CULCYT. Cultura Científica y Tecnológica
Vol. 23 | N.º 1 | Edición Especial "Estrategia de Gestión para la Transición hacia una Economía Circular" | Enero-Abril 2026 | PP E119-E131

ISSN (electrónico) 2007-0411

DOI: 10.20983/culcyt.2026.1.2e.11

e23113

ARTÍCULO DE INVESTIGACIÓN

Factores críticos de desempeño y seguridad en SI mediante TOPSIS: determinantes para la sustentabilidad empresarial

Critical Performance and Security Factors in SI using TOPSIS: Determinants of Business Sustainability

Monserrat Reséndiz Leos[1a], *Patricia Parroquin-Amaya*[1ab] ✉ iD, *Iván Juan Carlos Pérez-Olguín*[2] iD, *Karla Miroslava Olmos-Sánchez*[1ac] iD

[1] {[a] Programa de Ingeniería en Sistemas Computacionales}, {[b] Maestría en Tecnología}, {[c] Maestría en Ciberseguridad}, Departamento de Ingeniería Eléctrica y Computación, Instituto de Ingeniería y Tecnología, Universidad Autónoma de Ciudad Juárez; Ciudad Juárez, Chihuahua, México

[2] Programa de Ingeniería Industrial y de Sistemas, Doctorado en Tecnología, Departamento de Ingeniería Industrial y Manufactura, Instituto de Ingeniería y Tecnología, Universidad Autónoma de Ciudad Juárez; Ciudad Juárez, Chihuahua, México

RESUMEN

Este estudio tuvo como objetivo identificar y jerarquizar los factores críticos que inciden en el desempeño y seguridad de los Sistemas de Información (SI) para apoyar la toma de decisiones estratégicas y fortalecer la sustentabilidad empresarial. La investigación se desarrolló bajo un diseño transversal con enfoque mixto, integrando la revisión sistemática de literatura mediante la metodología PRISMA y un análisis cuantitativo para construir y validar un instrumento de evaluación. Se identificaron 68 factores críticos y, tras la validación de contenido, se retuvieron 56. Estos fueron jerarquizados mediante el método multicriterio TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) [1]-[3]. Los hallazgos muestran que la transformación digital y la gobernanza de los SI son determinantes clave de la resiliencia y la sustentabilidad organizacional [4]-[5], ya que impulsan la eficiencia, la transparencia y la toma de decisiones basada en datos [6]-[7]. La originalidad del estudio radica en la integración de PRISMA y TOPSIS para priorizar factores estratégicos de desempeño y seguridad en SI. En conclusión, los resultados contribuyen al diseño de un modelo de toma de decisiones multicriterio que apoye le evaluación de inversiones, políticas de seguridad y monitoreo de SI, reforzando la sustentabilidad organizacional [8].

PALABRAS CLAVE: desempeño y seguridad de SI; TOPSIS; PRISMA; sustentabilidad.

ABSTRACT

This study aimed to identify and rank the critical factors that affect the performance and security of Information Systems (IS) to support strategic decision-making and strengthen business sustainability. The research was conducted using a cross-sectional design with a mixed approach, integrating a systematic literature review using the PRISMA methodology and a quantitative analysis to construct and validate an assessment tool. Sixty-eight critical factors were identified, and after content validation, 56 were retained. These were ranked using the TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) multicriteria method [1]–[3]. The findings show that digital transformation and IS governance are key determinants of organizational resilience and sustainability [4]-[5], as they drive efficiency, transparency, and data-driven decision-making [6]-[7]. The originality of the study lies in the integration of PRISMA and TOPSIS to prioritize strategic performance and security factors in IS. In conclusion, the results contribute to the design of a multi-criteria decision-making model that supports the evaluation of investments, security policies, and IS monitoring, reinforcing organizational sustainability [8].

KEYWORDS: IS performance and security; TOPSIS; PRISMA, sustainability.

Correspondencia:
DESTINATARIO: Patricia Parroquin-Amaya
INSTITUCIÓN: Universidad Autónoma de Ciudad Juárez / Instituto de Ingeniería y Tecnología
DIRECCIÓN: Ave. del Charro núm. 450 norte, C. P. 32320, Ciudad Juárez, Chih., México
CORREO ELECTRÓNICO: pparroqu@uacj.mx

Fecha de recepción: 28 de octubre de 2025. Fecha de aceptación: 19 de marzo de 2026. Fecha de publicación: 30 de abril de 2026.

acceso abierto UACJ

REVISTA ARBITRADA

I. INTRODUCCIÓN

La era digital y cognitiva se refiere a la creación de cantidades muy significativas de datos que deben estructurarse, analizarse y presentarse con precisión para obtener beneficios a partir de la información y conocimiento derivado de los mismos [9]. Esta era ha llevado a diversas organizaciones a incorporar o mejorar sus Sistemas de Información (SI), así como su infraestructura tecnológica, para gestionar de manera eficiente sus procesos.

Una gestión adecuada de los SI permite una administración más eficiente de recursos con el fin de mejorar la calidad de sus procesos y hacer un uso más eficaz de los recursos financieros [6]-[7]. La incorporación de los SI en las organizaciones abre una serie de oportunidades, sin embargo, también es necesario garantizar el rendimiento y proteger la información contenida en estos sistemas. En México, la mayoría de las organizaciones siguen normativas y estándares para garantizar el rendimiento y la seguridad de los SI. A continuación se describen algunos de estos estándares y su contextualización en México:

- ISO/IEC 27001: Gestión de la seguridad de la información [10]. Este es un estándar ampliamente utilizado por instituciones financieras, organismos gubernamentales y proveedores de servicios de Tecnologías de Información (TI) para gestionar y proteger la información confidencial. Aunque no es obligatoria, esta certificación suele ser exigida en las licitaciones públicas y por los clientes internacionales, ademas es compatible con la ley de protección de datos de México lo que la hace relevante en un marco normativo nacional.

- NIST SP 800: Marcos de ciberseguridad [11]. Este marco se utiliza como referencia de buenas prácticas y, aunque no es una política oficial de México, las directrices del NIST (como la SP 800-53) se integran a menudo en las políticas de seguridad interna y las estrategias de gestión de riesgos.

- PCI DSS: Norma de seguridad de datos de la industria de tarjetas de pago [12]. En México, la norma PCI DSS es obligatoria para empresas que manejan datos de tarjetas de crédito o débito, incluidas las empresas minoristas, *fintech* y de comercio electrónico. Es exigida por los bancos y los procesadores de pagos; su cumplimiento evita sanciones y garantiza la confianza en las transacciones en línea.

- RGPD: Reglamento General de Protección de Datos [13]. A pesar de que el RGPD no aplica en México, complementa la legislación local y las empresas adoptan en sus prácticas el RGPD para garantizar el cumplimiento internacional.

