REVISTA
YACHAY
ISSN: 2412-2963
e-ISSN: 2520-9051

# Actualización del currículum universitario ante las vulnerabilidades digitales

**Lorenza Ríos**
Facultad de Educación, Escuela de Formación Pedagógica, Departamento de Currículum, Universidad de Panamá, Panamá.
lorenza.lin@up.ac.pa

**Ibrain Kadir Lin Ríos**
Facultad de Informática Electrónica y Comunicación (FIEC), Departamento de Informática, Universidad de Panamá, Panamá.
Ibrain.lin@up.ac.pa

**Recibido:** 20/12/2025
**Revisado:** 10/02/2026
**Aceptado:** 10/03/2026
**Publicado:** 25/03/2026

**Cómo citar:**

Ríos, L. y Lin Ríos, IK. (2026). Actualización del currículum universitario ante las vulnerabilidades digitales. *Yachay*, 15(1). e150102. DOI: 10.36881/yachay.v15i1.1281

**Fuente de financiamiento:**
La presente investigación no recibió financiamiento externo.

**Declaración de conflictos de interés:** los autores declaran no tener conflictos de intereses económicos, institucionales ni personal que puedan haber influido en los resultados o interpretación del presente artículo.

## Resumen

Las universidades enfrentan la contradicción de contar con la tecnología para transformar la educación y esta misma tecnología crea vulnerabilidades digitales que crecen exponencialmente, convirtiendo a las IES en blanco de los ciberdelincuentes. Esta investigación cualitativa con diseño de revisión de literatura analizó las bases para incorporar la seguridad informática en los currículos universitarios como competencia transversal. La muestra incluyó 32 documentos académicos, informes institucionales y marcos normativos (2001-2026) sobre competencia digital, ciberseguridad y diseño curricular. Los resultados muestran falta de integración porque las carreras técnicas han avanzado en asignaturas específicas, mientras que en ciencias sociales, educación, salud y derecho la ausencia es notable. Las vulnerabilidades detectadas son técnicas y formativas. Se identificó la desconexión entre las unidades técnicas de seguridad y las unidades académicas responsables del currículo. Como bases curriculares se proponen enfoques de integración que combinen transversalidad con espacios específicos, niveles, características de la competencia y estrategias didácticas como el aprendizaje basado en problemas y simulaciones. Se concluye que la actualización curricular es necesaria pero no suficiente, porque se requiere inversión en formación docente, coordinación interdisciplinar y análisis contextualizado por campo profesional.

**Palabras clave:** Elaboración del programa educativo, plan de estudios universitarios, programa de formación de docentes, programa obligatorio común, protección de datos, tendencia educacional.

# Updating the university curriculum in response to digital vulnerabilities

## Abstract

Universities face the contradiction of having the technology to transform education while this same technology creates exponentially growing digital vulnerabilities, making higher education institutions (HEIs) targets for cybercriminals. This qualitative research, using a literature review design, analyzed the foundations for incorporating cybersecurity into university curricula as a cross-cutting competency. The sample included 32 academic documents, institutional reports, and regulatory frameworks (2001-2026) on digital competence, cybersecurity, and curriculum design. The results show a lack of integration, as technical programs have made progress in specific subjects, while in social sciences, education, health, and law, the absence is notable. The vulnerabilities detected are both technical and educational. A disconnect was identified between technical security units and the academic units responsible for the curriculum. Curricular foundations are proposed for integration approaches that combine cross-cutting themes with specific spaces, levels, competency characteristics, and teaching strategies such as problem-based learning and simulations. It is concluded that curriculum updating is necessary but not sufficient, because investment in teacher training, interdisciplinary coordination, and contextualized analysis by professional

DOI: 10.36881/yachay.v15i1.1281

field are also required.

**Key words:** Educational program development, university curriculum, teacher training program, common core curriculum, data protection, educational trends.

## INTRODUCCIÓN

Las universidades se están enfrentando a una contradicción sin precedentes donde la tecnología está transformando los procesos de enseñanza y aprendizaje, así como la gestión institucional, al mismo tiempo que la vulnerabilidad digital aparece como una amenaza en crecimiento que va poniendo en riesgo los datos institucionales y la formación de los estudiantes. La velocidad a la que se desarrolla la inteligencia artificial, el aumento del *phishing*, los *deepfakes* y de los ataques de *ransomware* han hecho que las Instituciones de Educación Superior (IES) sean el blanco de los ciberdelincuentes (Robert et al., 2024). El problema de la ciberseguridad dejó de ser un problema de ingenieros o de los departamentos de sistemas; el hecho de que las universidades sean un blanco fácil de hackers por la cantidad de datos valiosos que manejan y su cultura de libre acceso, está obligando a pensar qué se enseña y cómo se enseña, es decir, integrar esta reforma en los planes de estudios y en la práctica docente.

El problema que aborda esta investigación se sitúa entre dos áreas del conocimiento que forman una intersección entre la transformación digital universitaria y la formación en competencias digitales para la seguridad: educación universitaria desde la formación pedagógica y currículum, y la auditoría de sistemas. Aunque las universidades han avanzado en la integración de la tecnología digital en sus procesos educativos, todavía falta incorporar la ciberseguridad como componente curricular transversal (Barberá-Gregori & Suárez-Guerrero, 2021).

En América Latina, los datos indican que en el período 2023-2024 hubo un aumento del 56% en ataques contra las instituciones de enseñanza e investigación en Brasil, de acuerdo con la Red Nacional de Enseñanza e Investigación (RNP) de Brasil (Schmidt, 2025). IQSEC, una empresa de ciberseguridad también presentó un reporte en el año 2024 donde registraba 388 incidencias por día en IES de Latinoamérica (Castañeda Girón, 2024). Para el segundo trimestre de 2024, el sector educativo fue registrado como el más atacado a nivel mundial, con un promedio de 3,086 ataques semanales por organización (Check Point, 2024). Para el tercer trimestre de 2024, estudios de ciberseguridad mencionados en análisis sectorial cuantificaron que América Latina era la tercera región más atacada del mundo con un incremento interanual de amenazas superior al 72% (LinkedIn, 2025).

A estos datos se le añade que las titulaciones universitarias integran la competencia digital de manera desigual, pues mientras las carreras técnicas incorporan indicadores de alfabetización tecnológica, otras áreas del conocimiento desarrollan la alfabetización informacional sin tratar sistemáticamente las áreas éticas, de privacidad y seguridad que requiere el entorno digital contemporáneo (Fernández-Sánchez & Quiroz, 2022).

