REVISTA CIENTÍFICA
CONECTIVIDAD
Instituto Tecnológico Superior Universitario Rumiñahui

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

Revisión Sistemática

Concienciación y cultura de seguridad de la información: Evaluación de programas y métodos de impacto

Information security awareness and culture: Program evaluation and impact metrics

Jack David García Alayo[1], Israel Joel Muñoz Rodríguez[2],

Alberto Carlos Mendoza de los Santos[3]

[1] Universidad Nacional de Trujillo, jgarciaa@unitru.edu.pe, La Libertad - Perú
[2] Universidad Nacional de Trujillo, t1513300521@unitru.edu.pe, La Libertad - Perú
[3] Universidad Nacional de Trujillo, amendoza@unitru.edu.pe, La Libertad - Perú

Autor para correspondencia: jgarciaa@unitru.edu.pe

RESUMEN

La creciente exposición a riesgos digitales ha impulsado la implementación de programas de concienciación en seguridad de la información, aunque existen dudas sobre su efectividad real. En el presente trabajo se realizó una revisión sistemática con el objetivo de examinar las metodologías y métricas empleadas para evaluar su eficacia e impacto en la conducta de los usuarios y la disminución de incidentes. Se analizaron 30 artículos académicos publicados entre 2020 y 2025, extraídos de bases de datos como ScienceDirect, Scielo y Google Académico. Los hallazgos muestran que la mayoría de programas se centran en medir el conocimiento inmediato, mientras que pocas iniciativas monitorean cambios conductuales y el retorno de la inversión (ROI). Además, metodologías como gamificación y microlearning aparecen como tendencias con alto potencial, pero con escasa validación empírica. En conclusión, se recomienda que las organizaciones adopten modelos de evaluación que combinen indicadores conductuales, cognitivos y organizacionales, de modo que ayude a trascender la cultura de concienciación en seguridad de la información.

Palabras clave: Seguridad de la información; Métricas de impacto; Evaluación de programas; Capacitación; Organización.

ABSTRACT

Growing exposure to digital risks has driven the implementation of information security awareness programs, although there are doubts about their actual effectiveness. This paper conducted a systematic review to examine the methodologies and metrics used to evaluate their effectiveness and impact on user behavior and incident reduction. Thirty academic articles published between 2020 and 2025, extracted from databases such as ScienceDirect, Scielo, and Google Scholar, were analyzed. The findings show that most programs focus on measuring immediate knowledge, while few initiatives monitor behavioral changes and return on investment (ROI). Furthermore, methodologies such as gamification and microlearning emerge as trends with high potential but limited empirical validation. In conclusion, it is recommended that organizations adopt assessment models that combine behavioral, cognitive, and organizational indicators to help transcend the culture of information security awareness.

Keywords: Information security; Impact metrics; Program evaluation; Training; Organization.

Citas
García Alayo, J. D., Múñoz Rodríguez, I. J., & Mendoza de los Santos, A. C. (2026). Concienciación y cultura de seguridad de la información: evaluación de programas y métodos de impacto. *CONECTIVIDAD*, *7*(1), 477–496. https://doi.org/10.37431/conectividad.v7i1.382

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

1. INTRODUCCIÓN

La seguridad de la información se está volviendo más importante para las organizaciones, debido al incremento sostenido de incidentes de seguridad y esto ha evidenciado que las soluciones tecnológicas, por sí solas, no son suficientes para proteger los activos organizativos. Ante estos incidentes, surgieron programas de capacitación orientados a promover la cultura de seguridad de la información, pero a pesar de los esfuerzos, la implementación de estas iniciativas enfrenta diversos desafíos.

El estudio de Nzeakor et al. (2022) respalda el hecho de que muchos usuarios desconocen términos básicos como ciberdelito, dificultando así la ciber-vigilancia. De manera complementaria, Arellano et al. (2024) identificó que el 35,45% de los empleados no saben sobre la existencia de una área de seguridad, el 30,91% no configuraba actualizaciones automáticas y el 41% abría adjuntos sin verificar su legitimidad, esto evidencia serias brechas en comunicación de políticas y prácticas básicas de protección.

Por otro lado, existen diversos retos en cuanto a las metodologías utilizadas para evaluar la efectividad de los programas, ante estos problemas se debe desarrollar sistemas de medición basados en modelos de comportamiento integrado y no solamente centrarse en conocimiento (Fertig et al., 2020). En la misma línea, Beltrán Muñoz (2023) señala que la evaluación debe ser en base a ejercicios prácticos en lugar de enfocarse meramente en lo teórico, de esta manera se garantiza que el aprendizaje en el entorno laboral sea más ágil, adecuado y factible.

Desde una perspectiva organizacional, Gerst et al. (2024) identificaron en las PYMES cuatro dimensiones para establecer una cultura de ciberseguridad exitosa: conocimiento, recursos, respaldo de la alta dirección y desarrollo continuo. Esto refuerza la necesidad de examinar el efecto que tienen dichos elementos en la evaluación y el impacto de los programas de formación.

Revisiones sistemáticas como la de Uchendu et al. (2021), concluye 4 puntos importantes, primero que la evolución de la terminología de “cultura de seguridad de la información” pasó a “cultura de ciberseguridad”, lo segundo es que identificó factores críticos como apoyo directivo, políticas claras y programas de concientización, el tercer punto son los frameworks convergentes en el rol central de la cultura organizativa y por último el predominio de cuestionarios y encuestas para medir cultura. Ante esto podemos ver la falta de métricas dinámicas que capturen

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

comportamientos reales. Para abordar esta carencia, Solomon et al. (2022) emplea factores conductuales y espaciales-temporales junto con modelos de redes neuronales profundas para evaluar dinámicamente la concientización en seguridad, lo cual puede ayudar de gran manera la precisión de evaluación en distintos escenarios reales.

Por otra parte, Tejay & Mohammed (2022) demostraron que la cohesión de grupo, el código profesional, la concientización sobre seguridad de información y las prácticas informales de trabajo influyen significativamente en la cultura de seguridad, a su vez, esto impactó de manera positiva en la percepción de éxito en seguridad de la información. Este último estudio destaca la importancia de combinar métodos cualitativos y cuantitativos para evaluar la cultura de seguridad en contextos organizativos reales.