- HIPAA: Ley de privacidad de los datos sanitarios de EE.UU. [14]. Aunque no es obligatoria en México, se espera su cumplimiento cuando se trata de servicios sanitarios transfronterizos, especialmente en telemedicina o externalización médica.

Aunque el cumplimiento de las normas de seguridad y calidad es un componente fundamental de la gobernanza de los SI, las organizaciones comprometidas con la mejora continua deberían ir más allá de los marcos de cumplimiento estáticos. En este contexto, la adopción de un modelo que permita el seguimiento y la medición continuos, tanto del rendimiento como de la seguridad de la información, se vuelve esencial.

En concreto, mantenerse dentro de un ciclo de mejora continua, como el modelo Planificar-Hacer-Verificar-Actuar, requiere mecanismos dinámicos que garanticen la adaptabilidad y la resiliencia. El modelo PDCA, que es un método de gestión iterativo creado por Walter Shewhart y modificado por Edward Deming, se utiliza para lograr la mejora continua mediante la planificación sistemática de acciones, su implementación, la verificación de los resultados y la realización de ajustes necesarios [10].

Desde la perspectiva de los profesionales de la seguridad de la información, este enfoque es crucial porque permite a las organizaciones responder de manera proactiva a las amenazas emergentes, evaluar la eficacia de los controles implementados y mantener la alineación con los objetivos estratégicos en un entorno digital en constante evolución [3].

Para cumplir los objetivos de la fase de verificación del modelo PDCA [7], es esencial implementar un modelo de evaluación desarrollado desde la perspectiva de expertos en la materia, con el fin de evaluar los factores críticos que influyen en la gestión eficaz de los sistemas de información. Un modelo de apoyo a la toma de decisiones en la gestión de los SI constituye una herramienta estratégica para las organizaciones, ya que facilita la supervisión continua del rendimiento de los sistemas, permite identificar las áreas críticas de mejora y respalda la toma de

decisiones fundamentales en evidencia. En un entorno tecnológico dinámico y altamente competitivo, disponer de un modelo de evaluación robusto no solo contribuye a optimizar la gestión de los SI, sino que también fortalece la resiliencia organizacional y la alineación con los objetivos de sustentabilidad empresariales [4].

Este estudio contribuye a la construcción del modelo de toma de decisiones, identificando los criterios clave en el desempeño y seguridad de los sistemas de información y, asimismo, se identifican los factores críticos que intervienen para la evaluación y mejora de los SI, presentando una jerarquía de los mismos realizada mediante el Método de Toma de Decisiones Multicriterio (MCDM, por sus siglas en inglés) TOPSIS. En la siguiente sección de metodología se describen de manera detallada los pasos que se llevaron a cabo para identificar y jerarquizar los factores críticos para el desempeño y seguridad de los SI.

II. METODOLOGÍA

El estudio se llevó a cabo a través de tres fases que se describen a continuación:

Análisis sistémico. La metodología empleada fue un enfoque sistémico suave, basado en el conocimiento y diseñado para proporcionar una perspectiva completa y estructurada del dominio denominado Estrategia de Gestión del Conocimiento con Análisis de Sistemas Suaves (KMoS-SSA). Este enfoque incorporó la construcción de un léxico del lenguaje empleado, el desarrollo de un modelo conceptual global, un modelo sistémico y la aplicación del marco CATWOE.

Revisión sistémica de literatura. Se usó la metodología PRISMA para la revisión de la literatura que llevó a identificar los factores críticos de los SI y las áreas clave que fueron consideradas como criterios de selección en el método TOPSIS.

MCDM. Se utilizó el método TOPSIS para jerarquizar los factores críticos para la mejora del desempeño y seguridad de los SI identificados, considerando los criterios de selección.

A. ESTRATEGIA METODOLÓGICA KMoS-SSA

KMoS-SSA [5], [9] está diseñada para abordar problemas complejos en contextos en los que no existe una solución única y clara. Este enfoque da prioridad a la comprensión de las percepciones y necesidades de las partes involucradas mediante el uso de modelos conceptuales flexibles para explorar diversas perspectivas y formular soluciones social y políticamente viables. Su proceso incluye la identificación del problema, el análisis de múltiples puntos de vista, el desarrollo de un modelo conceptual holístico, la exploración de posibles soluciones y la selección, por consenso entre los actores del dominio, de la opción más aceptable y viable. KMoS-SSA se basa en los tres principios clave de la metodología de sistemas blandos:

1. Rechazar la noción de que los sistemas del mundo real solo necesitan ser reparados y, en su lugar, aceptar la complejidad y el dinamismo del entorno.

2. Reconocer y construir múltiples modelos de actividad sistémica desde diferentes puntos de vista, lo que favorece la resolución de problemas complejos y mejora la toma de decisiones estratégicas.

3. Enmarcar los problemas complejos como situaciones que requieren modelos conceptuales para mejorar la comprensión y fomentar el aprendizaje, en lugar de reducir los componentes del mundo real a partes excesivamente simplificadas. La selección de soluciones adecuadas tiene en cuenta no solo las perspectivas actuales, sino también la historia, la cultura y las aspiraciones de las partes interesadas.

KMoS-SSA [9] proporciona métodos e instrumentos para modelar comportamientos dinámicos, fomentar la reflexión crítica y apoyar las decisiones estratégicas.

B. METODOLOGÍA PRISMA

La revisión bibliográfica se llevó a cabo utilizando la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [15], un marco metodológico diseñado para mejorar la transparencia y la calidad de las revisiones sistemáticas y los meta-análisis. Esta metodología proporciona un enfoque estructurado para identificar, seleccionar, evaluar y sintetizar las pruebas de investigación. A continuación, se describe la aplicación de la metodología:

1. Definición de la pregunta de investigación. En este estudio se formularon dos preguntas de investigación (RQ) basadas en las necesidades del tema

elegido, que guiaron la investigación hacia la búsqueda de respuestas.

- RQ1: ¿cómo contribuyen el rendimiento y la seguridad de los sistemas de información a la mejora de los proyectos de TI?
- RQ2: ¿cuáles son los factores críticos del rendimiento y la seguridad de los sistemas de información que contribuyen positivamente a la productividad de los proyectos de TI?

2. Desarrollo del protocolo. En este paso se definieron el objetivo y los criterios de inclusión y exclusión.

   - Objetivo: identificar los factores críticos de éxito relacionados con el rendimiento y la seguridad de los sistemas de información (SI).

   - Términos de inclusión: "Factores críticos de éxito en el rendimiento y la seguridad de los SI", "seguridad de los SI", "evaluación del rendimiento de los SI", "rendimiento y seguridad de los SI en las organizaciones".

