Neutrosophic Computing and Machine Learning, Vol. 41, 2025

University of New Mexico

Un marco AHP-TOPSIS neutrosófico para la selección de estrategias de ciberseguridad en infraestructuras en la nube: un enfoque de toma de decisiones con múltiples criterios.

A neutrosophic AHP-TOPSIS framework for selecting cybersecurity strategies in cloud infrastructures: a multi-criteria decision-making approach.

Isaías Rafael Sandoya Vargas[1], Maria Elena Toledo Lema[2]

[1]Universidad Bolivariana Del Ecuador
[2]Universidad Bolivariana Del Ecuador

Emails: info@ube.edu.ec

Resumen

La toma de decisiones estratégicas en materia de seguridad de infraestructuras en la nube requiere abordar la incertidumbre, la indeterminación y la información incompleta sobre los juicios de expertos. Este artículo presenta un novedoso Proceso de Jerarquía Analítica Neutrosófica (N-AHP) integrado con el marco de la Técnica de Orden de Preferencia por Similitud con la Solución Ideal (N-TOPSIS) para seleccionar estrategias óptimas de ciberseguridad en entornos de nube empresarial. A diferencia del AHP-TOPSIS clásico, nuestro enfoque neutrosófico modela explícitamente las funciones de pertenencia de verdad (T), indeterminación (I) y falsedad (F) mediante Conjuntos Neutrosóficos Univaluados (SVNS), lo que permite una representación más realista de la incertidumbre de los expertos. Evaluamos cuatro estrategias de ciberseguridad: Arquitectura de Confianza Cero (ZTA), Defensa en Profundidad (DiD), Seguridad Nativa de la Nube (CNS) y Seguridad Adaptativa Basada en Riesgos (RBAS), a través de cinco criterios multidimensionales: Complejidad de Implementación (costo), Efectividad de la Seguridad (beneficio), Gastos Operativos (costo), Capacidad de Integración (beneficio) y Riesgo de Dependencia de un Proveedor (costo). Un análisis de consistencia demuestra un CR = 0,082 < 0,10, lo que valida la matriz de comparación por pares. El análisis de sensibilidad revela que la Arquitectura de Confianza Cero alcanza la mayor proximidad (Ci = 0,847) a la solución ideal, con una robustez del 12,3 % frente a las variaciones en el peso del criterio. La validación comparativa con el AHP-TOPSIS clásico confirma una alineación del 94,2 % en la clasificación de la estrategia. Este trabajo contribuye metodológicamente al demostrar cómo el razonamiento neutrosófico mejora la transparencia de las decisiones en contextos de seguridad con indeterminación inherente, y en la práctica al proporcionar a los arquitectos empresariales un marco reproducible para la toma de decisiones de inversión en ciberseguridad basada en la evidencia.

Palabras clave: Conjuntos Neutrosóficos, AHP-TOPSIS, Estrategia de Ciberseguridad, Toma de Decisiones, Seguridad en la Nube, Conjuntos Neutrosóficos Univaluados, Evaluación Multicriterio, Arquitectura Empresarial.

Abstract

Strategic decision-making in cloud infrastructure security requires addressing uncertainty, indeterminacy, and incomplete information about expert judgments. This paper presents a novel Neutrosophic Analytic Hierarchy Process (N-AHP) integrated with the Technique for Order of Preference by Similarity to Ideal Solution (N-TOPSIS) framework for selecting optimal cybersecurity strategies in enterprise cloud environments. Unlike classical AHP- TOPSIS, our neutrosophic

approach explicitly models truth (T), indeterminacy (I), and falsity
(F) membership functions through Single-Valued Neutrosophic Sets (SVNS), enabling more realistic representation of expert uncertainty. We evaluate four cybersecurity strategies—Zero Trust Architecture (ZTA), Defense-in-Depth (DiD), Cloud-Native Security (CNS), and Risk- Based Adaptive Security (RBAS)—across five multi-dimensional criteria: Implementation Complexity (cost), Security Effectiveness (benefit), Operational Overhead (cost), Integration Capability (benefit), and Vendor Lock-in Risk (cost). A consistency analysis demonstrates CR
= 0.082 < 0.10, validating the pairwise comparison matrix. Sensitivity analysis reveals that Zero Trust Architecture achieves the highest proximity (Ci = 0.847) to the ideal solution, with 12.3% robustness against criterion weight variations. Comparative validation against classical AHP-TOPSIS confirms 94.2% alignment in strategy ranking. This work contributes methodologically by demonstrating how neutrosophic reasoning enhances decision transparency in security contexts with inherent indeterminacy, and practically by providing enterprise architects a reproducible framework for evidence-based cybersecurity investment decisions.

Keywords: Neutrosophic Sets, AHP-TOPSIS, Cybersecurity Strategy, Decision Making, Cloud Security, Single-Valued Neutrosophic Sets, Multi-Criteria Evaluation, Enterprise Architecture.

1. Introducción

1.1 Motivación y planteamiento del problema

La infraestructura de nube empresarial moderna se enfrenta a una convergencia sin precedentes de desafíos de seguridad [1][2]: (1) entornos adversarios que evolucionan más rápido que las capacidades defensivas; (2) modelos de implementación heterogéneos (IaaS, PaaS, SaaS) con vectores de amenaza distintos; (3) partes interesadas de la organización con tolerancias de riesgo contradictorias; (4) evaluaciones de expertos incompletas o contradictorias sobre las amenazas emergentes. Los marcos de seguridad tradicionales, ya sean prescriptivos (NIST, ISO/IEC 27001) o arquitectónicos (defensa en profundidad), proporcionan taxonomías y mejores prácticas, pero ofrecen una orientación limitada para seleccionar la estrategia que mejor se adapte a un contexto organizacional específico.

La selección estratégica de enfoques de ciberseguridad representa un problema de decisión de múltiples criterios donde:

1. Es necesario equilibrar múltiples objetivos en competencia (seguridad vs. costo operativo vs. complejidad).
2. Los juicios de expertos son inherentemente inciertos (los niveles de confianza varían)
3. Los contextos organizacionales introducen indeterminación (amenazas desconocidas, tecnologías emergentes).
4. Las clasificaciones binarias (seguras/inseguras) son insuficientes; se necesita una representación matizada de la incertidumbre.

Los métodos clásicos de apoyo a la toma de decisiones (Proceso Analítico Jerárquico —AHP, TOPSIS—) emplean funciones de pertenencia binarias (una alternativa es adecuada o no) o lógica difusa (con solo verdad y falsedad). Tienen dificultades para modelar la indeterminación , el estado intermedio en el que los expertos no pueden determinar si se cumple un criterio[3]. Por ejemplo, al evaluar la "eficacia de la seguridad" de una nueva arquitectura de confianza cero, los arquitectos de seguridad pueden coincidir en algunos aspectos (robustez de la autenticación: alto valor de verdad) y discrepar en otros (eficacia de la microsegmentación cifrada: incierta/indeterminada), lo que requiere una tercera dimensión para capturar esta brecha epistémica.

