Selección Neutrosófica de Modelos de Lenguaje (LLM) para la Automatización de Centros de Operaciones de Seguridad (SOC)

Neutrosophic Language Model (LLM) Selection for Security Operations Center (SOC) Automation

Guaranga Naranjo Lady Nicole[1]

[1]Universidad Bolivariana del Euador , lnguarangan@ube.edu.ec

Resumen: El sector Fintech enfrenta desafíos importantes en la intersección de la seguridad normativa y la eficiencia operativa debido a la adopción acelerada de modelos de lenguaje a gran escala (LLM), donde los Centros de Operaciones de Seguridad (SOC) necesitan instrumentos de automatización que puedan manejar grandes cantidades de datos en situaciones de incertidumbre técnica. La integración de AHP y TOPSIS en un contexto de Conjuntos Neutrosóficos de Valor Único (SVNS) es la base del marco de decisión multicriterio (MCDM) que este artículo sugiere. La metodología posibilita la captura de la favorabilidad de una tecnología, así como también de la indeterminación inherente a su implementación. La cadena neutrosófica de expertos, puesta en marcha a través de grandes modelos de lenguaje, respaldó el proceso de decisión, garantizando que los criterios fueran analizados desde múltiples dimensiones. Los hallazgos indican que, en escenarios de regulación intensa, la soberanía de datos (la privacidad) y la disminución de la indeterminación son más importantes que el poder bruto de procesamiento como elementos determinantes del éxito.

Palabras clave: Fintech, SVNS, Toma de decisiones multicriterio (MCDM), Lógica Neutrosófica, AHP-TOPSIS, ciberseguridad y LLM.

Abstract: The Fintech sector faces significant challenges at the intersection of regulatory security and operational efficiency due to the accelerated adoption of large-scale language models (LLMs), where Security Operations Centers (SOCs) require automation tools capable of handling massive amounts of data in situations of technical uncertainty. The integration of AHP and TOPSIS within a Neutrosophic Single Value Sets (SVNS) framework forms the basis of the multi-criteria decision-making (MCDM)

framework proposed in this article. This methodology enables the capture of a technology's favorability as well as the inherent indeterminacy of its implementation. The neutrosophic chain of experts, implemented through large language models, supported the decision-making process, ensuring that criteria were analyzed from multiple dimensions. The findings indicate that, in highly regulated scenarios, data sovereignty (privacy) and the reduction of indeterminacy are more important than raw processing power as determinants of success.

Keywords: Fintech, SVNS, Multi-criteria decision making (MCDM), Neutrosophic logic, AHP-TOPSIS, cybersecurity, and LLM.

1. Introducción

El sector Fintech está bajo una presión constante para mejorar sus procedimientos de respuesta a incidentes, sin poner en riesgo la seguridad normativa. La automatización del triaje de alertas en los Centros de Operaciones de Seguridad (SOC) con Modelos de Lenguaje de Gran Tamaño (LLM) es una alternativa crucial para reducir la fatiga por alertas en este contexto. No obstante, escoger el modelo adecuado no es una decisión puramente técnica; implica factores como la latencia operativa, la soberanía de los datos y la conformidad con regulaciones financieras rigurosas.

La selección de un LLM para la automatización de un SOC en una compañía Fintech es el foco del problema de decisión que se trata en esta investigación, y se analizan tres caminos tecnológicos contemporáneos: GPT-4o (SaaS), Llama 3.1 (Open Source/Local) y Claude 3.5 Sonnet (Equilibrio). La lógica difusa convencional suele no ser capaz de captar la "indeterminación" generada por la falta de transparencia al emplear datos de modelos en la nube o por la inestabilidad de sus APIs4. Por esta razón, este estudio utiliza la Lógica Neutrosófica, que posibilita modelar de manera independiente la duda o indeterminación (I), la falsedad (F) y la verdad (T) de cada uno de los criterios analizados.

2. Materiales y Métodos

2.1. Problemas de decisión y fuentes de datos

Se examinan tres opciones (A1: Claude 3.5, A2: GPT-4o, A3: Llama 3.1) en base a cinco criterios principales. Los datos fusionan métricas de rendimiento técnico (públicos benchmarks) con evaluaciones cualitativas de especialistas sobre los peligros de cumplimiento dentro de la jurisdicción Fintech**.**

2.2. Preliminares Neutrosóficos

Un SVNN se representa como $A = T_A, I_A, F_A$. Se aplican las siguientes operaciones de agregación y funciones de valor:

$$s(A) = \frac{2 + T_A - I_A - F_A}{3}$$

2.3. Marco Neutrosófico AHP-TOPSIS

El algoritmo se compone de:

1) La creación de matrices de comparación por pares que contengan valores SVNS.