   - Criterios de inclusión:

     – Criterio 1: artículos publicados en la última década que contengan los términos de inclusión.
     – Criterio 2: artículos que incluyan los términos de inclusión especificados.
     – Criterio 3: estudios que cumplen el criterio 2 y son resultado de una investigación empírica.
     – Criterio 4: estudios que cumplen el criterio 2 y son resultado de una revisión bibliográfica sistemática.

3. Búsqueda bibliográfica sistemática. La búsqueda se llevó a cabo en las siguientes bases de datos: ScienceDirect, Google Scholar, ResearchGate e IEEE Xplore.

4. Selección de estudios. En este paso, los estudios identificados se seleccionan en dos etapas: en la primera etapa (4a) se revisan los títulos y los resúmenes, y en la segunda etapa (4b) se evalúa el texto completo según los criterios de inclusión y exclusión.

5. Extracción de datos. Se recopiló la información esencial de cada estudio seleccionado, centrándose en identificar los factores críticos de éxito relacionados con el rendimiento y la seguridad de los sistemas de información.

C. VALIDEZ DE CONTENIDO DEL INSTRUMENTO DE EVALUACIÓN

Se diseñó un instrumento de evaluación y la validez de contenido se hizo un juicio de expertos para analizar su opinión, los expertos analizaron cuáles de los 68 factores (ítems) identificados en la revisión de literatura, debieran considerarse por su impacto en el desempeño y seguridad de los SI. Con el fin de medir el grado de acuerdo entre los evaluadores, se calculó el coeficiente kappa de Fleiss.

Kappa de Fleiss [16]-[17] es usado para medir el nivel de acuerdo general entre múltiples evaluadores. Se define como:

$$\text{kappa } (\kappa) = \frac{Po - Pe}{1 - Pe} \tag{1}$$

donde Po es el acuerdo observado promedio y Pe es el acuerdo esperado. Po se calcula con la siguiente fórmula:

$$Po = \frac{1}{N}\sum_{i=1}^{N} Pi \tag{2}$$

donde Pi es la proporción de acuerdo observada para el elemento i, la cual se define como sigue:

$$P_i = \frac{1}{n(n-1)}\sum_{j=1}^{k} n_{ij}(n_{ij} - 1) \tag{3}$$

donde n es la cantidad total de sujetos o elementos evaluados, k es el número de categorías posibles, n_{ij} es el número de evaluadores que asignaron el sujeto i a la categoría j y Pe es el acuerdo esperado, el cual se calcula como sigue:

$$Pe = \sum_{j=1}^{k} p_j^2 \tag{4}$$

donde P_j se obtiene con la fórmula siguiente:

$$P_j = \frac{1}{N \cdot m}\sum_{i=1}^{N} n_{ij} \tag{5}$$

donde N son los números de ítems, m el número de jueces y n_{ij} representa el número de jueces que clasificaron el ítem i en la categoría j.

El nivel de concordancia obtenido [16] en las dos aplicaciones del instrumento para la evaluación de expertos fue aceptable y los coeficientes obtenidos y la categoría conseguida para cada caso se observan en la Tabla 1. Después de atender las observaciones de los expertos en la primera evaluación se actualizaron los ítems, quedando 56.

TABLA 1
NIVEL DE CONCORDANCIA OBTENIDO

NÚM.	ÍTEMS	KAPPA DE FLEISS	CONCORDANCIA
1	68	0.3846	Aceptable
2	56	0.4011	Aceptable

Para la priorización de los 56 ítems correspondientes a los factores críticos de desempeño y seguridad de los SI, se empleó el MCDM TOPSIS (Technique for Order Preference by Similarity to Ideal Solution). Este método permite comparar la distancia relativa de cada alternativa respecto a la solución ideal positiva y a la solución ideal negativa, lo que permite establecer un orden de preferencia entre las alternativas evaluadas [3]. En la siguiente sección se presentan los resultados derivados de la aplicación de este método, así como las prioridades obtenidas.

III. RESULTADOS

En esta sección se presentan los modelos derivados de la aplicación del marco metodológico KMoS- SSA, los factores críticos identificados y los resultados obtenidos de aplicar el método TOPSIS.

A. ANÁLISIS SISTÉMICO

Léxico Extendido del Lenguaje

El Léxico Extendido del Lenguaje (LEL) es una recopilación estructurada de términos clasificados en sujetos, objetos, verbos y estados que son contextualmente relevantes para un dominio de aplicación específico [18]. A diferencia de un glosario estándar, que proporciona definiciones simples, un LEL tiene como objetivo capturar los matices, los supuestos implícitos y los patrones de uso de los términos tal y como los entienden y comunican los expertos en la materia y las partes interesadas. En el contexto de ámbitos complejos, en los que prevalecen la ambigüedad, la incertidumbre y las perspectivas de múltiples partes interesadas, el LEL facilita el entendimiento común, favorece la alineación semántica y permite una comunicación más precisa entre disciplinas y fronteras culturales u organizativas. Además, mejora el proceso de modelización conceptual al aclarar significados y descubrir supuestos ocultos que pueden influir en la toma de decisiones, el diseño de sistemas o implementación de políticas. Se obtuvo un léxico comprendido de 4 sujetos, 25 objetos, 14 verbos y 13 estados.

Visión Enriquecida

Como parte del proceso de comprensión del dominio, se desarrolló el modelo de visión general basándose en la información extraída del léxico de lenguaje ampliado. Este modelo proporciona una representación sistémica de alto nivel de los componentes clave y las interacciones dentro del dominio, lo que facilita una visión holística de su estructura y dinámica. Al mapear visualmente las relaciones entre los actores, los objetos, las acciones y los estados, el modelo de visión general ayuda a identificar los elementos críticos y las áreas potenciales de mejora, como se ilustra en la Figura 1.

Modelo Sistémico

Un enfoque sistémico requiere no solo el análisis de un sistema de forma aislada, sino también sus relaciones con otros sistemas interconectados. En esta investigación se examinaron los enfoques de varias organizaciones internacionales para comprender perspectivas más amplias sobre los sistemas de información.

Las Tablas 2, 3, 4 y 5 presentan cómo diferentes organizaciones internacionales, como la OCDE, la UNESCO, el Banco Mundial y el Banco Interamericano de Desarrollo (BID) [19]-[20], abordan los sistemas de información desde diversas perspectivas, entre ellas la gobernanza de las TI, la innovación y el desarrollo, la formación y la educación, y la interoperabilidad y el acceso. Estos aspectos son esenciales para establecer normas para el intercambio de datos, la conectividad inclusiva y la integración tecnológica. Aunque cada organización adapta su enfoque a su contexto específico, todas comparten un objetivo común: mejorar la eficiencia de los procesos y garantizar el acceso a la información.

