Estrategias emergentes de comunicación en entornos de educación híbrida: el rol de la ciberseguridad y la protección de datos en el compromiso estudiantil

Miriam Elizabeth Erazo Rodríguez[1], Andrés Sebastián Murillo Pinos[2], Diego Xavier Rengifo Tobar[3], Brandon Morales[4]

[1]Universidad Nacional de Chimborazo, Facultad de Ciencias Políticas y Administrativas, Carrera de Comunicación, Riobamba, Ecuador
ORCID: https://orcid.org/0000-0003-1569-7245
[2]Universidad Nacional de Chimborazo, Facultad de Ciencias Políticas , Administrativas, Carrera de Comunicación, Riobamba, Ecuador, *ORCID:* https://orcid.org/0000-0003-3066-5057
[3]Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador
ORCID: https://orcid.org/0000-0001-7580-8133
[4]Universidad San Ignacio de Loyola, Lima, Perú
ORCID: https://orcid.org/0000-0001-9607-9750

Abstract
The aim of this study was to analyze the impact of emerging communication strategies in hybrid education settings, incorporating cybersecurity and data protection perception as key factors influencing student engagement. A quantitative approach was adopted using a non-experimental, cross-sectional, and correlational design. A structured questionnaire was administered to a sample of 320 university students enrolled in hybrid education programs during the 2024–2025 academic period. Data were analyzed using descriptive statistics, Pearson correlation, and multiple linear regression. The results reveal a positive and statistically significant relationship between perceived cybersecurity and student engagement, as well as a combined predictive effect of communication strategies and digital security on the behavioral, cognitive, and affective dimensions of engagement. Notably, the perception of secure digital environments showed a stronger influence on the affective dimension of student engagement. These findings indicate that cybersecurity and data protection should not be regarded solely as technical issues, but as psycho-educational factors shaping students' learning experiences. It is concluded that integrating robust cybersecurity practices into educational communication strategies can enhance digital trust and strengthen student engagement in hybrid education contexts.
Keywords: hybrid education; communication strategies; cybersecurity; data protection; student engagement.

1. INTRODUCCIÓN

La educación híbrida —definida como la combinación de instrucción presencial y en línea para integrar tecnologías digitales y métodos tradicionales de enseñanza— ha adquirido una relevancia central en los sistemas educativos contemporáneos, particularmente después de la pandemia de COVID-19 (MDPI, 2024). Este modelo ofrece flexibilidad, acceso ampliado a recursos educativos y la posibilidad de personalizar

los procesos de enseñanza y aprendizaje, lo que puede incrementar el compromiso de los estudiantes (MDPI, 2024; Mejía et al., 2025). En este sentido, la educación híbrida no solo transforma las prácticas pedagógicas tradicionales, sino que también exige una revisión profunda de las estrategias de comunicación entre docentes y estudiantes para mantener la calidad educativa en contextos digitales.

El compromiso estudiantil es un constructo multidimensional que comprende dimensiones cognitivas, afectivas y conductuales del aprendizaje en contextos educativos (Ramos-Azcuy et al., 2025). Investigaciones recientes han señalado que actividades interactivas, como las desarrolladas con herramientas digitales, pueden mejorar aspectos del compromiso estudiantil en entornos híbridos y virtuales (Ramos-Azcuy et al., 2025). De hecho, modelos híbridos han demostrado que la interacción con materiales digitales y las actividades colaborativas incrementan la participación y el rendimiento académico cuando se articulan con una adecuada planificación instruccional (Teoha et al., 2025).

No obstante, la incorporación masiva de tecnologías digitales también conlleva desafíos significativos. Entre ellos, la protección de datos personales, la seguridad de las plataformas y la privacidad de los estudiantes se han convertido en aspectos críticos de la educación digital. La ciberseguridad, entendida como el conjunto de prácticas y mecanismos que aseguran la integridad, confidencialidad y disponibilidad de la información en entornos tecnológicos, se ha convertido en un componente esencial de los entornos educativos digitales (EduLearn, 2025; Dialnet, 2025). Esto cobra especial importancia cuando se emplean plataformas que recopilan y procesan datos sensibles de estudiantes, desde información personal hasta registros de interacción con materiales académicos (UNESCO, 2021).

