Candanedo-Yau, R. M. (2026). Ciberseguridad como gestión sostenible: Defensa crítica ante la ingeniería social y ataques informáticos en la educación superior. *Investigación y Ciencia de la Universidad Autónoma de Aguascalientes*, *34*(98), e8640

Ciberseguridad como gestión sostenible: Defensa crítica ante la ingeniería social y ataques informáticos en la educación superior

Cybersecurity as sustainable management:
Critical defense against social engineering and cyberattacks in higher education

[1]*Ricardo M. Candanedo Yau

[1]Facultad de Informática, Electrónica y Comunicación, Universidad de Panamá. Centro Regional Universitario de Panamá Este (CRUPE), Calle Principal de Chepo, República de Panamá. Correo electrónico: ricardo.candanedo@up.c.pa ORCID: https://orcid.org/0009-0002-5017-9830
*Autor de correspondencia.

Recibido: 18 de diciembre de 2025
Aceptado: 25 de junio de 2026
Publicado: 1 de julio de 2026
https://doi.org/10.33064/iycuaa2026988640
e8640

RESUMEN

La ciberseguridad constituye un eje estratégico para la gestión sostenible de las instituciones de educación superior frente al incremento de la ingeniería social y los ataques informáticos que comprometen la seguridad de la información y la continuidad académica. Este estudio tuvo como objetivo identificar los principales riesgos cibernéticos y analizar estrategias de prevención y respuesta desde las dimensiones tecnológica, organizativa y humana. La investigación se desarrolló mediante un enfoque cualitativo de carácter documental, basado en la revisión analítica de literatura científica, normativa y estudios especializados. Los resultados muestran que el phishing, el malware y la ingeniería social representan las amenazas más frecuentes, mientras que la insuficiente capacitación, la ausencia de políticas integrales y el comportamiento de los usuarios constituyen las principales vulnerabilidades. Se concluye que la ciberseguridad debe asumirse como un proceso continuo que fortalezca la resiliencia organizacional y la protección de la información institucional.

Palabras Clave: Ataques informáticos; ciberseguridad; cultura digital; educación superior; gestión sostenible; ingeniería social.

ABSTRACT

Cybersecurity is a strategic component of sustainable management in higher education institutions amid the growing incidence of social engineering and cyberattacks that threaten information security and academic continuity. This study aimed to identify the main cybersecurity risks and analyze prevention and response strategies from technological, organizational, and human perspectives. A qualitative documentary approach was

employed through an analytical review of scientific literature, regulations, and specialized studies. The findings show that phishing, malware, and social engineering are the most common threats, while insufficient training, the lack of comprehensive policies, and user behavior are the main vulnerabilities. It is concluded that cybersecurity should be understood as a continuous process that strengthens organizational resilience and safeguards institutional information.

Keywords: Cyberattacks; cybersecurity; digital culture; higher education; social engineering; sustainable management.

INTRODUCCIÓN

La creciente digitalización de los procesos académicos, administrativos y de investigación en las instituciones de educación superior ha transformado de manera sustantiva la producción, gestión y difusión del conocimiento. El uso intensivo de plataformas virtuales, sistemas de gestión académica, repositorios digitales, servicios en la nube y redes institucionales se ha consolidado como un componente esencial para el cumplimiento de la misión universitaria, en consonancia con los procesos de transformación digital y gestión sostenible que caracterizan a las universidades contemporáneas (Martínez & López, 2019). No obstante, estas infraestructuras digitales constituyen activos críticos cuya vulnerabilidad puede afectar la información institucional y la continuidad de los procesos educativos y administrativos, lo que refuerza la necesidad de enfoques integrales de gestión de la seguridad de la información (Soomro, Shah & Ahmed, 2016; Von Solms & Von Solms, 2018).

En este contexto, el aumento de la superficie de exposición tecnológica ha venido acompañado de un incremento significativo de los riesgos cibernéticos. Las amenazas actuales incluyen ataques complejos que afectan la confidencialidad, integridad y disponibilidad de la información, superando las tradicionales fallas técnicas o vulnerabilidades de software (Ahmad, Maynard & Park, 2014; Tøndel, Line & Jaatun, 2014). Entre ellas, la ingeniería social se posiciona como una de las principales amenazas para las instituciones de educación superior, al explotar debilidades asociadas al comportamiento humano, la falta de capacitación especializada y la ausencia de una cultura de seguridad digital consolidada (Schneier, 2015; Pérez & Salinas, 2022; Yeboah-Boateng & Amanor, 2014).

