se verifica si se muestra un mensaje de error apropiado. | CORRECTO |
| Caja Blanca | Integración entre módulos de registro e inicio de sesión | Salomón Forero | Se verifica la correcta integración entre los módulos de registro e inicio de sesión. Se comprueba si los datos ingresados durante el registro se almacenan correctamente y se pueden utilizar para iniciar sesión exitosamente. | CORRECTO |
| Caja Blanca | Contraseña ingresada cumple con los requisitos | Paula Barrera | Se verifica si la contraseña ingresada durante el registro cumple con los requisitos especificados (al menos 8 caracteres, una minúscula, una mayúscula, un número y un carácter especial). Se utilizan diferentes combinaciones de contraseñas para verificar la validez de la validación. | CORRECTO |
| Caja Blanca | Agregar Usuario | Salomón Forero | Se verifica si los datos ingresados durante la creación de un nuevo usuario se almacenan correctamente en la base de datos y si se aplican las validaciones necesarias (como la longitud mínima de contraseña y el formato de correo electrónico). Se revisa el código fuente para asegurar que se implementen correctamente las validaciones. | CORRECTO |
| Caja Negra | Agregar Usuario | Paula Barrera | Se simula la creación de un nuevo usuario utilizando diferentes combinaciones de datos de entrada, incluyendo datos válidos e inválidos. Se comprueba si el usuario se crea correctamente en la base de datos y si se muestran mensajes de error adecuados en caso de datos incorrectos o faltantes. | CORRECTO |
| Caja Blanca | Mostrar Usuario | Paula Barrera | Se verifica si el sistema recupera correctamente la información de un usuario específico de la base de datos. Se revisa el código fuente para asegurar que se implemente correctamente la lógica de recuperación de datos. | CORRECTO |
| Caja Negra | Mostrar Usuario | Paula Barrera | Se simula la visualización de la información de un usuario. Se comprueba si se muestran todos los datos relevantes del usuario y si la presentación es clara y fácil de entender para los usuarios finales. | CORRECTO |
| Caja Blanca | Listar Usuarios | Salomón Forero | Se verifica si el sistema recupera correctamente la lista de usuarios de la base de datos y si se ordena correctamente. | CORRECTO |
| Caja Negra | Listar Usuarios | Salomón Forero | Se simula la visualización de la lista de usuarios utilizando diferentes perfiles de usuario. Se comprueba si se muestran todos los usuarios registrados en el sistema y si la presentación es clara y fácil de entender para los administradores. | CORRECTO |
| Caja Blanca | Editar Usuario | Paula Barrera | Se verifica si los cambios realizados en la información de un usuario existente se aplican correctamente en la base de datos. Se revisa el código fuente para asegurar que se implemente correctamente la lógica de actualización de datos. | CORRECTO |
| Caja Negra | Editar Usuario | Paula Barrera | Se simula la edición de la información de un usuario utilizando diferentes combinaciones de datos de entrada. Se comprueba si los cambios se reflejan correctamente en la base de datos y si se muestran mensajes de éxito o error adecuados. | CORRECTO |
| Caja Blanca | Generar Estadística | Salomón Forero | Se verifica si el sistema genera estadísticas correctamente utilizando los datos disponibles en la base de datos y si se utilizan adecuadamente para crear gráficos con Google Charts. Se comprueba si las estadísticas generadas son precisas y relevantes para el análisis del aprendizaje en temas de ciberseguridad. | CORRECTO |
|  |  | Salomón Forero | Se analizan las funciones internas que se encargan de recopilar y procesar los datos para generar las estadísticas y los gráficos. Se verifican los algoritmos y las consultas utilizadas para asegurar que la información se extraiga, se calcule según los puntajes y se visualice de manera precisa y eficiente. | CORRECTO |