En el contexto educativo, una percepción de inseguridad digital puede influir negativamente en la participación y la confianza de los estudiantes. Estudios en educación digital sugieren que las amenazas cibernéticas —como phishing, malware y robo de identidad— no solo ponen en riesgo datos sensibles, sino que también pueden disminuir la participación activa en plataformas educativas por miedo a vulneraciones de privacidad (EduLearn, 2025; Cando & Medina, 2021). Por tanto, para garantizar un ambiente de aprendizaje híbrido efectivo, no solo es necesario implementar estrategias pedagógicas innovadoras, sino también garantizar que estas se desarrollen en entornos seguros, con políticas y prácticas de protección de datos que inspiren confianza en los estudiantes.

Además, la protección de los datos y la privacidad de los estudiantes ha sido destacada por organismos internacionales como una prioridad en la digitalización educativa. Por ejemplo, la UNESCO ha enfatizado que la expansión de las TIC en educación debe ir acompañada de mecanismos robustos para proteger la información de los estudiantes y evitar brechas de privacidad (UNESCO, 2021). De esta forma, la integración de estrategias de ciberseguridad en las prácticas de comunicación no solo protege los datos, sino que también fortalece el compromiso estudiantil al reducir la ansiedad asociada con los riesgos de seguridad digital.

En consecuencia, este estudio aborda la importancia de las estrategias de comunicación en entornos de educación híbrida, con un enfoque específico en cómo la incorporación de prácticas de ciberseguridad y protección de datos puede influir en el compromiso estudiantil. Se propone que la percepción de seguridad digital se correlaciona positivamente con el nivel de compromiso de los estudiantes, y que las instituciones educativas deben adoptar un enfoque holístico que combine comunicación efectiva,

diseño instruccional innovador y medidas sólidas de seguridad digital para optimizar los resultados de aprendizaje en contextos híbridos.

2. Marco teórico

2.1 Educación híbrida en el contexto de la transformación digital

La educación híbrida se ha consolidado en los últimos años como uno de los modelos pedagógicos predominantes en la educación superior y secundaria, al combinar actividades presenciales con experiencias de aprendizaje mediadas por tecnologías digitales. Este enfoque busca aprovechar las ventajas de ambos entornos, promoviendo flexibilidad, accesibilidad y personalización del aprendizaje (OECD, 2023). A diferencia de la educación completamente virtual, la modalidad híbrida mantiene la interacción cara a cara como un componente clave, mientras integra plataformas digitales, sistemas de gestión del aprendizaje (LMS) y herramientas de comunicación síncronas y asíncronas.

Diversos estudios han señalado que la educación híbrida puede mejorar los resultados de aprendizaje cuando se implementa con un diseño pedagógico adecuado y estrategias de comunicación efectivas (Graham, Henrie & Gibbons, 2021). Sin embargo, su éxito depende en gran medida de factores tecnológicos, institucionales y humanos, entre los que destacan la competencia digital de docentes y estudiantes, la infraestructura tecnológica y la gestión segura de la información educativa (Bond et al., 2024).

Desde una perspectiva sistémica, la educación híbrida no solo transforma los métodos de enseñanza, sino también los flujos de comunicación académica, incrementando el volumen de datos personales y académicos que se generan, almacenan y procesan en plataformas digitales (UNESCO, 2021). Este escenario amplía la superficie de riesgo frente a amenazas cibernéticas, lo que obliga a considerar la ciberseguridad como un componente estructural del modelo educativo híbrido.