El presente trabajo examina la ciberseguridad como un componente estratégico de la gestión sostenible en la educación superior, con énfasis en la defensa crítica frente a la

ingeniería social y los ataques informáticos. Desde esta perspectiva, la ciberseguridad trasciende su concepción meramente técnica para ser entendida como un proceso organizacional integral, alineado con la sostenibilidad institucional, la gestión del riesgo y la resiliencia organizacional (Furnell & Clarke, 2012; Wang, Li & Rao, 2020). En consecuencia, la protección de la información y de los sistemas digitales se reconoce como un factor determinante para garantizar la estabilidad, la confianza y la continuidad de las funciones universitarias (Bordoff & Green, 2021; Sánchez & Torres, 2021).

A partir de este planteamiento, surge la siguiente pregunta de investigación: *¿De qué manera la incorporación de la ciberseguridad como un eje de gestión sostenible contribuye a la defensa crítica frente a la ingeniería social y los ataques informáticos en las instituciones de educación superior?*

En correspondencia con esta pregunta, el objetivo general del estudio es analizar los principales riesgos digitales que afectan a la comunidad académica y evaluar estrategias institucionales de prevención y respuesta que integren dimensiones tecnológicas, organizativas y humanas desde un enfoque de gestión sostenible. Como objetivos específicos, se propone identificar las vulnerabilidades asociadas al factor humano, analizar el estado actual de la ciberseguridad en las instituciones de educación superior y valorar su relación con la sostenibilidad institucional y la resiliencia organizacional (Ifinedo, 2014; Puhakainen & Siponen, 2010).

Los antecedentes teóricos y empíricos evidencian que, pese a la implementación de soluciones técnicas avanzadas, las brechas de seguridad persisten debido a deficiencias en la cultura organizacional, la gestión integral del riesgo y la formación continua de los usuarios (Da Veiga & Eloff, 2010; Alshaikh, 2020; Zwilling, Lesjak, Wiechetek, Cetin & Basim, 2022). En este escenario, la ingeniería social continúa siendo altamente efectiva al explotar la confianza, el desconocimiento y la sobrecarga cognitiva de docentes, estudiantes y personal administrativo (Hadlington, 2018; Bada, Sasse & Nurse, 2019; González & Ramírez, 2020).

A partir de este contexto, se plantea como hipótesis que la incorporación de la ciberseguridad como un eje de gestión sostenible, basada en un enfoque integral que articule tecnología, políticas institucionales y formación continua, contribuye a reducir la incidencia de ataques informáticos y a fortalecer la resiliencia organizacional en las instituciones de educación superior (Soomro et al., 2016; Von Solms & Von Solms, 2018).

DESARROLLO

La presente investigación se desarrolló bajo un enfoque cualitativo de carácter documental, correspondiente a una revisión de la literatura de tipo analítico y crítico, orientada a examinar la ciberseguridad como un componente de la gestión sostenible en las instituciones de educación superior. La adopción de este enfoque se fundamenta en la necesidad de analizar, interpretar y sintetizar evidencia científica, documentos normativos y estudios especializados relacionados con la ingeniería social, los ataques informáticos y las estrategias institucionales de ciberseguridad, con el propósito de identificar tendencias, patrones conceptuales y relaciones teóricas presentes en la literatura académica.

La metodología documental utilizada se justifica en el hecho de que el objetivo del estudio no consiste en la medición de variables ni en la obtención de datos empíricos de una población específica, sino en el análisis crítico del conocimiento científico disponible sobre la relación entre la ciberseguridad, la sostenibilidad institucional y la protección frente a la ingeniería social en la educación superior. En este sentido, la revisión de literatura permite integrar hallazgos provenientes de investigaciones desarrolladas en distintos contextos institucionales y geográficos, lo cual facilita la construcción de una visión amplia y estructurada del fenómeno estudiado, así como la identificación de coincidencias y divergencias teóricas reportadas en la literatura especializada.