| Caja Negra | Generar Estadística | Salomón Forero | Se verifica si los usuarios autorizados pueden acceder a las estadísticas generadas y a los gráficos a través de la interfaz de usuario proporcionada por el sistema. Se prueban diferentes escenarios para validar que las estadísticas se presenten correctamente y sean comprensibles para los usuarios finales. | CORRECTO |
|  |  | Salomón Forero | Se comprueba si las estadísticas y los gráficos se muestran con precisión y si se presentan de una manera clara y fácil de entender, utilizando Google Charts. Se valida también que los usuarios autorizados puedan filtrar y personalizar las estadísticas según sus necesidades específicas. | CORRECTO |
| Caja Blanca | Mostrar Estadística | Paula Barrera | Se verifica si el sistema muestra correctamente las estadísticas y los gráficos generados a los usuarios autorizados. Se comprueba si la presentación de las estadísticas y los gráficos es clara y comprensible, utilizando Google Charts. Se prueban diferentes tipos de estadísticas para validar la funcionalidad. | CORRECTO |
|  |  | Paula Barrera | Se inspeccionan las funciones internas que manejan la presentación de las estadísticas y los gráficos para garantizar que se muestren correctamente en la interfaz de usuario. Se valida que los usuarios autorizados puedan acceder fácilmente a las estadísticas y los gráficos relevantes a través de la interfaz. | CORRECTO |
| Caja Negra | Mostrar Estadística | Salomón Forero | Se verifica si los usuarios autorizados pueden acceder y visualizar las estadísticas y los gráficos a través de la interfaz de usuario proporcionada por el sistema. Se prueban diferentes escenarios para validar que las estadísticas y los gráficos se muestren correctamente y sean comprensibles para los usuarios finales. | CORRECTO |
|  |  | Salomón Forero | Se comprueba si la presentación de las estadísticas y los gráficos es clara y fácil de entender, utilizando Google Charts. Se valida también que los usuarios autorizados puedan filtrar y personalizar las estadísticas según sus necesidades específicas. | CORRECTO |
| Caja Blanca | Listar Estadística | Paula Barrera | Se verifica si el sistema muestra una lista completa y precisa. Se comprueba si la lista incluye todos los detalles relevantes de cada estadística y si se presenta de forma ordenada y fácil de navegar para los usuarios autorizados. | CORRECTO |
|  |  | Paula Barrera | Se inspeccionan las funciones internas que manejan la recuperación y presentación de las estadísticas y los gráficos para garantizar que se muestren correctamente en la interfaz de usuario. | CORRECTO |
| Caja Negra | Listar Estadística | Salomón Forero | Se verifica si los usuarios autorizados pueden acceder y visualizar una lista completa. Se comprueba si la lista incluye todos los detalles relevantes de cada estadística y si se presenta de forma ordenada y fácil de navegar para los usuarios finales. | CORRECTO |
|  |  | Salomón Forero | Se comprueba si la presentación de la lista de estadísticas y los gráficos es clara y fácil de entender, utilizando Google Charts. Se valida también que los usuarios autorizados puedan filtrar y personalizar las estadísticas. | CORRECTO |
| Caja Negra | Juego 1: Pescador | Salomón Forero | Se verifica si el juego 1 funciona correctamente, incluyendo la captura de peces, la aparición de preguntas y la acumulación de puntos. Se prueban diferentes escenarios de juego para garantizar la funcionalidad y la experiencia del usuario. | CORRECTO |
| Caja Negra | Juego 2: mensajes spam | Paula Barrera | Se verifica si el juego 2 funciona correctamente, incluyendo la aparición de mensajes spam, la capacidad de los jugadores para disparar a los mensajes y la acumulación de puntos. Se prueban diferentes escenarios de juego para garantizar la funcionalidad y la experiencia del usuario. | CORRECTO |
| Caja Negra | Visualización de puntajes | Salomón Forero | Se verifica si el administrador puede acceder correctamente a la sección de visualización de puntajes y si los datos se muestran de manera clara y comprensible. Se prueban diferentes navegadores y dispositivos para asegurar la compatibilidad. | CORRECTO |