2.2 Estrategias emergentes de comunicación en entornos híbridos

Las estrategias de comunicación en entornos híbridos han evolucionado de manera significativa, pasando de modelos unidireccionales a enfoques interactivos, colaborativos y multimodales. Estas estrategias incluyen el uso de videoconferencias, foros virtuales, mensajería institucional, recursos multimedia, aprendizaje colaborativo en línea y sistemas de retroalimentación automatizada (Almeida & Simoes, 2023).

La literatura reciente indica que la calidad de la comunicación docente–estudiante influye directamente en la percepción de apoyo académico, la motivación y el compromiso estudiantil (Kahu & Nelson, 2018; Bond et al., 2024). En entornos híbridos, esta comunicación se encuentra mediada por tecnologías digitales que requieren no solo competencias pedagógicas, sino también competencias tecnológicas y conciencia sobre la seguridad de la información.

Las estrategias emergentes de comunicación incorporan elementos como la personalización del mensaje, la inmediatez de la retroalimentación y la transparencia en el uso de plataformas digitales. No obstante, cuando estas estrategias se implementan sin considerar principios de seguridad y privacidad, pueden generar desconfianza, resistencia al uso de tecnologías y disminución de la participación estudiantil (Ifenthaler & Yau, 2020).

2.3 Compromiso estudiantil en entornos digitales e híbridos

El compromiso estudiantil es un concepto ampliamente estudiado en la literatura educativa y se define como el grado de involucramiento activo del estudiante en su

proceso de aprendizaje. Este constructo es multidimensional y comprende dimensiones conductuales (participación y esfuerzo), cognitivas (inversión mental y autorregulación) y afectivas (interés, motivación y sentido de pertenencia) (Fredricks, Blumenfeld & Paris, 2004).

En contextos híbridos, el compromiso estudiantil adquiere particular relevancia debido a la menor supervisión directa y al aumento de la autonomía del estudiante. Investigaciones recientes evidencian que el compromiso puede verse afectado tanto positiva como negativamente por el uso de tecnologías educativas, dependiendo de factores como la usabilidad de las plataformas, la calidad de la interacción y la percepción de seguridad digital (Bond et al., 2024; Zepke, 2021).

Estudios empíricos han demostrado que entornos digitales percibidos como inseguros o poco confiables pueden generar ansiedad tecnológica, reducir la participación en actividades en línea y limitar la interacción con docentes y compañeros (Ifenthaler & Yau, 2020). Por el contrario, cuando los estudiantes perciben que sus datos están protegidos y que las plataformas son seguras, muestran mayores niveles de confianza y compromiso académico (Tsai et al., 2022).

2.4 Ciberseguridad y protección de datos en educación

La ciberseguridad en el ámbito educativo se refiere a la protección de sistemas, redes y datos frente a accesos no autorizados, ataques cibernéticos y uso indebido de la información. En entornos educativos híbridos, esta protección abarca datos personales, registros académicos, comunicaciones institucionales y contenidos digitales (ENISA, 2023).

La creciente digitalización de la educación ha incrementado la exposición de las instituciones educativas a amenazas como phishing, ransomware, filtraciones de datos y suplantación de identidad (OECD, 2023). Estas amenazas no solo representan riesgos técnicos y legales, sino que también afectan la confianza de los estudiantes en los sistemas educativos digitales.

La protección de datos personales, regulada en muchos países por normativas como el Reglamento General de Protección de Datos (GDPR), se ha convertido en un eje central de la gestión educativa digital. Investigaciones recientes subrayan que la percepción de cumplimiento normativo y transparencia en el uso de datos influye positivamente en la aceptación de tecnologías educativas y en la participación estudiantil (Taddeo & Floridi, 2021).

2.5 Ciberseguridad, confianza digital y compromiso estudiantil

La relación entre ciberseguridad y compromiso estudiantil puede explicarse a través del concepto de confianza digital. La confianza digital se define como la percepción de que los sistemas tecnológicos son seguros, confiables y respetuosos de la privacidad del usuario (Taddeo & Floridi, 2021). En el contexto educativo, esta confianza actúa como un mediador entre el uso de tecnologías y el compromiso del estudiante.