Centrándose en la relación entre estas dos áreas, la pregunta de investigación ¿de qué manera se incorpora la seguridad informática como componente curricular en los planes de estudio universitarios?, define el objetivo de este estudio que es analizar los fundamentos que sustentan la incorporación de la seguridad informática en los planes de estudio universitarios. La hipótesis que lo orienta sostiene que la actualización del currículum universitario para incorporar la seguridad informática como competencia transversal es una condición necesaria para formar profesionales que sean capaces de responder a este tipo de vulnerabilidades digitales contemporáneas.

El estudio tiene relevancia social, ya que formar a los profesionales para que sean conscientes de los riesgos informáticos y que estén capacitados para actuar de forma preventiva contribuye a la seguridad institucional y a fortalecer la cultura digital responsable en la sociedad (OEA, 2025). La pertinencia institucional proviene de reconocer que las universidades resguardan importantes datos de investigación e información personal de estudiantes y docentes, por lo que se necesita que toda su comunidad y no solamente los especialistas en tecnologías, comprenda y aplique los principios básicos de seguridad digital (Organización de Estados Iberoamericanos, 2022). También se debe justificar su oportunidad disciplinar, porque desde la especialidad de currículum y formación pedagógica es necesario realizar este tipo de investigaciones que permitan explicar los problemas tecnológicos y transformarlos en propuestas educativas para situar el problema en el terreno de la formación integral del estudiante.

Los antecedentes de esta investigación se enmarcan en dos líneas que convergen. Por un lado, los estudios sobre competencia digital en educación superior han experimentado un desarrollo importante en la última década. Analizando el nivel de integración de la competencia digital en los planes de estudio, Sánchez-Caballé et al. (2021) demostraron las diferencias entre las áreas de conocimiento y la necesidad de contar con enfoques institucionales más coherentes. En la otra línea de investigación, los estudios sobre ciberseguridad a nivel universitario han documentado el incremento de amenazas y las particularidades que hacen vulnerables a las IES por la existencia de sistemas fragmentados, brechas de habilidades en materia de seguridad y financiamiento insuficiente para proteger las infraestructuras consideradas críticas (Robert et al., 2024).

Un antecedente considerado relevante lo constituyen los marcos de competencia digital desarrollados por organismos internacionales como el DigComp 2.1 de la Unión Europea (Pozo-Sánchez et al., 2022) que incluyen áreas relacionadas con la seguridad y la resolución de problemas. Sin embargo, estos marcos han sido implementados de manera desigual en las IES, y su traslado a los diseños curriculares todavía está pendiente en muchos contextos universitarios.

DOI: 10.36881/yachay.v15i1.1281

Esta investigación expone el tema de la seguridad informática en la educación universitaria desde una perspectiva interdisciplinaria que fusiona el campo pedagógico y curricular con el técnico de los sistemas de información. La integración ayuda a evitar centrarse solamente en el aspecto tecnológico centrado en las infraestructuras, para analizar cómo los planes de estudio pueden formar profesionales que sean conscientes y que tengan una visión preventiva ante los riesgos digitales. Se parte de la premisa de que las vulnerabilidades digitales también son curriculares, al demostrarse que la falta de formación de los estudiantes para el entorno digital de la actualidad es parte de la solución ante la evolución de amenazas como el *phishing* o los *deepfakes* que han sido impulsados por la inteligencia artificial (Cybersecurity and Infrastructure Security Agency [CISA], 2023).

## Material y método

Todo el estudio se enmarca en un enfoque cualitativo con un diseño de revisión de literatura. El alcance es descriptivo y analítico para caracterizar la actualidad de la incorporación de la seguridad informática en los currículos universitarios y analizar las bases curriculares que lo sustentan. Se ha considerado un diseño adecuado por cuanto el objetivo es sintetizar el conocimiento sobre un fenómeno emergente y multidimensional como la relación entre ciberseguridad y currículum universitario (Sánchez-Caballé et al., 2021).

La población corresponde a la literatura académica y los informes institucionales sobre competencia digital, ciberseguridad en educación superior y diseño curricular universitario. Para seleccionar la muestra se utilizó el muestreo intencional basado en la pertinencia temática, la relevancia académica y la actualidad de los temas. La muestra final de 32 referencias se clasificó en las siguientes categorías:

**Artículos de revistas científicas indexadas**: representan la base de la literatura especializada donde se incluyeron estudios empíricos y revisiones teóricas publicadas en revistas de alto impacto como RIED y Educar, y bases de datos reconocidas (como los estudios de Sánchez-Caballé et al., 2021; Fernández-Sánchez & Quiroz, 2022; Orosco-Fabian, 2024). Estas fuentes resultaron fundamentales para contrastar los hallazgos sobre competencia digital e integración curricular.

**Informes de organismos internacionales y entidades de ciberseguridad:** se consultaron documentos de la UNESCO (2011), la OEI (2012), la OEA (2025), EDUCAUSE (Robert et al., 2024) y CISA (Cybersecurity and Infrastructure Security Agency, 2023). Estos informes contienen datos macros sobre tendencias, políticas educativas y el panorama global de las amenazas digitales que otorgaron el marco contextual al estudio.

**Fuentes institucionales y del sector educativo:** se incluyeron programas de universidades (Excelsior University, 2025; Cambridge College, 2025) que se utilizaron para ejemplificar los enfoques curriculares; también se utilizaron análisis de empresas de ciberseguridad como Kaspersky (2026) y Check Point (2024) las cuales, aunque no son académicas, son muy actuales y documentan con cifras la realidad de los ataques.

**Documentos normativos y legislativos:** se incorporaron marcos de competencias como la Recomendación del Parlamento Europeo (Parlamento Europeo & Consejo de la Unión Europea, 2006) y el proyecto DeSeCo de la OCDE (Rychen & Salganik, 2001), porque a partir de ellos se realizó el rastreo sobre el origen y la evolución de los llamados a integrar la competencia digital desde principios de la década del 2000.

**Tesis doctorales y literatura gris:** se consideró una tesis doctoral (Rodríguez Jiménez, 2024) y artículos de profesionales publicados en plataformas como LinkedIn (Rojas, 2024) o medios especializados como *Times Higher Education* (Rowsell, 2024), para complementar el análisis, ya que son estudios que cuentan con diferentes niveles de revisiones por pares.

La escogencia de la bibliografía combinó pedagogía, currículum, tecnología y políticas públicas para demostrar la interdisciplinariedad del tema. Al incluir informes de ciberseguridad de los años 2024 al 2026 y estudios empíricos recientes se demuestra la actualidad y pertinencia. Además de ello, el nivel académico se expresa en el uso de revistas indexadas y marcos de referencia internacionales (Unesco, OCDE, UE) y considera el contexto, al incluir estudios y reportes sobre América Latina (Okoye et al., 2023; Orosco-Fabian et al., 2025; Schmidt, 2025).