Para el desarrollo del estudio se realizó una revisión sistematizada de literatura científica entre 2010 y 2025, enfocada en investigaciones relacionadas con ciberseguridad, ingeniería social, sostenibilidad institucional y educación superior. Las fuentes incluyeron artículos indexados, informes técnicos y documentos normativos relevantes, seleccionados bajo criterios de pertinencia, actualidad y rigor académico.

La búsqueda documental se llevó a cabo mediante la consulta de bases de datos académicas como Scopus, Web of Science, Google Scholar e IEEE Xplore, utilizando combinaciones de palabras clave en español e inglés tales como ciberseguridad, ingeniería social, educación superior, seguridad de la información, gestión sostenible y resiliencia organizacional. En una primera fase se identificaron 78 documentos potencialmente relevantes, los cuales fueron sometidos a un proceso de depuración basado en criterios de inclusión y exclusión relacionados con la calidad metodológica, la actualidad de la publicación y la disponibilidad del texto completo. Como resultado de este proceso, se seleccionaron 42 documentos para su análisis final, entre los que destacan

los aportes de Soomro et al. (2016), Von Solms y Von Solms (2018), Da Veiga y Eloff (2010), Furnell y Clarke (2012), Puhakainen y Siponen (2010), Alshaikh (2020), Wang et al. (2020) y Zwilling et al. (2022), los cuales permitieron sustentar el análisis desde perspectivas tecnológicas, organizacionales y humanas.

De manera complementaria, se realizó un análisis documental de políticas institucionales, marcos normativos y modelos de gestión de ciberseguridad aplicados en instituciones de educación superior, lo que permitió identificar enfoques de gobernanza digital, niveles de madurez organizacional y estrategias de gestión del riesgo reportadas en la literatura. Este análisis facilitó la comprensión del grado de integración de la ciberseguridad en los procesos institucionales y su relación con enfoques de sostenibilidad organizacional, en coherencia con lo descrito en estudios previos sobre gobernanza de la seguridad de la información.

Como parte del procedimiento analítico, se empleó la técnica de categorización temática, mediante la cual se organizaron los contenidos revisados en torno a dimensiones analíticas relacionadas con amenazas cibernéticas, vulnerabilidades institucionales, factor humano, estrategias de mitigación y sostenibilidad institucional. Este proceso permitió sistematizar la información disponible en la literatura, facilitando la identificación de patrones recurrentes y relaciones conceptuales entre las variables estudiadas, en concordancia con enfoques metodológicos utilizados en revisiones de seguridad de la información.

Las tablas y síntesis incluidas en la sección de análisis fueron elaboradas a partir de la organización temática de la literatura revisada, tomando como base la recurrencia de los temas identificados en los estudios analizados. En este sentido, los valores y categorías presentados deben interpretarse como indicadores cualitativos de frecuencia relativa dentro de la muestra documental, orientados a facilitar la comparación entre tendencias, y no como resultados estadísticos derivados de mediciones empíricas o de una población específica.

El procedimiento metodológico incluyó la selección, depuración y lectura crítica de las fuentes, así como su análisis comparativo y posterior sistematización, lo que permitió identificar convergencias y divergencias en la literatura especializada. Este proceso facilitó el análisis de la relación entre ciberseguridad, sostenibilidad institucional y resiliencia organizacional en el contexto de la educación superior, desde una perspectiva analítica sustentada en evidencia secundaria.

Los resultados derivados del análisis de la literatura científica muestran que las instituciones de educación superior enfrentan una amplia diversidad de amenazas cibernéticas. Entre las más recurrentes se identifican el phishing, el malware, el ransomware y otros ataques informáticos orientados a la obtención indebida de información sensible o a la interrupción de servicios académicos y administrativos. Estos riesgos se ven intensificados por el uso extensivo de plataformas digitales, la virtualización de los procesos educativos y administrativos, y la creciente interconexión de los sistemas institucionales, factores que amplían de manera significativa la superficie de ataque.