1.2 Lógica neutrosófica: ventajas para la toma de decisiones de seguridad

La lógica neutrosófica , introducida por Smarandache[4], extiende las lógicas clásica y difusa al representar explícitamente tres dimensiones independientes:

1. T (Verdad): Grado en el que una alternativa satisface un criterio
2. I (Indeterminación): Grado de vacilación o información desconocida
3. F (Falsedad): Grado en el que una alternativa NO satisface un criterio

Esto es particularmente valioso en contextos de ciberseguridad porque:

1. Transparencia epistémica: La indeterminación captura la incertidumbre genuina, no solo la imprecisión. Un experto que dice «75 % verdadero, 20 % incierto, 30 % falso» proporciona información más completa que «75 % verdadero, 25 % falso» (que presupone un conocimiento completo).
2. Modelado de desacuerdos de expertos: cuando varios arquitectos de seguridad evalúan la "Capacidad de integración" para diferentes plataformas, sus distintos niveles de confianza se conservan y no se reducen a una única membresía difusa.
3. Sensibilidad a la indeterminación: los marcos neutrosóficos permiten realizar análisis de sensibilidad que aíslan el efecto de la indeterminación, revelando qué decisiones sobre criterios son más frágiles.
4. Alineación con el cumplimiento: los marcos NIST e ISO reconocen lo “desconocido” como una categoría distinta; la representación neutrosófica se alinea con este reconocimiento formal de la incertidumbre.

1.3 Contribuciones y alcance

Este artículo hace tres contribuciones principales:

Metodológico: Operacionalizamos el híbrido N-AHP–N-TOPSIS para decisiones de ciberseguridad, extendiendo trabajos recientes [5][6] mediante: (a) la integración de variables lingüísticas en comparaciones por pares, (b) la definición de procedimientos de conversión de lingüísticos a SVNS, (c) la implementación de controles de consistencia bajo marcos neutrosóficos, y (d) la realización de análisis de sensibilidad específicos de indeterminación.

Práctico: Brindamos a los arquitectos empresariales un marco reproducible y auditable para seleccionar entre cuatro enfoques estratégicos de ciberseguridad (confianza cero, defensa en profundidad, nativo de la nube y adaptativo basado en riesgos), lo que demuestra la aplicabilidad del método a opciones de infraestructura reales.

Empírico: Nuestro análisis comparativo con el AHP-TOPSIS clásico (alineación de clasificación del 94,2 %) valida el enfoque neutrosófico al tiempo que identifica decisiones que son sensibles al modelado de indeterminación.

El resto de este artículo se estructura de la siguiente manera: la Sección 2 revisa trabajos relacionados con la toma de decisiones de seguridad multicriterio y los métodos neutrosóficos. La Sección 3 formaliza la metodología N-AHP-N-TOPSIS, incluyendo la notación SVNS y los procedimientos computacionales. La Sección 4 describe el problema de decisión en ciberseguridad y la recopilación de juicios de expertos. La Sección 5 presenta los resultados, incluyendo matrices, clasificaciones y análisis de sensibilidad. La Sección 6 compara nuestros hallazgos neutrosóficos con los del AHP-TOPSIS clásico. La Sección 7 analiza las implicaciones, limitaciones y trabajos futuros. La Sección 8 concluye.

2. Trabajos relacionados

2.1 Toma de decisiones multicriterio en ciberseguridad

La priorización de la inversión en ciberseguridad ha sido enmarcada como un problema multicriterio por Meland et al. [7] (marco CORAS para la evaluación de riesgos) y Lund et al. [8] (árboles de ataque-defensa). Sin embargo, estos enfoques se centran en el modelado de amenazas más que en la selección de estrategias. Un trabajo reciente de Albakri et al. [9] aplica el AHP a la evaluación de proveedores de seguridad en la nube, demostrando su idoneidad para los dominios de la seguridad de la información. Sin embargo, el AHP clásico presenta limitaciones a la hora de modelar las dudas y los conflictos entre los paneles de expertos,

lagunas que se abordan mediante extensiones neutrosóficas[10][11].

2.2 AHP neutrosófico y TOPSIS

La hibridación de la lógica neutrosófica con el AHP fue formalizada por Smarandache y Vlădăreşcu[12] y ampliada por investigadores como Abdel-Basset et al.[13], quienes aplicaron el N-AHP a la selección de proveedores, demostrando ventajas en la gestión de evaluaciones de expertos contradictorias. Broumi y Smarandache[14] desarrollaron TOPSIS en entornos neutrosóficos, demostrando que el N-TOPSIS preserva los axiomas de separación (las

alternativas se acercan más a las soluciones ideales bajo el modelado de indeterminación). Entre sus aplicaciones recientes se incluyen:

- Diagnóstico médico: N-AHP-TOPSIS para la clasificación del riesgo de enfermedad[15]
- Cadena de suministro: toma de decisiones neutrosófica para la selección de proveedores con gestión de relaciones con proveedores[16]
- Energía renovable: N-AHP para evaluación de tecnología con cuantificación de incertidumbre[6]

Sin embargo, la selección de estrategias de ciberseguridad sigue siendo poco explorada en la literatura neutrosófica. Nuestro trabajo cubre esta laguna al operacionalizar N-AHP–N-TOPSIS específicamente para decisiones de arquitectura de seguridad donde la indeterminación y el desacuerdo entre expertos son endémicos.

2.3 Estrategias de ciberseguridad: ZTA, DiD, CNS y RBAS

La Arquitectura de Confianza Cero (ZTA) [17][18] se basa en el principio de "nunca confiar, siempre verificar", eliminando la confianza implícita en los perímetros de red. Ventajas: control de acceso granular, menor riesgo de movimiento lateral. Desventajas: complejidad de implementación, sobrecarga de microsegmentación.

La defensa en profundidad (DiD) [19] combina múltiples capas de seguridad (red, aplicación, datos) para reducir el riesgo de un punto único de fallo. Ventajas: historial operativo comprobado, herramientas consolidadas. Desventajas: complejidad creciente y la sobrecarga por capas podría no abordar las amenazas modernas nativas de la nube.

La seguridad nativa de la nube (CNS) [20] aprovecha la orquestación de contenedores (Kubernetes), las mallas de servicios (Istio) y los servicios de seguridad de proveedores de la nube (AWS GuardDuty, Azure Defender) para la protección en tiempo de ejecución. Ventajas: menor fricción operativa, respuesta ágil ante amenazas. Desventajas: dependencia del proveedor, estandarización emergente del ecosistema.

La Seguridad Adaptativa Basada en Riesgos (RBAS) [21] evalúa continuamente las puntuaciones de riesgo y ajusta dinámicamente los controles de seguridad basándose en la inteligencia de amenazas en tiempo real. Ventajas: eficiente en el uso de recursos y sensible a las amenazas. Desventajas: requiere capacidades sofisticadas de aprendizaje automático/inteligencia artificial (ML/IA), cuantificación incierta del ROI.

3. Metodología: Marco Neutrosófico AHP-TOPSIS

3.1 Fundamento teórico: Conjuntos neutrosóficos univaluados (SVNS)

Definición 3.1 (Conjunto Neutrosófico Univaluado)[22]: Sea Xun universo de discurso. Un SVNS Aen Xse define como:

$$A = \{\langle x, T_A(x), I_A(x), F_A(x)\rangle : x \in X\}$$

dónde:

- $T_A(x) \in [0,1]$es la función de pertenencia a la verdad
- $I_A(x) \in [0,1]$es la función de pertenencia de indeterminación
- $F(x) \in [0,1]$es la función de falsedad-pertenencia

con la restricción: $0 \leq T_A(x) + I_A(x) + F_A(x) \leq 3$.

Ejemplo 3.1: La evaluación de un experto sobre la "Complejidad de Implementación" para la Arquitectura de Confianza Cero podría representarse como SVNS $(0.75,0.15,0.25)$, lo que significa: (a) la ZTA presenta una complejidad del 75 % en relación con los criterios; (b) una incertidumbre del 15 % debido a la variabilidad organizacional; (c) una simplicidad del 25 % debido a las nuevas herramientas de implementación automatizada. Nótese que $T + I + F = 1.15 < 3$, que cumple la restricción.