* **Elaboración:**

Se realizaron pruebas exhaustivas de caja blanca para garantizar la funcionalidad del sistema. Salomón Forero y Paula Barrera, encargados de las pruebas, verificaron con éxito la capacidad de iniciar sesión con el usuario Administrador, integración entre módulos, y la generación precisa de estadísticas. Paula Barrera se aseguró de que el sistema manejara correctamente situaciones como iniciar sesión con un usuario sin privilegios y verificar la validez de contraseñas. Ambos evaluaron la creación, edición, y visualización de usuarios, así como la presentación adecuada de estadísticas y gráficos.

* **Construcción:**

Las pruebas de caja negra se centraron en simular diversas interacciones del usuario para garantizar la robustez del sistema. Paula Barrera supervisó la simulación de la creación, edición y visualización de usuarios, mientras que Salomón Forero se encargó de juegos y visualización de puntajes. Se verificó con éxito el correcto funcionamiento de los juegos, la presentación de mensajes de error adecuados, y la accesibilidad a las estadísticas generadas. En resumen, todas las pruebas, tanto de caja blanca como negra, arrojaron resultados satisfactorios, validando la estabilidad y funcionalidad integral del sistema.

* **Transición:**

Con los resultados de los reportes de las pruebas de caja blanca como de caja negra a las funcionalidades del prototipo, con la supervisión de los encargados, podemos concluir que el software está funcionando de manera correcta y sin fallos.

## **Costo del proyecto**

En la siguiente tabla se muestran los costos de los recursos necesarios para la realización del proyecto, tomando en cuenta papelería, transporte, internet, software, hardware, asesorías, imprevistos y otros.

1. Recursos financieros

|  |  |  |
| --- | --- | --- |
| **Recurso** | **Costo mensual** | **Costo total**  **(6 Meses)** |
| **Papelería** | $ 0 | $ 0 |
| **Transporte** | $ 134.400 | $ 1.075.200 |
| **Internet** | $ 120.000 | $ 960.000 |
| **Software**  **(Hosting)** | $ 100.000 | $ 100.000 |
| **Hardware** | $ 0 | $ 0 |
| **Asesoría** | $ 50.000 | $ 100.000 |
| **Imprevistos** | $ 100.000 | $ 200.000 |
| **Otros** | $ 50.000 | $ 100.000 |
|  | **Total** | $ 2.535.200 |

# **TESTER**

Dentro de la metodología del proyecto se determinaron las pruebas de caja blanca y caja negra de las funcionalidades del prototipo y se realizaron con un encargado, los cuales fueron los desarrolladores del proyecto en cuestión, de los resultados de las pruebas de caja blanca y caja negra se generaron reportes con conclusiones del software, viéndose en la Tabla 13.

# **CAPITULO 4**

# **CONCLUSIONES**

* La gamificación se presenta como una estrategia efectiva para promover prácticas seguras en línea entre los jóvenes, al fomentar la concienciación y la participación en el aprendizaje de habilidades de ciberseguridad.
* Es fundamental desarrollar herramientas educativas interactivas que motiven a los estudiantes a participar activamente en la adquisición de habilidades de ciberseguridad, contribuyendo así a crear un entorno universitario más seguro y consciente de los riesgos asociados con la información en internet.

Principio del formulario

# **RECOMENDACIONES**

* Implementar un sistema que permita realizar un seguimiento del progreso de cada estudiante en el prototipo web, identificando áreas de mejora y brindando retroalimentación personalizada a los estudiantes para maximizar el aprendizaje individual.
* Integrar funciones que promuevan la colaboración entre los estudiantes, como foros de discusión, grupos de estudio en línea o actividades cooperativas, para fomentar el aprendizaje colaborativo y el intercambio de conocimientos sobre ciberseguridad.
* Incluir casos de estudio reales y ejemplos prácticos de situaciones de ciberseguridad para ilustrar los conceptos teóricos y ayudar a los estudiantes a comprender mejor la relevancia y la aplicación práctica de las buenas prácticas en este ámbito.