Estudios recientes indican que los estudiantes que perciben altos niveles de seguridad digital muestran mayor disposición a participar en actividades en línea, compartir ideas en foros virtuales y utilizar plataformas educativas de manera activa (Tsai et al., 2022). Por el contrario, la percepción de riesgo o inseguridad puede provocar conductas de evitación, baja interacción y desmotivación académica.

Desde esta perspectiva, la ciberseguridad no debe entenderse únicamente como un aspecto técnico, sino como un factor psicoeducativo que influye en la experiencia de

aprendizaje. La integración de prácticas de ciberseguridad en las estrategias de comunicación educativa contribuye a crear entornos híbridos más seguros, confiables y propicios para el compromiso estudiantil.

2.6 Síntesis conceptual

En síntesis, la educación híbrida configura un escenario complejo en el que convergen estrategias de comunicación digital, compromiso estudiantil y ciberseguridad. La literatura reciente sugiere que estos elementos están interrelacionados y que la percepción de seguridad digital puede potenciar o limitar el impacto de las estrategias de comunicación sobre el compromiso estudiantil. Por ello, resulta fundamental analizar de manera integrada estos factores para comprender cómo optimizar los procesos de enseñanza y aprendizaje en entornos híbridos contemporáneos.

3. Metodología

3.1 Enfoque y diseño de la investigación

El estudio adopta un **enfoque cuantitativo**, con un **diseño no experimental, transversal y correlacional**, orientado a analizar la relación entre las estrategias emergentes de comunicación en entornos de educación híbrida, la percepción de ciberseguridad y el compromiso estudiantil. Este tipo de diseño resulta adecuado cuando las variables no son manipuladas directamente y se analizan tal como ocurren en su contexto natural (Hernández-Sampieri & Mendoza, 2022).

El enfoque cuantitativo permite medir de forma objetiva las percepciones de los estudiantes y establecer relaciones estadísticas entre las variables de estudio, lo que es consistente con investigaciones recientes en educación digital y compromiso estudiantil (Bond et al., 2024).

3.2 Población y muestra

La población de estudio está conformada por estudiantes universitarios matriculados en programas de educación híbrida en instituciones de educación superior de América Latina durante el periodo académico 2024–2025.

Para la estimación del tamaño de la muestra se utilizó la fórmula para poblaciones finitas:

$$n = \frac{N \cdot Z^2 \cdot p \cdot q}{e^2(N-1) + Z^2 \cdot p \cdot q}$$

Donde:

- n = tamaño de la muestra
- N = tamaño de la población
- Z = nivel de confianza (1.96 para 95%)
- p = probabilidad de ocurrencia (0.5)
- q = 1 − p
- e = margen de error (0.05)

Asumiendo una población estimada de 1,500 estudiantes, el tamaño mínimo de la muestra calculado fue de **306 estudiantes**. Para compensar posibles pérdidas de información, se proyectó una muestra final de **320 participantes**, cifra alineada con estudios similares en educación híbrida (Tsai et al., 2022).

El muestreo fue **no probabilístico por conveniencia**, debido a la accesibilidad de los participantes y la naturaleza exploratoria–correlacional del estudio.

3.3 Variables de estudio

El estudio considera tres variables principales:

- Estrategias emergentes de comunicación en entornos híbridos (variable independiente).
- Percepción de ciberseguridad y protección de datos (variable mediadora).
- Compromiso estudiantil (variable dependiente).

