Revista Especializada de Ingeniería
y Ciencias de la Tierra
VOL: 6 Nº 1 julio - diciembre 2026
ISSN L: 2805-1874

# Percepción y Conocimiento de Competencias en Ciencia de Datos aplicada a la Ciberseguridad en Estudiantes de Informática

# Perception and Knowledge of Competencies in Data Science Applied to Cybersecurity in Computer Science Students

Javier Garrido Córdoba
Universidad de Panamá. Centro Regional Universitario de San Miguelito, Panamá
javier.garrido@up.ac.pa.
https://orcid.org/0009-0000-4234-5267

Rafael Armando Díaz Bonfante
Universidad de Panamá. Centro Regional Universitario de San Miguelito. Panamá
Rafael.diaz@up.ac.pa.
https://orcid.org/0009-0006-8627-090x

**Recibido: 9/2/2026 Aceptado: 10/5/2026**

**DOI https://doi.org/10.48204/reicit.v6n1.10121**

## RESUMEN

El estudio analiza el nivel de percepción y conocimiento de competencias en Ciencia de Datos aplicada a Ciberseguridad en estudiantes de Informática, en un contexto marcado por el incremento de amenazas digitales y la creciente demanda de perfiles profesionales híbridos. El objetivo fue evaluar dichos niveles y explorar su relación con el interés de especialización en estas áreas emergentes. La metodología se basó en un enfoque cuantitativo, con diseño no experimental, transversal y correlacional. Se aplicó un cuestionario en línea a estudiantes de informática, utilizando escalas tipo Likert para medir conocimientos percibidos, competencias y autoeficacia en tareas relacionadas con análisis de datos y ciberseguridad. La muestra fue no probabilística por conveniencia y se analizaron los datos mediante técnicas descriptivas e inferenciales. Los resultados evidencian que la percepción de conocimientos y competencias es moderada y heterogénea. Menos del 50 %

de los estudiantes se considera competente en tareas clave como detección de intrusiones o análisis de datos de seguridad. Asimismo, se identificó poca integración curricular entre Ciencia de Datos y Ciberseguridad, con escasas oportunidades prácticas. No obstante, aproximadamente la mitad de los estudiantes manifestó interés en especializarse en estas áreas. Se concluye que existe una brecha entre la formación recibida y las demandas del entorno profesional. Aunque los estudiantes reconocen la importancia de integrar ambas disciplinas y muestran disposición a especializarse, perciben una preparación insuficiente. Se destaca la necesidad de rediseñar los planes de estudio, incorporando enfoques integrados y experiencias prácticas que fortalezcan competencias y mejoren la autoeficacia en este campo.

**Palabras Clave**: competencias, ciberseguridad, ciencia de datos, percepción, conocimiento

## ABSTRACT

This study analyzes the level of perceived and knowledgeable skills in Data Science applied to Cybersecurity among Computer Science students, in a context marked by the increase in digital threats and the growing demand for hybrid professional profiles. The objective was to evaluate these levels and explore their relationship with interest in specializing in these emerging areas. The methodology was based on a quantitative approach, with a non-experimental, cross-sectional, and correlational design. An online questionnaire was administered to Computer Science students, using Likert-type scales to measure perceived knowledge, skills, and self-efficacy in tasks related to data analysis and cybersecurity. The sample was non-probabilistic and selected for convenience, and the data were analyzed using descriptive and inferential techniques. The results show that the perception of knowledge and skills is moderate and heterogeneous. Less than 50% of students consider themselves competent in key tasks such as intrusion detection or security data analysis. Furthermore, little curricular integration between Data Science and Cybersecurity was identified, with limited practical opportunities. However, approximately half of the students expressed interest in specializing in these areas. It is concluded that a gap exists between the training received and the demands of the professional environment. Although students recognize the importance of integrating both disciplines and show a willingness to specialize, they perceive their preparation as insufficient. The need to redesign curricula is highlighted, incorporating integrated approaches and practical experiences that strengthen competencies and improve self-efficacy in this field.

**Keywords**: skills, cybersecurity, data science, perception, knowledge

## INTRODUCCIÓN

La aceleración de la transformación digital en la última década ha incrementado de manera significativa la superficie de exposición de individuos, organizaciones y gobiernos a

incidentes de seguridad de la información, tales como ataques de ransomware, filtraciones masivas de datos y explotación de vulnerabilidades en sistemas críticos (ENISA, 2023; PwC, 2023). Este escenario ha consolidado la ciberseguridad como un eje estratégico no solo para el sector productivo, sino también para los sistemas educativos, en particular en la educación superior vinculada a las Tecnologías de la Información y la Comunicación (TIC), Jimenez,et.al. (2025). Paralelamente, la Ciencia de Datos se ha posicionado como disciplina clave para la extracción de conocimiento a partir de grandes volúmenes de información, facilitando la identificación de patrones, anomalías y tendencias que no serían evidentes mediante métodos tradicionales (Provost y Fawcett, 2013). En el ámbito de la ciberseguridad, estas capacidades analíticas se han aplicado al desarrollo de sistemas de detección de intrusiones basados en machine learning, detección de anomalías en tráfico de red, análisis de malware y sistemas de respuesta automatizada ante incidentes (Sommer, Paxson, 2010; Buczak y Guven, 2016).

La integración de competencias de Ciencia de Datos en la formación en Ciberseguridad ofrece un potencial significativo para mejorar la anticipación, detección temprana y mitigación de amenazas en entornos digitales complejos. No se trata únicamente de formar especialistas en seguridad, sino de desarrollar perfiles híbridos capaces de articular fundamentos de protección de sistemas y datos con el uso avanzado de técnicas analíticas (estadística, minería de datos, aprendizaje automático) para la toma de decisiones en contextos de riesgo cibernético. En este sentido, las carreras de Ingeniería en Informática, Ingeniería en Sistemas y programas afines enfrentan el reto de rediseñar sus planes de estudio para responder a la creciente demanda de profesionales con competencias técnicas, analíticas y de gestión. Diversos estudios evidencian la existencia de una brecha entre las competencias que los estudiantes perciben poseer al egresar y aquellas requeridas en el contexto profesional, particularmente en áreas digitales como la seguridad de la información y el análisis de datos. Investigaciones sobre el mercado laboral en tecnologías de la información muestran que los empleadores demandan habilidades prácticas y especializadas que no siempre son desarrolladas durante la formación académica, generando un desajuste en la inserción laboral. En el ámbito de la ciberseguridad, esta brecha se manifiesta en la escasez de profesionales con competencias técnicas actualizadas, mientras que en el análisis de datos se identifican carencias en habilidades analíticas avanzadas y manejo de herramientas especializadas (Marios Belanger et al., 2019; Whitman y Mattord, 2018; Alshaikh, 2020; International Data Corporation, 2021).