Como técnica se utilizó el análisis documental, complementado con la revisión bibliográfica, utilizando como instrumento una matriz de análisis documental en hoja de cálculo diseñada para registrar autores, año, tipo de documento, enlace o DOI, objetivo general, metodología, resultados principales sobre integración curricular de la ciberseguridad, vulnerabilidades identificadas y propuestas curriculares.

La información se procesó organizando los documentos recuperados y clasificándolos según su aporte en las siguientes categorías: integración curricular de ciberseguridad, vulnerabilidades digitales en IES, bases curriculares y marcos de competencia digital. Posteriormente se realizó el análisis de contenido aplicando la técnica de análisis temático para identificar convergencias y divergencias en la literatura, de acuerdo con los lineamientos citados en Sánchez-Caballé et al. (2021). Finalmente, se realizó una agrupación de categorías para definir temas y el orden de la presentación de los resultados del estudio.

## Resultados

Para comprender el alcance de los resultados que se presenta a continuación, se deben situar en el contexto de los antecedentes que desde hace más de una década han venido llamando la atención sobre la necesidad de incorporar la competencia digital (y dentro de ella la seguridad) en la formación de los profesionales.

### Antecedentes

DOI: 10.36881/yachay.v15i1.1281

**2001:** la OCDE, a través del proyecto DeSeCo, sienta las bases teóricas y conceptuales de las competencias para la sociedad de la información (Rychen & Salganik, 2001).

**2006:** el Parlamento Europeo incluye oficialmente la competencia digital como clave para el aprendizaje permanente en la Recomendación 2006/962/CE (Parlamento Europeo & Consejo de la Unión Europea, 2006).

**2010-2012:** la estrategia Europa 2020 y el desarrollo inicial del marco DigComp refuerzan este llamado (Ferrari, 2012).

**2011**: la UNESCO (2011) publica el marco de competencias TIC para docentes, que incluye áreas de seguridad.

**2012:** la OEI incorpora las competencias digitales en las Metas Educativas 2021 (Organización de Estados Iberoamericanos, 2012).

**2013:** el marco DigComp 1.0 refuerza la seguridad como un área específica de la competencia digital (Pozo-Sánchez et al., 2022).

A pesar de estas referencias, los resultados de la investigación son una evidencia de que la incorporación de la ciberseguridad en los currículos universitarios todavía no se ha llegado a generalizar.

### Integración de la ciberseguridad en los currículos universitarios

La incorporación de contenidos de ciberseguridad en los planes de estudio se concentra casi exclusivamente en las carreras técnicas. Los programas de ingeniería informática, sistemas de información y carreras afines han avanzado en la inclusión de asignaturas específicas sobre seguridad digital, hacking ético, criptografía y análisis forense, como respuesta a la demanda del mercado laboral y a la necesidad de satisfacer los estándares internacionales de formación (Excelsior University, 2025).

Es una tendencia que se observa en las IES de los países subdesarrollados y en las universidades latinoamericanas que han empezado a rediseñar sus planes de estudio para incorporar estas competencias (Orosco-Fabian, 2024). Sin embargo, en las áreas de ciencias sociales, humanidades, educación, derecho y ciencias de la salud, la presencia de la ciberseguridad en los currículos es prácticamente inexistente o, en el mejor de los casos, se menciona de manera tangencial y no sistemática (Rojas, 2024).

Este desfase disciplinar es preocupante si se considera que los egresados de estas carreras se insertarán en áreas profesionales que están mediadas por tecnologías digitales donde la protección de datos, la privacidad y la seguridad de la información son características del ejercicio profesional (da Costa Faria et al., 2026). La ausencia de formación en estas áreas la explican Orosco-Fabian et al. (2025), quienes constataron que, aunque los estudiantes utilizan cotidianamente las tecnologías digitales, les falta formación específica que les permita identificar y gestionar los riesgos asociados a su uso profesional.

### Tipo de enfoque pedagógico predominante

En las carreras donde se ha incorporado la ciberseguridad se identifican dos enfoques que están claramente diferenciados: el instrumental-técnico, y el informacional-actitudinal.

**Instrumental y técnico:** está centrado en el manejo de las herramientas específicas, los protocolos de seguridad y aspectos fundamentales. Es propio de las ingenierías y carreras técnicas, y forma a los estudiantes como operadores de sistemas de seguridad, pero no necesariamente les desarrolla la comprensión de las implicaciones éticas, sociales y legales de la seguridad digital (Excelsior University, 2025).

Los programas de grado en ciberseguridad que ofrecen las universidades internacionales son un ejemplo de esta orientación, con currículos que enfatizan las competencias en seguridad de redes, análisis forense digital, respuesta a incidentes y preparación para certificaciones técnicas como "CompTIA Security + y Certified Information Security Manager (CISM)" (Cambridge College, 2025, secc. 4).

**Informacional y actitudinal:** predomina en las pocas experiencias de incorporación de ciberseguridad en carreras que no son técnicas, donde se contempla la alfabetización digital básica, el uso seguro de plataformas y la concientización sobre los riesgos tipo *phishing* o de suplantación de identidad (Rodríguez Jiménez, 2024). Sin embargo, este enfoque muy pocas veces alcanza el nivel de profundidad necesario para formar profesionales capaces de gestionar los desafíos de ciberseguridad que son propios de cada campo disciplinar como la protección de datos clínicos en ciencias de la salud, la seguridad de las transacciones financieras en administración o la privacidad de los expedientes educativos en pedagogía (Rojas, 2024).

La investigación de Rodríguez Jiménez (2024) con estudiantes de Ciencias de la Educación de la Universidad de Granada confirma que, a pesar de que la seguridad digital aparece como contenido transversal en los programas de estudio, termina siendo el área menos desarrollada de la competencia digital en la formación inicial de los futuros docentes.

### Presencia de la ciberseguridad en los perfiles de egreso

Se constató que la mayoría de las universidades carecen de declaraciones sobre competencias en ciberseguridad en los perfiles de egreso de las titulaciones. Cuando aparecen, lo hacen a modo de denominaciones genéricas como 'competencia digital' o 'uso ético de las tecnologías', sin especificar las dimensiones relacionadas con la protección de datos, la privacidad o la seguridad de la información (da Costa Faria et al., 2026).

Esa ausencia contrasta con el reconocimiento institucional que se está dando a la importancia de la ciberseguridad. Diversos organismos internacionales han desarrollado marcos de competencia digital que incluyen la seguridad, como sucede con el Marco Europeo de Competencia Digital DigComp 2.1 que define la competencia digital como el uso seguro, crítico y creativo de las tecnologías e identifica la seguridad como una de las cinco áreas clave, cubriendo la protección

de dispositivos, la protección de los datos personales, la protección de la salud y la protección del entorno (Orosco-Fabian et al., 2025). Sin embargo, la conversión de estos marcos a diseños curriculares para las IES todavía no se concreta.