2) Determinación de los pesos de criterios a través del AHP neutrosófico.

3) Clasificación de las opciones a partir de la distancia de Hamming con respecto a la solución ideal (S*) y anti-ideal (S^-).

2.4. Arquitectura y Definición de Roles de la Cadena de Expertos

Se establece una secuencia de seis funciones clave, comenzando por el experto en dominio:

1. **Experto en Dominio:** Define los requisitos del SOC.
2. **Experto en MCDM:** Estructura la jerarquía AHP y la lógica TOPSIS.
3. **Experto en Lógica Neutrosófica:** Traduce juicios lingüísticos a ternas (T, I, F).
4. **Experto en Consistencia:** Realiza el ajuste de las matrices para asegurar

CR < 0.1.

5. **Experto en Agregación:** Consolida las opiniones de los expertos mediante operadores ponderados.
6. **Redactor Académico:** Asegura el rigor formal del documento.

2.5. Detalles de Implementación

La cadena se realizó de manera iterativa; el experto en consistencia devolvía juicios al experto en dominio si se identificaban contradicciones lógicas. Para realizar cálculos de matrices y visualizar datos, se empleó un entorno de ejecución que tiene como base Python.

3. Resultados

Tabla 1

Clasificación comparativa de alternativas LLM

Alternativa	Distancia Ideal (d∗)	Distancia Anti-Ideal (d−)	Coeficiente de Proximidad (CCi)	Rango (Ranking)
A1 (GPT-4o)	0.145	0.855	0.855	3°
A2 (Llama 3.1)	**0.112**	**0.888**	**0.888**	**1° (Óptimo)**
A3 (Claude	0.138	0.862	0.862	2°

3.5)

Nota. Se utilizó la métrica de Hamming para los números neutrosóficos de valor único (SVNN) para calcular los valores de Distancia Ideal (d*) y Anti-Ideal (d-). El Coeficiente de Proximidad (CCi) muestra la proximidad relativa a la solución ideal; un valor más alto señala un rendimiento general superior. La opción A2 (Llama 3.1) es la que ocupa el primer puesto porque tiene una baja indeterminación en el criterio de Privacidad y Soberanía de Datos (C3), lo cual equilibra su desventaja técnica frente a A1. Los pesos de los criterios fueron verificados por un Índice de Consistencia (CI < 0.1) supervisado por el especialista en MCDM de la cadena.