Este desajuste entre las necesidades del entorno y la formación recibida resalta la importancia de explorar no solo el nivel objetivo de conocimientos, sino también la percepción que los estudiantes tienen sobre sus propias competencias, especialmente en áreas emergentes que combinan Ciencia de Datos y Ciberseguridad. La percepción de competencia se relaciona con la autoeficacia académica y profesional y tiene efectos directos sobre la motivación, la elección de itinerarios formativos y la intención de especialización (Bandura, 1997; Gamarra

Camargo et al., 2024). Sin embargo, la literatura reciente evidencia que los programas formativos en tecnologías digitales tienden a estructurar la ciberseguridad y la ciencia de datos como dominios separados, lo que limita el desarrollo de competencias interdisciplinarias necesarias en el contexto profesional. Diversos estudios señalan que, aunque ambas áreas convergen en aplicaciones reales, como la detección de amenazas mediante aprendizaje automático, su integración en los planes de estudio sigue siendo incipiente y requiere rediseños curriculares específicos basados en enfoques interdisciplinarios y aprendizaje práctico. Esta fragmentación ha sido identificada como un factor que contribuye a la brecha entre la formación académica y las demandas del mercado laboral, particularmente en competencias híbridas que combinan analítica de datos y seguridad de la información (Tian, 2025; Sharon L. Burton, 2025; Frontiers in Education, 2026). De esta forma, se limita el desarrollo de competencias interdisciplinarias necesarias en el contexto profesional (Tian, 2025; Buczak y Guven, 2020; Cabaj et al., 2018).

Los antecedentes nacionales e internacionales sobre formación en ciberseguridad y competencias digitales evidencian retos pedagógicos y curriculares. Bishop (2018) plantea que la naturaleza dinámica de las amenazas exige enfoques activos y basados en problemas; Davara Fernández de Marcos (2019) subraya la necesidad de integrar la ciberseguridad y la protección de datos como competencias transversales, más allá de asignaturas aisladas. Alshaikh (2020) y Hall y Davis (2020) encontraron que, aunque el nivel básico de conocimiento en ciberseguridad suele ser aceptable, la autoeficacia para aplicar dichos conocimientos en contextos reales es moderada o baja, y que los estudiantes perciben dificultades para conectar la teoría con casos de uso concretos. En el contexto iberoamericano, Mendivil Caldentey et al. (2022) describen modelos educativos en ciberseguridad aún incipientes y centrados en contenidos, con menor énfasis en habilidades prácticas y capacidades analíticas. En paralelo, la literatura sobre formación en Ciencia de Datos destaca la importancia de integrar habilidades analíticas, de programación y comprensión estadística, pero rara vez profundiza en su cruce con la ciberseguridad (Provost y Fawcett, 2013; Sandoya, 2022).

Desde la perspectiva de la industria, Buczak y Guven (2016), muestran que las soluciones de seguridad dependen cada vez más de técnicas de machine learning y data mining para detectar comportamientos anómalos, clasificar tráfico malicioso y priorizar alertas, lo cual demanda egresados con competencias integradas en análisis de datos y ciberseguridad. No obstante, persiste un vacío investigativo: la mayoría de los estudios analiza por separado la formación en Ciberseguridad y Ciencia de Datos y son escasos los trabajos que exploran la percepción estudiantil sobre sus competencias conjuntas o que vinculan dicha percepción con la intención de especialización profesional.

En este marco, el problema en contextos específicos como el del Centro Regional Universitario de San Miguelito, donde los estudiantes de Ingeniería en Informática cursan

asignaturas relacionadas con Ciencia de Datos y Ciberseguridad, pero se desconoce en qué medida perciben estar preparados para aplicar técnicas analíticas a problemas de seguridad. El ecosistema digital contemporáneo exige profesionales capaces de interpretar grandes volúmenes de datos, incluyendo información proveniente de logs, tráfico de red y sistemas de monitoreo, para anticipar y mitigar amenazas (European Unión Agency for Cybersecurity, 2023; Rasheed Olawoyin et al., 2022).

Sin embargo, la transición desde modelos formativos centrados en habilidades tradicionales hacia modelos integrados no ha sido suficientemente analizada desde la perspectiva del estudiante. La percepción que los alumnos tienen sobre su nivel de conocimiento y sus competencias en Ciencia de Datos aplicada a Ciberseguridad constituye, por tanto, un indicador clave de la pertinencia y eficacia de la formación recibida y puede incidir en su intención de especialización mediante posgrados, certificaciones o inserción en perfiles profesionales híbridos (Lent et al., 2018; Martínez-Caro et al., 2020).

A partir de esta problemática, se formula la siguiente pregunta de investigación: ¿Cuál es el nivel de conocimiento y la percepción de competencias en Ciencia de Datos aplicada a Ciberseguridad entre estudiantes universitarios de Informática, y cómo esta percepción influye en su interés de especialización profesional en dichas áreas? Esta cuestión orienta el estudio y justifica la necesidad de generar evidencia empírica que contribuya al rediseño curricular y al fortalecimiento de perfiles híbridos acordes con las demandas actuales del mercado laboral.

## MATERIALES Y MÉTODOS

En el diseño de investigación de este estudio adoptó un enfoque cuantitativo, con un diseño no experimental, de tipo transversal. (Hernández-Sampieri et al., 2023). No se manipularon variables independientes; por el contrario, se observaron y analizaron en su contexto natural las relaciones entre el nivel de conocimiento, la percepción de competencias en Ciencia de Datos aplicada a Ciberseguridad y el interés de especialización profesional. El carácter transversal implicó que la recolección de datos se realizara en un único momento temporal, permitiendo describir el estado de las variables y explorar asociaciones entre ellas.

La población objetivo estuvo conformada por estudiantes universitarios de la carrera de Ingeniería en Informática, Electrónica y Comunicación del Centro Regional Universitario de San Miguelito, específicamente aquellos que cursaban los cursos de III y IV año. Se asumió que, a este nivel, los estudiantes habían tenido contacto formal con asignaturas vinculadas a Ciencia de Datos y/o Ciberseguridad (por ejemplo, Minería de Datos, Aprendizaje Automático, Análisis de Datos, Seguridad Informática, Redes Seguras, Criptografía).