El análisis comparativo de los estudios revisados permitió identificar una elevada exposición a riesgos cibernéticos en el ámbito universitario, particularmente aquellos asociados a la ingeniería social y a la gestión inadecuada del factor humano. Asimismo, se observaron patrones comunes en los tipos de ataques reportados, en las vulnerabilidades institucionales más frecuentes y en las estrategias de mitigación adoptadas, lo que facilitó la sistematización de los hallazgos en información comparable.

Antes de la presentación de la tabla 1, se destaca que la frecuencia de los ataques informáticos varía en función del nivel de madurez digital de las instituciones; no obstante, se identifican patrones recurrentes independientemente del contexto geográfico o del tamaño institucional.

Tabla 1
Tipos de ataques informáticos frecuentes en instituciones de educación superior

Tipo de ataque	Frecuencia estimada (%)
Phishing	42
Malware	21
Ransomware	18
Ataques a contraseñas	11
Otros ataques informáticos	8

Nota. Los porcentajes representan la frecuencia relativa de aparición de cada tipo de ataque dentro de los 42 estudios analizados durante la revisión documental.
Elaboración propia a partir de la literatura científica revisada.

El análisis de la tabla muestra que el phishing y otras técnicas asociadas a la ingeniería social concentran la mayor proporción de incidentes reportados. Este resultado pone de manifiesto que los atacantes priorizan la manipulación del usuario como principal vía de

acceso a los sistemas institucionales, por encima de la explotación directa de vulnerabilidades técnicas.

Previo a la tabla 2, se observa que las vulnerabilidades de carácter organizacional y humano incrementan de manera significativa el impacto de los ataques informáticos en el entorno universitario.

Tabla 2
Principales vulnerabilidades identificadas en instituciones de educación superior

Vulnerabilidad identificada	Nivel de incidencia
Falta de formación en ciberseguridad	Alto
Ausencia de políticas integrales	Alto
Uso de contraseñas débiles	Medio
Falta de protocolos de respuesta a incidentes	Medio
Infraestructura tecnológica obsoleta	Bajo

Nota. El nivel de incidencia fue determinado según la recurrencia reportada en los estudios analizados: alto (más del 60 % de los documentos), medio (entre 30 % y 59 %) y bajo (menos del 30 %).
Elaboración propia.

Los resultados evidencian que las debilidades relacionadas con la formación en ciberseguridad y con la gobernanza institucional constituyen los principales puntos críticos de la seguridad digital en las instituciones de educación superior, superando incluso a las limitaciones asociadas a la infraestructura tecnológica.

Antes de la tabla 3, los hallazgos permiten establecer una relación directa entre la ciberseguridad y los principios de sostenibilidad institucional.

Tabla 3
Dimensiones de la sostenibilidad vinculadas a la ciberseguridad

Dimensión de sostenibilidad	Aporte de la ciberseguridad
Organizacional	Continuidad operativa
Tecnológica	Protección de sistemas
Humana	Cultura de seguridad
Económica	Reducción de costos por incidentes

Nota. La tabla sintetiza la contribución de la ciberseguridad a la sostenibilidad institucional. Elaboración propia.

El análisis muestra que las instituciones que integran la ciberseguridad dentro de una gestión sostenible presentan una mayor capacidad de adaptación y recuperación frente a incidentes, lo que se traduce en un fortalecimiento de la resiliencia organizacional.

Previo a la tabla 4, se identifican las estrategias integrales de ciberseguridad con mayor recurrencia y efectividad en el contexto universitario.

Tabla 4
Estrategias integrales de ciberseguridad en educación superior

Estrategia implementada	Impacto observado
Programas de concienciación	Alto
Políticas institucionales formales	Alto
Actualización tecnológica continua	Medio
Simulacros y planes de respuesta	Medio

Nota. La clasificación del impacto observado y del nivel de riesgo se realizó mediante análisis temático y comparación de la evidencia reportada en la literatura especializada.
Elaboración propia.

Con el fin de complementar los resultados y reforzar el análisis del factor humano, se presenta la tabla 5, que sintetiza los principales comportamientos de riesgo identificados en la literatura revisada.

Tabla 5
Comportamientos de riesgo asociados al factor humano en educación superior

Comportamiento identificado	Nivel de riesgo
Apertura de enlaces sospechosos	Alto
Reutilización de contraseñas	Alto
Falta de verificación de remitentes	Medio
Desconocimiento de protocolos de seguridad	Medio
Uso de dispositivos personales sin protección	Bajo

Nota. La clasificación del impacto observado y del nivel de riesgo se realizó mediante análisis temático y comparación de la evidencia reportada en la literatura especializada.
Elaboración propia.