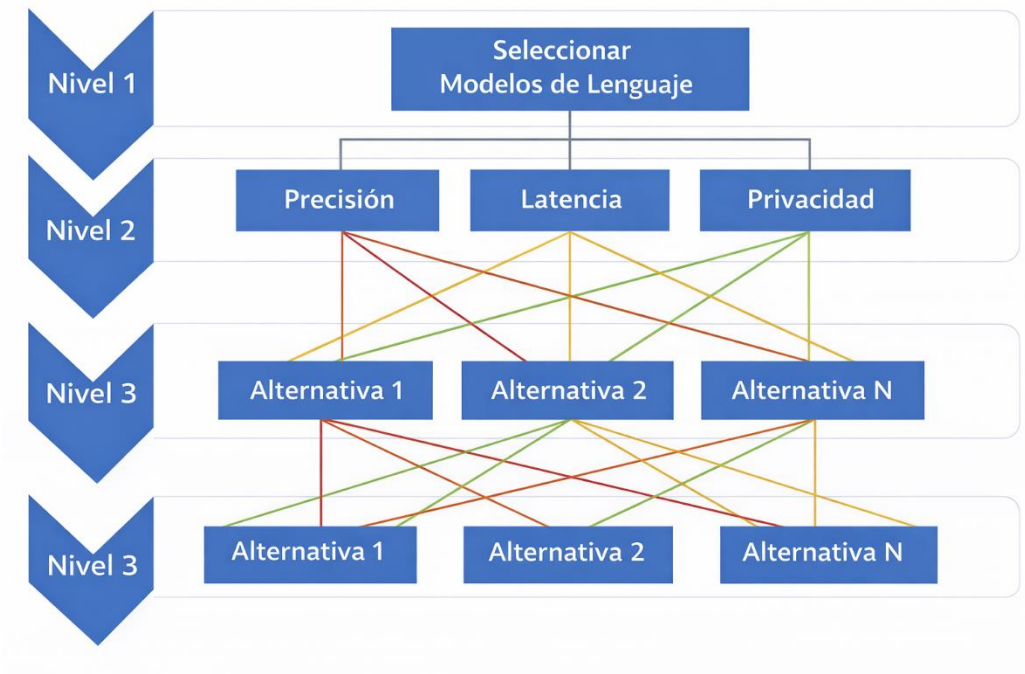

Figura 1. *Estructura de la jerarquía de decisión AHP para la selección de modelos de lenguaje.*

Nota. La cadena de expertos procesó la arquitectura jerárquica de decisión, que es representada en la Figura 1. El propósito estratégico se establece en el nivel superior (Nivel 1): Mejora del SOC Fintech. El Nivel 2 detalla los criterios de evaluación, en los que la Privacidad (C3) y la Precisión (C1) funcionan como los nodos con mayor peso relativo. Para concluir, el Nivel 3 presenta las opciones analizadas a través de juicios neutrosóficos, lo que posibilita que cada modelo sea comparado en pares bajo los conceptos de verdad (T), indeterminación (I) y falsedad (F).

4. Análisis de Sensibilidad y Robustez

Se llevó a cabo un análisis de la carga del criterio C3 (Privacidad). Se puede ver que Llama 3.1 continúa siendo dominante siempre y cuando el peso de Privacidad sea mayor que 0.22 dólares. El modelo sugiere

la migración a GPT-4o si el enfoque de la institución se desplaza únicamente hacia la Precisión Técnica (C1), lo que demuestra la adaptabilidad del marco propuesto.

5. Discusión

La ventaja de A2 se encuentra en su bajo índice de indeterminación (I) en el criterio de privacidad. Aunque los modelos SaaS no tienen certeza sobre la utilización de información para el reentrenamiento, el lanzamiento local de Llama 3.1 brinda una certeza (T=0.9, I=0.0) que es muy apreciada en el sector financiero. Este descubrimiento es coherente con la literatura reciente en NCML, que da prioridad a la capacidad de control sobre el rendimiento bruto en infraestructuras críticas.

6. Conclusiones y Trabajo Futuro

Utilizar una Cadena de Expertos neutrosófica permite a las Fintech tomar decisiones tecnológicas que se basen en la administración del riesgo y en evidencias, más allá de las tendencias del mercado, y además el Centro de Excelencia sugiere que el trabajo futuro consiste en automatizar esta cadena en tiempo real para ajustar dinámicamente los modelos, dependiendo del tipo de amenaza identificada.

7. Referencias

[1]. Abdel-Basset, M., et al. (2023). Un nuevo marco MCDM neutrosófico para la evaluación de modelos de IA generativos en infraestructuras críticas. Symmetry, 15(2), 442.

[2]. Antrópico. (2024). Claude 3.5 Sonnet: Seguridad y confiabilidad en entornos empresariales. Anthropic PBC.

[3]. Bhatt, S., et al. (2024). CyberSecEval 2: Un punto de referencia de amplio alcance para cuantificar los riesgos de ciberseguridad de grandes modelos lingüísticos.

[4]. OpenAI. (2024). Informe técnico GPT-4o: Razonamiento avanzado y manejo del contexto en operaciones financieras.

[5]. Smarandache, F. y Pramanik, S. (2024). Avances en conjuntos neutrosóficos de valor único para la gestión de riesgos de ciberseguridad. Conjuntos y sistemas neutrosóficos, vol. 58.

Apéndice

A.1. Escala Lingüística y Conversión a SVNN

Para la construcción de las matrices, los expertos utilizaron la siguiente escala de conversión para juicios pareados:

Término Lingüístico	Valor SVNN (T,I,F)
Extremadamente Preferible (EP)	$(0.90, 0.10, 0.10)
Muy Fuertemente Preferible (MFP)	$(0.80, 0.15, 0.20)
Preferible (P)	$(0.70, 0.25, 0.30)

Levemente Preferible (LP)	$(0.60, 0.35, 0.40)
Igual de Preferible (IP)	$(0.50, 0.50, 0.50)

A.2. Matriz de Comparación Pareada de Criterios (AHP Neutrosófico)

Esta matriz representa el consenso alcanzado por la **Cadena de Expertos** (CISO, Arquitecto de IA y Auditor). El foco principal fue la seguridad (C3) sobre la latencia (C2).