Se utilizó un muestreo no probabilístico por conveniencia, atendiendo a la accesibilidad del grupo objetivo y a las condiciones logísticas de aplicación del instrumento. Se procuró alcanzar un tamaño de la muestra de 20 participantes, considerado suficiente para el análisis correlacional básico y pruebas de significación en estudios exploratorios (Cohen, 1992; Hernández-Sampieri et al., 2023).

Se elaboró un cuestionario estructurado, auto administrado y en formato en línea, compuesto por cuatro secciones principales:

- Dimensión 1. Nivel de conocimiento en Ciencia de Datos y Ciberseguridad

  Nivel percibido de conocimiento en Ciencia de Datos y Ciberseguridad: ítems tipo Likert (1 = "muy bajo" a 5 = "muy alto") para evaluar la percepción de conocimiento en conceptos clave de Ciencia de Datos (estadística básica, modelos de clasificación, análisis de datos, programación para análisis de datos) y de Ciberseguridad (tipos de ataques, buenas prácticas de seguridad, criptografía básica, seguridad en redes, gestión de incidentes).

- Dimensión 2. Percepción de competencias para aplicar Ciencia de Datos en Ciberseguridad.
  Percepción de competencias e intención de especialización: ítems tipo Likert que midieron la autoeficacia percibida para aplicar técnicas de análisis de datos a problemas de seguridad (detección de anomalías en tráfico de red, análisis de logs, clasificación de eventos sospechosos, diseño básico de modelos de aprendizaje automático para detectar intrusiones). así como el grado de intención de cursar posgrados, certificaciones o especializaciones en Ciencia de Datos, Ciberseguridad o su intersección.
- Dimensión 3. Integración formativa y experiencias de aprendizaje

  Datos académicos: año de estudio, experiencia laboral en áreas afines (si la hubiese), participación en cursos o certificaciones adicionales en Ciencia de Datos y/o Ciberseguridad, promedio académico aproximado, entre otros.
- Dimensión 4. Interés en la especialización y proyección profesional
  Interés en cursar posgrados, maestrías y/o doctorados, certificaciones o especializaciones en Ciencia de Datos, Ciberseguridad o Ciencias de datos aplicada a Ciberseguridad.

El instrumento se diseñó tomando como referencia escalas previas de autoeficacia y percepción de competencias en contextos tecnológicos (Bandura, 1997; Alshaikh, 2020; Lent et al., 2018), adaptadas al ámbito específico de Ciencia de Datos aplicada a Ciberseguridad.En cuanto a la validez y confiabilidad el cuestionario fue sometido a juicio

de expertos con experiencia en educación tecnológica, Ciberseguridad y Ciencia de Datos. Se les solicitó valorar claridad, pertinencia y relevancia de los ítems respecto a los objetivos del estudio. Sus observaciones se incorporaron en una versión revisada del instrumento, ajustando redacción, orden y formulación de algunos ítems. Posteriormente se realizó una prueba piloto con un grupo reducido de 10 estudiantes que cumplían los criterios de inclusión. Esta fase permitió identificar posibles problemas de comprensión, ambigüedades y tiempos de respuesta excesivos. Con base en los resultados y comentarios de los participantes, se efectuaron ajustes finales al cuestionario. Una vez aplicada la versión definitiva, se calculó el coeficiente alfa de Cronbach para cada dimensión (conocimiento percibido, percepción de competencias, currículo, interés de especialización) a fin de evaluar la consistencia interna. Se consideraron aceptables valores de $\alpha \geq .70$, conforme a los criterios usuales en investigación social y educativa (Hernández-Sampieri et al., 2023).

El cuestionario se implementó en una plataforma digital (Google Forms). Los estudiantes fueron invitados mediante correo institucional y/o WhatsApp. Se garantizó el carácter voluntario y anónimo de la participación, obteniendo consentimiento informado y asegurando confidencialidad y uso exclusivo de los datos con fines académicos, en concordancia con los principios éticos de la APA (American Psychological Association, 2020). Para la recolección y depuración de datos se habilitó un periodo de respuesta de aproximadamente 2–3 semanas. Al cierre, se descargó la base de datos y se procedió a la depuración (eliminación de registros incompletos, revisión de inconsistencias y detección preliminar de valores atípicos). El análisis estadístico se realizó con el software IBM SPSS Statistics en donde se aplicaron estadísticos descriptivos: frecuencias y porcentajes para variables categóricas de las escalas de conocimiento percibido, percepción de competencias, currículo e interés de especialización.

## RESULTADOS

### Dimensión 1. Nivel de conocimiento en Ciencia de Datos y Ciberseguridad

**Figura 1**

*Conocimiento sobre conceptos básicos de Ciencia de Datos*

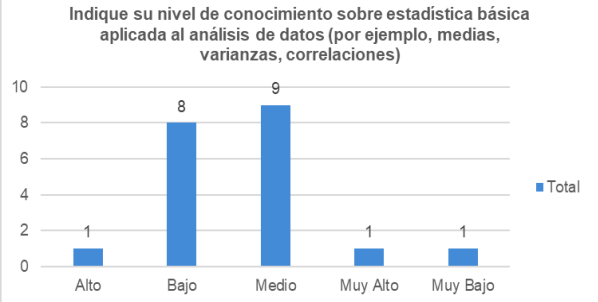

***Nota:*** Se observa en la figura 1 los resultados obtenidos en la primera pregunta, referida al

nivel de conocimiento sobre conceptos básicos de Ciencia de Datos.

De un total de 20 participantes, la mayoría se ubicó en un nivel intermedio de dominio. En conjunto, estos resultados muestran que alrededor de ocho de cada diez estudiantes perciben tener al menos un conocimiento moderado de los conceptos fundamentales de Ciencia de Datos, aunque persiste un segmento que reconoce limitaciones importantes en este ámbito.

**Figura 2**

*Conocimiento sobre estadística básica aplicada al análisis de datos*

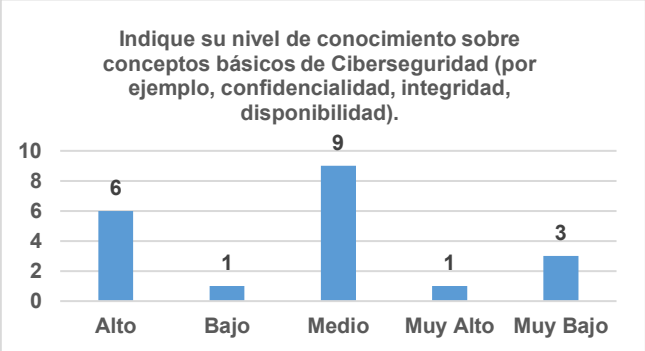



*Nota:* En la pregunta #2 «Indique su nivel de conocimiento sobre estadística básica aplicada al análisis de datos», en la figura se observa que las respuestas reflejan una distribución relativamente equilibrada entre quienes se perciben con un dominio suficiente y quienes reconocen limitaciones.