# **PROYECCIONES**

* Se espera que esta herramienta genere conciencia sobre los riesgos asociados con la información en línea y proporcione a los estudiantes las habilidades necesarias para reducir estos riesgos.
* Al fomentar la concienciación y la participación de los estudiantes en el aprendizaje de habilidades de ciberseguridad, el proyecto contribuirá a crear un entorno universitario más seguro y consciente de los riesgos en internet.
* La integración de la gamificación como estrategia educativa en ciberseguridad puede servir como un modelo innovador para futuros proyectos educativos en la institución, promoviendo un enfoque interactivo y motivador para el aprendizaje de habilidades técnicas.
* Al proporcionar a los estudiantes herramientas interactivas, desafíos y recompensas, el proyecto busca estimular el interés de los estudiantes y promover un aprendizaje colaborativo en el campo de la ciberseguridad.

# **REFERENCIAS BIBLIOGRÁFICAS**

1. World Economic Forum, Marsh McLennan, SK Group y Zurich Insurance Group. (2022). *The Global Risks: Report 2022* World Economic Forum. Edición 17.
2. Acurio Del Pino, S. (2022). *Delitos Informáticos: Generalidades*. Infolibros. https://shorturl.at/hkG68
3. Escuela de Inteligencia y Contrainteligencia (ESICI). (2022). *EL RIESGO DE LOS CIBERATAQUES PARA COLOMBIA*. Boletín No 5.
4. Ahumada Ortiz, T (2020). *Campaña de sensibilización y buenas prácticas de ciberseguridad*. Universidad Andrés Bello. https://shorturl.at/lptAG
5. Peña, M. A. y Sánchez, D. M. (2022). “*Guía de buenas prácticas para reducir riesgos de engaños a menores entre 13 a 15 años en redes sociales”*. Fundación Universitaria Los Libertadores. Sede Bogotá. <http://hdl.handle.net/11371/5402>.
6. Álvarez, L (2021). “*Desarrollo de una herramienta para plan de concienciación en ciberseguridad basada en gamificación*”. Biblioteca Universitaria Campus Sur. <https://oa.upm.es/70726/>
7. Weitl-Harms, S, Spanier, A, Hastings, J y Rokusek, M (2023). “*A Systematic Mapping Study on Gamification Applications for Undergraduate Cybersecurity Education*”. Kennesaw State University. Primera Edición. https://shorturl.at/desBT
8. Orlando Cruz, F. (2022). “*Análisis de la metodología RUP en el desarrollo de software académico mediante la herramienta DJANGO*”. Recimundo. https://shorturl.at/gvBO9
9. INTERPOL. (2020). *Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19.* https://shorturl.at/gqFLX
10. Torres Toukoumidis, A. & Romero Rodríguez, L. (2018). “GAMIFICACIÓN EN IBEROAMÉRICA”. Universidad Politécnica Salesiana. 1era Edición. ISBN:   
    978-9978-10-323-4
11. Cisco. (2024). *¿Qué es la ciberseguridad?*. https:// t.ly/r-jD3
12. García, I. J. B. (2021). *Backend y Frontend, ¿Qué es y cómo funcionan en la programación?.* Servnet. https://t.ly/paY5L
13. Equipo editorial de IONOS. (2023). *¿Cómo funciona el modelo cliente-servidor?* IONOS Digital Guide. https://t.ly/\_deAE
14. Oracle. (s. f.). *¿Qué es una base de datos?*. https://t.ly/f4Zl8
15. MicroStrategy. (2024). *Cómo ver un informe como gráfico: vista de gráfico*. https://t.ly/j4CPN
16. Samsoodeen, S. (2024). *Cómo crear una línea de tiempo para proyectos en 6 pasos (Con plantillas)*. Blog de Creately. https://t.ly/uPVQ-
17. Herrera Castellanos, M. (s. f.). *FORMULA PARA CÁLCULO DE LA MUESTRA POBLACIONES FINITAS*. Hospital Roosevelt.