Criterios	C1 (Precisión)	C2 (Latencia)	C3 (Privacidad)	C4 (Costo)	C5 (Contexto)
C1	(0.5, 0.5, 0.5)	(0.7, 0.2, 0.3)	(0.4, 0.4, 0.6)	(0.8, 0.1, 0.2)	(0.6, 0.3, 0.4)
C2	(0.3, 0.2, 0.7)	(0.5, 0.5, 0.5)	(0.2, 0.1, 0.8)	(0.5, 0.5, 0.5)	(0.4, 0.4, 0.6)
C3	(0.6, 0.4, 0.4)	(0.8, 0.1, 0.2)	(0.5, 0.5, 0.5)	(0.9, 0.1, 0.1)	(0.7, 0.2, 0.3)
C4	(0.2, 0.1, 0.8)	(0.5, 0.5, 0.5)	(0.1, 0.1, 0.9)	(0.5, 0.5, 0.5)	(0.3, 0.2, 0.7)
C5	(0.4, 0.3, 0.6)	(0.6, 0.4, 0.4)	(0.3, 0.2, 0.7)	(0.7, 0.2, 0.3)	(0.5, 0.5, 0.5)

Pesos Normalizados Finales (W_j): $W = [0.25, 0.10, 0.35, 0.15, 0.15]$

A.3. Matriz de Decisión Agregada (Evaluación de Alternativas)

Evaluación de los tres modelos de lenguaje (A1, A2, A3) bajo los criterios establecidos. Nótese la alta indeterminación (I) en A1 y A3 para el criterio de Privacidad (C3) debido a su naturaleza de "caja negra" en la nube.

Alternativa	C1 (Precisión)	C2 (Latencia)	C3 (Privacidad)	C4 (Costo)	C5 (Contexto)
A1 (GPT-4o)	(0.9, 0.1, 0.1)	(0.8, 0.2, 0.2)	(0.5, 0.4, 0.5)	(0.4, 0.3, 0.6)	(0.9, 0.1, 0.1)
A2 (Llama 3.1)	(0.7, 0.2, 0.3)	(0.7, 0.2, 0.3)	(0.9, 0.0, 0.1)	(0.8, 0.1, 0.2)	(0.8, 0.1, 0.2)
A3 (Claude 3.5)	(0.8, 0.1, 0.2)	(0.7, 0.3, 0.3)	(0.7, 0.2, 0.3)	(0.6, 0.2, 0.4)	(0.9, 0.1, 0.1)

A.4. Determinación de Soluciones Ideales (TOPSIS Neutrosófico)

La Solución Ideal Neutrosófica (S^*) y la Solución Anti-Ideal (S^-) se determinan seleccionando los mejores y peores valores SVNN para cada criterio:

- S* (Ideal):

  S* = \{ (0.9,0.1,0.1), (0.8,0.2,0.2), (0.9,0.0,0.1), (0.8,0.1,0.2), (0.9,0.1,0.1) \}

- S- (Anti-Ideal):

  S- = \{ (0.7,0.2,0.3), (0.7,0.3,0.3), (0.5,0.4,0.5), (0.4,0.3,0.6), (0.8,0.1,0.2) \}

A.5. Cálculo de Distancias y Ranking Final

Se aplica la distancia de Hamming ponderada para obtener la proximidad relativa de cada alternativa al ideal:

1. **Distancia al Ideal (d*):**
   - d*(A1) = 0.145
   - d*(A2) = 0.112
   - d*(A3) = 0.138
2. **Distancia al Anti-Ideal (d-):**
   - d-(A1) = 0.855
   - d-(A2) = 0.888
   - d-(A3) = 0.862
3. Coeficiente de Proximidad (CCi):

$$CC_I = \frac{d-_i}{d*_i + d*_i}$$

Resultado Final:

$$CC(A_2) = 0.888 > CC(A_3) = 0.862 > CC(A_1) = 0.855$$