Orosco-Fabian (2024) identificó teóricamente que, sobre la producción científica en ciberseguridad y educación superior, este campo ha experimentado un crecimiento exponencial desde el año 2018, con un énfasis en temas de conciencia en ciberseguridad, violación de la ciberseguridad y educación en ciberseguridad. Este incremento de la producción científica es un reflejo de la preocupación académica por la formación en esta área, pero también demuestra que la investigación todavía no se ha convertido en una transformación curricular.

### Vulnerabilidades digitales que afectan a las IES

En este punto se expone una realidad donde se combinan las debilidades técnicas e institucionales con las carencias formativas que se encuentran arraigadas y representan un riesgo para las IES ante las amenazas que cada vez son más sofisticadas. Se describen las técnico-institucionales y las vinculadas con la formación de los miembros de la comunidad universitaria.

**Técnicas e institucionales:** las IES presentan características que las convierten en espacios muy vulnerables desde el punto de vista técnico y organizacional. La primera y más relevante es la fragmentación de los sistemas informáticos, que es la existencia de una arquitectura tecnológica descentralizada conformada por sistemas, plataformas y bases de datos que funcionan de manera independiente, frecuentemente con poca integración entre sí, y que son gestionados por distintas unidades académicas o administrativas que no mantienen una coordinación central (Pathify, 2025).

A diferencia de las empresas privadas, donde existe una arquitectura tecnológica centralizada que funciona de forma homogénea, históricamente las universidades han desarrollado o adquirido en las facultades, los departamentos y los centros de investigación sus propias soluciones tecnológicas de manera autónoma (Lawinski, 2026). Es una situación que dificulta implementar políticas de seguridad uniformes y crea múltiples puntos de entrada potenciales para los ciberdelincuentes (Robert et al., 2024).

Esta fragmentación se agrava por el hecho de que los planes de estudio siguen dándole prioridad a la alfabetización tecnológica funcional, en vez de hacerlo desde la seguridad digital y la ciudadanía digital crítica (Cortes Coss, 2024), generando una falta de conexión entre la infraestructura tecnológica y la formación curricular que es más preocupante si se considera que los ataques contra las universidades aumentan con dos objetivos: robar datos de información personal de los estudiantes, empleados e investigadores para exigir rescates económicos mediante *ransomware* (Kwon, 2025).

La obsolescencia tecnológica también es un factor de vulnerabilidad, demostrado en el hecho de que muchas universidades, particularmente en contextos de restricción presupuestaria, funcionan con hardware y software que ya superaron su ciclo de vida útil, lo que implica que no cuentan con actualizaciones de seguridad y parches críticos que proporcionan los mismos fabricantes (Rowsell, 2024).

El análisis de incidentes de seguridad reportados en el sector educativo durante el período 2025-2026 muestra el incremento exponencial de los ataques de *ransomware* dirigidos a las universidades. Kaspersky Team (2026) documenta cómo las IES grandes como la Universidad La Sapienza de Roma han sufrido interrupciones de sus sistemas durante días, y eso demuestra la vulnerabilidad del entorno académico. El gobierno del Reino Unido (citado en el informe Kaspersky) reportó que el 91% de las universidades británicas se han visto afectadas por incidentes cibernéticos, mientras que otros estudios estadounidenses señalan un aumento global del 69% en los ataques de este tipo al sector educativo durante el primer trimestre de 2025 en comparación con el año anterior.

Se indica que el problema de fondo está en la digitalización tan rápida que se ha dado en los servicios universitarios que van desde las plataformas de aprendizaje a distancia hasta los sistemas de admisión y almacenamiento en la nube, que han aumentado la magnitud del ataque. El mismo estudio señala que, al haber permanecido el sector educativo durante años fuera del foco de los ciberdelincuentes, la formación en ciberseguridad para el personal y los estudiantes nunca fue una prioridad. Esta es una carencia formativa que convierte incluso a los docentes con más experiencia en blancos vulnerables ante las campañas de *phishing,* y expone a las redes universitarias a riesgos provenientes de prácticas cotidianas como el uso de las memorias USB infectadas que circulan entre los dispositivos personales y los de las IES.

Esas campañas de *phishing* dirigido se han consolidado como una de las amenazas más frecuentes porque son las que más éxito tienen a nivel universitario y los atacantes explotan la estructura abierta y la cultura de colaboración que caracteriza a las instituciones académicas para diseñar las campañas de suplantación de identidad personalizadas, que están dirigidas al personal administrativo con acceso a los sistemas sensibles, y a los investigadores que manejan propiedad intelectual. Esto se ve potenciado por la alta rotación de la comunidad universitaria por el ingreso anual de nuevos estudiantes, la incorporación de personal temporal y visitantes internacionales; así se dificulta mantener programas de concientización continuos y actualizados (Cybersecurity and Infrastructure Security Agency [CISA], 2023). Aunque se confía en medidas de seguridad perimetral tradicionales que son insuficientes ante las amenazas mencionadas, la falta de evaluaciones periódicas de vulnerabilidades, pruebas de penetración y planes de respuesta a incidentes actualizados es una debilidad que incrementa el impacto potencial de cualquier ataque exitoso.

**Formativas:** son vulnerabilidades que se subestiman desde los enfoques tradicionales de ciberseguridad, y son el eslabón más débil en la cadena de protección institucional. La primera que detectan los especialistas en seguridad de la información

DOI: 10.36881/yachay.v15i1.1281

es la relacionada con el desconocimiento generalizado de las prácticas básicas de seguridad por parte de los estudiantes, docentes y personal administrativo. Aunque utilicen tecnologías digitales, no necesariamente cuentan con formación que les permita identificar las amenazas, tomar conductas preventivas y responder ante los incidentes de forma adecuada (Sánchez-Caballé et al., 2021).

Se trata de un déficit formativo que se manifiesta en prácticas habituales como el uso de una sola contraseña en múltiples servicios, el desconocimiento de los riesgos asociados a la conexión de redes públicas que no son seguras, la incapacidad para identificar correos de *phishing* y el almacenamiento inadecuado de información sensible. Hay que añadir que a la mayor parte de las universidades le faltan programas de alfabetización en seguridad digital que estén dirigidos a toda la comunidad y, cuando existen, son iniciativas aisladas o voluntarias que no tienen el debido alcance (Sánchez-Caballé et al., 2021).