En conjunto, algo más de la mitad (55 %) de los encuestados considera poseer al menos un conocimiento moderado en estadística básica aplicada al análisis de datos, mientras que casi la mitad (45 %) reconoce un dominio limitado, lo que sugiere una base formativa desigual en este componente fundamental para la Ciencia de Datos.

**Figura 3**

*Conocimiento sobre conceptos básicos de Ciberseguridad (por ejemplo, confidencialidad, integridad, disponibilidad).*




*Nota:* En la figura 3 se presentan las respuestas a la pregunta: «Indique su nivel de conocimiento sobre conceptos básicos de Ciberseguridad (por ejemplo, confidencialidad,

integridad, disponibilidad)». De los 20 estudiantes participantes, 9 (45 %) indicaron tener un nivel medio de conocimiento sobre estos conceptos básicos, conformando el grupo más numeroso. Estos resultados evidencian la presencia de un grupo mayoritario que considera disponer de una base conceptual aceptable en Ciberseguridad, junto con un segmento minoritario que presenta carencias relevantes en estos conceptos esenciales.

**Tabla 1**

*Nivel de conocimiento en Ciencia de Datos y Ciberseguridad*

| Ítems | Nivel de conocimiento | Frecuencia | Porcentaje % |
|---|---|---|---|
| Conocimiento sobre conceptos básicos de Ciencia de Datos | Muy bajo | 1 | 5,0 |
| | Bajo | 3 | 15,0 |
| | Medio | 11 | 55,0 |
| | Alto | 4 | 20,0 |
| | Muy alto | 1 | 5,0 |
| Conocimiento sobre estadística básica aplicada al análisis de datos | Muy bajo | 1 | 5,0 |
| | Bajo | 8 | 40,0 |
| | Medio | 9 | 45,0 |
| | Alto | 1 | 5,0 |
| | Muy alto | 1 | 5,0 |
| Conocimiento sobre conceptos básicos de Ciberseguridad (confidencialidad, integridad, disponibilidad) | Muy bajo | 3 | 15,0 |
| | Bajo | 1 | 5,0 |
| | Medio | 9 | 45,0 |
| | Alto | 1 | 5,0 |
| | Muy alto | 1 | 5,0 |
| Conocimiento sobre tipos de ataques informáticos (phishing, malware, ataques de fuerza bruta) | Muy bajo | 1 | 5,0 |
| | Bajo | 2 | 10,0 |
| | Medio | 10 | 50,0 |
| | Alto | 6 | 30,0 |
| | Muy alto | 1 | 5,0 |
| Conocimiento sobre gestión de incidentes de seguridad (identificación, contención, erradicación, recuperación) | Muy bajo | 2 | 10,0 |
| | Bajo | 5 | 25,0 |
| | Medio | 10 | 50,0 |
| | Alto | 1 | 5,0 |
| | Muy alto | 2 | 10,0 |

Nota. Elaboración propia a partir de los resultados de la encuesta.

La Tabla 1 presenta la distribución de respuestas de 20 estudiantes respecto a su nivel de conocimiento en Ciencia de Datos y Ciberseguridad, medido mediante una escala Likert de 5 puntos (1 = muy bajo, 5 = muy alto).

En relación con los conceptos básicos de Ciencia de Datos, la mayoría se concentra en el nivel medio (55 %), seguido por niveles alto (20 %) y muy alto (5 %), mientras que el 20 % restante se ubica entre muy bajo (5 %) y bajo (15 %). Esto indica que cerca de cuatro quintas partes del grupo perciben al menos un conocimiento moderado en este ámbito. En cuanto al conocimiento de estadística básica aplicada al análisis de datos, las respuestas se distribuyen

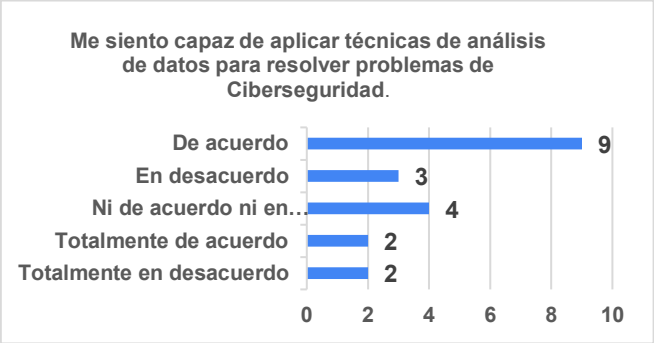
entre niveles bajo (40 %) y medio (45 %) principalmente, con solo un 10 % en niveles alto o muy alto y un 5 % en muy bajo. Se observa aquí una base formativa más desigual, con casi la mitad de los estudiantes reconociendo limitaciones importantes. Respecto a los conceptos básicos de Ciberseguridad (confidencialidad, integridad, disponibilidad), el 55 % declara un nivel medio a muy alto (45 % medio, 5 % alto, 5 % muy alto), mientras que un 20 % se ubica en los niveles bajo y muy bajo (5 % bajo, 15 % muy bajo). Predomina, por tanto, la percepción de una base conceptual aceptable, aunque con un grupo minoritario que reconoce carencias relevantes. En el ítem sobre tipos de ataques informáticos (phishing, malware, fuerza bruta), se observa una de las percepciones de dominio más altas: alrededor de la mitad se sitúa en nivel medio y casi un tercio en nivel alto, con una proporción muy reducida en niveles bajos. Esto sugiere una familiaridad relativamente extendida con las categorías básicas de ataques. Finalmente, en gestión de incidentes de seguridad (identificación, contención, erradicación, recuperación), la mitad del estudiantado se ubica en un nivel medio, y un 15 % en niveles alto o muy alto, mientras que el 35 % se sitúa en niveles bajo o muy bajo. En conjunto, se aprecia una ligera mayoría con una base funcional en gestión de incidentes, pero también un grupo importante que percibe deficiencias en estas competencias clave para la práctica profesional en Ciberseguridad.

En síntesis, la tabla evidencia un perfil donde el conocimiento percibido es mayor en conceptos generales de Ciencia de Datos y, sobre todo, en tipos de ataques, mientras que se muestran más debilidades en estadística básica y en gestión de incidentes de seguridad.