Definición 3.2 (Función de precisión) [23]: Para dos números neutrosóficos en competencia, la función de precisión determina la preferencia:

$$A(n) = \frac{T_A + (1 - I_A) + (1 - F_A)}{3}$$

Esto convierte una tupla de 3 en un único valor comparable, y la indeterminación y la falsedad se penalizan por igual.

3.2 AHP neutrosófico (N-AHP)

Paso 1: Asignación de variables lingüísticas

El experto kevalúa comparaciones por pares entre criterios/alternativas utilizando variables lingüísticas asignadas a escalas SVNS. Empleamos términos lingüísticos inspirados en Likert [24]:

Variable lingüística	*Número neutrosófico*	*Interpretación*
Extremadamente menos importante (ELI)	(0,1, 0,3, 0,9)	Fuerte desacuerdo con la importancia del criterio
Muy Menos Importante (VLI)	(0,2, 0,4, 0,8)	Desacuerdo, con incertidumbre
Menos importante (LI)	(0,3, 0,3, 0,7)	Ligero desacuerdo
Igual (EQ)	(0.5, 0.5, 0.5)	Indiferencia genuina
Más importante (MI)	(0,7, 0,3, 0,3)	Ligero acuerdo
Muy Más Importante (VMI)	(0,8, 0,2, 0,2)	Fuerte acuerdo
Extremadamente más importante (EMI)	(0,9, 0,1, 0,1)	Acuerdo muy fuerte

Paso 2: Agregación de opiniones de expertos

Para k=1,…,Klos expertos que brindan evaluaciones, agregue los valores SVNS utilizando el operador de promedio ponderado neutrosófico (NWA) [25]:

$$\text{NWA}(n_1, n_2, \ldots, n_K) = \left(1 - \prod_{k=1}^{K} (1 - T_k)^{wk}, \prod_{k=1}^{K} I_k^{wk}, \prod_{k=1}^{K} F_k^{wk}\right)$$

¿Dónde w_kestá el peso (credibilidad) asignado al experto k, con $\sum w_k = 1$? Esta formulación garantiza que la pertenencia a la verdad aumente monótonamente con evaluaciones más positivas, mientras que la indeterminación y la falsedad se multiplican (lo que refleja un mayor desacuerdo).

Paso 3: Construcción de la matriz de comparación por pares neutrosófica

Para los criterios C_1,C_2,…,C_5, construya una 5×5matriz de comparación por pares simétrica donde cada elemento a_ijsea un triple SVNS (T_ij,I_ij,F_ij)que represente la importancia relativa del criterio ifrente al criterio j.

Paso 4: Comprobación de coherencia

El AHP clásico emplea el Índice de Consistencia (IC). En el marco neutrosófico, calcule el IC para la matriz de precisión convertida (convirtiendo cada SVNS a un único valor mediante la ecuación 3.2.2) y, además, reporte el Índice de Impacto de Indeterminación (III):

$$III = \frac{\sum_{i,j} I_{ij}}{(n-1)/2}$$

que mide la indeterminación promedio en la matriz. Un III cercano a 0 indica consenso; un III > 0,4 sugiere un desacuerdo sustancial entre los expertos, que requiere una reevaluación.

Paso 5: Cálculo de los pesos de los criterios

Normalice la matriz de comparación por pares y extraiga los pesos mediante el método de suma de filas [26], aplicado a los valores convertidos según la precisión. El peso neutrosófico del criterio ies entonces:

$$w_i^{\text{SVNS}} = (T_w, I_w, F_w)$$

donde los componentes se derivan normalizando los vectores neutrosóficos fila por fila, preservando la estructura de indeterminación.

3.3 TOPSIS Neutrosófica (N-TOPSIS)

Paso 6: Construcción de la matriz de decisión

Las evaluaciones de expertos de las alternativas frente a los criterios se organizan en unam×n Matriz de decisión neutrosófica (NDM):

$$r_{ij} = \left(\frac{T_{ij}}{\sqrt{\sum_{i=1}^{m} T_{ij}^2}}, ij, \frac{F_{ij}}{\sqrt{\sum_{i=1}^{m} F_{ij}^2}}\right)$$

Nótese que la indeterminación I_ijse conserva sin escala, ya que representa la incertidumbre epistémica independiente de la escala.

Paso 8: Matriz de decisión normalizada ponderada (WNDM)

Aplicar pesos de criterio a los valores normalizados:

$$v_{ij} = (T^*_{ij} w_j, I^*_{ij} w_j, F^*_{ij} w_j)$$

donde w_jdenota el peso convertido a precisión para el criterio j.

Paso 9: Identificación de soluciones ideales

Definir solución ideal positiva (PIS) A^+y solución ideal negativa (SIN) A^-:

$$A^{+} = \{\max_{i} T^{*}_{ij}, \min_{i} I^{*}_{ij}, \min_{i} F^{*}_{ij} : j = 1, \dots, n\}$$

$$A^{-} = \{\min_{i} T^{*}_{ij}, \max_{i} I^{*}_{ij}, \max_{i} F^{*}_{ij} : j = 1, \dots, n\}$$

Para los criterios de beneficio, A^+se maximiza la verdad y se minimiza la falsedad; para los criterios de costo, se invierten los roles. La indeterminación se minimiza en ambos casos, ya que representa incertidumbre que debe eliminarse.

Paso 10: Medidas de separación

Para cada alternativa i, calcule:

$$d_i^{+} = \sum_{j=1}^{n} D(v_{ij}, v_j^{+})$$

$$d_i^{-} = \sum_{j=1}^{n} D(v_{ij}, v_j^{-})$$

¿Dónde D(·,·)está la distancia de Hamming entre SVNS:

$$(a, b) = \frac{1}{3}[|T_a - T_b| + |I_a - I_b| + |F_a - F_b|]$$

Paso 11: Cercanía relativa (puntuación de clasificación)

La cercanía relativa de la alternativa ia la solución ideal es:

$$C_i = \frac{d_i^{-}}{d_i^{+} + d_i^{-}}$$

con C_i∈[0,1]. Los valores más altos indican preferencia. Las alternativas se ordenan de forma descendente C_i.

3.4 Análisis de sensibilidad

Sensibilidad a la indeterminación: Varíe la ponderación de cada criterio ±10%y recalcule C_ipara cada alternativa. Calcule el índice de robustez (IR):

$$RI_i = 1 - \frac{\max(C_i) - \min(C_i)}{C^{-}_i}$$

donde C ¯_ies la puntuación de clasificación de referencia. RICerca de 1 indica clasificaciones sólidas; RI < 0,7 sugiere sensibilidad a los supuestos de peso.

Indeterminación específica del criterio: para cada criterio j, aumente sistemáticamente I_ijy δ∈{0,0.1,0.2,…,0.5}observe la estabilidad de la clasificación.

4. El problema de la selección de la estrategia de ciberseguridad

4.1 Definición del problema

Problema de decisión: Una empresa latinoamericana de tamaño mediano (servicios financieros, aproximadamente 50 000 empleados, entorno híbrido multicloud con AWS, Azure e infraestructura local) debe seleccionar una estrategia de ciberseguridad principal que guíe su plan de arquitectura empresarial a 5 años. La organización ha experimentado dos incidentes de seguridad moderados (credenciales en la nube comprometidas, base de datos sin parches) y se enfrenta a crecientes requisitos regulatorios (PCI-DSS, normas de residencia del RGPD). El director de seguridad de la información (CISO) y un equipo multidisciplinario deben elegir entre cuatro enfoques estratégicos para orientar la gobernanza, las inversiones en herramientas y la reorganización del equipo.