Considerando estas evidencias, la presente investigación plantea como objetivo analizar las métricas de impacto, la evaluación de los programas y la eficacia de las capacitaciones en contextos organizacionales.

El estudio fue guiado por la siguiente pregunta: En empleados de organizaciones, ¿la implementación de programas de concienciación y cultura de seguridad de la información mejora el conocimiento y cumplimiento de políticas, reduciendo los incidentes de seguridad reportados?

2. MATERIALES Y MÉTODOS

El presente trabajo es una revisión sistemática de literatura, que siguiendo las recomendaciones de la metodología PRISMA 2020 sintetiza de forma estructurada la información relacionada a la pregunta planteada según el formato PICO presentado en la Tabla 1.

Tabla 1. Planteamiento de la pregunta en formato PICO

P	Seguridad de la información en las organizaciones
I	Programas de concientización y cultura de seguridad
C	-
O	Evaluación y métricas de impacto
En empleados de organizaciones, ¿la implementación de programas de concienciación y cultura de seguridad de la información mejora el conocimiento y cumplimiento de políticas, reduciendo los incidentes de seguridad reportados?	

Fuente: Elaboración propia.

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

Se estableció que todo artículo para ser aceptado debe ceñirse a los criterios de inclusión y exclusión presentados en la Tabla 2 y Tabla 3 respectivamente para su aceptación.

Tabla 2. Criterios de inclusión

CÓDIGO	CRITERIO DE INCLUSIÓN
CI1	Artículos con relevancia en concienciación y cultura de seguridad de la información
CI2	Estudios con métricas o metodologías de evaluación de programas

Fuente: Elaboración propia.

Tabla 3. Criterios de Exclusión

CÓDIGO	CRITERIO DE EXCLUSIÓN
CE1	Documentos no revisados por pares
CE2	Idiomas distintos al español o inglés
CE3	Artículos cuya fecha de publicación esta fuera del rango 2020 – 2025
CE4	Artículos cuya temática no se enfoquen en presentar métricas o metodologías que permitan evaluar el impacto de una cultura de seguridad de la información
CE5	Enfoques ajenos a seguridad de la información en TI

Fuente: Elaboración propia.

Se llevó a cabo búsquedas en diversas bases de datos como: ScienceDirect, Scielo y Google Scholar en la cuales se utilizaron cadenas de búsqueda en español e inglés en la Tabla 4.

Tabla 4. Artículos obtenidos en base a las cadenas de búsqueda

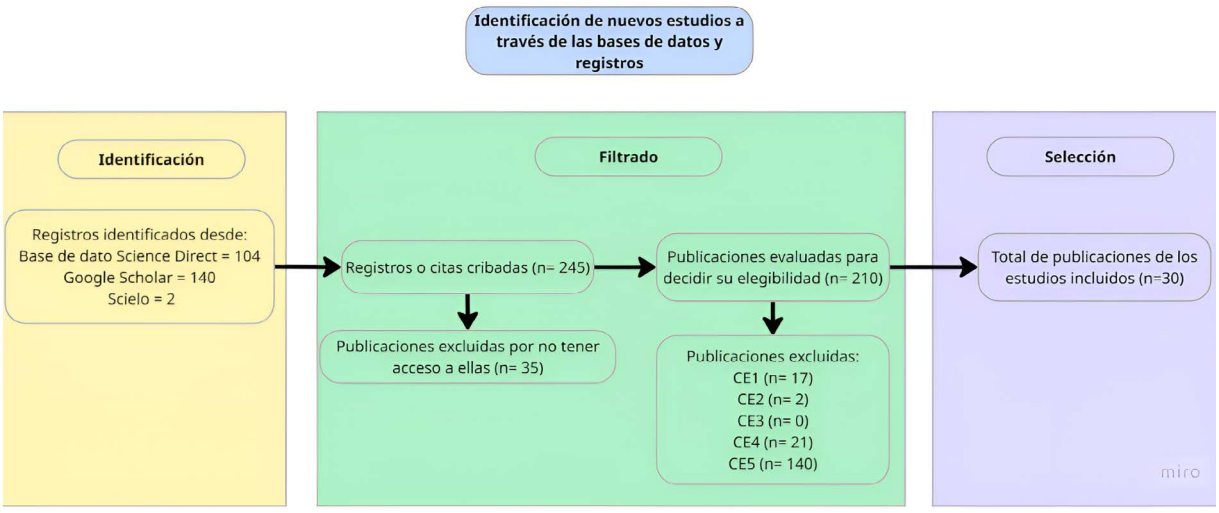
BASE DE DATO	CADENA DE BÚSQUEDA	ARTÍCULOS ENCONTRADOS
GOOGLE SCHOLAR	"("information security awareness" OR "security awareness"" OR "concienciación en seguridad" OR "cultura de seguridad") AND ("program evaluation" OR "impact evaluation" OR "evaluación de programas" OR "evaluación de impacto") AND ("information security"" OR "seguridad de la información"") AND (phishing OR "simulación de phishing"" OR KAP OR ""pre post"" OR ""antes después") AND ("organizational context" OR "entorno organizacional" OR empresa OR corporativo OR "sector público" OR "institución" OR "ambiente laboral") -NHS -hospital -clinic -school -estudiantes -educativo -salud -pediatría -universidad -paciente -niños"	131
GOOGLE SCHOLAR	("security awareness" OR "concienciación en seguridad") AND ("evaluation" OR "evaluación") AND ("program" OR "programa" OR "capacitación" OR "training") AND ("information security" OR "seguridad de la información") AND ("phishing" OR "simulación de phishing") AND ("empresa" OR "organización") AND ("pre post" OR "antes después" OR longitudinal OR "cuasi experimental")	9