## Dimensión 2. Percepción de competencias para aplicar Ciencia de Datos en Ciberseguridad

### Figura 4

*Capacidad de aplicar técnicas de análisis de datos para resolver problemas de Ciberseguridad*

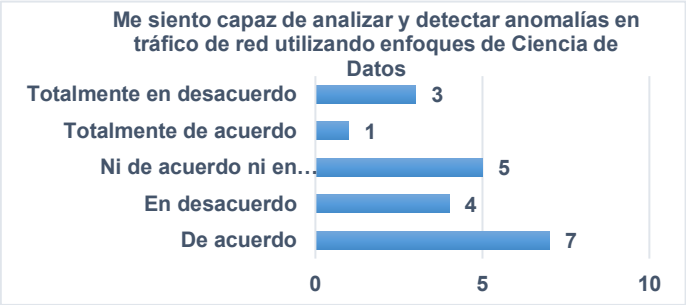



***Nota***: En la Figura 4 se presenta las percepciones de los estudiantes frente a la afirmación "Me siento capaz de aplicar técnicas de análisis de datos para resolver problemas de Ciberseguridad". Del total de 20 participantes, el 45 % (n=9) manifestó estar de acuerdo y el 10 % (n=2) totalmente de acuerdo, lo que indica que un 55 % de los encuestados presenta

una autopercepción positiva de su capacidad en este ámbito. Estos resultados sugieren que, si bien más de la mitad de los participantes se perciben capaces en esta área, existe aún un porcentaje significativo que no se siente plenamente competente o que no tiene una percepción clara de su nivel de dominio.

**Figura 5**

*Capacidad de analizar y detectar anomalías en tráfico de red utilizando enfoques de Ciencias de Datos*




*Nota:* En la Figura 5 se presentan las percepciones de los estudiantes frente a la afirmación "Me siento capaz de analizar y detectar anomalías en tráfico de red utilizando enfoques de Ciencias de Datos". Del total de 20 participantes, el 35 % (n = 7) manifestó estar de acuerdo y el 5 % (n = 1) totalmente de acuerdo, de modo que un 40 % expresa una autopercepción positiva respecto a esta competencia. Estos resultados muestran que menos de la mitad de los estudiantes se perciben capaces de analizar y detectar anomalías en el tráfico de red mediante enfoques de Ciencias de Datos, mientras que una proporción considerable presenta dudas o una percepción desfavorable de sus competencias en este ámbito.

**Tabla 2**

*Percepción de competencias para aplicar Ciencia de Datos en Ciberseguridad*

| Ítems | Totalmente en desacuerdo | En desacuerdo | Ni de acuerdo ni en desacuerdo | De acuerdo | Totalmente de acuerdo |
|---|---|---|---|---|---|
| Capacidad de aplicar técnicas de análisis de datos para resolver problemas de Ciberseguridad | 2 (10 %) | 3(15%) | 4 (20 %) | 9 (45 %) | 2 (10 %) |
| Capacidad de analizar y detectar anomalías en tráfico de red utilizando enfoques de Ciencias de Datos | 3 (15 %) | 4 (20 %) | 5 (25 %) | 7 (35 %) | 1 (5 %) |
| Capacidad para clasificar amenazas o eventos de seguridad usando herramientas | 1 (5,3 %) | 4 (21,1 %) | 5 (26,3 %) | 8 (42,1 %) | 1 (5,3 %) |

| | | | | | |
|---|---|---|---|---|---|
| o modelos básicos de análisis de datos | | | | | |
| Capacidad de interpretar los resultados de modelos de datos en contextos de riesgos cibernéticos | 2 (10 %) | 6 (30 %) | 5 (25 %) | 5 (25 %) | 2 (10 %) |
| Capacidad de comunicar de forma clara los resultados de un análisis de datos aplicado a un problema de Ciberseguridad | 2 (10 %) | 4(20 %) | 6 (30 %) | 6 (30 %) | 2 (10 %) |

*Nota:* Resultados de la encuesta.

La Tabla 2 sintetiza la percepción de 20 estudiantes sobre sus competencias para aplicar Ciencia de Datos en Ciberseguridad. En general, se observa que entre el 35 % y el 55 % de los participantes se ubica en las categorías "de acuerdo" o "totalmente de acuerdo" con las afirmaciones planteadas, lo que indica una autopercepción moderadamente positiva en varias de las competencias evaluadas.

La mayor confianza se aprecia en la capacidad para aplicar técnicas de análisis de datos a problemas de Ciberseguridad, donde el 55 % de los estudiantes expresa acuerdo, frente a un 25 % que manifiesta desacuerdo y un 20 % que se mantiene neutral. De forma similar, cerca de la mitad de los encuestados se percibe capaz de clasificar amenazas o eventos de seguridad con herramientas o modelos básicos de análisis de datos, aunque más de una cuarta parte se muestra indecisa y otro grupo relevante declara no sentirse competente.

En las competencias más especializadas —analizar y detectar anomalías en tráfico de red usando enfoques de Ciencia de Datos, interpretar resultados de modelos de datos en contextos de riesgo cibernético y comunicar de forma clara los resultados de un análisis de datos aplicado a Ciberseguridad— las percepciones positivas son menores (entre 35 % y 40 %). En estos ítems se incrementan tanto las respuestas de desacuerdo (entre 30 % y 40 % en algunos casos) como las posiciones neutrales (hasta un 30 %), lo que sugiere un nivel significativo de inseguridad o falta de experiencia en tareas que exigen un mayor grado de integración entre Ciencia de Datos y Ciberseguridad.

En conjunto, la tabla pone de relieve que, aunque existe un núcleo de estudiantes que se percibe con competencias básicas para aplicar técnicas de análisis de datos en el ámbito de la Ciberseguridad, persiste una proporción importante que se declara indecisa o no competente, especialmente en habilidades de análisis avanzado, interpretación y comunicación de resultados.