En el contexto latinoamericano, se confirma que las principales barreras para la integración de las tecnologías digitales en educación superior no son exclusivamente técnicas. Okoye et al. (2023) realizaron un estudio en nueve países de la región, identificando que la falta de formación (*training*) constituye uno de los principales desafíos para el proceso de enseñanza-aprendizaje, junto con las limitaciones de infraestructura y acceso a las plataformas digitales. Este dato es un hallazgo que refuerza la tesis de que las vulnerabilidades digitales también son básicamente de orden curricular y formativo.

Con estos incidentes de seguridad se puede establecer una relación directa entre los niveles de formación y las tasas de incidentes, dado que las IES han implementado programas de concientización reportan menores tasas de incidentes relacionados con factores humanos, particularmente en lo que respecta a los ataques de *phishing* y suplantación de identidad. Solo en las universidades donde no existen estos programas se ha experimentado una mayor cantidad de incidencia de brechas de seguridad derivadas de errores humanos, configuraciones inseguras y prácticas de riesgo por parte de los usuarios (Robert et al., 2024).

Los docentes e investigadores cuentan con propiedad intelectual y datos de investigación sensibles, presentando necesidades formativas que muy pocas veces son atendidas por los programas institucionales. La presión por publicar, la colaboración internacional y la movilidad académica los exponen a robos de propiedad intelectual, espionaje académico y filtraciones de datos (Orosco-Fabian, 2024).

Las unidades técnicas, que son las responsables de la seguridad informática, también están desconectadas de las unidades académicas que están encargadas de la formación. Son capaces de identificar las vulnerabilidades y los patrones de comportamiento de riesgo, pero no lo comunican a quienes diseñan los planes de estudio y esta es una forma de perder una oportunidad valiosa para orientar la formación hacia las verdaderas necesidades, confirmando que el desequilibrio entre el saber técnico y el pedagógico es parte de lo que mantiene esa falta de protección tan necesaria (Sánchez-Caballé et al., 2021).

## Integración de la seguridad informática en la universidad

Del planteamiento anterior surge la necesidad de establecer principios pedagógicos y curriculares que orienten la incorporación de la seguridad informática en la formación universitaria. Se identificaron las bases y se organizan en cuatro bloques: integración curricular, niveles de formación, características de la competencia y estrategias didácticas.

**Integración curricular:** la decisión para las IES es cómo incorporar la seguridad informática en los planes de estudio, y se identifican dos puntos que no son excluyentes sino complementarios. El primero es con respecto a las asignaturas específicas, que crea espacios curriculares que se dediquen exclusivamente a la seguridad digital. Este modelo, adoptado por carreras técnicas como las descritas por Excelsior University (2025) o Cambridge College (2025), mejora el nivel de especialización, pero no es viable para todas las titulaciones y puede reforzar la idea de que la seguridad es algo exclusivamente para los técnicos.

El segundo es el tratamiento transversal, que propone desarrollar competencias en seguridad a lo largo del currículo, integradas en diversas asignaturas y adaptadas a cada disciplina. Como señalan Sánchez-Caballé et al. (2021) las áreas que no son técnicas necesitan un enfoque diferente a los de las ingenierías. Este modelo reconoce que un abogado debe formarse en protección de datos, un docente en privacidad de expedientes educativos y un administrador en seguridad de transacciones financieras (Rojas, 2024). De acuerdo con la revisión, se entiende que los modelos más exitosos combinan una base común transversal para todos los estudiantes y espacios de especialización para quienes lo requieran.

**Niveles de formación:** deben graduarse según las necesidades de cada perfil profesional. Primero está la alfabetización en seguridad digital, dirigida a toda la comunidad universitaria y comprende competencias como la gestión segura de contraseñas, identificación de *phishing* y configuración básica de privacidad (da Costa Faria et al., 2026), porque son la base que cualquier profesional necesita.

El segundo nivel son las competencias profesionales en seguridad digital orientadas a todos los graduados con independencia de su disciplina, pero contextualizadas en cada campo. En este nivel se profundiza en lo que implica específicamente la seguridad en el ejercicio profesional como sucede con la protección de datos clínicos en salud o la privacidad de los expedientes en educación (Rodríguez Jiménez, 2024). El tercer nivel es la especialización en ciberseguridad, que está reservada para quienes se van a dedicar profesionalmente a este campo, con competencias técnicas avanzadas en áreas como el análisis forense o la auditoría de sistemas (Excelsior University, 2025). De esta forma se puede ajustar la formación según las necesidades sin sobredimensionar los currículos.

**Características de la competencia:** la competencia en

seguridad digital debe concebirse como multidimensional, que va más allá del enfoque técnico. El Marco Europeo DigComp 2.1 (Pozo-Sánchez et al., 2022) ofrece una referencia importante al identificar la seguridad como un área clave. A partir de este y otros marcos se identifican cuatro características.

1) La técnica comprende el conocimiento y manejo de herramientas, protocolos y procedimientos de seguridad. Es la más desarrollada en la formación de los especialistas, pero por lo general está ausente en otras áreas (Sánchez-Caballé et al., 2021). 2) La ética se refiere a los principios que orientan el comportamiento en los entornos digitales: respeto a la privacidad, responsabilidad sobre la información compartida e integridad en el manejo de los datos (OEA, 2025).

3) La legal comprende el conocimiento de la normativa aplicable como la protección de los datos personales que cada día cobra más relevancia en el ejercicio profesional (da Costa Faria et al., 2026). 4) La social y crítica implica la capacidad de analizar las consecuencias de la seguridad digital como las desigualdades en el acceso, las políticas de vigilancia y la participación informada en los debates públicos (Cortes Coss, 2024). Integrar estas cuatro características de forma equilibrada es un verdadero reto en los procesos curriculares.

**Estrategias didácticas:** la enseñanza de la seguridad informática se debe presentar con estrategias con metodologías participativas y contextualizadas (conocidas como activas y situadas). El aprendizaje basado en problemas ABP es pertinente, porque presenta a los estudiantes escenarios de vulnerabilidad o ataque adaptados a cada área profesional (Rodríguez Jiménez, 2024). Las simulaciones de incidentes también permiten experimentar en entornos controlados la presión de una crisis de seguridad, practicando situaciones de detección, respuesta y comunicación (Robert et al., 2024).

Cuando se analizan casos reales como los ataques a las universidades descritos por Kwon (2025) o Kaspersky (2026), se alcanza el aprendizaje significativo sobre las causas, consecuencias y lecciones aprendidas que mejora los resultados académicos como la capacidad de transferir el conocimiento a contextos profesionales (Olivan-Blázquez et al., 2022). Los proyectos interdisciplinarios ofrecen la oportunidad de abordar la seguridad digital desde diferentes perspectivas, integrando a estudiantes de distintas carreras (Sánchez-Caballé et al., 2021). Por otro lado, las actividades de concientización que se dirigen a toda la comunidad universitaria complementan la formación curricular y ayudan a crear una cultura institucional de seguridad digital (Okoye et al., 2023).