En conjunto, los resultados evidencian que la adopción de estrategias integrales de ciberseguridad reduce de manera significativa la recurrencia de incidentes y fortalece la resiliencia organizacional. Uno de los hallazgos más relevantes es la centralidad del factor humano como principal vulnerabilidad en los sistemas de seguridad, dado que la falta de formación, la baja percepción del riesgo y las prácticas inadecuadas de los usuarios facilitan el éxito de la ingeniería social, incluso en entornos con infraestructuras tecnológicas avanzadas.

En el marco de la relación entre sostenibilidad institucional y ciberseguridad, resulta pertinente presentar una representación conceptual que integre los componentes tecnológicos, organizacionales y ambientales asociados a la gestión digital en entornos educativos, como se muestra en la figura 1.

Figura 1. Sostenibilidad y ciberseguridad en armonía
Nota: Vista conceptual de un campus moderno que integra energías renovables (solar y eólica) con un centro de datos protegido digitalmente, simbolizando la gestión sostenible de la información.
Elaboración propia.

La figura presentada permite visualizar la convergencia entre la infraestructura tecnológica y los principios de sostenibilidad institucional, destacando la interdependencia entre los sistemas de información y los entornos operativos seguros. Esta integración refuerza el enfoque del estudio, en el que la ciberseguridad se concibe como un componente transversal de la gestión sostenible en la educación superior.

Asimismo, se observa que numerosas instituciones carecen de políticas integrales de ciberseguridad alineadas con una visión de sostenibilidad, lo que limita su capacidad de respuesta y recuperación ante incidentes. En contraste, aquellas que adoptan enfoques integrados, combinando medidas técnicas con acciones organizativas y educativas, logran mitigar de manera más efectiva el impacto de los ataques informáticos y proteger los procesos académicos y administrativos.

En el análisis de los hallazgos de la literatura coinciden en que la ingeniería social representa una de las principales amenazas en la educación superior, debido a su capacidad para explotar el comportamiento humano y evadir controles técnicos (Schneier, 2015; Pérez & Salinas, 2022; Yeboah-Boateng & Amanor, 2014). Este enfoque evidencia la necesidad de comprender la ciberseguridad desde una perspectiva integral que incluya dimensiones tecnológicas, organizativas y humanas (Furnell & Clarke, 2012; Alshaikh, 2020; Soomro et al., 2016).

Una de las principales contribuciones identificadas en la literatura analizada es la vinculación entre la ciberseguridad y los principios de la sostenibilidad institucional. Este enfoque amplía el análisis más allá de la protección de los sistemas informáticos, al considerar la ciberseguridad como un elemento estratégico asociado a la prevención de incidentes, la continuidad operativa y el fortalecimiento de la cultura organizacional, según reporta la literatura especializada (Martínez & López, 2019; Von Solms & Von Solms, 2018). A diferencia de investigaciones que abordan estos aspectos de forma aislada, los estudios revisados permiten comprender la seguridad digital como un proceso transversal que se relaciona con la estabilidad y resiliencia de las instituciones de educación superior desde una perspectiva analítica (Bordoff & Green, 2021; Sánchez & Torres, 2021).
La literatura también sugiere que la ciberseguridad se ha posicionado como un componente estratégico de la gestión universitaria. La creciente dependencia de los entornos digitales ha llevado a diversos autores a señalar la necesidad de transitar desde enfoques reactivos centrados en la respuesta a incidentes hacia modelos preventivos y proactivos de gestión del riesgo (Ahmad et al., 2014; Tøndel et al., 2014). En este contexto, la ingeniería social se presenta como un desafío relevante, ya que evidencia la importancia de abordar la seguridad desde una perspectiva centrada en las personas, la formación continua y el desarrollo de una cultura de seguridad compartida (Schneier, 2015; Da Veiga & Eloff, 2010).