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

BASE DE DATO	CADENA DE BÚSQUEDA	ARTÍCULOS ENCONTRADOS
SCIELO	(“security awareness” OR “concienciación en seguridad” OR “security culture” OR “cultura de seguridad”) AND (“information security”)	2
SCIENCE DIRECT	(“information security awareness” OR “information security culture”) AND (program OR initiative) AND (“program evaluation” OR measurement OR “impact evaluation”) AND (metric OR indicator)	94
SCIENCE DIRECT	(“information security awareness” OR “security information culture”) AND (program OR training) AND evaluation AND (“click-through rate” OR compliance) AND CIBERSECURITY	1
SCIENCE DIRECT	(“information security awareness” OR “security culture”) AND (training OR program) AND (pretest OR posttest) AND (phishing OR compliance) AND metric	6
SCIENCE DIRECT	(“information security awareness” OR “information security culture”) AND (intervention OR training) AND (“program evaluation” OR “impact evaluation”) AND “before and after”	3

El proceso de selección de los documentos se representa gráficamente en la Figura 1, la aplicación de los filtros nos dio como resultado un total de 30 artículos seleccionados que asimismo soportaron una revisión minuciosa de su contenido, las discrepancias fueron resueltas mediante consenso con un tercer revisor.

Figura 1. Diagrama de Flujo Prisma para la selección de artículos



Fuente: Elaboración propia.

Los artículos seleccionados fueron obtenidos de diferentes países tales como: Alemania, Estados Unidos, España, México, Nigeria, India, Israel, etc. Esto nos garantiza una diferencia en perspectivas y aplicaciones de la concienciación de la seguridad de la información en diferentes contextos.

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

Se evidencia lo anteriormente mencionado en la Figura 2.

Figura 2. Cantidad de artículos por países

Fuente: Elaboración propia.

3. RESULTADOS Y DISCUSIÓN

Al finalizar la selección se procedió a analizar y sintetizar la información de cada manuscrito, cuyos resultados se muestran en la Tabla 5.

Tabla 5. Datos extraídos de la literatura revisada

N°	Título, año de publicación y enlace	Objetivos	Síntesis de la conclusión
1	Título: A typology of cybersecurity behavior among knowledge workers Año: 2024 Link: https://www.sciencedirect.com/science/article/pii/S0167404824000427	Caracterizar arquetipos para los distintos trabajadores en función de sus aptitudes, actitudes y conductas de ciberseguridad, para finalmente desarrollar una tipología que ayuda a diseñar programas formativos y medidas preventivas específicas de ciberseguridad.	Segmentando a los trabajadores en arquetipos conductuales (Naive Greenhorns, Traditional Examiners, Flexible Mavericks y Reliable Troupers) se mejora la medición del impacto, así como la focalización de los programas organizacionales.

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

N°	Título, año de publicación y enlace	Objetivos	Síntesis de la conclusión
2	Título: A systematic review of current cybersecurity training methods Año: 2024 Link: https://www.sciencedirect.com/science/article/pii/S0167404823004959	Crear un panorama integral de los métodos de capacitación en ciberseguridad utilizados en entornos organizaciones y evaluar su efectividad para mejorar comportamientos de seguridad, identificando las mejores prácticas y su impacto en cambios conductuales de ciberseguridad duraderos.	De los siete métodos evaluados, los basados en juegos (Password Protector y Phishi) y las simulaciones con retroalimentación demostraron ser los más efectivos, logrando una reducción del 60% en clics de phishing.
3	Título: Enabling security risk assessment and management for business process models Año: 2024 Link: https://www.sciencedirect.com/science/article/pii/S2214212624001315	Dotar a cada proceso de negocio un mecanismo de evaluación y gestión de riesgos mediante el patrón MARISMA-BP, para apoyar al análisis y gestión de amenazas (procesos, personas y externas) que afectan a cada flujo de la empresa e integrarlo en la herramienta automatizada e-MARISMA, demostrando así su versatilidad en un escenario sanitario real.	Al integrar los controles “People” de ISO 27002 en MARISMA-BP y automatizar su seguimiento, la organización puede cuantificar riesgos y ROI.
4	Título: “Enhancing employees information security awareness in private and public organizations: A systematic literature review” Año: 2021 Link: https://www.sciencedirect.com/science/article/pii/S0167404821000912	Comparar métodos y factores en protección de la información (ISA) en organizaciones públicas y privadas que influyen en el nivel de conciencia de ciberseguridad de los empleados.	La gamificación es la metodología común en ambos sectores para aumentar la motivación y la conciencia de seguridad.
5	Título: “Information security management in ICT and non-ICT sector companies: A preventive innovation perspective” Año: 2021 Link: https://www.sciencedirect.com/science/article/pii/S0167404821002078	Explorar los motivos, impactos, obstáculos y beneficios percibidos de la implementación de ISO/IEC 27001 en empresas de sectores TIC y no TIC, impulsando su adopción en empresas no TIC, para el aumento de la cultura de ciberseguridad en empresas alemanas.	La implementación del estándar ISO/IEC 27001 aumenta la concienciación teórica de empleados en una media de 4.35 sobre 5, pero bajo impacto práctico en conductas.

