

Abstract

Proyecto: Fenrir CiberWolf

Versión: 1.0

Historial de revisiones y versionamiento.

|  |  |  |  |
| --- | --- | --- | --- |
| Versión | Autor(es) | Descripción | Fecha |
| 1.0 | Cristian Ramirez Soto | Creación del documento | 01/09/2024 |
|  |  |  |  |

Índice

[1 Abstract](#_heading=h.gjdgxs)……………………………………………………………….1

Español

Ingles

# 1 Abstract

## Español

El proyecto "FenrirCyberWolf" busca integrar técnicas avanzadas de ciencia de datos con ciberseguridad para desarrollar soluciones proactivas que aborden las crecientes amenazas cibernéticas en el entorno digital. Junto a Ricardo Alcantar, hemos diseñado un sistema que permite detectar, prevenir y mitigar ataques como malware, phishing, y fuerza bruta a través de la recopilación y análisis de grandes volúmenes de datos provenientes de registros de seguridad, tráfico de red y dispositivos IoT. El uso de algoritmos de minería de datos y aprendizaje automático nos ayudará a identificar patrones y anomalías que, de otra manera, podrían pasar desapercibidos, permitiendo una respuesta más efectiva ante incidentes cibernéticos.

El proyecto se divide en varias fases que se extienden a lo largo de 18 semanas, comenzando con la planificación y el diseño del sistema, seguidas de la recopilación y procesamiento de datos de múltiples fuentes, el desarrollo de modelos predictivos y la implementación de un sistema automatizado de respuesta a incidentes. La metodología ágil que hemos adoptado, basada en Scrum, facilita la adaptación a cambios en los requisitos y permite la entrega continua de mejoras incrementales a lo largo del proyecto. Además, utilizamos el marco de gestión de riesgos NIST RMS para asegurar que se identifiquen, evalúen y mitiguen de manera efectiva los riesgos asociados con el proyecto.

Desde el punto de vista académico y profesional, "FenrirCyberWolf" está estrechamente alineado con las competencias del perfil de egreso de nuestra carrera de Ingeniería en Informática. En mi caso, aplicaré habilidades como el análisis integral de procesos empresariales, la transformación de datos para la toma de decisiones y la programación de consultas complejas que permitan manipular grandes volúmenes de información. Por su parte, Ricardo contribuye con competencias relacionadas con el desarrollo de soluciones informáticas y la integración de sistemas según los requerimientos de la organización. Este proyecto también nos permite poner en práctica habilidades clave en áreas de alta demanda como la ciberseguridad, el análisis de datos y la inteligencia artificial, lo que nos prepara para enfrentar los desafíos del mercado laboral actual.

La relevancia del proyecto no solo radica en su capacidad para mitigar las amenazas cibernéticas, sino también en su impacto en el campo laboral. A medida que las empresas, organizaciones e instituciones gubernamentales dependen más de la tecnología digital, la seguridad de los sistemas informáticos se ha vuelto crucial. La implementación de soluciones como las que proponemos no solo protegerá los datos sensibles de las organizaciones, sino que también nos posicionará como profesionales altamente capacitados en un área en constante crecimiento. Además, "FenrirCyberWolf" contribuye a un enfoque de seguridad más proactivo y automatizado, lo que incrementa la capacidad de respuesta ante incidentes y reduce significativamente los riesgos asociados a la cibercriminalidad.

## Inglés

The “FenrirCyberWolf” project seeks to integrate advanced data science techniques with cybersecurity to develop proactive solutions to address the growing cyber threats in the digital environment. Together with Ricardo Alcantar, we have designed a system that allows detecting, preventing and mitigating attacks such as malware, phishing, and brute force through the collection and analysis of large volumes of data from security logs, network traffic and IoT devices. The use of data mining and machine learning algorithms will help us identify patterns and anomalies that might otherwise go unnoticed, enabling a more effective response to cyber incidents.

The project is divided into several phases spanning 18 weeks, beginning with system planning and design, followed by data collection and processing from multiple sources, development of predictive models, and implementation of an automated incident response system. The agile methodology we have adopted, based on Scrum, facilitates adaptation to changes in requirements and enables continuous delivery of incremental improvements throughout the project. In addition, we use the NIST RMS risk management framework to ensure that risks associated with the project are effectively identified, assessed and mitigated.

From an academic and professional point of view, “FenrirCyberWolf” is closely aligned with the competencies of the graduate profile of our Computer Engineering degree. In my case, I will apply skills such as the integral analysis of business processes, data transformation for decision making and the programming of complex queries that allow the manipulation of large volumes of information. On the other hand, Ricardo contributes with skills related to the development of IT solutions and the integration of systems according to the requirements of the organization. This project also allows us to put into practice key skills in high-demand areas such as cybersecurity, data analysis and artificial intelligence, which prepares us to face the challenges of today's labor market.

The relevance of the project lies not only in its ability to mitigate cyber threats, but also in its impact on the job field. As companies, organizations and government institutions become more dependent on digital technology, the security of computer systems has become crucial. Implementing solutions such as the ones we propose will not only protect organizations' sensitive data, but will also position us as highly skilled professionals in a constantly growing area. In addition, “FenrirCyberWolf” contributes to a more proactive and automated security approach, which increases the incident response capability and significantly reduces the number of incidents.

# 2. Conclusiones

## Ricardo Alcantar

**Integration of Data Science and Cybersecurity:** The “FenrirCyberWolf” project combines advanced data science techniques with cybersecurity to develop proactive and automated solutions to detect, prevent and mitigate cyber attacks. The application of data mining and machine learning algorithms facilitates the identification of patterns and anomalies, improving incident response and strengthening the security of digital systems.

## Cristian Ramirez

**Impact on the Workplace and Professional Preparation:** The implementation of “FenrirCyberWolf” not only addresses current cyber threats, but also prepares participants to face challenges in the job market. The experience gained in key areas such as cybersecurity, data analytics and artificial intelligence improves incident response capabilities and strengthens professional training, positioning developers as experts in a constantly evolving industry.

# 3. Reflexiones

## Ricardo Alcantar

**Proactivity in Cybersecurity:** The integration of data science into cybersecurity represents a significant advance towards a proactive approach to protecting computer systems. Rather than reacting to attacks once they occur, “FenrirCyberWolf” uses big data analytics to anticipate and prevent threats before they can cause harm. This strategy not only improves the effectiveness of incident responses, but also highlights the importance of continuous innovation and technological adaptation in the fight against cybercrime.

## Cristian Ramirez

**Preparation for the Professional Future:** The practical and advanced approach of the project demonstrates how the combination of technical and methodological competencies can prepare professionals for the challenges of the labor market. The expertise in cybersecurity, data analytics and artificial intelligence gained through “FenrirCyberWolf” not only strengthens the professional profile of the participants, but also reflects the growing demand for specialized skills in an increasingly complex digital environment. This type of project underlines the importance of keeping up with technological trends and developing innovative solutions to emerging problems.