Desde el punto de vista teórico, los estudios revisados indican que la sostenibilidad institucional y la ciberseguridad comparten principios comunes, tales como la prevención, la adaptación al cambio y la mejora continua (Soomro et al., 2016; Von Solms & Von Solms, 2018). Integrar estos principios en la gestión universitaria implica reconocer que la protección de la información, la disponibilidad de los sistemas y la continuidad de los servicios educativos constituyen condiciones relevantes para el cumplimiento de la misión académica, según lo reportado en la literatura (Martínez & López, 2019). Asimismo, los

estudios destacan la importancia de la gobernanza institucional y del liderazgo organizacional en la consolidación de políticas de ciberseguridad coherentes y sostenidas en el tiempo (Bordoff & Green, 2021; Sánchez & Torres, 2021).

Este enfoque se sintetiza en el modelo conceptual que integra la ciberseguridad como eje transversal de la gestión sostenible en la educación superior, el cual se presenta en la figura 2.

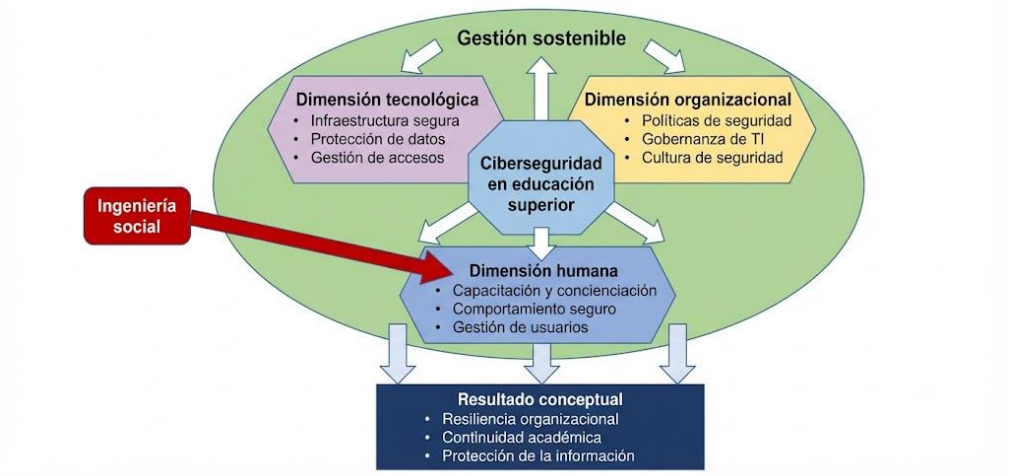

Figura 2. *Modelo conceptual de la ciberseguridad como eje de gestión sostenible en la educación superior.* La figura representa la integración conceptual de la ciberseguridad como un eje transversal de la gestión sostenible en las instituciones de educación superior, articulando dimensiones tecnológicas, organizacionales y humanas, con énfasis en la influencia del factor humano y la ingeniería social.
Elaboración propia.

A partir de este modelo conceptual, se observa la interacción entre los componentes tecnológicos, organizacionales y humanos, lo que permite comprender la ciberseguridad como un proceso integral asociado a la sostenibilidad institucional y no únicamente como un componente técnico aislado.

Este modelo permite comprender que la efectividad de la ciberseguridad en el contexto universitario no depende únicamente de la implementación de herramientas tecnológicas, sino de la articulación coherente entre políticas institucionales, prácticas organizacionales y comportamientos individuales. En consecuencia, la ingeniería social adquiere un papel central como punto crítico de vulnerabilidad, lo que refuerza la necesidad de estrategias integradas de formación, gobernanza y cultura digital orientadas a la sostenibilidad institucional.

El análisis documental también sugiere que la ciberseguridad debe entenderse como un proceso dinámico y transversal que involucra a toda la comunidad académica. La formación permanente, la comunicación efectiva y la evaluación sistemática de riesgos se presentan en la literatura como elementos clave para enfrentar un entorno digital caracterizado por amenazas cada vez más sofisticadas y cambiantes (Puhakainen & Siponen, 2010; Wang et al., 2020). En este sentido, los programas de concienciación y las estrategias educativas son frecuentemente señalados como factores asociados a la reducción de vulnerabilidades vinculadas al comportamiento de los usuarios (Alshaikh, 2020; Zwilling et al., 2022).