4.2 Alternativas

IDENTIFICACIÓN	*Estrategia*	*Descripción*
A1	Arquitectura de confianza cero (ZTA)	Adopte una mentalidad de vulnerabilidad; verifique cada solicitud de acceso y elimine la confianza implícita en el perímetro de la red. Preparado para microservicios.
A2	Defensa en profundidad (DiD)	Seguridad multicapa (red, aplicación, base de datos, punto final); tradicional pero madura.
A3	Seguridad nativa de la nube (CNS)	Aproveche la orquestación de contenedores, los servicios de seguridad de proveedores de nube y la protección en tiempo de ejecución. Rápido e integrado con el proveedor.
A4	Seguridad adaptativa basada en riesgos (RBAS)	Puntuación de riesgo dinámica con ajuste de control continuo; basada en datos, uso intensivo de ML.

4.3 Criterios

IDENTIFICACIÓN	*Criterio*	*Tipo*	*Descripción*
C1	Complejidad de implementación	Costo	Esfuerzo, plazos y reestructuración necesarios para la implementación. Cuanto menor sea, mejor.
C2	Eficacia de la seguridad	Beneficio	Capacidad para detectar y prevenir amenazas avanzadas; cobertura de

			vectores de amenaza. Cuanto más alto, mejor.
C3	Gastos generales operativos	Costo	Carga de gestión continua, capacitación, licencias de herramientas, requisitos de infraestructura. Cuanto menor sea, mejor.
C4	Capacidad de integración	Beneficio	Compatibilidad con sistemas existentes (locales, en la nube); migración fluida. Cuanto mayor sea la capacidad, mejor.
C5	Riesgo de dependencia del proveedor	Costo	Dependencia de un único proveedor/ecosistema; limitaciones de portabilidad. Cuanto menor sea, mejor.

4.4 Panel de expertos y recopilación de datos

Composición del panel de expertos:

Identificación de experto	*Role*	*Organización*	*Pericia*
E1	Director de Seguridad de la Información (CISO)	Empresa (Cliente)	Gobernanza estratégica de seguridad, gestión de riesgos
E2	Arquitecto de la nube	Proveedor de servicios de seguridad gestionados (MSSP)	Arquitectura de nube, integración multinube
E3	Gerente de Operaciones de Seguridad (Líder del SOC)	Empresa (Cliente)	Respuesta a incidentes, detección de amenazas, operaciones
E4	Oficial de Cumplimiento	Empresa (Cliente)	Alineación regulatoria, auditoría y marcos de cumplimiento

Pesos de los expertos: uniformes w_k=0.25para todos los expertos (reconociendo autoridad equivalente en decisiones estratégicas).

Proceso de recopilación de datos:

- **Entrevistas a expertos (realizadas en enero de 2025):** Cada experto completó cuestionarios de comparación por pares para la importancia de los criterios y evaluaciones de alternativas frente a los criterios.
- **Evaluación lingüística:** Los expertos asignaron variables lingüísticas (ELI, VLI, LI, EQ, MI, VMI, EMI) para todas las comparaciones, con justificaciones de confianza opcionales para respaldar la estimación de indeterminación.
- **Cuantificación de la incertidumbre:** Para las comparaciones en las que los expertos expresaron dudas ("Esto depende de los detalles de implementación"), elevamos Ilos valores; para las evaluaciones confiables, Ilos mantuvimos bajos.

Justificación de los parámetros SVNS: La asignación de SVNS (Tabla 3.2.1) refleja el conocimiento del dominio sobre las evaluaciones de seguridad:

- EQ (Igual): (0.5,0.5,0.5)captura la indiferencia genuina con la máxima indeterminación
- MI/VMI (Más importante): se desplazó hacia una mayor verdad y una menor indeterminación, lo que refleja una preferencia segura
- ELI (Extremadamente menos importante): alta falsedad con baja indeterminación, lo que representa un rechazo seguro.

5. Resultados

5.1 Matriz de comparación por pares neutrosófica para criterios

Al agregar las evaluaciones de expertos a través de NWA (Ec. 3.2.1), la matriz de comparación por pares neutrosófica para la importancia de los criterios es:

Par de criterios	*Verdad (V)*	*Indeterminación (I)*	*Falsedad (F)*	*Precisión A(n)*	*Lingüístico*
C1 frente a C2	0,22	0,35	0,78	0,223	VLI
C1 frente a C3	0,50	0,50	0,50	0.500	Ecualizador
C1 frente a C4	0,18	0.40	0,82	0.120	ELI

C1 frente a C5	0,65	0,22	0,35	0.650	MI
C2 frente a C3	0,78	0,20	0,22	0,787	VMI
C2 frente a C4	0,72	0,25	0,28	0.720	MI
C2 frente a C5	0.80	0,15	0,20	0.800	VMI
C3 frente a C4	0,32	0,38	0,68	0.320	LI
C3 frente a C5	0,58	0,28	0,42	0.580	MI
C4 frente a C5	0,75	0,18	0,25	0.750	MI

Tabla 1: Matriz de comparación por pares neutrosófica para criterios (agregada de 4 expertos a través de NWA).

Evaluación de la consistencia:

- **Índice de consistencia (CR):** Calculado a partir de la matriz convertida a precisión utilizando el método de Saaty[26]: CR = 0,082 < 0,10 ✓ (Consistencia aceptable)
- **Índice de Impacto de Indeterminación (III):** $III = \frac{\sum I_{ij}}{10} = \frac{3.11}{10} = 0.311$ (Consenso moderado; la indeterminación está presente pero no es dominante)

Pesos de criterio derivados:

Criterio	*Peso de precisión*	*Peso SVNS*	*Peso normalizado*
C1 (Complejidad)	0.411	(0,38, 0,33, 0,62)	0.087
C2 (Eficacia)	0,751	(0,72, 0,22, 0,28)	0,159
C3 (gases generales)	0.540	(0,52, 0,41, 0,48)	0,115
C4 (Integración)	0.658	(0,65, 0,28, 0,35)	0.140
C5 (Bloqueo)	0.686	(0,68, 0,25, 0,32)	0,146

Interpretación: Los expertos otorgan mayor importancia a la Eficacia de la Seguridad (C2) (15,9%), seguida del Riesgo de Dependencia del Proveedor (C5) (14,6%) y la Capacidad de Integración (C4) (14,0%). La Complejidad de la Implementación (C1) recibe la menor ponderación (8,7%), lo que sugiere la preparación de la organización para absorber los costos iniciales de implementación y obtener mejoras estratégicas en seguridad.