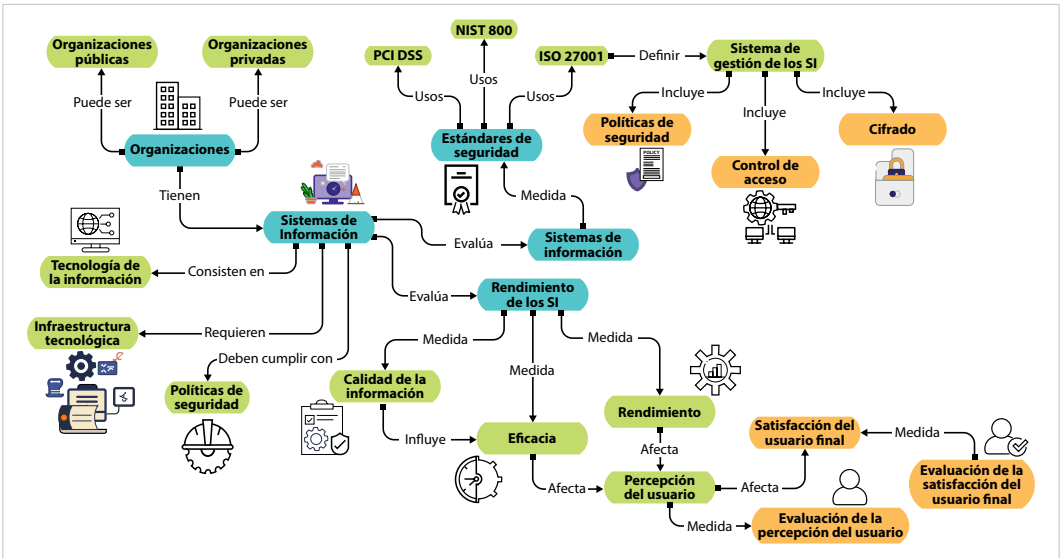

Figura 1. Modelo de representación sistémica.

TABLA 2
ÁMBITO DE GOBERNANZA DE TI

INSTITUCIÓN	PILARES DE LOS SI	PILARES DE LA SEGURIDAD
OCDE	• Eficiencia de los procesos y acceso a la información	• Cumplimiento y auditoría de la seguridad de la información • Auditoría de seguridad
UNESCO	• Promoción de datos abiertos • Datos y acceso equitativo	• Privacidad • Normas de personal • Protección de datos
Banco Mundial	• Transparencia y mejora de la infraestructura	• Gestión y marco regulatorio
IDB	• Integración de sistemas y digitalización	• Control

TABLA 3
ÁMBITO: INNOVACIÓN Y DESARROLLO

INSTITUCIÓN	PILARES DE LOS SI	PILARES DE LA SEGURIDAD
OCDE	• Eficiencia de los procesos y acceso a la información	• Monitorización continua y mitigación de vulnerabilidades
UNESCO	• Inclusión digital y educación en TIC	• Formación de seguridad • Mejores prácticas
Banco Mundial	• Tecnologías de la información • Infraestructura • Estrategias de innovación	• Evaluación de amenazas • Respuesta a incidentes
IDB	• Conocimiento y redes colaborativas	• Desarrollo de capacidades • Análisis de amenazas cibernéticas

TABLA 4
ÁMBITO: FORMACIÓN Y EDUCACIÓN

INSTITUCIÓN	PILARES DE LOS SI	PILARES DE LA SEGURIDAD
OCDE	• Formación y alfabetización digital • Programas de alfabetización	• Concientización sobre la seguridad
UNESCO	• Educación continua • Accesibilidad para todos	• Privacidad y protección • Normas de uso
Banco Mundial	• Habilidades: desarrollo y formación técnica	• Resiliencia ante ciberataques • Política de seguridad
IDB	• Formación en tecnologías de la información • Innovación educativa	• Evaluación de riesgos • Estrategias de recuperación

TABLA 5
ÁMBITO: INTEROPERABILIDAD Y ACCESO

INSTITUCIÓN	PILARES DE LOS SI	PILARES DE LA SEGURIDAD
OCDE	• Interoperabilidad y norma de intercambio de datos	• Seguridad de la transmisión de datos • Protección de redes
UNESCO	• Acceso e interoperabilidad entre instituciones	• Protección de datos sensibles • Cifrado de la información
Banco Mundial	• Conectividad y acceso inclusivo	• Control de acceso • Seguridad de la información
IDB	• Integración tecnológica • Cooperación regional	• Evaluación continua • Respuesta ante amenaza

CATWOE

CATWOE es una herramienta de diagnóstico dentro del Enfoque de Sistemas Suaves que apoya el análisis de situaciones problemáticas complejas mediante la identificación de seis elementos clave: Clientes (C), Actores (A), Proceso de transformación (T), Cosmovisión o *Weltanschauung* (W), Propietarios (O) y Restricciones ambientales.

El objetivo principal de CATWOE es estructurar diferentes perspectivas y permitir la formulación de modelos de actividad con un propósito definido en ámbitos socialmente complejos [21].

En esta investigación se aplicó el marco CATWOE para conceptualizar el desarrollo de un modelo de evaluación del rendimiento y la seguridad de los sistemas de información en las instituciones de educación superior. Los elementos se definieron de la siguiente manera:

- Cliente (C): área de Gestión de la Función de Ciberseguridad, como principal beneficiaria de las mejoras en las prácticas de evaluación.
- Actores (A): directores de Tecnologías de la Información, desarrolladores, usuarios finales y administradores de seguridad, que participan en la transformación o influyen en ella.
- Transformación (T): identificación de los factores prioritarios para evaluar la seguridad de los SI, basándose en las perspectivas de los expertos.
- Visión del mundo (W): esta transformación se justifica por su contribución a la mejora de la asignación de recursos financieros, los procesos de toma de decisiones y la satisfacción de los usuarios finales.
- Propietario (O): equipo de investigación
- Entorno (E): planes de desarrollo institucional, normas y políticas de seguridad, planes de calidad del software y modelos de toma de decisiones.

Tras el análisis CATWOE, se formula una definición raíz utilizando la estructura PQR, que articula lo que hará el sistema (P), cómo se hará (Q) y por qué es necesario (R). Esta estructura mejora la claridad y la coherencia en el modelado de la actividad intencionada. El PQR se definió de la siguiente manera:

- P (qué hacer): jerarquizar los factores críticos para la evaluación del rendimiento y la seguridad de los SI que sirvan para modelos de toma de decisiones.
- Q (cómo hacerlo): identificar los factores críticos desde la perspectiva de expertos mediante una revisión de la literatura y la evaluación de la opinión de expertos.
- R (por qué hacerlo): permitir a los directores de TI evaluar y mejorar el rendimiento y la seguridad de los sistemas de información, mejorar la experiencia del usuario, garantizar la protección de la información, reducir los costes operativos, validar las inversiones en TI y promover la innovación y la competitividad.