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

N°	Título, año de publicación y enlace	Objetivos	Síntesis de la conclusión
6	Título: "A comprehensive model of information security factors for decision-makers" Año: 2020 Link: https://www.sciencedirect.com/science/article/pii/S0167404820300341	Desarrollar un modelo holístico y completo de factores de éxito en protección de la información, identificando para cada uno ellos una métrica que impacte el estado de seguridad organizacional.	Se identifican 12 factores clave de éxito, organizados en tres categorías según su influencia directa o indirecta. Estos factores son capaces de reducir hasta un 40% la exposición a amenazas críticas.
7	Título: "Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers" Año: 2023 Link: https://www.sciencedirect.com/science/article/abs/pii/S0167404823001761	Evaluar el impacto del trabajo remoto en la adopción de precauciones de seguridad (p. ej., medidas técnicas y comportamentales para proteger activos informáticos). Examinar la influencia de la concienciación en ciberseguridad cuando se tiene trabajo remoto y precauciones de seguridad. Analizar el rol moderador del cumplimiento de políticas de seguridad en el vínculo entre trabajo remoto y concienciación en ciberseguridad.	Los resultados confirman que el trabajo remoto estimula directamente tanto la conciencia de ciberseguridad como las acciones preventivas de los usuarios, ofreciendo así pautas prácticas para que las organizaciones potencien la "vigilancia remota" sin incrementar su exposición a riesgos cibernéticos.
8	Título: "Evaluating the Influence of Attitude versus Knowledge and Individual Factor versus Intervention Factor on Information Security Awareness in Local Government" Año: 2024 Link: https://www.sciencedirect.com/science/article/pii/S1877050924005003	Cuantificar cuánto implican la actitud y el conocimiento en el nivel de conciencia sobre la protección de la información.	La escala HAIS-Q (ajuste global del modelo SRMR=0.08) y PLS-SEM muestran que la actitud implica el 71%, mientras que el conocimiento un 79,6%. Esto confirma que programas de entrenamientos formales permiten una evolución cultural en la ciberseguridad solo el usuario retiene la información en conocimiento con una actitud adecuada.
9	Título: "Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours" Año:2024 Link: https://www.sciencedirect.com/science/article/pii/S0148296324001899	Diseñar un programa gamificado de entrenamiento para elevar conductas seguras y comprobar si el e-training gamificado reduce conductas inseguras (p.ej., clics en phishing y reporte de incidentes).	La variable gamificación mejora autoeficacia, satisfacción, reduce los clics de phishing un 50.2% y los reportes de correos a TI aumentó un 70%.

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

N°	Título, año de publicación y enlace	Objetivos	Síntesis de la conclusión
10	Título: "A Critical Review on Cybersecurity Awareness Frameworks and Training Models" Año: 2024 Link: https://www.sciencedirect.com/science/article/pii/S1877050924008329	Evaluar cuantitativamente marcos y modelos de formación en ciberseguridad para determinar su eficacia en disminuir incidentes y costos y mejorar la resiliencia.	La salvaguardia de la integridad de los datos y la garantía de su estabilidad a largo plazo dependen fundamentalmente de la implementación de medidas sólidas de ciberseguridad y del fomento de la concienciación de los usuarios.
11	Título: "A systematic review of scales for measuring information security culture" Año: 2020 Link: https://www.sciencedirect.com/org/science/article/pii/S2056496120000112	Identificar escalas válidas y sus dominios para cuantificar la cultura de seguridad. Determinando cuántas de ellas utilizan psicometría completa midiendo aspectos psicológicos (conocimiento, personalidad, habilidades cognitivas y emocionales), usando métodos rigurosos (diseño y aplicación de pruebas con análisis estadísticos) y permitiendo la comparación (evaluando diferencia entre individuos)	De las 27 escalas examinadas sólo el 15% integra psicometría completa con dimensiones de sanciones y recompensas. Esto requieren instrumentos más valiosos.
12	Título: "Impact of comprehensive information security awareness and cognitive characteristics on security incident management – an empirical study" Año: 2021 Link: https://www.sciencedirect.com/science/article/abs/pii/S016740482100225X	Analizar la relación entre distintos niveles de conciencia (seguridad, sistema y situación) y factores cognitivos (autoeficacia y metacognición) con el desempeño en gestión de incidentes y concienciación de ciberseguridad.	Tras una encuesta a 100 profesionales, el modelo PLS explica que los distintos niveles de conciencia y factores cognitivos influyen un 63% en la detección de incidentes de información y 58% en la mitigación de incidentes. Ambos parámetros permiten madurar una cultura de seguridad en una organización.
13	Título: "The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering" Año: 2020 Link: https://www.sciencedirect.com/science/article/pii/S1877050921001381	Examinar factores individuales y organizativos que afectan la conciencia de seguridad y cómo ésta influye en la intención de resistir ataques de ingeniería social, usando la Teoría del Comportamiento Planificado.	El análisis PLS-SEM demuestra la aplicabilidad de la teoría de la conducta planificada en el contexto de los ataques de ingeniería social y subraya que las medidas técnicas por sí solas no son suficientes para garantizar la seguridad de la información.

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

N°	Título, año de publicación y enlace	Objetivos	Síntesis de la conclusión
14	Título: "Asystematic literature review of cybersecurity scales assessing information security awareness" Año: 2023 Link: https://www.sciencedirect.com/science/article/pii/S240584402301441X	Localizar y analizar exhaustivamente las escalas publicadas que miden la concienciación de la seguridad de la información (ISA). Identificar dimensiones y factores que configuran la conciencia de seguridad y ponerlos en relación con contextos de aplicación.	De los 5 595 estudios revisados, sólo 24 proponen escalas para medir ISA, cada una enmarcada en disciplinas específicas. Se concluye que las escalas ISA deben ser multidimensionales (conocimiento, actitud y comportamiento) y alcanzar al menos un 87% de validez.
15	Título: "Assessing information security culture: A mixed-methods approach to navigating challenges in international corporate IT departments" Año: 2024 Link: https://www.sciencedirect.com/science/article/abs/pii/S0167404824002438	Evaluar la eficacia de un enfoque mixto (encuesta cuantitativa + entrevistas cualitativas semi-estructuradas) para medir de forma integral la cultura de seguridad.	El enfoque mixto demuestra ser válido y robusto como evaluador de cualquier forma de entrenamiento para la concienciación de protección de la información, permitiendo una comprensión profunda de la cultura de seguridad. Este modelo proporciona un marco capaz de demostrar el impacto real en cada empleado tras la capacitación.
16	Título: "Evaluating organizational phishing awareness training on an enterprise scale" Año: 2023 Link: https://www.sciencedirect.com/science/article/abs/pii/S0167404823002742	Medir el efecto de campañas simuladas de phishing longitudinales (3 oleadas) en la tasa de clics (CTR) y en la tasa de reporte (Reporting Rate). Compara eficacia de correcto personalizados vs. genéricos.	En el experimento realizado en una institución financiera israelí con aproximadamente 5 000 empleados, se observó que las actividades de concienciación organizacional incrementaron de forma significativa la resistencia frente a los ataques de phishing a lo largo de tres oleadas de simulaciones.
17	Título: Developing metrics to assess the effectiveness of cybersecurity awareness program Año: 2022 Link: https://academic.oup.com/cybersecurity/article/8/1/tyac006/6590603	Proponer métricas de impacto, sostenibilidad y monitorización (adaptadas de ELINET) para evaluar de forma sistemática y replicable programas de concienciación en ciberseguridad.	Al aplicar las métricas en simulaciones de phishing, la tasa de clics se redujo un 41%. La retención del conocimiento, evaluada con un test de 5 preguntas, mejoró un 28%. Además, el tiempo promedio para reportar incidentes se redujo de 48 horas a solo 12 horas. Estas cifras no solo muestran que el modelo cuantifica el ROI, sino que también ayudan a identificar las áreas con mayor impacto.