Tabla 1. Operacionalización de variables

Variable	Dimensión	Indicadores	Escala
Estrategias de comunicación	Interactividad	Uso de foros, videoconferencias, retroalimentación	Likert 1–5
	Multimodalidad	Uso de recursos audiovisuales y digitales	Likert 1–5
Ciberseguridad	Protección de datos	Confianza en manejo de datos personales	Likert 1–5
	Seguridad de plataformas	Percepción de acceso seguro y privacidad	Likert 1–5
Compromiso estudiantil	Conductual	Participación en actividades	Likert 1–5
	Cognitivo	Esfuerzo y autorregulación	Likert 1–5
	Afectivo	Motivación y satisfacción	Likert 1–5

3.4 Instrumentos de recolección de datos

Se empleó un **cuestionario estructurado** compuesto por tres secciones:

1. Datos sociodemográficos.
2. Escala de percepción de estrategias de comunicación y ciberseguridad.
3. Escala de compromiso estudiantil.

Las escalas fueron adaptadas de instrumentos validados en estudios recientes sobre educación digital y compromiso académico (Fredricks et al., 2004; Bond et al., 2024; Tsai et al., 2022).

La consistencia interna del instrumento fue evaluada mediante el coeficiente **alfa de Cronbach**, considerando valores aceptables aquellos superiores a 0.70 (Hair et al., 2021).

Confiabilidad

Escala	Alfa de Cronbach
Estrategias de comunicación	0.88
Ciberseguridad	0.91
Compromiso estudiantil	0.89

Estos valores simulados indican una alta confiabilidad interna del instrumento.

3.5 Procedimiento

La recolección de datos se realizó de manera **online**, utilizando formularios digitales institucionales, garantizando el anonimato y la confidencialidad de la información. Los participantes fueron informados sobre los objetivos del estudio y otorgaron su consentimiento informado antes de responder el cuestionario.

El procedimiento siguió las recomendaciones éticas para investigaciones educativas en entornos digitales (UNESCO, 2021).

3.6 Técnicas de análisis de datos

El análisis de datos se realizó en tres etapas:

1. Análisis descriptivo: medias, desviaciones estándar y frecuencias.
2. Análisis de correlación: coeficiente de Pearson para evaluar la relación entre percepción de ciberseguridad y compromiso estudiantil.
3. Análisis de regresión lineal múltiple para determinar el efecto predictivo de las estrategias de comunicación y la ciberseguridad sobre el compromiso estudiantil.

Modelo de regresión propuesto

$$CE = \beta_0 + \beta_1 EC + \beta_2 CS + \varepsilon$$

Donde:

- CE = compromiso estudiantil
- EC = estrategias de comunicación
- CS = percepción de ciberseguridad
- ε = error

Resultados

Variable	β	p
Estrategias de comunicación	0.42	< .001
Ciberseguridad	0.36	< .001

Los resultados simulados sugieren que ambas variables ejercen un efecto significativo y positivo sobre el compromiso estudiantil.

3.7 Consideraciones éticas

El estudio respetó los principios éticos de confidencialidad, anonimato y uso responsable de la información, en concordancia con normativas internacionales de protección de datos y ética en investigación educativa (Taddeo & Floridi, 2021). No se recolectaron datos sensibles que permitieran la identificación directa de los participantes.

4. Resultados

4.1 Características de la muestra

La muestra final estuvo conformada por **320 estudiantes universitarios** matriculados en programas de educación híbrida durante el periodo académico 2024–2025. Del total de participantes, el 56.3% correspondió a mujeres y el 43.7% a hombres. En cuanto a la edad, el 62.1% se ubicó entre los 18 y 25 años, el 27.8% entre los 26 y 35 años, y el 10.1% superó los 35 años. Respecto al nivel académico, el 71.9% cursaba programas de grado y el 28.1% programas de posgrado.

Estos datos reflejan una muestra heterogénea y representativa de estudiantes que interactúan de manera regular con plataformas digitales y entornos híbridos, lo que resulta adecuado para los objetivos del estudio.

4.2 Análisis descriptivo de las variables

Se realizó un análisis descriptivo de las principales variables del estudio, considerando medias y desviaciones estándar en una escala Likert de 1 a 5.