B. FACTORES EXTRAÍDOS DE LA REVISIÓN BIBLIOGRÁFICA

La Tabla 6 presenta la clasificación y codificación de los 68 factores críticos del rendimiento y la seguridad de los SI generados de la revisión de literatura.

La identificación y clasificación precisas de estos factores son esenciales para utilizarse en la toma de decisiones estratégicas y la mejora continua de los SI dentro de las organizaciones.

Cada factor se codificó utilizando un sistema de identificación que facilita su análisis y referencia. Los factores relacionados con el rendimiento de los SI se etiquetan con el prefijo IS, seguido de un número secuencial (por ejemplo, IS1, IS2, ...), mientras que los factores específicamente asociados a la seguridad se codifican con el prefijo SEC (por ejemplo, SEC1, SEC2, ...).

La Tabla 6 organiza la información de manera estructurada, incluyendo códigos de identificación, las variables correspondientes y sus respectivas referencias bibliográficas. Esta disposición no solo mejora la comprensión de la relación entre cada factor y su influencia en el rendimiento y la seguridad de los SI, sino que también facilita su aplicación en el proceso de toma de decisiones estratégicas.

TABLA 6
FACTORES EXTRAÍDOS

CÓDIGO	FACTOR	REFERENCIAS
IS1	Educación, formación y sensibilización	[22]-[27], [34]
IS2	Política, social y ética	[28]-[30]
IS3	Concientización y formación	[22], [24]-[25], [30]-[32], [34]
IS4	Ética en las comunicaciones	[22], [24], [27], [30]
IS5	Intercambio de información entre miembros	[22]-[26], [30], [32]
IS6	Normas y reglamentos gubernamentales	[23]-[24], [26]-[28], [31]-[32], [34]-[36]
IS7	Cumplimiento de las disposiciones reglamentarias	[22]-[23], [25]-[26], [28], [30]-[32], [34], [35]
IS8	Confianza	[25]-[27], [32], [35]-[36]
IS9	Satisfacción del usuario final	[27], [28]-[30], [31]-[32], [36]
IS10	Impacto individual de la seguridad	[23]-[24], [27]-[28], [30], [32],[35]
IS11	Impacto colectivo de la seguridad	[22], [24], [31]
IS12	Servicio eficiente y empático que atiende a las necesidades del usuario final	[23], [25], [28], [32], [35]
IS13	Política de seguridad definida	[24], [26]-[27], [30],[34]
IS14	Implementación de políticas de seguridad	[25],[28], [31]-[32],[34]
IS15	Implementación de planes de gestión del sistema	[25], [27]-[28], [32]
IS16	Aprobación y apoyo de la alta dirección a las políticas, procedimientos y controles	[24], [26], [30], [34]
IS17	Apoyo a la gestión de personas mayores	[22]-[23], [30]
IS18	Gestión de recursos organizacionales para la gestión de sistema	[22], [24] ,[27], [31]
IS19	Disponibilidad de recursos	[32], [35]
IS20	Recursos humanos	[22], [25]-[27], [35]
IS21	Garantizar los recursos financieros y tecnológicos	[23], [28]-[29], [31], [35]
IS22	Compromiso de financiación	[24], [26]
IS23	Estructura empresarial	[25], [27], [32], [35]
IS24	Gestión de proyectos	[22], [24], [26], [28], [32]
IS25	Desarrollar, mantener, documentar y mejorar el sistema	[23]-[25], [27]
IS26	Evaluación del sistema	[25], [28], [30]-[31]
IS27	Implementación de controles de seguridad	[24], [27]-[28]
IS28	Implementación de controles de seguridad eficaces	[26]-[27], [35]
IS29	Procedimiento para la implementación y gestión continua de IS	[22], [28], [32]
IS30	Infraestructura tecnológica	[25]-[26], [31], [35]
IS31	Mantenimiento de hardware y software	[24], [26]-[27], [30], [35]
IS32	Tecnologías de la información	[28], [32]
IS33	Uso de medios para operar y gestionar los negocios	[23], [26]-[28]
IS34	Utilización de tecnología para operar y gestionar sus negocios	[22], [30], [33], [35]
IS35	Calidad de la información	[18], [26], [31]
IS36	Calidad de los datos	[24], [28], [32], [35]
IS37	Disponibilidad y precisión de la información	[22], [24]-[25], [27], [31], [36]
IS38	Calidad del sistema	[27], [32], [35]
IS39	Calidad del servicio	[23], [25]-[26], [31]
IS40	Calidad del soporte	[22], [24], [27], [30]
IS41	Velocidad en la captura, procesamiento y entrega de información	[25]-[28], [35]
IS42	Eficacia del sistema	[24], [27], [32]
IS43	Utilidad de uso	[28], [30]-[32], [35]
IS44	Aplicación de los sistemas	[23]-[24]
SEC45	Seguridad en contextos específicos	[25], [27], [32], [35]
SEC46	Resultados organizacionales	[22] ,[24], [28], [31]
SEC47	Protección de la información y activos	[26], [30], [33], [35]
SEC48	Preservar la confidencialidad e integridad	[24], [26]-[28], [32]

TABLA 6 (CONT.)
FACTORES EXTRAÍDOS

CÓDIGO	FACTOR	REFERENCIAS
SEC49	Cultura organizacional inseguridad de la información	[25], [27], [34]-[35]
SEC50	Comunicación eficaz con las principales partes interesadas en la seguridad	[22]-[23], [26], [27], [34]
SEC51	Mejora continua	[24], [30], [32], [35]
SEC52	Auditorías y certificaciones	[22], [25]
SEC53	Identificación y planificación de riesgo	[23]-[24], [32]
SEC54	Gestión	[26], [28], [35]
SEC55	Caracterización y ponderación de activos, amenazas y medidas de seguridad	[23]-[24], [27], [31]-[32]
SEC56	Sistemas de gestión de la seguridad	[22], [32], [35]
SEC57	Verificación de la eficacia de los controles de seguridad	[25]-[27], [30]
SEC58	Optimización de la gestión de servicios	[24], [28], [31]-[32]
SEC59	Estrategias y gestión de alto rendimiento	[23], [26], [30], [35]
SEC60	Diseño estratégico para una gestión eficiente	[26]-[27], [32]
SEC61	Uso estratégico de herramientas informáticas	[22]-[24], [27]
SEC62	Apoyo a la toma de decisiones	[28], [30]
SEC63	Apoyo técnico interno y externo	[25]-[27], [35]
SEC64	Flexibilidad y adaptación al entorno económico	[24], [26], [28], [32]
SEC65	Auditoría externa	[22]-[23], [35]
SEC66	Normas de seguridad para la gestión de la seguridad de la información	[26], [32]
SEC67	Alineación de objetivos	[23]-[25], [27]
SEC68	Seguridad de los sistemas de información	[22],[26], [35]

C. FACTORES CRÍTICOS DETERMINADOS

Para validar los factores críticos de éxito identificados y mostrados en la Tabla 6, se realizó el juicio de expertos, recabando opiniones a través de un instrumento de evaluación, con el fin de evaluar la relevancia y la importancia de cada factor. El juicio de expertos, comúnmente utilizado para respaldar decisiones sobre variables cualitativas o validar constructos de la literatura, se aplicó aquí para medir el consenso sobre la aceptación o el rechazo de cada factor en función de su impacto en el rendimiento y la seguridad de los SI.