## Discusión

Incorporar la seguridad informática en los currículos universitarios no es sencillo y los resultados confirman que la incorporación de la ciberseguridad en los planes de estudio se concentra prácticamente en las carreras técnicas, mientras que en ciencias sociales, humanidades, educación y salud es prácticamente inexistente. El contraste coincide con Sánchez-Caballé et al. (2021) cuando explican que las titulaciones más técnicas integran indicadores de alfabetización tecnológica, mientras que otras áreas del conocimiento desarrollan básicamente la alfabetización informacional. A más de una década de los primeros llamados a integrar la competencia digital de forma transversal, esta es una señal de que existe más resistencia al cambio curricular de lo que se pensaba.

Una posible explicación la ofrece Cortes Coss (2024), al hablar de la concepción restringida de la seguridad informática, según la cual las IES consideran que la ciberseguridad es un asunto técnico y aunque se debe enseñar a la comunidad universitaria a identificar los sitios seguros "en muchas carreras sobre todo de ingeniería existe una materia en el plan de estudios que tiene como objeto este tema, sin embargo; en la mayoría de las carreras universitarias no se contempla" (p. 84). Al ser una visión arraigada en las culturas institucionales, se explica por qué los marcos de competencia digital como DigComp 2.1 (Pozo-Sánchez et al., 2022), que incluyen explícitamente la seguridad, no llegan a convertirse en cambios curriculares para las universidades.

Orosco-Fabian (2024) aporta un dato relevante cuando señala que, aunque la producción científica sobre ciberseguridad en educación superior ha crecido exponencialmente desde el año 2018, no ha impactado en el cambio curricular generalizado. Es decir, que la investigación y la práctica curricular se encuentran desconectadas, porque se demuestra que los canales de transferencia del conocimiento académico a las políticas institucionales son prácticamente inexistentes.

Otro hallazgo de este estudio es la confirmación de que las vulnerabilidades formativas son el eslabón más débil en la cadena de protección institucional. Los datos aportados por Kaspersky (2026) sobre el impacto del *ransomware* en universidades europeas, y los de Kwon (2025) sobre las consecuencias de los ciberataques para la investigación adquieren otra magnitud cuando se interpretan desde esta perspectiva, dado que son problemas de formación y no técnicos como es la creencia general.

La investigación de Rodríguez Jiménez (2024) con estudiantes de Ciencias de la Educación indica que, aunque la seguridad digital aparece como contenido transversal en los programas de estudio, es el área menos desarrollada de la competencia digital en la formación inicial de los estudiantes de docencia. Se puede comparar este desbalance entre la declaración curricular y el desarrollo de las competencias con lo observado por Okoye et al. (2023) en nueve países latinoamericanos, donde la falta de formación es uno de los principales obstáculos para el proceso de enseñanza-aprendizaje con tecnologías digitales.

Al estudiar la diferencia entre la percepción de seguridad y la preparación de los usuarios universitarios presentada por Robert et al. (2024) se encuentra una explicación convincente, porque si los estudiantes y docentes no reciben formación en seguridad digital, muy difícilmente pueden identificar las amenazas posibles, tener conductas preventivas o responder a los incidentes y esta conclusión refuerza la base de este estudio, de que las vulnerabilidades digitales también son

DOI: 10.36881/yachay.v15i1.1281

curriculares.

Cuando se trata de la desconexión encontrada entre las unidades técnicas responsables de la seguridad informática y las instancias académicas encargadas de la formación documentada por Sánchez-Caballé et al. (2021), hay que pensar en las implicaciones que tiene para el desarrollo curricular. Por un lado están las unidades técnicas que generan conocimiento sobre las vulnerabilidades que afectan a las IES, cuáles son los patrones de comportamiento de riesgo de los usuarios y las amenazas que surgen cada día, pero es un conocimiento que no se comunica a los que diseñan los planes de estudio y se pierde una oportunidad invaluable de orientar la formación hacia esas necesidades. Por otro lado, esa falta de conocimiento de las unidades académicas lleva a diseñar currículos sin considerar esa realidad tecnológica y los riesgos que enfrentarán los egresados en su ejercicio profesional.

El caso se agrava por la fragmentación de sistemas que explican Pathify (2025) y Lawinski (2026), porque es una debilidad que solamente se puede afrontar con mecanismos institucionales de coordinación y diálogo interdisciplinar. Las universidades que han avanzado en este aspecto (Robert et al., 2024) muestran tasas menores de incidentes relacionados con factores humanos, lo que refuerza la importancia de su integración.

Las bases curriculares propuestas en esta investigación están respaldadas en las fuentes utilizadas, pero también se plantean preguntas sobre su viabilidad cuando se interponen los recursos. La propuesta de combinar enfoques transversales con asignaturas específicas, inspirada en las recomendaciones de Excelsior University (2025) y Cambridge College (2025) parece ser lo más prometedor, pero también se deben considerar los contras en las universidades públicas latinoamericanas que cuentan con limitaciones presupuestarias graves (Rowsell, 2024). Presentarlo por niveles, aunque es lógico desde el aspecto pedagógico, necesita de otros análisis sobre las necesidades de cada campo profesional y muy pocas instituciones lo han realizado.

Las cuatro características de la competencia en seguridad digital que se derivan de los marcos DigComp 2.1 (Pozo-Sánchez et al., 2022) y las recomendaciones de la OEA (2025) ofrecen una visión más amplia que supera los enfoques reduccionistas. Sin embargo, para implementarlo se necesita que el profesorado esté formado en las áreas técnicas, éticas, legales y sociales (DigComp 2.1), un problema de formación docente identificado por Rodríguez Jiménez (2024) y Okoye et al. (2023).

Las estrategias didácticas propuestas son consistentes con las recomendaciones de la literatura sobre educación en ciberseguridad que ofrecen Robert et al. (2024) y da Costa Faria et al. (2026), pero para su aplicación se necesitan las condiciones institucionales de tiempo, recursos, formación docente e infraestructura, que no siempre están garantizadas.

### Limitaciones y futuras líneas de investigación

Se deben considerar dos aspectos como limitantes: a) el área de ciberseguridad toma en cuenta que las vulnerabilidades identificadas evolucionan rápidamente y esto debe reflejarse en las propuestas curriculares, que necesitarían ser actualizadas continuamente; b) el estudio es teórico y no de campo, por lo que no aporta datos propios para contrastar sus resultados con la realidad presentada por los autores; sin embargo, en otras investigaciones por realizar se pueden considerar al menos tres líneas.