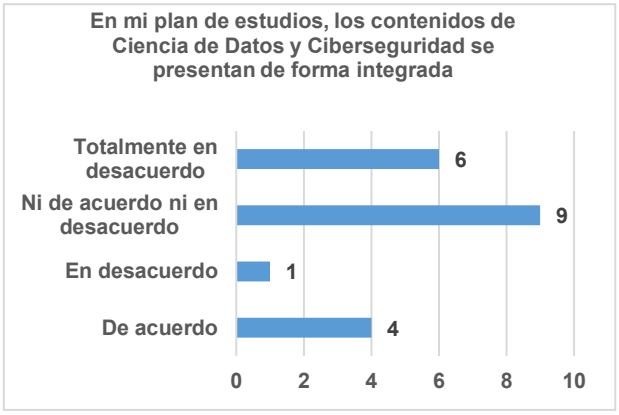
**Dimensión 3. Integración formativa y experiencias de aprendizaje**

**Figura 6**

*Plan de estudio, contenidos de Ciencia de Datos y Ciberseguridad se presentan de forma integrada*

existe o no una articulación sistemática entre ambas áreas en su trayectoria formativa En relación con la afirmación: «En mi plan de estudio, los contenidos de Ciencia de Datos y Ciberseguridad se presentan de forma integrada», las respuestas de los 20 estudiantes muestran una percepción mayoritariamente crítica respecto de la articulación curricular entre ambas áreas. En primer lugar, 4 participantes señalaron estar "de acuerdo" con la afirmación, lo que representa el 20% de la muestra, y ninguno manifestó estar "totalmente de acuerdo" (0 %). Es decir, solo uno de cada cinco estudiantes percibe que su plan de estudio integra de manera explícita los contenidos de Ciencia de Datos y Ciberseguridad. Por otra parte, 9 estudiantes (45 %) seleccionaron la opción "ni de acuerdo ni en desacuerdo", evidenciando un elevado nivel de neutralidad o indefinición sobre el grado de integración curricular. Este porcentaje sugiere que casi la mitad del grupo no identifica con claridad si.

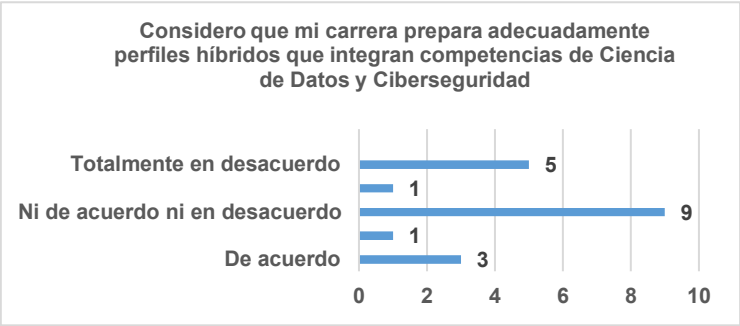
Finalmente, 1 estudiante (5 %) declaró estar "en desacuerdo" y 6 (30 %) "totalmente en




desacuerdo", sumando un 35 % que percibe de forma explícita que los contenidos de Ciencia de Datos y Ciberseguridad no se presentan de forma integrada en el plan de estudios. De manera integral, la proporción de estudiantes que no reconoce integración (35 %) y la alta proporción de neutralidad (45 %) superan ampliamente a quienes perciben integración (20 %), lo que sugiere que, para la mayoría del estudiantado, la relación entre Ciencia de Datos y Ciberseguridad no se visualiza como un eje articulador claro dentro del currículo, sino más bien como bloques formativos separados o poco conectados.

**Figura 7**

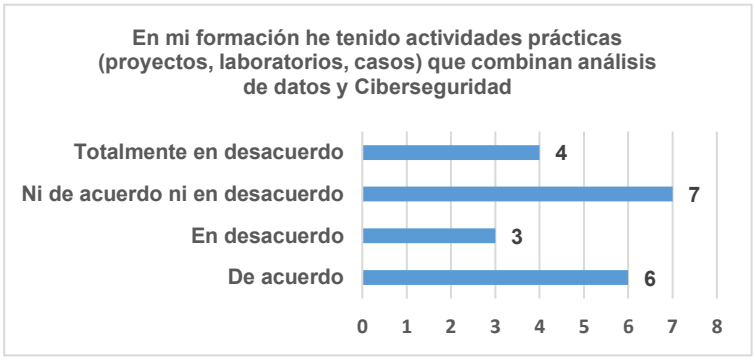
*Formación en actividades prácticas (proyectos, laboratorios, casos) que combinan análisis de datos y ciberseguridad*




***Nota:*** La tabla 7 presenta la preparación perfiles hibrido

Figura 8

*Preparación profesional en perfiles híbridos que integran competencias de Ciencia de Datos y Ciberseguridad*




*Nota:* En relación con la afirmación: «En mi formación he tenido actividades prácticas (proyectos, laboratorios, casos) que combinan análisis de datos y ciberseguridad», las respuestas de los 20 estudiantes muestran una percepción más bien limitada respecto a la presencia de este tipo de experiencias integradas en su formación.

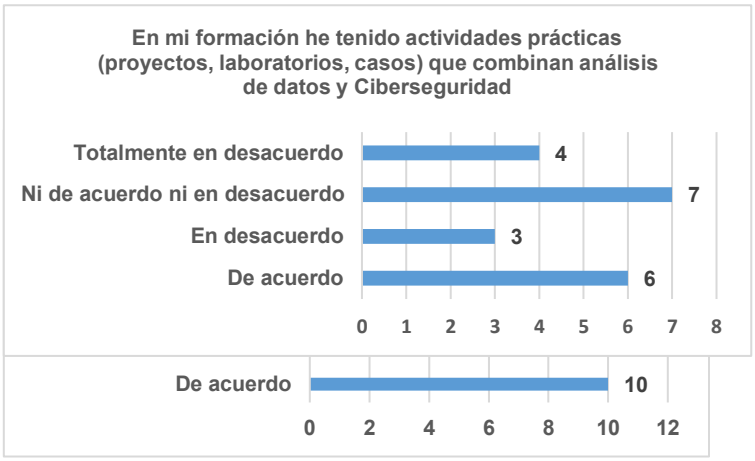
En primer lugar, 6 participantes indicaron estar “de acuerdo” con la afirmación, lo que representa el 30 % de la muestra, mientras que ninguno seleccionó la opción “totalmente de acuerdo” (0 %). Es decir, solo tres de cada diez estudiantes reconocen haber participado en actividades prácticas que combinen explícitamente análisis de datos y ciberseguridad. Por otra parte, 7 estudiantes (35 %) eligieron la opción “ni de acuerdo ni en desacuerdo”, lo que

evidencia un grado relevante de neutralidad o falta de claridad sobre la existencia o la naturaleza de estas actividades integradas. Este porcentaje sugiere que más de un tercio del grupo no identifica con certeza si su formación ha incluido experiencias prácticas que articulen ambas áreas. Finalmente, 3 estudiantes (15 %) manifestaron estar "en desacuerdo" y 4 (20 %) "totalmente en desacuerdo", sumando un 35 % que percibe explícitamente que no ha tenido actividades prácticas que combinen análisis de datos y ciberseguridad. La proporción de estudiantes que no reconoce este tipo de experiencias (35 %) y la elevada neutralidad (35 %) superan ligeramente a quienes sí las identifican (30 %). Esto sugiere que, para la mayoría de los estudiantes, las oportunidades prácticas de integración entre Ciencia de Datos y Ciberseguridad son escasas, puntuales o poco visibles dentro de su trayectoria formativa.