Para garantizar la objetividad, se utilizó un formulario estructurado para las evaluaciones individuales con los 68 ítems y se calculó el coeficiente Kappa de Fleiss para evaluar la concordancia entre los evaluadores más allá del azar. Una vez analizada la concordancia y atendidas las sugerencias, se determinaron 56 ítems que representaban los 56 factores críticos.

Los resultados de coeficiente kappa de Fleiss pueden ser consultados en la Tabla 1, donde se observa una mejora en la concordancia de las respuestas de los evaluadores en la segunda aplicación del instrumento, el cual contenía los 56 ítems. La Tabla 7 muestra los ítems que se descartaron después de analizar las observaciones de los expertos en la aplicación de la primera evaluación.

TABLA 7
FACTORES DESCARTADOS

CÓDIGO	FACTOR
IS25	Desarrollar, mantener, documentar y mejorar el sistema
IS27	Implementación de controles de seguridad
IS30	Infraestructura tecnológica
IS34	Uso de medios tecnológicos para operar y gestionar sus negocios
IS36	Calidad de los datos
IS39	Calidad del servicio
IS40	Calidad del soporte
IS41	Rapidez en la captura coma el procesamiento y entrega de información
IS42	Eficacia del sistema
IS43	Utilidad
IS44	Aplicación utilidad sostenida de los sistemas
SEC65	Auditoría externa

Para priorizar los 56 ítems correspondientes a los factores críticos de desempeño y seguridad de los SI, se empleó el método para toma de decisiones multicriterio TOPSIS. Este recurso permite comparar la distancia relativa de cada alternativa respecto a la solución ideal positiva y a la solución ideal negativa, lo que posibilita establecer un orden de preferencia entre las alternativas evaluadas [3], tal como se aprecia en la Tabla 8.

TABLA 8
DISTANCIA EUCLIDIANA (V_j^+ Y V_j^-), *SCORE* DE DESEMPEÑO (*Pi*) Y JERARQUÍA (*RANK*)

CÓDIGO	V_j^+	V_j^-	*Pi*	*RANK*
SI01	0.0490	0.0535	0.5220	32
SI02	0.0421	0.0536	0.5600	22
SI03	0.0391	0.0558	0.5879	15
SI04	0.0533	0.0475	0.4716	46
SI05	0.0578	0.0359	0.3833	54
SI06	0.0472	0.0493	0.5108	39
SI07	0.0441	0.0477	0.5193	33
SI08	0.0223	0.0729	0.7660	1
SI09	0.0575	0.0348	0.3767	55
SI10	0.0532	0.0359	0.4027	51
SI11	0.0568	0.0360	0.3879	53
SI12	0.0500	0.0392	0.4393	48
SI13	0.0484	0.0398	0.4516	47
SI14	0.0390	0.0491	0.5573	23
SI15	0.0467	0.0426	0.4766	45
SI16	0.0418	0.0477	0.5331	28
SI17	0.0323	0.0570	0.6384	10
SI18	0.0405	0.0469	0.5368	26
SI19	0.0380	0.0506	0.5716	18
SI20	0.0403	0.0522	0.5643	21
SI21	0.0390	0.0540	0.5803	17
SI22	0.0420	0.0471	0.5287	29
SI23	0.0433	0.0454	0.5121	36
SI24	0.0479	0.0459	0.4895	42
SI25	0.0407	0.0506	0.5543	25
SI26	0.0399	0.0529	0.5697	19
SI27	0.0584	0.0432	0.4254	49
SI28	0.0510	0.0376	0.4243	50
SI29	0.0440	0.0470	0.5168	35
SI30	0.0468	0.0434	0.4808	43
SI31	0.0424	0.0473	0.5272	31
SI32	0.0435	0.0467	0.5177	34
SEG33	0.0374	0.0565	0.6020	11
SEG34	0.0454	0.0450	0.4978	41
SEG35	0.0450	0.0472	0.5118	38
SEG36	0.0384	0.0483	0.5572	24
SEG37	0.0531	0.0346	0.3946	52
SEG38	0.0424	0.0474	0.5279	30
SEG39	0.0426	0.0447	0.5121	37
SEG40	0.0302	0.0573	0.6552	7
SEG41	0.0310	0.0586	0.6543	8
SEG42	0.0327	0.0577	0.6384	9
SEG43	0.0319	0.0629	0.6636	6
SEG44	0.0357	0.0537	0.6007	12
SEG45	0.0445	0.0450	0.5028	40
SEG46	0.0362	0.0536	0.5972	13
SEG47	0.0371	0.0531	0.5888	14
SEG48	0.0405	0.0468	0.5363	27
SEG49	0.0382	0.0496	0.5645	20
SEG50	0.0276	0.0606	0.6871	5
SEG51	0.0274	0.0627	0.6962	4
SEG52	0.0678	0.0259	0.2767	56
SEG53	0.0489	0.0447	0.4778	44
SEG54	0.0266	0.0619	0.6998	3
SEG55	0.0262	0.0629	0.7060	2
SEG56	0.0368	0.0515	0.5834	16

Una vez aplicado el método TOPSIS, los resultados obtenidos están directamente relacionados con la pregunta de investigación: ¿cuáles son los factores críticos en el desempeño y seguridad de los sistemas de información y cuál es su orden de importancia? La respuesta a dichos cuestionamientos y los resultados de la investigación se ilustran en las Tablas 9 y 10.

En la Tabla 8 se muestra cómo el cálculo de los valores ideales con V_j^+ para el mejor y V_j^- para el peor, considerando cada uno de los criterios de desempeño y seguridad de los sistemas de información. Se calculó la distancia euclidiana de cada alternativa usando los valores previos y con respecto a los valores V_j^+ y V_j^- obtenidos previamente. Enseguida, usando los valores obtenidos en el cálculo de la distancia euclidiana, se procedió a obtener el *score* de desempeño y la jerarquía de cada factor (*rank*) [37].

En la Tabla 9 se muestra la jerarquía de los factores que impactan en el desempeño de los SI y en la Tabla 10, a su vez, los factores que impactan en la seguridad de los SI obtenidos mediante la aplicación del método TOPSIS. Dichas tablas presentan los códigos, nombres y jerarquías (*rank*) de cada factor, siendo el *rank* 1 el de mayor prioridad.