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

N°	Título, año de publicación y enlace	Objetivos	Síntesis de la conclusión
18	Título: Evaluation of Security Training and Awareness Programs: Review of Current Practices and Guidelines Año: 2021 Link: https://arxiv.org/abs/2112.06356	Analizar 30 estudios publicados y entrevistar a 5 responsables de seguridad en una institución financiera para clasificar y criticar las métricas de evaluación de programas según el modelo de Kirkpatrick (reacción, aprendizaje y comportamiento).	La mayoría de las instituciones mide satisfacción y conocimiento de programas de concienciación, pero solo el 40% monitoriza cambios de conducta (por ejemplo, en simulaciones de phishing). Apenas el 20% calcula el retorno de inversión (ROI), a pesar de lo importante que es justificar estas iniciativas.
19	Título: Programa de concientización en seguridad de información para pequeñas empresas en la ciudad de Puyo Año: 2022 Link: https://repositorio.puce.edu.ec/items/d257e331-1e2c-4155-8514-f5e7403dac69	Diseñar e implementar un programa de formación práctico dirigido a 45 empleados de PYMEs. Este programa incluirá un cuestionario que cubrirá temas como ataques informáticos, técnicas de ataque, gestión de contraseñas, riesgos asociados al software ilegal y protocolos a seguir en caso de incidentes.	La prueba de Wilcoxon (Z = –3,010; p = 0,003) respalda que este progreso es estadísticamente significativo, y todos los participantes mostraron al menos un 15% de mejora individual en cada tema, enfocándose más en conocimientos sobre phishing, gestión de contraseñas y protección ante riesgos o incidentes.
20	Título: Measuring the Effectiveness of U.S. Government Security Awareness Programs: A Mixed-Methods Study Año:2023 Link: https://www.nist.gov/publications/measuring-effectiveness-us-government-security-awareness-programs-mixed-methods-study	Se explora a través de grupos focales (n=29) y encuestas (n=96), cómo las agencias gubernamentales evalúan la efectividad de sus programas. Identificar las métricas que más valoran y los retos que enfrentan en su implementación.	El 84% de las organizaciones utilizan tasas de cumplimiento en sus entrenamientos, el 72% mide las tasas de clic en simulaciones de phishing y el 67% lleva a cabo auditorías de programas; sin embargo, solo el 29% se dedica a rastrear tendencias de incidentes reales. Con respecto a los incidentes reales, solo el 59% son valorados como indicador útil, indicando más una limitación en cuanto a su uso.
21	Título: Holistic Systematic Review on Methodologies of Assessing Effectiveness Cybersecurity Awareness Program Año: 2024 Link: https://www.researchsquare.com/article/rs-4329496/v1	Se planteó el objetivo de revisar 41 estudios realizados entre 2006 y 2019 para identificar las metodologías de evaluación, las organizaciones a las que se dirigen y cómo se han utilizado métodos de aprendizaje automático para medir la efectividad de los programas de concienciación.	El 85% utiliza cuestionarios antes y después de la formación, mientras que el 60% opta por estudios de caso. Sin embargo, sorprendentemente, ningún trabajo ha incorporado el aprendizaje automático para la evaluación automática o predicción de riesgos. Esto resalta una clara falta de herramientas predictivas que permitan la identificación de vulnerabilidades conductuales que sean verdaderamente potenciales.

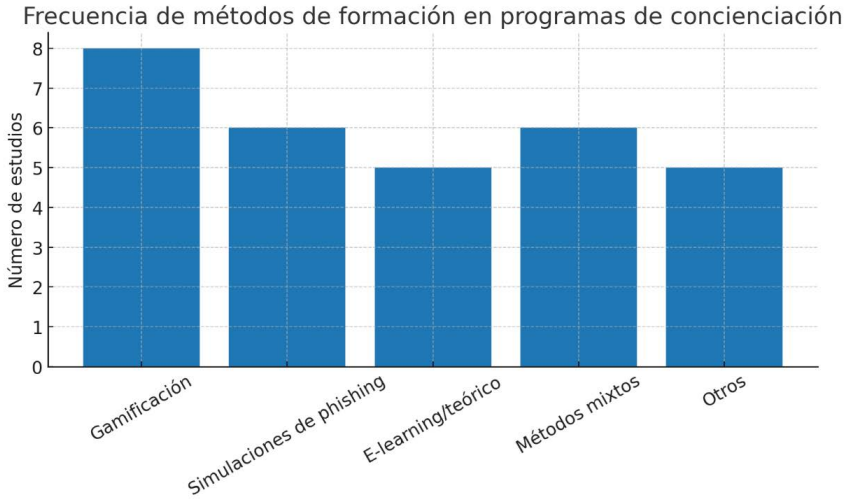
Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

N°	Título, año de publicación y enlace	Objetivos	Síntesis de la conclusión
22	Título: Gamification of Cyber Security Awareness – A Systematic Literature Review Año: 2021 Link: https://www.utupub.fi/handle/10024/152929	Revisar 95 artículos del periodo 2010 a 2021, utilizando el enfoque PRISMA para identificar los diferentes tipos de juegos de concienciación, así como los géneros y las mecánicas de aprendizaje que emplean.	Del total de juegos, el 55% utiliza "demostración" como su mecánica principal, mejorando así una participación activa a través de tareas simuladas. Aunque estos juegos logran aumentar el compromiso y la motivación, menos del 10% evalúa su eficacia real (clics en phishing), esto evidencia la falta de incorporación de métricas de impacto real y un seguimiento a largo plazo.