La primera sería la de estudios empíricos que evalúen el nivel de competencias en seguridad digital de los estudiantes y docentes en las IES panameñas, utilizando instrumentos validados como el que han desarrollado Orosco-Fabian et al. (2025). La segunda serían investigaciones-acción que implementen y evalúen estudios piloto con la incorporación de la ciberseguridad en distintas disciplinas, para documentar bajo qué condiciones logran ser exitosas y cuáles son los obstáculos. La tercera línea estaría conformada por estudios comparativos que analicen cómo las universidades presentan este desafío, identificando las buenas prácticas y qué puede ser transferido a otros contextos.

## Conclusiones

Se analizaron los fundamentos para incorporar la seguridad informática en los planes de estudio universitarios, partiendo de la hipótesis de que su actualización como competencia transversal es una condición necesaria para formar profesionales capaces de responder a las vulnerabilidades digitales de la actualidad. Por lo tanto, los hallazgos permiten concluir lo siguiente:

La integración de la ciberseguridad en los currículos universitarios es desigual, ya que mientras las carreras técnicas han avanzado en la inclusión de asignaturas específicas y competencias especializadas, en el área de las ciencias sociales, humanidades, educación, derecho y salud el nivel de formación es muy bajo. Esa diferencia se considera una brecha disciplinar que contradice el reconocimiento que ha cobrado la seguridad digital para cualquier práctica profesional actual y futura.

Las vulnerabilidades digitales que afectan a las IES son técnicas e institucionales porque se derivan de la fragmentación de los sistemas, la obsolescencia tecnológica y el aumento de ataque de *ransomware* y *phishing*. Las vulnerabilidades formativas son el eslabón más débil si se toma en cuenta el desconocimiento generalizado de las prácticas básicas de seguridad por parte de los estudiantes, docentes y personal administrativo, junto con la ausencia de programas de alfabetización digital; esto expone a las universidades a riesgos que pueden ser minimizados con educación y formación en el área.

La falta de conexión entre las unidades técnicas responsables de la seguridad informática y las unidades académicas encargadas de los diseños curriculares se convierte en un problema estructural que impide que el conocimiento generado sobre situaciones de riesgo se convierta en orientaciones para la formación, además de ser una manera de mantener desprotegida a la comunidad universitaria.

Las bases curriculares para incorporar la seguridad informática

en la universidad deben agruparse en torno a los enfoques de integración que combinen la transversalidad con espacios específicos; niveles que distingan entre alfabetización básica, competencias profesionales y especialización; características de la competencia que integren lo técnico, ético, legal y social; y estrategias didácticas como el aprendizaje basado en problemas, simulaciones y proyectos interdisciplinarios.

La hipótesis presentada se confirma parcialmente, porque la actualización curricular es una condición necesaria, pero no suficiente. Si no hay inversión sostenida en la formación del profesorado, ni mecanismos de coordinación entre las unidades técnicas y académicas, o un análisis de las necesidades de cada campo, cualquier tipo de reforma curricular que se presente se quedará solamente en una propuesta de intenciones que no tendrá impacto en los estudiantes.

El estudio presenta limitaciones que deben considerarse a la hora de analizarlo, como el ser bibliográfico, o que se debe tomar en cuenta la rapidez con la que evoluciona la ciberseguridad y la falta de estudios de campo para contrastar con la literatura. Se sugiere realizar investigaciones empíricas para evaluar cuál es el nivel de las competencias en seguridad digital de los estudiantes y docentes, así como también estudios piloto en diseños curriculares que incorporen el tema en distintas áreas del conocimiento.

Las universidades tienen que dejar de ver la ciberseguridad como un asunto exclusivamente técnico y deben verla como un pilar de la formación profesional. Las vulnerabilidades digitales son técnicas y curriculares, por lo tanto, la respuesta no puede provenir solo de los departamentos de sistemas; hace falta transformar esta visión e involucrar a los diseñadores curriculares, y a las facultades de educación que egresan a docentes y especialistas en didáctica, porque el futuro de la universidad depende en gran medida de su capacidad para comprender sus consecuencias y asumir la formación en seguridad digital como una responsabilidad.

## Contribuciones de autores

**Lorenza Ríos:** Conceptualización, Investigación, Metodología, Análisis, Escritura - Borrador original, Revisión y Edición.

**Ibrain Kadir Lin Ríos:** Conceptualización, Investigación, Metodología, Análisis, Escritura - Borrador original, Revisión y Edición.

## REFERENCIAS

Barberá-Gregori, E. & Suárez-Guerrero, C. (2021). Evaluación de la educación digital y digitalización de la evaluación. *RIED-Revista Iberoamericana de Educación a Distancia*, 24(2), 33-40. https://doi.org/10.5944/ried.24.2.30289

Cambridge College. (2025). *Escuela de Empresas y Tecnología. Ciberseguridad. Licenciatura en Ciencias*. https://www.cambridgecollege.edu/es/acad%C3%A9micos/t%C3%ADtulos-certificados/licenciatura/ciberseguridad

Castañeda Girón, C. (2024). *Educación e investigación, sectores prioritarios de ciberataques en América Latina en 2024*. https://u-gob.com/educacion-e-investigacion-sectores-prioritarios-de-ciberataques-en-america-latina-en-2024/

Check Point. (2024). *Check Point Research Warns Every Day is a School Day for Cyber Criminals with the Education Sector as the Top Target in 2024*. https://blog.checkpoint.com/research/check-point-research-warns-every-day-is-a-school-day-for-cybercriminals-with-the-education-sector-as-the-top-target-in-2024/

Cortes Coss, A. (2024). El rol de la seguridad informática en Entornos Educativos. *Revista Cubana de Educación Superior*, 43(3), 82-92. http://scielo.sld.cu/pdf/rces/v43n3/0257-4314-rces-43-03-e6.pdf

Cybersecurity and Infrastructure Security Agency. (2023). *Protecting our Future: Partnering to Safeguard K–12 Organizations from Cybersecurity Threats. U.S. Department of Homeland Security*. https://www.cisa.gov/sites/default/files/2023-01/K-12report_FINAL_V2_508c_0.pdf

da Costa Faria, L., Cordero Verdugo, R. R. & Pérez Suárez, J. R. (2026). Competencias digitales e integración profesional: el papel mediador de la percepción de la seguridad y los riesgos en línea. *Tendencias Sociales. Revista de Sociología*, 1(15), 5-28. https://doi.org/10.5944/ts.2026.47751

Excelsior University. (2025). *¿Qué puede hacer usted con un título en ciberseguridad?* https://www.excelsior.edu/es/article/careers-in-cybersecurity/