TABLA 9
JERARQUÍA DE FACTORES PARA EL DESEMPEÑO DE LOS SI

CÓDIGO	FACTORES	*RANK*
SI08	Satisfacción del usuario final	1
SI17	Recursos organizacionales de gestión del sistema	2
SI03	Sensibilización y formación	3
SI21	Compromiso de financiamiento	4
SI19	Recursos humanos	5
SI26	Procedimiento para la aplicación y gestión continua de SI	6
SI20	Garantizar los recursos financieros informáticos	7
SI02	Político, social y ético	8
SI14	Implementación de planes para la gestión del sistema	9
SI25	Implementación de controles eficientes para la seguridad	10
SI18	Disponibilidad de recursos	11
SI16	Apoyo a la alta dirección	12
SI22	Estructura empresarial	13
SI31	Disponibilidad y exactitud de la información	14
SI01	Educación, formación y concienciación	15
SI07	Cumplimiento de normas	16
SI32	Calidad del sistema	17
SI29	Utilización de medios tecnológicos para operar y administrar sus negocios	18
SI23	Gestión de proyectos	19
SI06	Normas y reglamentos gubernamentales	20
SI24	Evaluación del sistema	21
SI30	Calidad de la información	22
SI15	Aprobación y apoyo de la alta gerencia para políticas, procedimientos y controles	23
SI04	Ética en las comunicaciones	24
SI13	Implementación de políticas de seguridad	25
SI12	Política de seguridad definida	26
SI27	Mantenimiento de hardware y software	27
SI28	Tecnologías de la información	28

TABLA 9 (CONT.)
JERARQUÍA DE FACTORES PARA EL DESEMPEÑO DE LOS SI

CÓDIGO	FACTORES	*RANK*
SI10	Impacto grupal de la seguridad	29
SI11	Servicio eficiente y empático con las necesidades del usuario final	30
SI05	Intercambio de información entre los miembros	31
SI09	Impacto individual de la seguridad	32

TABLA 10
JERARQUÍA DE FACTORES PARA EL DESEMPEÑO DE LOS SI

CÓDIGO	FACTORES	*RANK*
SEG55	Alineación de objetivos	1
SEG54	Gestión de estándares de seguridad	2
SEG51	Soporte técnico interno y externo	3
SEG50	Apoyo a la toma de decisiones	4
SEG43	Caracterización y ponderación de activos, amenazas y salvaguardas	5
SEG40	Auditorías y certificaciones	6
SEG41	Identificación y planificación del riesgo	7
SEG42	Gestión de riesgos	8
SEG33	Seguridad en contextos específicos	9
SEG44	Sistema de gestión de seguridad	10
SEG46	Gestión de servicios optimizado	11
SEG47	Estrategias y administración de alto rendimiento	12
SEG56	Seguridad de los SI	13
SEG49	Uso estratégico de las herramientas informáticas	14
SEG36	Preservar la confidencialidad e integridad	15
SEG48	Diseño estratégico de gestión eficiente	16
SEG38	Comunicación efectiva con actores clave en seguridad	17
SEG39	Mejora continua	18
SEG35	Protección de activos de información	19
SEG45	Verificación de la eficacia de los controles de seguridad	20
SEG34	Resultados organizacionales	21
SEG53	Auditoría externa	22
SEG37	Cultura organizacional en seguridad de la información	23
SEG52	Flexibilidad y adaptación al entorno económico	24

IV. CONCLUSIONES

El estudio permitió identificar, a partir de la literatura y del juicio de expertos, un conjunto de 56 factores críticos relacionados con desempeño y la seguridad de los sistemas de información, integrando también dimensiones clave de la gobernanza de las tecnologías de la información.

La jerarquización de estos factores mediante el método multicriterio TOPSIS ofrece a las organizaciones una base objetiva para priorizar acciones de mejora, orientar la inversión y optimizar la gestión de recursos. Estos resultados contribuyen a la toma de decisiones estratégicas alineadas con la sustentabilidad empresarial, al favorecer el uso eficiente de los recursos y fortalecer la resiliencia de los sistemas de información frente a los desafíos actuales. Asimismo los hallazgos del estudio permitirán elaborar, en el futuro, un modelo de toma de decisiones sobre el desempeño y seguridad de los sistemas de información, sustentado en la priorización de factores críticos. Dicho modelo aportará beneficios, como una mejor asignación de recursos, el fortalecimiento de la seguridad y la resiliencia, el apoyo en la toma de decisiones estratégicas y la consolidación de la sustentabilidad organizacional.

REFERENCIAS

[1] A. Paul, N. Shukla, S. K. Paul y A. Trianni, "Sustainable supply chain management and multi-criteria decision-making methods: A systematic review", Sustainability, vol. 13, n.º 13, p. 7104, 2021, doi: 10.3390/su13137104.

[2] A. J. Villa-Silva *et al.*, "Una revisión de literatura de 1980 a 2018 de los métodos Multi-criterio", *Mundo Fesc*, vol. 9, n.º 18, pp. 89-102, 2019.

[3] D.-D. Ramírez-Ochoa, L. A. Pérez-Domínguez, E.-A. Martínez-Gómez y D. Luviano-Cruz, "PSO, a Swarm Intelligence-Based Evolutionary Algorithm as a Decision-Making Strategy: A Review", *Symmetry*, vol. 14, n.º 3, p. 455, 2022, 10.3390/sym14030455.

[4] I. Guandalini, "Sustainability through digital transformation: A systematic literature review for research guidance", *J. Bus. Res.*, vol. 148, pp. 456-471, 2022, doi: 10.1016/j.jbusres.2022.05.003.

[5] K. Olmos-Sánchez y J. Rodas-Osollo, "KMoS-RE: Knowledge management on a strategy to requirements engineering", *Requirements Engineering*, vol. 19, n.º 4, pp. 421-440, dic. 2014, doi: 10.1007/s00766-013-0178-3.

[6] J. Su y Y. Sun, "An improved TOPSIS model based on cumulative prospect theory: Application to ESG performance evaluation of state-owned mining enterprises", Sustainability, vol. 15, n.º 13, p. 10046, 2023, 10.3390/su151310046.

[7] L. Viera, W. Leal y E. Á. Pedrozo, "Transformative organisational learning for sustainability in higher education: A literature review and an international multi-case study", *J. Clean. Prod.*, vol. 447, p. 141634, 2024, 10.1016/j.jclepro.2024.141634.

[8] M. Madanchian y H. Taherdoost, "Applications of Multi-Criteria Decision Making in Information Systems for

Strategic and Operational Decisions", *Computers*, vol. 14, n.º 6, p. 208, 2025, doi: 10.3390/computers14060208.