En relación con la afirmación: «Considero que mi carrera prepara adecuadamente perfiles híbridos que integran competencias de Ciencia de Datos y Ciberseguridad», las respuestas de los 18 estudiantes encuestados reflejan una valoración predominantemente crítica o, al menos, poco definida sobre la capacidad formativa del programa para generar este tipo de perfiles. En primer lugar, únicamente 3 participantes señalaron estar "de acuerdo" con la afirmación, lo que representa el 16,7 % de la muestra. Ningún estudiante manifestó estar "totalmente de acuerdo" (0 %). Es decir, menos de dos de cada diez estudiantes consideran que su carrera efectivamente prepara de forma adecuada perfiles híbridos que combinen competencias de Ciencia de Datos y Ciberseguridad. Por otra parte, 9 estudiantes (50 %) seleccionaron la opción "ni de acuerdo ni en desacuerdo", lo que evidencia un alto grado de neutralidad o indefinición respecto de esta valoración. Este porcentaje sugiere que la mitad del grupo no tiene una percepción clara sobre si el programa realmente contribuye a la formación de estos perfiles integrados, lo que puede estar vinculado a una falta de comunicación explícita de este propósito formativo o a la ausencia de experiencias que lo hagan visible.

Finalmente, 1 estudiante (5,6 %) declaró estar "en desacuerdo" y 5 estudiantes (27,8 %) "totalmente en desacuerdo", sumando un 33,4 % que considera que la carrera no prepara adecuadamente perfiles híbridos Ciencia de Datos–Ciberseguridad. Desde una perspectiva descriptiva, la proporción de estudiantes que no perciben una preparación adecuada (33,4 %) y el elevado porcentaje de respuestas neutras (50 %) superan ampliamente a quienes valoran positivamente dicha preparación (16,7 %). Esto sugiere que, para la mayoría del estudiantado, la formación recibida no se traduce en una imagen clara ni sólida de un perfil profesional híbrido que integre de manera explícita competencias de Ciencia de Datos y Ciberseguridad.

**Figura 9**




*Contenidos y prácticas que integren ciencia de datos y ciberseguridad en el plan de estudio*

*Nota:* En relación con la afirmación: «Creo que sería necesario incorporar más contenidos y prácticas que integren Ciencia de Datos y Ciberseguridad en el plan de estudio», las respuestas de los 20 estudiantes reflejan un consenso ampliamente favorable hacia el fortalecimiento de esta integración curricular.

En primer lugar, 10 participantes indicaron estar "de acuerdo" con la afirmación, lo que representa el 50 % de la muestra, mientras que 8 estudiantes (40 %) manifestaron estar "totalmente de acuerdo". En conjunto, el 90 % de los encuestados considera necesaria la incorporación de más contenidos y actividades prácticas que articulen de manera explícita Ciencia de Datos y Ciberseguridad en la carrera. Por otra parte, solo 1 estudiante (5 %) seleccionó la opción "ni de acuerdo ni en desacuerdo", evidenciando un nivel prácticamente marginal de neutralidad frente a esta propuesta. Finalmente, 1 estudiante (5 %) declaró estar "totalmente en desacuerdo", constituyendo el único caso que no percibe necesaria dicha ampliación e integración. De forma general, la abrumadora mayoría de respuestas favorables (90 %) pone de manifiesto una demanda clara del estudiantado por un mayor énfasis formativo en la relación que debe darse entre Ciencia de Datos y Ciberseguridad, tanto a nivel de contenidos teóricos como de experiencias prácticas (proyectos, laboratorios, estudios de caso), mientras que la oposición a esta idea es prácticamente inexistente.

**Dimensión 4. Interés en la especialización y proyección profesional**

**Figura 11**

*Estudio en ciencia de datos*


***Nota:*** *Interés de realizar estudios elevados en ciencias de datos (maestrías y doctorados)*

Una distribución diversa en cuanto a sus aspiraciones académicas de máximo nivel. En primer lugar, 6 participantes indicaron estar "de acuerdo" con la afirmación, lo que representa el 27,3 % de la muestra, mientras que 4 estudiantes (18,2 %) manifestaron estar "totalmente de acuerdo". En conjunto, el 45,5 % de los encuestados expresa una intención positiva de realizar estudios de doctorado en Ciencia de Datos. Por otra parte, 5 estudiantes (22,7 %) seleccionaron la opción "ni de acuerdo ni en desacuerdo", lo que refleja un nivel moderado de indecisión o indefinición respecto a la proyección hacia estudios doctorales, posiblemente vinculado a la falta de claridad sobre oportunidades, requisitos o preferencias profesionales futuras. Finalmente, 3 estudiantes (13,6 %) declararon estar "en desacuerdo" y 4 (18,2 %) "totalmente en desacuerdo", sumando un 31,8 % que no tiene la intención de realizar estudios elevados en Ciencia de Datos.

De esta manera se observa que la proporción de estudiantes con interés de cursar un doctorado (45,5 %) es superior a la de quienes descartan esta opción (31,8 %), aunque existe aún un porcentaje relevante (22,7 %) que se mantiene en una posición neutral. Esto sugiere un interés considerable, pero no mayoritario ni plenamente definido, hacia trayectorias académicas avanzadas en el campo de la Ciencia de Datos.

## RESULTADOS

Los resultados evidencian un patrón consistente: aunque los estudiantes muestran un interés significativo y un nivel de conocimiento percibido moderado en Ciencia de Datos y Ciberseguridad, este no se traduce plenamente en competencias aplicadas ni en una percepción clara de formación interdisciplinaria.

En la Dimensión 1, se observa una base conceptual aceptable, pero con importantes desigualdades, especialmente en estadística básica y gestión de incidentes de seguridad. Estas brechas en componentes críticos pueden limitar el desarrollo de competencias avanzadas, en línea con estudios que identifican debilidades en habilidades técnicas especializadas dentro de estos campos (Muneer Ahmad et al., 2020; Katrin Becker et al., 2017; Abhijit Behl & Kritika Behl, 2017).