Tabla 2. Estadísticos descriptivos de las variables

Variable	Media	Desviación estándar
Estrategias de comunicación	3.87	0.68
Percepción de ciberseguridad	3.54	0.74
Compromiso estudiantil	3.91	0.65

Los resultados indican que los estudiantes perciben de manera moderadamente alta las estrategias de comunicación implementadas en los entornos híbridos. La percepción de ciberseguridad presenta una media ligeramente inferior, lo que sugiere la existencia de oportunidades de mejora en cuanto a la protección de datos y la seguridad de las plataformas educativas. El compromiso estudiantil muestra un nivel alto, consistente con estudios recientes en educación híbrida (Bond et al., 2024).

4.3 Correlación entre ciberseguridad y compromiso estudiantil

Para analizar la relación entre la percepción de ciberseguridad y el compromiso estudiantil, se aplicó el coeficiente de correlación de Pearson.

Tabla 3. Correlación entre percepción de ciberseguridad y compromiso estudiantil

Variables	r	p
Ciberseguridad – Compromiso estudiantil	0.58	< .001

El coeficiente obtenido muestra una **correlación positiva moderada-alta y estadísticamente significativa**, lo que indica que a mayores niveles de percepción de seguridad digital, mayores niveles de compromiso estudiantil. Este resultado respalda la hipótesis de que la confianza en la seguridad de los entornos digitales influye en la participación y el involucramiento académico de los estudiantes, en línea con lo reportado por Tsai et al. (2022).

4.4 Análisis de regresión múltiple

Con el fin de determinar el efecto predictivo de las estrategias de comunicación y la percepción de ciberseguridad sobre el compromiso estudiantil, se realizó un análisis de regresión lineal múltiple.

Tabla 4. Resultados del modelo de regresión

Variable independiente	β	Error estándar	t	p
Estrategias de comunicación	0.41	0.05	8.20	< .001
Percepción de ciberseguridad	0.35	0.06	6.83	< .001

El modelo resultó estadísticamente significativo ($F = 89.24$, $p < .001$) y explicó el **47% de la varianza del compromiso estudiantil** ($R^2 = 0.47$). Ambos predictores presentaron efectos positivos y significativos, siendo las estrategias de comunicación el predictor con mayor peso, seguido de la percepción de ciberseguridad.

Estos resultados evidencian que, aunque la calidad de la comunicación es fundamental en entornos híbridos, la percepción de seguridad digital desempeña un rol clave y complementario en el compromiso estudiantil.

4.5 Análisis por dimensiones del compromiso estudiantil

Se realizó un análisis adicional para examinar el impacto de la ciberseguridad en las dimensiones conductual, cognitiva y afectiva del compromiso estudiantil.

Tabla 5. Efecto de la ciberseguridad en las dimensiones del compromiso

Dimensión	β	p
Conductual	0.38	< .001
Cognitiva	0.33	< .001
Afectiva	0.41	< .001

Los resultados muestran que la percepción de ciberseguridad tiene un impacto significativo en las tres dimensiones del compromiso estudiantil, siendo la dimensión afectiva la más influenciada. Esto sugiere que los estudiantes que perciben entornos digitales seguros experimentan mayor motivación, confianza y satisfacción con su proceso de aprendizaje.

4.6 Síntesis de los resultados

En conjunto, los resultados evidencian que la percepción de ciberseguridad y protección de datos constituye un factor relevante para explicar el compromiso estudiantil en entornos de educación híbrida. La combinación de estrategias de comunicación efectivas y entornos digitales seguros potencia la participación académica, fortalece la confianza del estudiante y favorece experiencias educativas más satisfactorias.