[9] K. M. Olmos-Sánchez, J. Rodas-Osollo, A. A. Maldonado-Macías y A. Jiménez-Galina, "Harmonization of knowledge representation: Integrating systems thinking ideas with appropriate domain representation strategies", *Computación y Sistemas*, vol. 28, n.º 3, p. 1557-1575, 2024, doi: 10.13053/cys-28-3-5174.

[10] International Organization for Standardization, *ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements*, 2013.

[11] G. Culot, G. Nassimbeni, M. Podrecca y M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda", *The TQM Journal*, vol. 33, n.º 7, pp. 76-105, 2021, doi: 10.1108/TQM-09-2020-0202.

[12] M. N. M. Bhutta *et al.*, "Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS)", *Wirel. Commun. Mob. Comput.*, vol. 2022, n.º 1, p. 9942270, 2022, doi: 10.1155/2022/9942270.

[13] I. Tikkinen-Piri, A. Rohunen y J. Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", *Comput. Law Secur. Rev.*, vol. 37, 2021, doi: 10.1016/j.clsr.2017.05.015.

[14] M. Mehrtak *et al.*, "Security challenges and solutions using healthcare cloud computing", *J Med Life*, vol. 14, n.º 4, pp. 448-461, 2021, doi: 10.25122/jml-2021-0100.

[15] M. J. Page *et al.*, "PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews", *BMJ*, vol. 372, n.º 160, pp. 160, 2021.

[16] J. R. Landis y G. G. Koch, "The measurement of observer agreement for categorical data", *Biometrics*, vol. 33, n.º 1, pp. 159-174, 1997.

[17] J. L. Fleiss, B. Levin y M. C. Paik, *Statistical methods for rates and proportions*, 2.ª ed. Wiley, pp. 212-236, 1981.

[18] J. C. S. d. P. Leite y A. P. M. Franco, "A strategy for conceptual model acquisition", *[1993] Proceedings of the IEEE International Symposium on Requirements Engineering*, San Diego, CA, EUA, 1993, pp. 243-246, doi: 10.1109/ISRE.1993.324851.

[19] X. Liu, "A comparative study on the roles of the World Bank, the OECD and UNESCO in global education policy making", en *Proc. 2022 Int. Conf. on Creative Industry and Knowledge Economy (CIKE)*, Atlantis Press, 2022.

[20] M. A. Juárez-Merino, "Digital governance in Latin America: A comprehensive analysis and future perspectives", *Digit. Gov.: Res. Pract.*, vol. 4, n.º 4, 2025, doi: 10.1177/27723577251388360.

[21] P. Checkland y J. Poulter, "Soft systems methodology", en *Systems approaches to making change: A practical guide*, M. S. Reynolds y Holwell, eds. Londres: Springer, pp. 201-253, 2020, doi: 10.1007/978-1-4471-7472-1_5.

[22] J. J. Pérez y R. S. Delgadillo, "Modelo de evaluación de éxito de los sistemas de información, con énfasis en los factores políticos, social y ético en instituciones públicas del Perú", *Industrial Data*, vol. 22, n.º 1, pp. 181-200, 2019.

[23] J. R. Altamirano, A. Yupanqui y S. Bayona, "Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento", *RISTI*, vol. 25, pp. 112-134, 2017, doi: 10.17013/risti.25.112--134.

[24] M. R. Olmedo, "Riesgos relacionados al usuario final", *ScientiAmericana*, vol. 3, n.º 1, pp. 1-10, 2017.

[25] J. A. Ruíz-Tapia, C. E. Estrada-Gutiérrez y M. L. Sánchez-Paz, "Propuesta de un modelo de un sistema de gestión de calidad en seguridad de la información basado en la norma ISO 27001 para Instituciones Educativas", *RILCO*, vol. 2, n.º 5, p. 10, 2020.

[26] J. Mora, R. Díaz, E. Zhuma e I. E. Díaz, "The information security management system under NTE ISO/IEC 27001 in higher education institutions (Ecuador)", *ROCA*, vol. 16, pp. 549-559, 2020

[27] P. A. Briones, S. G. Molina y M. A. Avilés, "Modelo de evaluación de los sistemas de información aplicado a la calidad de la gestión administrativa universitaria", *Pro Sciences*, vol. 4, n.º 35, pp. 69-89, 2020, doi: 10.29018/issn.2588-1000vol4iss35.2020pp69-89.

[28] R. Moreno-Cevallos y B. L. Dueñas-Holguín, "Sistemas de información empresarial: la información como recurso estratégico", *DC*, vol. 4, n.º 1, pp. 141-154, 2018, doi: 10.23857/dc.v4i1.728.

[29] E. A. Rosales, R. J. Martelo y D. A. Franco, "Design of an information security management system for the administrative process of technological infrastructure in academic institutions based on Magerit", *Aglala*, vol. 11, n.º 1, pp. 227-245, 2020.

[30] E. M. D. Guevara, J. R. Delgado y A. C. Mendoza, "Importancia de la gestión de seguridad de la información en instituciones educativas con ITIL e ISO 27001", *Rev. Investig. Sist. Inform.*, vol. 15, n.º 1, pp. 113-123, 2022, doi: 10.15381/risi.v15i1.23362.

[31] G. I. Cruz, L. E. Delgado, B. R. Ponce y M. J. Marcillo, "Riesgos de seguridad de los datos en la web", *JTI*, vol. 1, n.º 2, pp. 43-49, 2022, doi: 10.47230/Journal.TechInnovation.v1.n2.2022.43-49.

[32] K. Arbanas y N. Žajdela, "Key success factors of information systems security", *J. Inf. Organ. Sci.*, vol. 43, n.º 2, pp. 131-144, 2019, doi: 10.31341/jios.43.2.1.

[33] J. L. Fleiss y J. Cohen, "The equivalence of weighted kappa and the intraclass correlation coefficient as measures of reliability", *Educ. Psychol. Meas.*, vol. 33, n.º 3, pp. 613-619, 1973.

[34] A. Da Veiga y J. H. P. Eloff, "A framework and assessment instrument for information security culture", *Computers & Security*, vol. 29, n.º 2, pp. 196-207, 2010, doi: 10.1016/j.cose.2009.09.002.

[35] S. AlGhamdi, K. T. Win y E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review", *Computers & Security*, vol. 99, p. 102030, dic. 2020, doi: 10.1016/j.cose.2020.102030.

[36] W. H. DeLone y E. R. McLean, "The DeLone and McLean model of information systems success: A ten-year update", *J. Manag. Inf. Syst.*, vol. 19, n.º 4, pp. 9-30, 2003, doi: 10.1080/07421222.2003.11045748.

[37] S. H. Almotiri, "Improving network resilience against DDoS attacks: A fuzzy TOPSIS-based quantitative assessment approach", *Heliyon*, vol. 10, n.º 22, p. e40413, nov. 2024, doi: 10.1016/j.heliyon.2024.e40413.