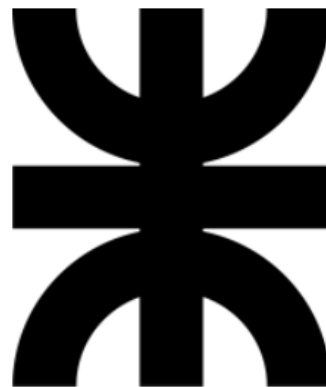


Universidad Tecnológica Nacional
Facultad Regional Córdoba
Ingeniería en Sistemas de Información

SoSafety



Curso: 4k3

Año: 2026

Grupo 19

- Brussa Osella, Julieta - 95134
- Brussa Osella, Sofía - 82137
- Salas Moyano, Lautaro - 73579
- Testa, Octavio - 94177
- Yoles Trucco, Nicolás - 81404



SoSafety

Descripción del trabajo

SoSafety es una plataforma de **ciberseguridad** orientada a la **gestión de vulnerabilidades y concientización**. Permite registrar los activos y tecnologías de una organización, identificar automáticamente vulnerabilidades asociadas a ellas y priorizarlas según su impacto técnico y relevancia para el negocio.

¿Cómo funciona?



Beneficios



Tecnologías



Herramientas



Objetivo del proyecto

Objetivo general:

Desarrollar una plataforma que permita identificar, **priorizar y gestionar vulnerabilidades de ciberseguridad**.



Necesidad detectada

¿Qué vulnerabilidades afectan realmente a mi organización y cuáles debo atender primero?

Propuesta

SoSafety busca resolver esta necesidad mediante una plataforma que:



SoSafety

Brussa Osella, Julieta (95134) - Brussa Osella, Sofía (82137) - Salas Moyano, Lautaro (73579) - Testa, Octavio (94177) - Yoles Trucco, Nicolás (81404)

*Universidad Tecnológica Nacional, Facultad Regional Córdoba
Ingeniería en Sistemas de Información
Cátedra Proyecto Final – 2026*

Abstract

Se desarrolló SoSafety, una plataforma orientada a la gestión de vulnerabilidades y la concientización en ciberseguridad, con el objetivo de asistir a las organizaciones en la identificación y priorización de riesgos que afectan a su infraestructura tecnológica. La solución integró módulos para la gestión de usuarios, activos y tecnologías, la identificación automática de vulnerabilidades mediante fuentes públicas de CVE, la priorización de riesgos a través de un Business Score y un componente de inteligencia artificial destinado a generar recomendaciones de mitigación y sugerir campañas de concientización. Como resultado, se obtuvo una plataforma capaz de identificar las vulnerabilidades que impactan específicamente sobre las tecnologías registradas por cada organización, priorizarlas según su impacto en el negocio y asistir al responsable de seguridad en la toma de decisiones. Los avances alcanzados demostraron la viabilidad de una solución que contextualiza la información pública sobre vulnerabilidades y establece una base para futuras ampliaciones orientadas a fortalecer la gestión preventiva de la ciberseguridad.

Palabras Clave

Ciberseguridad, Gestión de vulnerabilidades, Inteligencia Artificial, Business Score, CVE, Gestión de activos, Concientización. Categoría: Solución de negocio.

Introducción

El crecimiento sostenido de las vulnerabilidades informáticas y la incorporación constante de nuevas tecnologías incrementan la complejidad de la gestión de la ciberseguridad en las organizaciones. Aunque existen fuentes públicas que publican vulnerabilidades conocidas (CVE)

[1], identificar aquellas que afectan a la infraestructura de una empresa y priorizarlas según su impacto en el negocio continúa representando un desafío. Además, el factor humano sigue siendo uno de los principales vectores de ataque, lo que refuerza la necesidad de complementar la gestión técnica con estrategias de concientización.