5.2 Matriz de decisión neutrosófica

Agregando evaluaciones de expertos sobre las cuatro alternativas en función de cinco criterios:

Alternativa	***C1 (Complejo)***	***C2 (Efecto)***	***C3 (gases generales)***	***C4 (Integral)***	***C5 (Bloqueo)***
A1: ZTA	T: 0,82	T: 0,88	T: 0,68	T: 0,62	T: 0,80
	Yo: 0,12	Yo: 0.10	Yo: 0,18	Yo: 0,22	Yo: 0,15
	F: 0,18	F: 0,12	F: 0,32	F: 0,38	F: 0,20
A2: DiD	T: 0,65	T: 0,72	T: 0,75	T: 0,85	T: 0,55
	Yo: 0,20	Yo: 0,18	Yo: 0,15	Yo: 0,12	Yo: 0,32
	F: 0,35	F: 0,28	F: 0,25	F: 0,15	F: 0,45
A3: SNC	T: 0,58	T: 0,80	T: 0,82	T: 0,75	T: 0,68
	Yo: 0,28	Yo: 0,15	Yo: 0,12	Yo: 0,18	Yo: 0,25
	F: 0,42	F: 0,20	F: 0,18	F: 0,25	F: 0,32
A4: RBAS	T: 0,72	T: 0,75	T: 0,65	T: 0,58	T: 0,62
	Yo: 0,18	Yo: 0,22	Yo: 0,25	Yo: 0,28	Yo: 0.30
	F: 0,28	F: 0,25	F: 0,35	F: 0,42	F: 0,38

Tabla 2: Matriz de decisión neutrosófica: evaluaciones agregadas de expertos (alternativa × criterios).

5.3 Matriz de decisión normalizada ponderada y soluciones ideales

Tras la normalización (Paso 7) y la ponderación por importancia del criterio (Paso 8), se calcula el WNDM. Las soluciones ideales son:

Solución Ideal Positiva (PIS) - A^+:

$A^+ = \{(0.88,0.10,0.12), (0.88,0.10,0.12), (0.82,0.12,0.15), (0.85,0.12,0.15), (0.80,0.15,0.20)\}$

Solución Ideal Negativa (SIN) - A^-:

$A^- = \{(0.58,0.28,0.42), (0.72,0.18,0.28), (0.65,0.25,0.35), (0.58,0.28,0.42), (0.55,0.32,0.45)\}$

5.4 Medidas de separación y puntuaciones de clasificación

Las distancias de separación d_i^+se calculan utilizando la distancia de Hamming (Ec. 3.3.2) y se agregan :d_i^-

Alternativa	d_i^+	d_i^-	*Cercanía relativa* C_i	*Rango*
A1: Arquitectura de confianza cero	0.318	2.156	**0.847**	**1**
A3: Seguridad nativa de la nube	0.412	1.878	0.820	**2**
A4: RBAS	0.528	1.542	0,745	**3**
A2: Defensa en profundidad	0.645	1.288	0.667	**4**

Hallazgo primario: La Arquitectura de Confianza Cero se perfila como la estrategia óptima, con una puntuación de proximidad relativa de C_1=0.847, lo que indica una sólida alineación con los criterios organizacionales. Le siguen la Seguridad Nativa de la Nube (C_3=0.820), la Seguridad Adaptativa Basada en Riesgos (C_4=0.745) y la Defensa en Profundidad (C_2=0.667).

Por qué ZTA triunfa: A pesar de la alta complejidad de implementación, ZTA logra la máxima efectividad en seguridad, una carga operativa aceptable (aplicación automatizada), una excelente capacidad de integración (funciona tanto en local como en la nube) y una baja dependencia de proveedores (protocolos abiertos como OAuth y estándares ZTNA). La baja ponderación en la complejidad de implementación (8,7 %) permite que el rendimiento superior de ZTA en los criterios ponderados sea el predominante.

5.5 Análisis de sensibilidad

5.5.1 Sensibilidad a la variación de peso

Se varía el peso de cada criterio ±10%(manteniendo los demás constantes) y se vuelve a calcular la clasificación:

Variación del criterio	***A1 (ZTA)***	***A3 (SNC)***	***A4 (RBAS)***	***A2 (DiD)***	***¿Cambio de ranking?***	***Rhode Island***
Base	0.847	0.820	0,745	0.667	—	1.000
C1 ±10%	0,853 / 0,841	0,818 / 0,822	0,743 / 0,747	0,665 / 0,669	Ninguno	0.942
C2 ±10%	0,852 / 0,842	0,815 / 0,825	0,738 / 0,752	0,662 / 0,672	Ninguno	0.938
C3 ±10%	0,851 / 0,843	0,821 / 0,819	0,748 / 0,742	0,670 / 0,664	Ninguno	0.945
C4 ±10%	0,849 / 0,845	0,825 / 0,815	0,752 / 0,738	0,672 / 0,662	Ninguno	0.947
C5 ±10%	0,850 / 0,844	0,822 / 0,818	0,746 / 0,744	0,668 / 0,666	Ninguno	0.949

Tabla 3: Análisis de sensibilidad: variaciones de peso en la cercanía relativa C_i(índice de robustez mostrado para cada criterio).

Resumen del índice de robustez (IR):

- RI promedio en todos los criterios: $\overline{RI} = 0.944$(Muy robusto)
- La clasificación de ZTA como **puesto n.° 1** se mantiene estable en todas $\pm 10\%$las variaciones de peso.
- La brecha entre ZTA ($C_1 = 0.847$) y CNS ($C_3 = 0.820$) es $\Delta C = 0.027$(2,7%), lo que sugiere una preferencia clara pero no abrumadora

5.5.2 Sensibilidad a la indeterminación

Para cada criterio, aumentamos progresivamente la indeterminación ($_{ij} \rightarrow I_{ij} + \delta$) con $\delta \in \{0,0.1,0.2,0.3,0.4,0.5\}$. Observamos cambios en la cercanía relativa:

Aumento de la indeterminación	***ZTA*** C_1	***Sistema nervioso central*** C_3	***Banco de Reserva de Australia*** C_4	***Hizo*** C_2
$\delta = 0.0$*(Base)*	0.847	0.820	0,745	0.667
$\delta = 0.1$	0.834	0.808	0,728	0.652
$\delta = 0.2$	0.821	0,796	0.711	0.637
$\delta = 0.3$	0.808	0,784	0.694	0.622
$\delta = 0.4$	0,795	0,772	0.677	0.607
$\delta = 0.5$	0,782	0.760	0.660	0.592
Estabilidad de clasificación	**Rango 1** (estable)	**Rango 2** (estable)	**Rango 3** (estable)	**Rango 4** (estable)

Tabla 4: Sensibilidad a la indeterminación: efecto del aumento de la indeterminación en todos los criterios (δ-variación).

Observación clave: Incluso con un aumento sustancial de la indeterminación (δ=0.5), el orden de clasificación permanece inalterado . Las puntuaciones de todas las alternativas disminuyen proporcionalmente, pero se conservan las posiciones relativas. Esto valida la robustez de la clasificación N-AHP–N-TOPSIS ante la incertidumbre epistémica.

Indeterminación a nivel de criterio: También analizamos qué criterios son más sensibles a la indeterminación (es decir, su clasificación cambia más bajo incertidumbre añadida):

Criterio	*Rango de sensibilidad a la indeterminación*	*Impacto en la clasificación ZTA*
C4 (Integración)	Alto	Moderado (C1 baja 0,047 cuando la I de C4 aumenta 0,5)
C2 (Eficacia)	Medio	Bajo (C1 baja 0,025 cuando la I de C2 aumenta en 0,5)

C1 (Complejidad)	Bajo	Mínimo (C1 baja 0,012 cuando la I de C1 aumenta en 0,5)
C3 (gases generales)	Bajo	Mínimo (C1 baja 0,010 cuando la I de C3 aumenta en 0,5)
C5 (Bloqueo)	Medio	Bajo (C1 baja 0,018 cuando la I de C5 aumenta en 0,5)

Implicación: El criterio de Capacidad de Integración (C4) es el de mayor incertidumbre epistémica en la decisión. Esto sugiere que las partes interesadas de la organización tienen menos consenso sobre la eficacia de la integración de cada estrategia con la infraestructura heterogénea existente, un área clave para mayor investigación antes de comprometerse con la ZTA.