En relación con los resultados analizados en la literatura, se evidencia que los comportamientos de riesgo vinculados al factor humano constituyen uno de los principales vectores de vulnerabilidad en las instituciones de educación superior. Prácticas como la apertura de enlaces sospechosos, la reutilización de contraseñas y la falta de verificación de remitentes coinciden con lo reportado en estudios previos, los cuales señalan la baja percepción del riesgo y el desconocimiento de protocolos como factores asociados al éxito de la ingeniería social (Hadlington, 2018; Bada et al., 2019; González & Ramírez, 2020). Estos hallazgos sugieren que, incluso en contextos con infraestructuras tecnológicas avanzadas, el comportamiento de los usuarios continúa siendo un elemento crítico en la ocurrencia de incidentes de seguridad (Ifinedo, 2014).

De manera consistente con la literatura especializada, se observa que los enfoques centrados exclusivamente en soluciones técnicas presentan limitaciones para abordar de forma sostenida los riesgos cibernéticos (Furnell & Clarke, 2012; Soomro et al., 2016). La ausencia de políticas institucionales integrales y de una cultura organizacional orientada a la prevención se asocia en la literatura revisada con una mayor exposición a ataques informáticos (Da Veiga & Eloff, 2010; Alshaikh, 2020). En contraste, los estudios analizados reportan que las instituciones que implementan marcos normativos claros y programas sistemáticos de concienciación tienden a presentar menor recurrencia de incidentes y mejores capacidades de respuesta y recuperación (Puhakainen & Siponen, 2010; Bordoff & Green, 2021).

Es importante señalar que los resultados deben interpretarse considerando las limitaciones inherentes al diseño metodológico empleado. Al tratarse de una investigación documental basada en literatura científica y fuentes secundarias, los hallazgos reflejan la evidencia

reportada en estudios previos y no datos empíricos propios. En este sentido, se trata de una interpretación analítica de la literatura, sin inferencias causales directas. Futuras investigaciones podrían complementar estos hallazgos mediante estudios empíricos como encuestas, entrevistas o estudios de caso.

Finalmente, la literatura revisada sugiere una relación creciente entre ciberseguridad y sostenibilidad institucional (Martínez & López, 2019; Sánchez & Torres, 2021). La integración de la ciberseguridad dentro de enfoques de gestión sostenible se asocia en los estudios analizados con la protección de los activos de información, la estabilidad de los procesos educativos y el desarrollo de modelos de gobernanza digital más resilientes (Von Solms & Von Solms, 2018; Wang et al., 2020). En conjunto, la evidencia analizada permite sostener que la ciberseguridad, concebida como un proceso continuo y transversal, se vincula con el fortalecimiento de la gestión universitaria en la educación superior desde una perspectiva interpretativa basada en evidencia secundaria (Soomro et al., 2016).

CONCLUSIONES

El análisis realizado permite establecer que la ciberseguridad, cuando se integra dentro de los enfoques de gestión institucional en la educación superior, adquiere un carácter estratégico que trasciende su dimensión técnica. Su relevancia no solo se vincula con la protección de los sistemas de información, sino también con la continuidad de los procesos académicos y administrativos en entornos digitalizados.

Los hallazgos evidencian que las instituciones universitarias enfrentan un entorno de amenazas complejo, en el que predominan ataques que explotan principalmente las vulnerabilidades asociadas al comportamiento humano. En este escenario, la ingeniería social se consolida como un factor determinante en la exposición a incidentes de seguridad.

El aporte principal de este estudio radica en la integración conceptual de la ciberseguridad como un eje estructural de la gestión sostenible en instituciones de educación superior, a partir de la sistematización de evidencia documental reciente. Esta aproximación permite superar visiones aisladas del fenómeno y propone una lectura articulada que relaciona la ingeniería social, los riesgos digitales y la cultura organizacional con la sostenibilidad institucional, ofreciendo un marco analítico aplicable para futuras investigaciones y procesos de toma de decisiones en el ámbito universitario.

Asimismo, se observa que la integración de estrategias que articulan componentes tecnológicos, organizativos y formativos contribuye a una comprensión más amplia del fenómeno de la ciberseguridad, favoreciendo la gestión de los riesgos digitales desde una perspectiva institucional.