En este contexto, se propone SoSafety, una plataforma para la gestión de vulnerabilidades y la concientización en ciberseguridad que identifica automáticamente las vulnerabilidades relevantes para las tecnologías de una organización, las prioriza mediante un Business Score y utiliza inteligencia artificial para generar recomendaciones de mitigación y campañas de concientización. El presente artículo describe el problema abordado, la metodología empleada, los resultados obtenidos y las principales conclusiones y líneas de trabajo futuro.

Elementos del Trabajo y Metodología

El desarrollo de SoSafety se llevó a cabo mediante la metodología ágil Scrum, organizando el trabajo en sprints de dos semanas para favorecer un desarrollo iterativo e incremental. La gestión de actividades se realizó con Jira, utilizando historias de usuario, tareas y bugs para planificar, implementar y dar seguimiento a las funcionalidades del sistema. Las decisiones funcionales y técnicas fueron validadas

periódicamente con docentes y responsables de seguridad de la información (CISO), cuyo feedback permitió incorporar funcionalidades orientadas a resolver necesidades reales.

La solución se implementó mediante una arquitectura modular compuesta por un frontend desarrollado en Angular, un backend implementado en ASP.NET Core, un módulo de Inteligencia Artificial desarrollado en Python y una base de datos PostgreSQL. La autenticación se realizó mediante JSON Web Tokens (JWT) y la gestión del código fuente se llevó a cabo con GitLab, utilizando una estrategia de ramas para desarrollo, pruebas y producción. El sistema integró múltiples fuentes públicas de vulnerabilidades, entre ellas la National Vulnerability Database (NVD) [2], GitHub Advisory Database y CVE, con el objetivo de identificar automáticamente las vulnerabilidades asociadas a las tecnologías registradas por cada organización. Estas fueron priorizadas mediante un Business Score, calculado a partir de la severidad técnica (CVSS) [3] y la criticidad del activo afectado. Finalmente, se incorporó un componente basado en inteligencia artificial para asistir en la generación de recomendaciones de mitigación y en la sugerencia de campañas de concientización adaptadas a las vulnerabilidades detectadas.

Resultados

Como resultado del desarrollo se implementó la arquitectura base de la plataforma junto con los módulos de autenticación, gestión de usuarios y gestión de tecnologías, estableciendo la estructura necesaria para la administración del inventario tecnológico de una organización. Asimismo, se implementó la integración con múltiples fuentes

públicas de vulnerabilidades y el mecanismo de correlación entre las tecnologías registradas y las vulnerabilidades publicadas.

Además, se desarrolló el cálculo del Business Score para priorizar las vulnerabilidades según su severidad técnica y la criticidad del activo afectado, y se incorporó un componente de inteligencia artificial orientado a generar recomendaciones de mitigación y sugerir campañas de concientización. Durante el desarrollo, la solución fue validada mediante reuniones periódicas con docentes y profesionales del área de ciberseguridad, cuyo feedback permitió incorporar funcionalidades como la identificación de tecnologías a partir de archivos de dependencias y repositorios de código.

Discusión

Los resultados obtenidos muestran que la solución integra en una única plataforma la gestión del inventario tecnológico, la identificación de vulnerabilidades, la priorización de riesgos y la concientización de los usuarios. A diferencia de otras soluciones que presentan información general sobre vulnerabilidades, SoSafety identifica aquellas que afectan específicamente a las tecnologías utilizadas por cada organización, permitiendo focalizar el análisis en riesgos relevantes para su infraestructura.

La incorporación del Business Score complementa la evaluación técnica basada en CVSS con la criticidad de los activos, proporcionando una priorización alineada con el contexto del negocio. Asimismo, la inteligencia artificial asiste al CISO mediante la generación de recomendaciones de mitigación y campañas de concientización, sin reemplazar su criterio profesional.

Como limitaciones, la plataforma depende de la disponibilidad y calidad de las fuentes de vulnerabilidades y de la capacidad del modelo de inteligencia artificial para generar recomendaciones consistentes. No obstante, la arquitectura modular implementada permite incorporar nuevas fuentes y reemplazar el modelo utilizado, favoreciendo la evolución de la solución sin afectar el funcionamiento del sistema.