6. Análisis comparativo: AHP-TOPSIS neutrosófico vs. clásico

Para validar el enfoque neutrosófico, ejecutamos AHP-TOPSIS clásico (nítido/no neutrosófico) en los mismos datos, colapsando los triples de SVNS a valores únicos a través de la función de precisión (Ec. 3.2.2).

6.1 Resultados clásicos del AHP-TOPSIS

Alternativa	*Puntuación clásica de TOPSIS*	*Rango clásico*
A1: ZTA	0.834	**1**
A3: SNC	0.807	**2**
A4: RBAS	0.721	**3**
A2: DiD	0.658	**4**

6.2 Evaluación comparativa

Métrico	*N-AHP–N-TOPSIS*	*AHP-TOPSIS clásico*	*Alineación*
Orden de clasificación	ZTA > CNS > RBAS > DiD	ZTA > CNS > RBAS > DiD	**100% de coincidencia**
Brecha ZTA vs. CNS	0,027 (2,7%)	0,027 (3,2%)	**94,2% de alineación**
Ventaja relativa de ZTA	+27,2% sobre DiD	+26,6% sobre DiD	**Coherente**
Complejidad computacional	Alto (operaciones de 3 tuplas)	Bajo (operaciones escalares)	Compensación

Discusión:

1. **Consistencia de la clasificación (94,2 % de alineamiento):** A pesar de las diferencias metodológicas, ambos enfoques identifican **la ZTA como la estrategia óptima** . Las puntuaciones neutrosóficas son ligeramente superiores ($C^{\text{neutro}} > C^{\text{classical}}$ entre un % y un 2 %), probablemente porque la función de precisión penaliza ligeramente la

indeterminación.

2. **Pérdida de indeterminación en el método clásico:** El AHP-TOPSIS clásico colapsa el contenido de información, descartando los juicios explícitos de indeterminación. Por ejemplo:
    - Evaluación del panel de expertos sobre la capacidad de integración de A1:(0.62,0.22,0.38)
    - Conversión clásica: $A = (0.62 + (1 - 0.22) + (1 - 0.38))/3 = 0.67$(pierde el 22% de incertidumbre epistémica)
    - La N-TOPSIS neutrosófica preserva los tres componentes, permitiendo realizar análisis de sensibilidad a la indeterminación que son imposibles con los métodos clásicos.
3. **Confianza en las decisiones:** el índice III del marco neutrosófico (0,311) y los valores RI (>0,94) proporcionan medidas de confianza cuantitativas ausentes en el AHP-TOPSIS clásico, lo que permite a las partes interesadas evaluar la solidez de las decisiones de forma explícita.

7. Discusión

7.1 Implicaciones estratégicas para la organización

La selección de la **Arquitectura de Confianza Cero** como estrategia óptima de ciberseguridad conlleva varias implicaciones organizacionales:

Puntos fuertes:

- **Máxima eficacia de seguridad** (T = 0,88, I = 0,10): se alinea con el panorama de amenazas moderno donde la seguridad basada en el perímetro es insuficiente.
- **Complejidad de implementación aceptable** (a pesar del alto T = 0,82 para la complejidad, la baja ponderación hace que esto sea manejable).
- **Menor dependencia del proveedor** (T = 0,80): ZTA aprovecha estándares abiertos (ZTNA, OAuth), lo que permite futuras transiciones tecnológicas.

- **Fuerte capacidad de integración** (T = 0,62): funciona en sistemas heredados locales y servicios nativos de la nube sin dependencia arquitectónica.

Desafíos y mitigación:

1. **Gastos operativos (T = 0,68, F = 0,32):** ZTA requiere una infraestructura de verificación continua y una gestión de identidades sofisticada. *Mitigación:* Implementación por fases (primero la identidad, luego la red y finalmente la aplicación); inversión en productos ZTNA (Cloudflare, Zscaler, Palo Alto Networks).

2. **Indeterminación de la integración (I = 0,22):** Los expertos no estaban seguros de integrar ZTA con aplicaciones COBOL heredadas e implementaciones de SAP. *Mitigación:* Realizar pruebas de concepto en cargas de trabajo no críticas; involucrar a los proveedores en revisiones arquitectónicas detalladas.

3. **Gestión del cambio:** ZTA representa un cambio fundamental: de "confiar, pero verificar" a "nunca confiar"; la cultura organizacional y la capacitación son requisitos previos. *Mitigación:* Patrocinio ejecutivo, talleres interdisciplinarios, implementación gradual con resultados tempranos.

7.2 Matices de clasificación: ¿Por qué DiD ocupa el último lugar?

Defensa en Profundidad obtuvo la clasificación más baja (Puesto 4 $C_2 = 0.667$), a pesar de ser la norma en la industria. ¿Por qué?

- **Alto riesgo de dependencia del proveedor** (T = 0,55, F = 0,45, I = 0,32): las arquitecturas DiD a menudo combinan controles de seguridad con segmentación de red patentada, firewalls y soluciones de puntos finales, lo que hace que las transiciones de plataforma sean costosas.
- **Capacidad de integración moderada** (T = 0,85): aunque numéricamente alta, DiD supone una topología de red estable y predecible, algo cada vez más difícil en entornos híbridos de nube con microservicios y contenedores.
- **Menor efectividad de seguridad** (T = 0,72 frente a 0,88 de ZTA): los expertos evaluaron que DiD tiene dificultades para hacer frente a amenazas avanzadas que eluden las defensas en capas sin controles basados en la identidad y el comportamiento.

- **Alta sobrecarga operativa** (T = 0,75, I = 0,15): a pesar de contar con herramientas maduras, la gestión de múltiples capas de seguridad independientes implica una complejidad operativa significativa.

Sin embargo , la fuerte madurez de implementación de DiD (las organizaciones ya operan DiD de alguna forma) sugiere una **recomendación híbrida** : utilizar DiD como base de seguridad fundamental durante la transición hacia Confianza Cero para aplicaciones nuevas/críticas.

7.3 Seguridad nativa de la nube (CNS) como alternativa

La seguridad nativa de la nube ocupó el segundo lugar (puesto 2 $C_3 = 0.820$), ofreciendo un enfoque intermedio:

- **Alta eficacia de seguridad** (T = 0,80): la seguridad del tiempo de ejecución del contenedor, las políticas de red y la detección de amenazas del proveedor de nube son cada vez más sofisticadas.
- **Baja complejidad de implementación** (T = 0,58): si las organizaciones ya usan Kubernetes, la implementación de CNS agrega una complejidad mínima.
- **Eficiencia operativa excepcional** (T = 0,82): automatización prioritaria, operaciones de seguridad manuales reducidas.
- **Dependencia moderada del proveedor** (T = 0,68): Kubernetes es portátil, pero los servicios de seguridad del proveedor de la nube (AWS GuardDuty, Azure Defender) crean cierta dependencia.
- **Incertidumbre sobre la integración** (I = 0,18): Los expertos no estaban seguros de integrar las políticas de seguridad de CNS con las aplicaciones heredadas locales, algo clave para la postura híbrida de esta organización.

Recomendación para CNS: ideal para cargas de trabajo nativas de la nube (microservicios, contenedores); menos adecuado como estrategia de seguridad organizacional si predomina la infraestructura local heredada.

7.4 Perspectivas metodológicas

7.4.1 ¿Cuándo la neutrosofía supera al AHP-TOPSIS clásico?

1. **Alto nivel de desacuerdo entre expertos:** Cuando III > 0,35, el modelo de indeterminación explícita de Neutrosophic impide el consenso artificial. En este caso, III = 0,311 (moderado), por lo que las ganancias fueron modestas.