Fernández-Sánchez, M. R. & Quiroz, J. S. (2022). Evaluación de la competencia digital de futuros docentes desde una perspectiva de género. *RIED-Revista Iberoamericana de educación a distancia*, 25(2), 327-342. https://doi.org/10.5944/ried.25.2.32128

Ferrari, A. (2012). *Digital competence in practice. An analysis of frameworks. European Union*. https://op.europa.eu/en/publication-detail/-/publication/2547ebf4-bd21-46e8-88e9-f53c1b3b927f/language-en

Kaspersky. (2026). *Por qué el ransomware ataca cada vez más a las instituciones educativas. Kaspersky Team*. https://www.kaspersky.es/blog/ransomware-targets-education-sector/31901/

Kwon, D. (2025). Cyberattacks' harm to universities is growing—and so are their effects on research. *Nature*, 648(8092), 13-13. https://doi.org/10.1038/d41586-025-03484-9

Lawinski, J. (2026). *Why Higher Ed CIOs Must Rethink Cybersecurity. Decentralization and Sprawl Complicate University IT Programs.* https://www.careersinfosecurity.asia/higher-ed-cios-must-rethink-cybersecurity-a-30579

LinkedIn. (2025). *Ciberataques a instituciones educativas en América Latina: casos, impacto y tendencias*. https://www.linkedin.com/pulse/ciberataques-instituciones-educativas-en-am%C3%A9rica-latina-casos-impacto-cus5f/?trk=article-ssr-frontend-pulse_little-text-block

OEA. (2025). *Iniciativa Ciberseguridad en nuestras propias palabras*. https://www.oas.org/ext/es/seguridad/ciber-palabras-propias

Okoye, K., Hussein, H., Arrona-Palacios, A., Quintero, H. N., Ortega, L. O. P., Sánchez, A. L., ... & Hosseini, S. (2023). Impact of digital technologies upon teaching and learning in higher education in Latin America: an outlook on the reach, barriers, and bottlenecks. *Education and Information Technologies*, 28(2), 2291-2360. https://doi.org/10.1007/s10639-022-11214-1

Olivan-Blázquez, B., Asensio-Martínez, Á., Aguilar-Latorre, A., Samper-Pardo, M., León-Herrera, S. & de-la-Manzanara, F. M. L. (2022). From the analysis of a case study to the creation of storytelling as an active learning methodology and its comparison in relation to academic performance and satisfaction. *In EDULEARN22 Proceedings* (2936-2940). IATED. https://doi.org/10.21125/edulearn.2022.0743

**DOI**: 10.36881/yachay.v15i1.1281

Organización de Estados Iberoamericanos. (2012). *2021. Metas educativas. La educación que queremos para la generación de los bicentenarios*. OEI. https://oei.int/wp-content/uploads/2010/08/documento-final-la-educaciobn-que-queremos.pdf

Organización de Estados Iberoamericanos. (2022). *Informe diagnóstico sobre la educación superior y la ciencia post COVID-19 en Iberoamérica. Perspectivas y desafíos de futuro 2022*. OEI; CAF. https://oei.int/wp-content/uploads/2022/05/informe-diagnostico-educacion-superior-y-ciencia-post-covid-19-oei.pdf

Orosco-Fabian, J. R. (2024). Ciberseguridad en educación superior: una revisión bibliométrica. *Revista Digital de Investigación en Docencia Universitaria, 18(2),* e1933, 1-12. https://doi.org/10.19083/ridu.2024.1933

Orosco-Fabian, J. R., Pomasunco-Huaytalla, R., Gómez-Galindo, W. & Rosales-Puchoc, A. M. (2025). Evaluación de la Competencia Digital de Seguridad en Estudiantes de una Universidad del Centro del Perú. *Revista Tecnológica-Educativa Docentes 2.0*, 18(1), 472-486. https://doi.org/10.37843/rted.v18i1.632

Parlamento Europeo & Consejo de la Unión Europea. (2006). *Recomendación del Parlamento Europeo y del Consejo de 18 de diciembre de 2006 sobre las competencias clave para el aprendizaje permanente. Diario Oficial de la Unión Europea.* https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:32006H0962

Pathify. (2025). *Why System Consolidation Is Your Institution's Most Strategic Cybersecurity Move*. https://pathify.com/blog/why-system-consolidation-is-your-institutions-most-strategic-cybersecurity-move/

Pozo-Sánchez, S., Carmona-Serrano, N., López-Belmonte, J. & Aguilar-Álvarez, J. J. (2022). El marco de competencias digitales DIGCOMP 2.1 como referencia para la actualización tecnopedagógica. *Perspectivas y prospectivas en el nuevo escenario formativo*, 79-90. https://doi.org/10.2307/j.ctv2s0j5s4

Robert, J., Muscanell, N., Arbino, N., McCormack, M. & Reeves, J. (2024). *2024 EDUCAUSE Horizon Report, Cybersecurity and Privacy Edition*. Educause. https://library.educause.edu/-/media/files/library/2024/9/2024hrcybersecurityprivacy.pdf

Rodríguez Jiménez, C. (2024). *Análisis y percepción de las competencias digitales en seguridad adquiridas durante la formación inicial del alumnado universitario en Ciencias de la Educación.* [Tesis Doctoral]. Universidad de Granada. https://digibug.ugr.es/bitstream/handle/10481/90555/93687.pdf?sequence=4&isAllowed=y

Rojas, A. (2024). *La ciberseguridad como eje transversal en la educación universitaria.* LinkedIn. https://es.linkedin.com/pulse/la-ciberseguridad-como-eje-transversal-en-educaci%C3%B3n-adriana-rojas-p3a7e

Rowsell, J. (2024). *Funding crisis 'puts universities at higher risk of cyberattacks'*. https://www.timeshighereducation.com/news/funding-crisis-puts-universities-higher-risk-cyberattacks

Rychen, D. S. & Salganik, L. H. (2001). *Definition and selection of competencies-Theoretical and conceptual foundations. Organisation for Economic Co-operation and Development*. https://www.deseco.ch/RychSalg_Front.pdf

Sánchez-Caballé, A., Gisbert-Cervera, M. & Esteve-Món, F. (2021). La integración de la competencia digital en educación superior: un estudio de caso de una universidad catalana. *Educar,* 57(1), 241-258. https://doi.org/10.5565/rev/educar.1174

Schmidt, S. (2025). Aumentan los ataques cibernéticos a universidades e instituciones científicas en Brasil. *Revista Pesquisa FAPESP*, 352, 32-35. https://revistapesquisa.fapesp.br/leia-a-edicao-de-junho-de-2025/

UNESCO. (2011). UNESCO ICT. *Competency Framework for Teachers*. UNESCO and Microsoft. https://iite.unesco.org/pics/publications/en/files/3214694.pdf