Por otra parte, la ausencia de políticas estructuradas y de una cultura organizacional orientada a la seguridad digital se asocia con mayores niveles de vulnerabilidad, lo que evidencia la necesidad de consolidar marcos institucionales coherentes en este ámbito.
En conjunto, la ciberseguridad se configura como un componente transversal en los procesos de transformación digital en la educación superior, con implicaciones directas en la estabilidad operativa y en la protección de los activos de información institucional.

Finalmente, el presente estudio aporta una síntesis integradora de la relación entre ciberseguridad y gestión sostenible en la educación superior, al evidenciar que la seguridad digital no debe abordarse como un componente técnico aislado, sino como un eje transversal de gobernanza institucional. A diferencia de estudios previos centrados de manera fragmentada en aspectos tecnológicos o conductuales, esta investigación articula de forma sistemática las dimensiones tecnológicas, organizacionales y humanas, permitiendo una comprensión más holística del fenómeno. En este sentido, su principal contribución radica en consolidar un enfoque interpretativo que vincula la sostenibilidad institucional con la resiliencia cibernética, lo que puede servir como base conceptual para el diseño de políticas universitarias más integradas y preventivas.

Agradecimientos
Agradezco a Dios por la salud y la guía necesaria, y a mis seres queridos por su apoyo y motivación constante en el desarrollo de este ensayo científico.

REFERENCIAS

- Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*(2), 357–370. doi:10.1007/s10845-012-0670-6
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. doi: 10.1016/j.cose.2020.102003

- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv*. Recuperado de https://arxiv.org/abs/1901.02672
- Bordoff, J., & Green, A. (2021). Cybersecurity governance in higher education institutions. *Journal of Higher Education Policy and Management*, *43*(4), 389–403. doi:10.1080/1360080X.2021.1915383
- Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207. doi: 10.1016/j.cose.2009.09.002
- Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983–988. doi: 10.1016/j.cose.2012.08.004
- González, J., & Ramírez, M. (2020). Cultura de ciberseguridad en instituciones universitarias. *Revista Iberoamericana de Educación Superior*, *11*(31), 45–60. doi:10.22201/iisue.20072872e.2020.31.589
- Hadlington, L. (2018). Human factors in cybersecurity: Examining the link between impulsivity and risky security behaviors. *Heliyon*, *4*(7), e00646. doi: 10.1016/j.heliyon.2018.e00646
- Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69–79. doi:10.1016/j.im.2013.10.001
- Martínez, A., & López, P. (2019). Gestión sostenible y transformación digital en universidades. *Revista de Educación y Desarrollo*, *50*, 23–38. Recuperado de https://www.cucs.udg.mx/revistas/edu_desarrollo/anteriores/50/50_Martinez.pdf
- Pérez, L., & Salinas, R. (2022). Ingeniería social y riesgos digitales en entornos educativos. *Educación y Tecnología*, *16*(2), 77–91. Recuperado de https://revistas.uv.cl/index.php/edytec/article/view/3120
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757–778. doi:10.2307/25750704
- Sánchez, D., & Torres, J. (2021). Gobernanza digital y ciberseguridad universitaria. *Revista Latinoamericana de Tecnología Educativa*, *20*(1), 33–48. Recuperado de https://relatec.unex.es/article/view/3998
- Schneier, B. (2015). The human side of security. *Computer*, *48*(7), 66–68. doi:10.1109/MC.2015.198

- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. doi: 10.1016/j.ijinfomgt.2015.11.009
- Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, *45*, 42–57. doi: 10.1016/j.cose.2014.05.003
- Von Solms, R., & Von Solms, S. (2018). Cybersecurity and information security—What goes where? *Information & Computer Security*, *26*(1), 2–9. doi:10.1108/ICS-04-2017-0021
- Wang, J., Li, Y., & Rao, H. R. (2020). Coping responses in cybersecurity incidents: A socio-technical perspective. *Journal of Management Information Systems*, *37*(3), 837–865. doi:10.1080/07421222.2020.1790208
- Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297–307. Recuperado de https://www.cisjournal.org/journal_archive/papers/vol5no4/vol5no4_7.pdf
- Zwilling, M., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. doi:10.1080/08874417.2020.1712269