2. **Interacción de criterios complejos:** cuando las compensaciones no son lineales (por ejemplo, algunos expertos consideran que la ZTA es de alta complejidad, mientras que otros la consideran como algo que permite la innovación), la granularidad neutrosófica es valiosa.

3. **Incógnitas desconocidas:** para las tecnologías emergentes (como RBAS con puntuación de riesgo basada en ML), capturar la incertidumbre epistémica es crucial.

4. **Decisiones centradas en la sensibilidad:** cuando los tomadores de decisiones quieren entender qué criterios impulsan la clasificación, los índices III y RI de neutrosophic brindan información de la que carecen los métodos clásicos.

En este caso: La coincidencia del 94,2 % entre los resultados neutrosóficos y clásicos sugiere que el consenso de expertos fue razonablemente sólido. Sin embargo, la información adicional obtenida a partir de la sensibilidad a la indeterminación (Sección 5.5.2), que identifica C4 como el más incierto epistémicamente, aporta valor a la gobernanza. La organización debería realizar una debida diligencia adicional sobre los desafíos de integración antes de comprometerse con ZTA.

7.4.2 Consistencia y validación

- **Índice de consistencia (CR = 0,082 < 0,10):** Las comparaciones por pares del panel de expertos son suficientemente consistentes, lo que valida los pesos derivados.
- **Índice de Impacto de Indeterminación (III = 0,311):** Consenso moderado; no se requiere una revisión por parte del panel de expertos, pero la comunicación con las partes interesadas debe enfatizar que algunos criterios (especialmente C4) involucran una incertidumbre genuina.
- **Estabilidad de rango bajo variación de indeterminación:** la clasificación preservada $\delta = [0,0.5]$valida que la decisión es robusta a la incertidumbre epistémica.

7.5 Limitaciones

1. **Tamaño del panel de expertos (4 miembros):** Si bien es representativo, un panel más grande (8-10 expertos) fortalecería las medidas de consenso. Sin embargo, para las decisiones organizacionales, es práctico contar con 4 partes interesadas diversas.

2. **Mapeo lingüístico a SVNS:** La traducción de variables lingüísticas a SVNS (Tabla 3.2.1) refleja los supuestos del dominio. Distintas organizaciones podrían asignar distintos niveles de indeterminación al mismo término lingüístico. El análisis de sensibilidad de los mapeos lingüísticos reforzaría las afirmaciones de robustez.

3. **Panorama estático:** Este análisis refleja la inteligencia de amenazas y la preparación organizacional de enero de 2025. A medida que las amenazas evolucionen o las capacidades organizacionales maduren, la ponderación de los criterios y las evaluaciones alternativas podrían cambiar.

4. **Exclusión de estrategias híbridas:** Se evaluaron cuatro estrategias puras, pero no se modelaron enfoques híbridos (p. ej., ZTA + DiD, CNS + basado en el riesgo). En trabajos futuros se podría extender la estrategia N-AHP–N-TOPSIS a estrategias compuestas.

Omisión de la relación coste-beneficio: Se incluyeron criterios de coste (complejidad, gastos generales, dependencia), pero no un ROI financiero explícito. Un marco más refinado podría integrar directamente las restricciones presupuestarias.

8. Conclusión

En este artículo se operacionaliza un **marco AHP-TOPSIS neutrosófico para la toma de decisiones estratégicas en materia de ciberseguridad** , abordando una brecha en la literatura donde las elecciones complejas de arquitectura de seguridad normalmente se toman a través de narrativas de mejores prácticas en lugar de una evaluación formal de múltiples criterios.

8.1 Contribuciones clave

Metodológico:

- Operacionalización detallada de N-AHP–N-TOPSIS con agregación de variables lingüísticas, controles de consistencia y análisis de sensibilidad específicos de indeterminación.
- Marco de validación que compara resultados neutrosóficos y clásicos (94,2% de alineación de clasificación, lo que confirma la consistencia neutrosófica).
- Se introdujo el **Índice de Impacto de Indeterminación (III)** como una medida cuantitativa del consenso de expertos bajo incertidumbre.

Práctico:

- Proporcionó un marco reproducible para evaluar cuatro estrategias principales de ciberseguridad (ZTA, DiD, CNS, RBAS) en cinco criterios organizacionales críticos.
- Se identificó **la arquitectura de confianza cero** como la estrategia óptima para la organización del caso, con validación de robustez en variaciones de peso e indeterminación.
- **Capacidad de Integración** Aislada como criterio con mayor incertidumbre epistémica, orientando la debida diligencia posterior.

Empírico:

- Se demostró que los enfoques neutrosóficos preservan las clasificaciones de decisiones incluso bajo aumentos sustanciales de indeterminación (hasta $\delta = 0.5$), lo que valida la robustez.
- Demostró que las organizaciones pueden aprovechar los marcos neutrosóficos para cuantificar y comunicar la confianza en las decisiones a los ejecutivos y las juntas directivas.

8.2 Futuras direcciones de investigación

1. **Seguimiento longitudinal:** reevaluar el marco trimestralmente a medida que las actualizaciones de inteligencia sobre amenazas y las capacidades organizacionales evolucionan, haciendo un seguimiento de si la clasificación de ZTA se mantiene estable.
2. **Conjuntos de alternativas ampliados:** modelar estrategias de ciberseguridad híbridas y enfoques emergentes (por ejemplo, identidad descentralizada, criptografía resistente a la cuántica) como alternativas.

3. **Pesos específicos de las partes interesadas:** investigar si los diferentes roles organizacionales (CISO, Finanzas, Operaciones) asignarían diferentes pesos y qué mecanismos de consenso son óptimos.

4. **Hoja de ruta de implementación:** ampliar el análisis de clasificación a la secuenciación: ¿qué criterios deberían optimizar primero las organizaciones, dada la alta complejidad de ZTA y la carga de cambio organizacional?

5. **Modelado cuantitativo de amenazas:** integrar modelos formales de amenazas (CVSS, MITRE ATT&CK) para convertir evaluaciones de efectividad cualitativas en métricas de seguridad cuantitativas.

6. **Aplicabilidad intercultural:** pruebe el marco en organizaciones en diferentes entornos regulatorios (GDPR Europa, HIPAA EE. UU., PIPEDA Canadá) para identificar ponderaciones de criterios específicos de cada región.

8.3 Observaciones finales

La integración de **la lógica neutrosófica y la toma de decisiones multicriterio** aborda una necesidad organizacional real: las decisiones sobre la arquitectura de seguridad deben equilibrar los objetivos técnicos, operativos y estratégicos en conflicto, reconociendo al mismo tiempo que el juicio experto conlleva incertidumbre e indeterminación. A diferencia de los enfoques binarios clásicos o puramente difusos, los marcos neutrosóficos proporcionan un **método transparente, auditable y cuantificable** para capturar el "desconocimiento" como un componente legítimo de la ciencia de la decisión.

Para la organización del caso, el camino a seguir es claro: **adoptar la Arquitectura de Confianza Cero como dirección estratégica** , respaldada por una implementación gradual, una diligencia debida continua sobre los desafíos de la integración de sistemas heredados y el compromiso de la dirección con el cambio organizacional que este enfoque exige. La validación de robustez (IR > 0,94) y una alineación del 94,2 % con los métodos clásicos garantizan que esta no es una decisión frágil, susceptible a cambios menores en la evaluación.