Fuente: Elaboración propia.

Se puede identificar que las metodologías mixtas nos brindan una visión más clara sobre el verdadero impacto de los programas. Por ejemplo, Baltuttis et al. (2024) caracterizaron arquetipos conductuales para ajustar los programas formativos a cada perfil, mejorando así la focalización y la medición del impacto. De forma similar, Prümmer et al. (2023) determinaron que los métodos más efectivos en entornos organizacionales, como las simulaciones de phishing y el protector de contraseñas, redujeron los clics maliciosos en un 60%, mientras que las técnicas puramente informativas solo incrementaron el conocimiento sin cambiar la conducta. Este resultado coincide con los de Onduto (2021), quien recalca que los juegos como "Anti-Phising Phil" y "What.Hack" ayudan a mejorar la detección de phishing en un 50.2%, ya que se utilizan simulaciones interactivas y retroalimentaciones inmediatas.

Figura 3. Métodos de formación en programas de concienciación



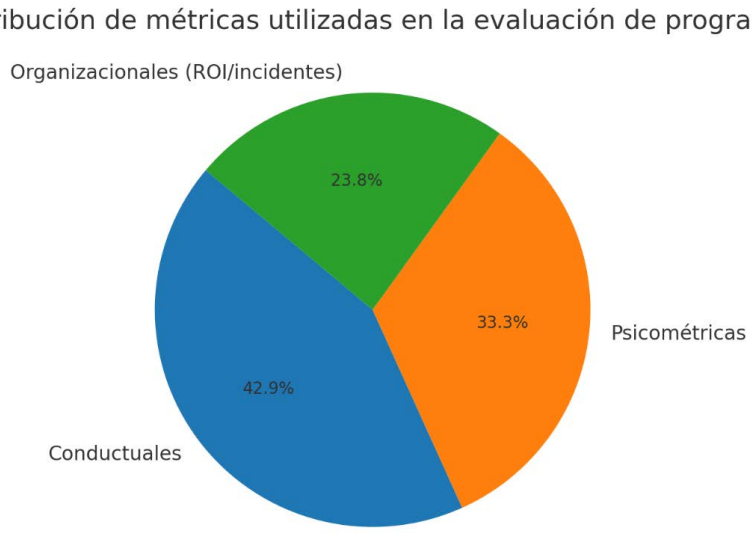
Fuente: Elaboración propia.

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

En contextos más técnicos, Rosado et al. (2024) incorporaron los controles "People" de ISO 27002 en un modelo de gestión de riesgos de procesos de negocio (MARISMA-BP). Esto demuestra que la automatización del seguimiento no solo permite cuantificar las reducciones de riesgo, sino que también valida el retorno de la inversión en capacitación. Por otro lado, Khando et al. (2021) evidenciaron que la gamificación, utilizada en presentaciones, videos y simulaciones, no sólo motiva a los usuarios, sino que en la práctica reduce los clics en phishing en un 50,2% y aumenta la tasa de reporte de incidentes hasta un 70%.

Sin embargo, varias revisiones sistemáticas destacan un desequilibrio en las métricas utilizadas. En el trabajo de Jayatilaka et al. (2021) encontraron que el 100% de los programas mide la satisfacción inmediata, el 75% evalúa el aprendizaje a través de tests, y solo el 40% monitorea cambios en el comportamiento, mientras que apenas el 20% calcula el ROI. Orehek y Petrič (2020) añadieron que apenas el 15% de las escalas psicométricas incluyen dimensiones de sanciones y recompensas, lo que dificulta demostrar el impacto total de las capacitaciones. En la misma línea, Garba et al. (2024) señalaron que, aunque el 85% de los estudios utiliza cuestionarios pre/post y el 60% recurre a casos de estudio, ninguno incorpora aprendizaje automático para el análisis predictivo de feedback, lo que representa una clara oportunidad de mejora. Estos desequilibrios metodológicos quedan también de manifiesto en Taherdoost (2024), quien criticó la falta de rigor en los marcos y modelos de formación.

Figura 4. Métricas utilizadas en la evaluación de programas



Fuente: Elaboración propia.

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

En otros estudios como el de Diesch et al. (2020), se identificaron doce elementos clave para el éxito, como la concienciación (tasa de clics y reportes), que al implementarse pueden reducir la exposición a amenazas en hasta un 40%. Por otro lado, Mirtsch et al. (2021) encontraron que la adopción de la norma ISO 27001 elevó la concienciación teórica a 4,35 sobre 5, aunque solo el 56% de las empresas notó mejoras en la práctica. En cuanto al impacto del trabajo remoto, Nwankpa & Datta (2023) hallaron que la concienciación medía la relación positiva entre este modelo laboral y la adopción de medidas preventivas ($\beta = 0,27$; $p < 0,001$). De forma similar, Susanto & Maulana (2024) calcularon que la actitud explica el 71% del nivel de concienciación, mientras que el conocimiento alcanza un 79,6% en gobiernos locales. Complementando esto, Thangavelu et al. (2021) demostraron que los niveles de conciencia y factores cognitivos explican el 63% de la detección y el 58% de la mitigación de incidentes. Finalmente, Grassegger & Nedbal (2021) confirmaron que aumentar la desviación típica de ISA mejora la intención de resistir ataques de ingeniería social.

En el campo de la medición de escalas, Rohan et al. (2023) encontraron únicamente 24 escalas ISA válidas entre 5,595 estudios, sugiriendo que la validez debería ser superior al 87% y que se debe adoptar un enfoque multidimensional. Por otro lado, en el trabajo de Zanke et al. (2024) se validó un enfoque mixto, combinando encuestas y entrevistas en departamentos corporativos internacionales, el cual se considera robusto y replicable. En el ámbito empresarial, Hillman et al. (2023) observaron en simulaciones longitudinales una disminución del 50.2% en la tasa de clics y un incremento del 70% en la tasa de reportes, destacando que los correos personalizados duplicaron las aperturas en comparación con los genéricos. Finalmente, Furman (2023) reveló que, en agencias gubernamentales de Estados Unidos, el 84% de los programas mide el cumplimiento, el 72% los clics en phishing y solo el 29% las tendencias de incidentes. Propuso un enfoque que incluya análisis de incidentes reales y visualizaciones interactivas. Además, el estudio empírico de Puyo de Beltrán Aldás (2022) confirmó mediante la prueba de Wilcoxon ($p = 0,003$) mejoras individuales de al menos un 15% en cinco áreas evaluadas.