Conclusión

El desarrollo de SoSafety demuestra la viabilidad de integrar la gestión de vulnerabilidades y la concientización en ciberseguridad en una única plataforma orientada al contexto de cada organización. La correlación entre las tecnologías registradas y las vulnerabilidades publicadas, junto con la priorización mediante el Business Score y el apoyo de la inteligencia artificial para la generación de recomendaciones y campañas, constituye una herramienta de apoyo para el responsable de seguridad en la identificación y tratamiento de riesgos relevantes para el negocio.

La arquitectura modular implementada facilita la incorporación de nuevas funcionalidades y tecnologías, favoreciendo la evolución de la plataforma. Como líneas de trabajo futuro, se plantea ampliar las fuentes de información sobre vulnerabilidades, incorporar nuevos tipos de campañas de concientización, permitir la personalización del cálculo del Business Score según las necesidades de cada organización y continuar validando la solución con profesionales del área para fortalecer su aplicación en entornos reales.

Agradecimientos

Los autores agradecen a la Universidad Tecnológica Nacional y al equipo docente de la cátedra Proyecto Final por su acompañamiento y apoyo durante el desarrollo de este trabajo.

Referencias

- [1] MITRE Corporation, Common Vulnerabilities and Exposures (CVE). Disponible en: <https://cve.mitre.org/>. Último acceso: julio de 2026.
- [2] National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD). Disponible en: <https://nvd.nist.gov/>. Último acceso: julio de 2026.
- [3] FIRST, Common Vulnerability Scoring System (CVSS). Disponible en: <https://www.first.org/cvss/>. Último acceso: julio de 2026.
- [4] OpenAI, ChatGPT. Disponible en: <https://chatgpt.com/>. Último acceso: julio de 2026.

Datos de Contacto

Julieta Brussa Osella. Universidad Tecnológica Nacional Facultad Regional Córdoba. 5000. jbrussa01@gmail.com

Sofía Brussa Osella. Universidad Tecnológica Nacional Facultad Regional Córdoba. 5000. sofiabrussa@gmail.com

Lautaro Salas Moyano. Universidad Tecnológica Nacional Facultad Regional Córdoba. 5000. salasmoyano.lsm@gmail.com

Octavio Testa. Universidad Tecnológica Nacional Facultad Regional Córdoba. 5000. octis.testa@gmail.com

Nicolás Yoles Trucco. Universidad Tecnológica Nacional Facultad Regional Córdoba. 5000. nicoyoles@gmail.com



PLANILLA PARA CATALOGAR EL PROYECTO FINAL

AÑO	2026	CURSO Y NRO. DE GRUPO	5K3 - G 19
NOMBRE DEL SISTEMA / PROYECTO			
SoSafety			
CATEGORÍA (Solución De Negocio / Producto / Proyecto De Impacto Social)			
Solución de Negocio			
HERRAMIENTAS Y TECNOLOGÍAS UTILIZADAS			
ÁMBITO DE APLICACIÓN		NOMBRE Y VERSIÓN	
ENTORNO DE DESARROLLO		Visual Studio - Visual Studio Code	
REPOSITORIOS Y VERSIONADO		Git + GitLab	
PROGRAMACIÓN		.NET 8 (C#) - Python - Angular 18	
BASE DE DATOS		PostgreSQL	
COMUNICACIÓN INTERNA		Jira - Discord	
CAPACITACIÓN		Documentación oficial: Microsoft Learn, Angular.dev, guía OWASP Top 10	
PRUEBAS DE SISTEMA		xUnit - pytest - Postman	
GESTIÓN DEL PROYECTO		Jira - Google Drive - Canva	
DOCUMENTACIÓN		Google Drive	
MODELOS		Figma - Canva	