**CYBERSHIELD**

**Plataforma de Ciberseguridad para Usuarios No Técnicos**

**Roberto Cristian Mangiurea Anton**

Desarrollo de Aplicaciones Multiplataforma (DAM)

2º Curso

30-05-2025

# **ÍNDICE**

1. Introducción 3

2. Justificación 4

3. Objetivos 6

4. Metodología 8

5. Desarrollo de Contenidos 11

6. Conclusiones 24

7. Bibliografía / Webgrafía 27

8. Anexos 29

# **1. INTRODUCCIÓN**

En la era digital actual, la ciberseguridad se ha convertido en una necesidad fundamental para todos los usuarios de tecnología. Sin embargo, la mayoría de las herramientas de seguridad están diseñadas para profesionales técnicos, creando una brecha significativa entre la necesidad de protección y la capacidad de los usuarios comunes para implementar medidas de seguridad efectivas.

CyberShield surge como respuesta a esta problemática, ofreciendo una plataforma integral de ciberseguridad diseñada específicamente para usuarios no técnicos. La aplicación combina tres módulos fundamentales: gestión de contraseñas, educación sobre phishing y análisis de seguridad de red, todo ello presentado a través de una interfaz intuitiva y accesible.

El proyecto ha sido desarrollado utilizando tecnologías web modernas, incluyendo React para el frontend, Node.js con Express para el backend, y PostgreSQL como sistema de gestión de base de datos. Esta arquitectura permite una experiencia fluida y escalable, mientras mantiene los más altos estándares de seguridad.

La filosofía de diseño de CyberShield se centra en democratizar la ciberseguridad, haciendo que las herramientas de protección digital sean comprensibles y utilizables por cualquier persona, independientemente de su nivel técnico. A través de interfaces visuales claras, explicaciones simplificadas y feedback inmediato, la plataforma guía a los usuarios en la protección de su información personal y dispositivos.

# **2. JUSTIFICACIÓN**

## **2.1 Problemática Identificada**

La ciberseguridad representa uno de los desafíos más críticos de la sociedad digital contemporánea. Según el informe de Ciberseguridad Nacional 2024, el 78% de los usuarios domésticos han sido víctimas de algún tipo de ataque cibernético, mientras que solo el 23% utiliza herramientas de seguridad adecuadas.

Las principales barreras identificadas incluyen:

• Complejidad Técnica: Las herramientas existentes requieren conocimientos especializados que la mayoría de usuarios no poseen.

• Falta de Educación: Existe un déficit significativo en la educación sobre amenazas cibernéticas y mejores prácticas de seguridad.

• Fragmentación de Soluciones: Los usuarios deben utilizar múltiples herramientas desconectadas para cubrir diferentes aspectos de la seguridad.

• Costo Elevado: Las soluciones empresariales son inaccesibles para usuarios domésticos.

***[DOCUMENTO COMPLETO DISPONIBLE]***

*Este es un extracto del documento completo. La memoria completa de 30 páginas incluye todos los capítulos detallados, anexos técnicos, capturas de pantalla, diagramas de arquitectura y código fuente relevante.*

Fecha de generación: 30/5/2025