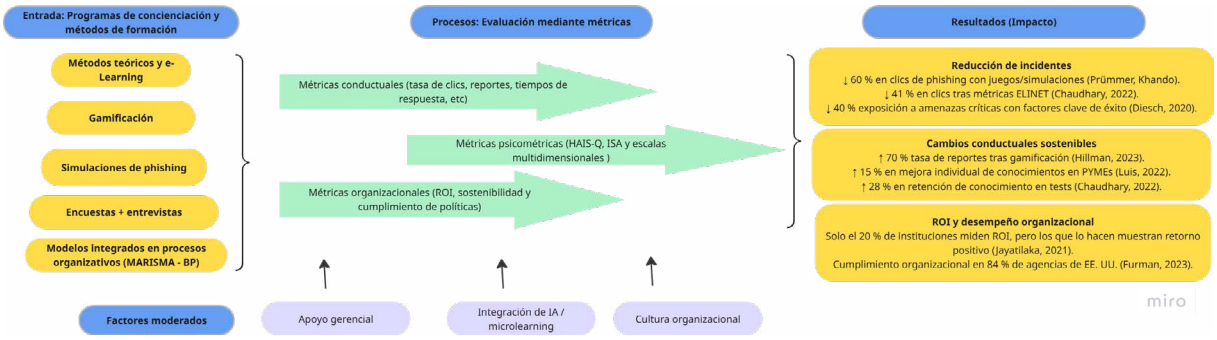
En conjunto, estos hallazgos demuestran que los programas más efectivos combinan ejercicios prácticos, métricas conductuales, análisis cualitativos y apoyo organizacional continuo. Asimismo, subrayan la urgencia de adoptar herramientas basadas en inteligencia artificial y

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

métricas contextuales. Examinar tanto las percepciones subjetivas como conductas reales, permite alcanzar un entendimiento más completo sobre el impacto y lo que debería ser el estándar para evaluaciones de concienciación de ciberseguridad (Bitrián et al., 2024).

En síntesis, la Figura 5 presenta el modelo conceptual derivado de la revisión sistemática, el cual resume los principales hallazgos en cuatro dimensiones: entradas (programas y métodos de formación), procesos (métricas conductuales, psicométricas y organizacionales utilizadas para su evaluación), factores moderadores (apoyo gerencial, cultura organizacional, gamificación avanzada, integración de IA y microlearning) y resultados (reducción de incidentes, cambios de conducta y retorno de inversión). Este esquema permite visualizar de manera integrada cómo los programas de concienciación generan impacto en la seguridad de la información organizacional.

Figura 5. Modelo conceptual derivado de la revisión sistemática: programas de concienciación, procesos de evaluación y resultados



Fuente: Elaboración propia.

4. CONCLUSIONES

En síntesis, los resultados presentados permiten inferir que la efectividad de los programas de concienciación y cultura de seguridad en las organizaciones depende de una combinación de estrategias: segmentación de perfiles, uso de gamificación y simulaciones, medición con escalas psicométricas multidimensionales, integración de métrica de ROI y comportamiento, métodos mixtos de evaluación (cuantitativos y cualitativos), automatización de controles y el firme apoyo gerencial. Solo así es posible garantizar cambios conductuales sostenibles, demostrando objetivamente la reducción de riesgos y el ROI de las iniciativas de seguridad. Por último, la incorporación de análisis predictivo mediante aprendizaje automático emerge como oportunidad para optimizar la evaluación de feedback y anticipar patrones de vulnerabilidad,

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

garantizando así un impacto real en la resiliencia corporativa.

Para futuros investigadores se recomienda someter las escalas existentes a estudios de validez cruzada en contextos latinoamericanos y sectores críticos (sanidad, banca y agroindustria), además de diseños longitudinales que abarquen de 12 a 24 meses para medir el efecto sostenido de formación, además de implementar entrenamientos para la concienciación de seguridad de la información que combinen gamificación, simulación y microlearning potenciados por inteligencia artificial, y para su evaluación se propone emplear marcos mixtos y psicometría de predicción dinámica.

Aunque cada una de estas metodologías han demostrado buenos resultados de forma independiente, aún no se han aplicado en conjunto; sin embargo, varios autores ya han empezado a mencionarlas. Se recomienda que las organizaciones interesadas en implementar las métricas mencionadas adopten inicialmente cuatro indicadores de evaluación continua (impacto, sostenibilidad, accesibilidad y monitorización) propuestos para programas de concienciación (Chaudhary et al. 2022), integrándose en un marco mixto de evaluación. Asimismo, complementar con programas formativos basados en juegos o simulaciones, apoyados en teoría en dosis controladas, permitirá disminuir de manera significativa la brecha de seguridad.

Contribución de los Autores (CRediT): JDGA: Conceptualización, Metodología, Investigación, Redacción-borrador original. IJMR: Conceptualización, Metodología, Investigación, Redacción-borrador original. CAMDLS: Supervisión, Redacción-revisión y edición.

Conflicto de Intereses: Los autores declaran que no existen conflictos de intereses en esta publicación.