En la Dimensión 2, la autopercepción de competencia es moderada y presenta altos niveles de incertidumbre, especialmente en tareas complejas. Esto puede explicarse a partir del concepto de autoeficacia de Albert Bandura (1997), que vincula la percepción de capacidad con la experiencia práctica. En este sentido, la limitada exposición a actividades aplicadas afecta el desarrollo de habilidades en ciberseguridad y análisis de datos (Michael J. Katz et al., 2014; Alessandro Oltramari et al., 2018).

En la Dimensión 3, la integración entre Ciencia de Datos y Ciberseguridad es percibida como débil o poco visible, lo que sugiere una formación fragmentada. Este resultado coincide con estudios que señalan la tendencia a abordar la ciberseguridad de forma aislada y con escasa articulación interdisciplinaria (Philip Pusey & William Sadera, 2011; Greg Conti et al., 2018).

En la Dimensión 4, pese a estas limitaciones, se observa un alto interés por la especialización en perfiles híbridos. Esta tendencia es coherente con la creciente demanda de competencias integradas en análisis de datos y ciberseguridad (Agnieszka L. Buczak & Erhan Guven, 2020), aunque también refleja la persistencia de una brecha entre formación y exigencias del entorno profesional (Muhammad Naseer et al., 2021).

En conjunto, los resultados evidencian una tensión entre el interés y la base conceptual de los estudiantes, y las limitaciones en la integración curricular y el desarrollo de competencias aplicadas. Esto sugiere la necesidad de fortalecer los fundamentos técnicos, promover una mayor articulación entre disciplinas y ampliar las experiencias prácticas interdisciplinarias.

## CONCLUSIONES

Los resultados de la presente investigación permiten concluir que los estudiantes encuestados presentan un nivel de conocimiento predominantemente intermedio en Ciencia de Datos y Ciberseguridad, con mayores fortalezas en conceptos generales y reconocimiento de tipos de ataques, pero con debilidades significativas en áreas clave como la estadística aplicada y la gestión de incidentes de seguridad. Esta situación evidencia una base formativa aceptable, aunque heterogénea y con vacíos relevantes en competencias fundamentales para el desempeño profesional.

En cuanto a la percepción de competencias, se identificó que, si bien una proporción importante de estudiantes manifiesta confianza en la aplicación básica de técnicas de análisis de datos, existe una disminución progresiva de la autoeficacia en tareas más complejas, como la detección de anomalías, la clasificación de amenazas y, especialmente, la interpretación de modelos de datos en contextos de ciberseguridad. Esto sugiere una brecha entre el conocimiento teórico y su aplicación práctica, así como limitaciones en el desarrollo de habilidades analíticas avanzadas.

Respecto a la integración formativa, los hallazgos evidencian una percepción mayoritariamente baja o indefinida sobre la articulación curricular entre Ciencia de Datos y Ciberseguridad. La escasa presencia de actividades prácticas integradas y la limitada identificación de un enfoque formativo orientado a perfiles híbridos reflejan una estructura curricular fragmentada, que dificulta la consolidación de competencias interdisciplinarias y la transferencia efectiva del conocimiento.

No obstante, en la dimensión de proyección profesional, se observa un interés significativo por la especialización, tanto en estudios avanzados en Ciencia de Datos como en la vinculación entre esta disciplina y la Ciberseguridad. Este interés, aunque no generalizado, representa una oportunidad para fortalecer la oferta académica mediante propuestas formativas más integradas, pertinentes y orientadas a las demandas del entorno profesional.

En conjunto, los resultados ponen de manifiesto la necesidad de fortalecer la formación en competencias aplicadas, promover la integración curricular entre disciplinas y ampliar las experiencias prácticas interdisciplinarias, con el fin de favorecer el desarrollo de perfiles

profesionales capaces de responder a los desafíos actuales en el ámbito de la Ciencia de Datos aplicada a la Ciberseguridad.

## REFERENCIAS BIBLIOGRÁFICAS


Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection [Un estudio sobre métodos de minería de datos y aprendizaje automático para la detección de intrusiones en ciberseguridad]. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Buczak, A. L., & Guven, E. (2020). Cybersecurity data science: An overview from machine learning perspective [Ciencia de datos en ciberseguridad: Una visión general desde la perspectiva del aprendizaje automático]. Journal of Big Data, 7(1). https://doi.org/10.1186/s40537-020-00318-5

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs [Educación en ciberseguridad: Evolución de la disciplina y análisis de programas de maestría]. Computers & Security, 75, 24–35.

European Unión Agency for Cybersecurity. (2023). ENISA threat landscape 2023: July 2022 to June 2023 [Panorama de amenazas ENISA 2023: Julio de 2022 a junio de 2023]. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

Gamarra Camargo, P. M., Camargo Zamata, P. M., & Rodríguez Saavedra, L. (2024). Autoeficacia académica y autoestima en estudiantes universitarios. Areté, Revista Digital del Doctorado en Educación, 10(19), 69–85. https://doi.org/10.55560/arete.2024.19.10.4

Jiménez Sánchez, V. G., Tipanluisa Masabanda, R. I., & León Espinoza, C. J. (2025). Ciberseguridad en la educación superior: Evaluación y estrategias de formación. Technology Rain Journal, 4(2). https://doi.org/10.55204/trj.v4i1.e94

Mikroyannidis, A., et al. (2024). Curriculum, pedagogy, and teaching/learning strategies in data science education [Currículo, pedagogía y estrategias de enseñanza-aprendizaje en la educación en ciencia de datos]. Education Sciences, 15(2).

PricewaterhouseCoopers. (2023). 2023 global digital trust insights: Main report [Perspectivas globales de confianza digital 2023: Informe principal]. https://es.scribd.com/document/610110785/pwc-2023-global-digital-trust-insights-main-report

Provost, F., & Fawcett, T. (2013). Data science and its relationship to big data and data-driven decision making [La ciencia de datos y su relación con big data y la toma de decisiones basada en datos]. Big Data, 1(1), 51–59. https://doi.org/10.1089/big.2013.1508

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection [Fuera del mundo cerrado: Sobre el uso del aprendizaje automático para la detección de intrusiones en redes]. In 2010 IEEE Symposium on Security and Privacy (pp. 305–316). https://doi.org/10.1109/SP.2010.25

Tian, J. (2025). Integrating artificial intelligence into the cybersecurity curriculum in higher education: A systematic literature review [Integración de la inteligencia artificial en el currículo de ciberseguridad en educación superior: Una revisión sistemática]. Education Sciences, 15(11), 1540. https://doi.org/10.3390/educsci15111540