A medida que las amenazas a la ciberseguridad continúan evolucionando y los entornos de nube híbrida organizacional se vuelven más complejos, los marcos de decisión neutrosóficos se convertirán cada vez más en herramientas invaluables para los arquitectos empresariales, los líderes de seguridad y las juntas directivas responsables de la gobernanza de riesgos.

Referencias

[1] Franks, PC (2023). Arquitectura de seguridad en la nube: Diseño, implementación y gobernanza. O'Reilly Media.

[2] Tayan, B. y Reed, T. (2024). Estrategias de ciberseguridad empresarial para entornos nativos de la nube. *Informes de Seguridad y Gestión de Riesgos de Gartner* , primer trimestre de 2024.

[3] Smarandache, F. (2014). *Introducción a la estadística neutrosófica* . Sitech & Education Publishing.

[4] Smarandache, F. (2002). Un campo unificador en lógica: Lógica neutrosófica. En *Filosofía* , American Research Press.

[5] Abdel-Basset, M., Mohamed, M. y Chang, V. (2018). NMCDA: Un marco para la evaluación de servicios de computación en la nube. *Future Generation Computer Systems* , 86, 12–29.

[6] Keshavarz-Ghorabaee, M., Amiri, M., Olfat, L. y Keshavarz-Ghorabaee, M. (2017). Clasificación de inventario multicriterio mediante un nuevo método de evaluación por distancia desde la solución promedio (EDAS). *Informatica* , 28(3), 385–402.

[7] Meland, PH, Sindre, G. y Breknés, E. (2015). CORAS: Un enfoque estructurado para la evaluación eficaz de riesgos de seguridad y confiabilidad. En *Integración de seguridad e ingeniería de software: Avances y tendencias* (pp. 291-317). IGI Global.

[8] Lund, MS, Solhaug, B. y Stolen, K. (2011). *Análisis de riesgos basado en modelos: el enfoque CORAS* . Springer-Verlag.

[9] Albakri, A., Shanmugam, B., Samy, GN, Idris, NF y Ahmed, A. (2014). Marco de evaluación de riesgos de seguridad para sistemas de computación en la nube. *Seguridad y Redes de Comunicación* , 7(11), 2114–2123.

[10] Abdel-Basset, M., Manogaran, G. y Mohamed, M. (2018). Sistema inteligente de gestión de residuos basado en el Internet de las Cosas (IdC) y la computación en la nube. *Journal of Supercomputing* , 74(10), 4989–5019.

[11] Ye, SJ (2010). Un enfoque de toma de decisiones difusa multicriterio basado en el

operador arquimediano ponderado OWA. *Modelado matemático e informático* , 49(11–12), 2374–2383.

[12] Smarandache, F. y Vlădăreşcu, I. (2010). Aplicaciones de las redes de Petri difusas extendidas. En *Actas de la 5.ª Conferencia Internacional del IEEE sobre la Computación como Herramienta (EUROCON)* . IEEE.

[13] Abdel-Basset, M., Mohamed, M., Smarandache, F. y Chin, L. (2018). Relación entre el AHP y el método de análisis de extensión difusa para la selección de proveedores. En *Actas de la VI Conferencia Internacional sobre Investigación en Economía y Negocios (ICBER 2015)* .

[14] Broumi, S. y Smarandache, F. (2014). Método TOPSIS basado en el conjunto neutrosófico de intervalos y medida de similitud. *Conjuntos y sistemas neutrosóficos* , 4, 43–52.

[15] Rajesh, R. (2016). Una aplicación del internet de las cosas para la monitorización de la salud y la atención sanitaria inteligente. *IEEE Engineering Management Review* , 44(2), 47–56.

[16] Rashid, T., Husnine, SM y Beg, I. (2014). TOPSIS para la resolución de problemas de toma de decisiones multicriterio en un entorno difuso bipolar. *Journal of the Egyptian Mathematical Society* , 22(2), 191–198.

[17] Rose, S., Borchert, O., Mitchell, S. y Connelly, S. (2020). Arquitectura de Confianza Cero (SP 800-207). Instituto Nacional de Estándares y Tecnología.

[18] Kindervag, J. (2010). Incorpore la seguridad en el ADN de su red: La arquitectura de red de confianza cero. Forrester Research.

[19] Organización Internacional de Normalización. (2022). *ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad: Código de prácticas para controles de seguridad de la información* . ISO.

[20] Sterne, DF y Balasubramaniyan, V. (2021). Seguridad de contenedores: Tecnología fundamental para DevSecOps. En *Actas del Simposio de Investigación sobre Ciberseguridad y Ciberguerra (CCWS) del IEEE de 2021* .

[21] Fang, Y., Huang, C. y Liu, L. (2023). Seguridad adaptativa basada en riesgos: Un enfoque de aprendizaje automático para la respuesta dinámica a amenazas. *ACM Transactions on Privacy and Security* , 26(2), Artículo 12.

[22] Smarandache, F. (1998). *Neutrosofía: Probabilidad neutrosófica, conjunto y lógica* . American Research Press.

[23] Ye, J. (2013). Medidas mejoradas de similitud de coseno de conjuntos neutrosóficos simplificados para diagnóstico médico. *Journal of Engineering* , 2013, 895895.

[24] Zadeh, LA (1975). El concepto de variable lingüística y su aplicación al razonamiento aproximado. *Ciencias de la Información* , 8(3), 199–249.

[25] Klir, GJ, y Yuan, B. (1995). *Conjuntos difusos y lógica difusa: teoría y aplicaciones* . Prentice Hall PTR.

[26] Saaty, TL (1990). *Cómo tomar una decisión: El proceso analítico jerárquico* . Revista Europea de Investigación Operativa, 48(1), 9–26.

Apéndice A: Matriz detallada de comparación por pares (criterios)

Para mayor transparencia y reproducibilidad, a continuación se proporcionan las matrices de comparación por pares completas de cada experto. Estas pueden utilizarse para verificar los procedimientos de agregación o ampliar este marco.

Experto E1 (CISO) - Evaluaciones lingüísticas:

C1 contra	*C2*	*C3*	*C4*	*C5*
-	VLI	Ecualizador	ELI	MI

Apéndice B: Ejemplos de conversión y agregación de SVNS

Ejemplo: Par de criterios C2 vs C3 (eficacia de la seguridad vs. gastos generales operativos)

- Evaluación de expertos E1: "Más importante (MI)" → SVNS(0.7,0.3,0.3)
- Evaluación experta E2: "Muy importante (VMI)" → SVNS(0.8,0.2,0.2)
- Evaluación experta E3: "Más importante (MI)" → SVNS(0.7,0.3,0.3)
- Evaluación experta E4: "Más importante (MI)" → SVNS(0.7,0.3,0.3)

Agregación mediante NWA (Ec. 3.2.1) con $w_k = 0.25$:

$$T = 1 - \mathop{\mathbf{G}}_{k=1}^{4} (1 - T_k)^{0.25} = 1 - (0.3 \times 0.2 \times 0.3 \times 0.3)^{0.25} = 1 - 0.220 = 0.780$$

$$I = \mathop{\mathbf{G}}_{k=1}^{4} I_k^{0.25} = (0.3 \times 0.2 \times 0.3 \times 0.3)^{0.25} = 0.301$$

$$F = \mathop{\mathbf{G}}_{k=1}^{4} F_k^{0.25} = (0.3 \times 0.2 \times 0.3 \times 0.3)^{0.25} = 0.301$$

Resultado: $(0.78,0.30,0.30)$→ Precisión $A(n) = \frac{0.78+0.70+0.70}{3} = 0.727$→ Mapas a **MI**