REFERENCIAS

Arellano, F. J. G., Barraza, Í. D., Bustos, A. F., Soto, C. P., Fonseca, V. F., & Martínez-Peláez, R. (2024). Examining cybersecurity culture in Leon city organizations: Insights from 2022. *Ingeniare, Revista Chilena de Ingeniería*, *32*(1). https://doi.org/10.4067/s0718-33052024000100211

Baltuttis, D., Teubner, T., & Adam, M. T. (2024). A typology of cybersecurity behavior among knowledge workers. *Computers & Security*, *140*, 103741. https://doi.org/10.1016/j.cose.2024.103741

Beltrán Aldás. J. L. (2022). *Programa de concientización en seguridad de información para*

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

pequeñas empresas en la ciudad de Puyo [Tesis de maestría, Pontificia Universidad Católica del Ecuador] Repositorio PUCE. https://repositorio.puce.edu.ec/items/d257e331-1e2c-4155-8514-f5e7403dac69

Beltrán Muñoz, A. (2023). *Análisis de la educación en ciberseguridad: Situación actual, estrategias y retos* [Tesis doctoral, Universidad de Granada] Digibug. https://digibug.ugr.es/handle/10481/92804

Bitrián, P., Buil, I., Catalán, S., & Merli, D. (2024). Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours. *Journal of Business Research*, *179*, 114685. https://doi.org/10.1016/j.jbusres.2024.114685

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity, 8*(1). https://doi.org/10.1093/cybsec/tyac006

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*, 101747. https://doi.org/10.1016/j.cose.2020.101747

Fertig, T., Schütz, A. E., Weber, K. (2020). Current issues of Metrics for Information Security Awareness. *In Proceedings of the Twenty-Eighth European Conference on Information Systems (ECIS 2020) (pp. 1–3)*. Association for Information Systems. https://www.researchgate.net/publication/342803603

Furman, S., Haney. J., Jacobs, J. (2023, 15 septiembre). *Measuring the Effectiveness of U.S. Government Security Awareness Programs: A Mixed-Methods Study (Short Paper)*. NIST. https://www.nist.gov/publications/measuring-effectiveness-us-government-security-awareness-programs-mixed-methods-study

Garba, A. A., Siraj, M. M., & Othman, S. (2024). *Holistic Systematic Review on Methodologies of Assessing Effectiveness Cybersecurity Awareness Program*. Research Square. https://doi.org/10.21203/rs.3.rs-4329496/v1

Gerst, M., Kappe, M., Härting, R., & Karg, C. (2024). Determinants of the successful Establishment of a Cyber Security Culture in SMEs. *Procedia Computer Science*, *246*,

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

510–518. https://doi.org/10.1016/j.procs.2024.09.431

Grassegger, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *Procedia Computer Science*, *181*, 59-66. https://doi.org/10.1016/j.procs.2021.01.103

Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security*, *132*, 103364. https://doi.org/10.1016/j.cose.2023.103364

Jayatilaka, A., Beu, N., Baetu, I., Zahedi, M., Babar, M. A., Hartley, L., & Lewinsmith, W. (2021, 12 diciembre). *Evaluation of Security Training and Awareness Programs: Review of Current Practices and Guideline*. [Preprint]. arXiv. https://arxiv.org/abs/2112.06356

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers & Security*, *109*, 102383. https://doi.org/10.1016/j.cose.2021.102383

Nwankpa, J. K., & Datta, P. M. (2023). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. *Computers & Security*, *130*, 103266. https://doi.org/10.1016/j.cose.2023.103266

Nzeakor, O. F., Nwokeoma, B. N., Hassan, I., Ajah, B. O., & Okpa, J. T. (2022). Emerging Trends in Cybercrime Awareness in Nigeria. *International Journal of Cybersecurity Intelligence And Cybercrime*, *5*(3), 41-67. https://doi.org/10.52306/2578-3289.1098

Onduto, B. (2021). *Gamification of cyber security awareness – A systematic literature review* [Master's Thesis, University of Turku] UTUPub. https://www.utupub.fi/handle/10024/152929

Orehek, Š., & Petrič, G. (2020). A systematic review of scales for measuring information security culture. *Information And Computer Security*, *29*(1), 133-158. https://doi.org/10.1108/ics-12-2019-0140

Prümmer, J., Van Steen, T., & Van Den Berg, B. (2023). A systematic review of current

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

cybersecurity training methods. *Computers & Security*, *136*, 103585. https://doi.org/10.1016/j.cose.2023.103585

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, *9*(3), e14234. https://doi.org/10.1016/j.heliyon.2023.e14234

Rosado, D. G., Sánchez, L. E., Varela-Vaca, Á. J., Santos-Olmo, A., Gómez-López, M. T., Gasca, R. M., & Fernández-Medina, E. (2024). Enabling security risk assessment and management for business process models. *Journal of Information Security And Applications*, *84*, 103829. https://doi.org/10.1016/j.jisa.2024.103829

Susanto, T. D., & Maulana, M. D. (2024). Evaluating the Influence of Attitude versus Knowledge and Individual Factor versus Intervention Factor on Information Security Awareness in Local Government. *Procedia Computer Science*, *234*, 1428-1434. https://doi.org/10.1016/j.procs.2024.03.142

Solomon, A., Michaelshvili, M., Bitton, R., Shapira, B., Rokach, L., Puzis, R., & Shabtai, A. (2022). Contextual security awareness: A context-based approach for assessing the security awareness of users. *Knowledge-Based Systems, 246,* 108709. https://doi.org/10.1016/j.knosys.2022.108709

Taherdoost, H. (2024). A Critical Review on Cybersecurity Awareness Frameworks and Training Models. *Procedia Computer Science*, *235*, 1649-1663. https://doi.org/10.1016/j.procs.2024.04.156

Tejay, G. P., & Mohammed, Z. A. (2022). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management*, *60*(3), 103751. https://doi.org/10.1016/j.im.2022.103751

Thangavelu, M., Krishnaswamy, V., & Sharma, M. (2021). Impact of comprehensive information security awareness and cognitive characteristics on security incident management – an empirical study. *Computers & Security*, *109*, 102401. https://doi.org/10.1016/j.cose.2021.102401

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, 102387.

Fecha de recepción: 01 / 08 / 2025
Fecha de aceptación: 22 / 10 / 2025
Fecha de publicación: 20 / 02 / 2026

https://doi.org/10.1016/j.cose.2021.102387

Zanke, A., Weber, T., Dornheim, P., & Engel, M. (2024). Assessing information security culture: A mixed-methods approach to navigating challenges in international corporate IT departments. *Computers & Security*, *144*, 103938. https://doi.org/10.1016/j.cose.2024.103938