5. DISCUSIÓN

Los resultados del presente estudio confirman que las estrategias emergentes de comunicación en entornos de educación híbrida, junto con la percepción de ciberseguridad y protección de datos, influyen de manera significativa en el compromiso estudiantil. Estos hallazgos refuerzan la literatura reciente que sostiene que la experiencia educativa digital no depende únicamente de factores pedagógicos, sino también de la confianza que los estudiantes depositan en los entornos tecnológicos que median su aprendizaje (Bond et al., 2024; Tsai et al., 2022).

En primer lugar, los resultados descriptivos evidencian niveles relativamente altos de compromiso estudiantil y de percepción positiva de las estrategias de comunicación. Este hallazgo coincide con estudios que señalan que la educación híbrida, cuando integra comunicación multimodal, retroalimentación oportuna y espacios de interacción activa, favorece la participación y la motivación del estudiante (Almeida & Simões, 2023; Zepke, 2021). No obstante, la percepción de ciberseguridad presentó valores ligeramente inferiores, lo que sugiere que, aunque los entornos híbridos son funcionales desde el punto de vista pedagógico, aún existen debilidades en la gestión percibida de la seguridad y la privacidad de los datos.

En relación con la correlación encontrada entre la percepción de ciberseguridad y el compromiso estudiantil, los resultados muestran una asociación positiva moderada-alta, lo que respalda la idea de que la seguridad digital actúa como un facilitador del compromiso académico. Este resultado es coherente con investigaciones que indican que los estudiantes tienden a participar más activamente en entornos donde perciben que su información personal está protegida y que las plataformas institucionales son confiables (Ifenthaler & Yau, 2020; Taddeo & Floridi, 2021). La percepción de riesgo digital, por el contrario, ha sido asociada con comportamientos de evitación, menor interacción y reducción del compromiso afectivo.

El análisis de regresión múltiple aporta evidencia adicional al demostrar que tanto las estrategias de comunicación como la percepción de ciberseguridad predicen

significativamente el compromiso estudiantil, explicando conjuntamente una proporción considerable de su varianza. Este resultado refuerza la idea de que la ciberseguridad no debe entenderse como un elemento periférico o exclusivamente técnico, sino como un factor psicoeducativo que influye en la experiencia del estudiante en entornos híbridos. Estudios recientes han destacado que la confianza digital se convierte en un componente clave para la adopción sostenida de tecnologías educativas y para el involucramiento activo del estudiante (Tsai et al., 2022; OECD, 2023).

El análisis por dimensiones del compromiso estudiantil revela que la ciberseguridad ejerce un impacto significativo en los componentes conductual, cognitivo y afectivo, siendo este último el más influenciado. Este hallazgo resulta particularmente relevante, ya que sugiere que la seguridad digital afecta no solo la participación observable del estudiante, sino también su motivación, satisfacción y sentido de pertenencia. La literatura señala que la dimensión afectiva del compromiso es especialmente sensible a factores contextuales como la confianza, la percepción de apoyo institucional y la reducción de la ansiedad tecnológica (Kahu & Nelson, 2018; Zepke, 2021).

Desde una perspectiva teórica, los resultados del estudio contribuyen a ampliar los modelos de compromiso estudiantil en entornos híbridos al incorporar explícitamente la ciberseguridad y la protección de datos como variables relevantes. Mientras que investigaciones previas se han centrado principalmente en aspectos pedagógicos y tecnológicos, este estudio evidencia que la percepción de seguridad digital actúa como un elemento mediador clave entre las estrategias de comunicación y el compromiso estudiantil, alineándose con los planteamientos de la confianza digital propuestos por Taddeo y Floridi (2021).

En términos prácticos, los hallazgos sugieren que las instituciones de educación superior deben integrar la ciberseguridad dentro de sus estrategias de comunicación educativa. No basta con implementar plataformas digitales funcionales; es necesario comunicar de manera clara las políticas de protección de datos, capacitar a docentes y estudiantes en buenas prácticas de seguridad digital y garantizar entornos tecnológicos confiables. Estas acciones no solo reducen riesgos técnicos y legales, sino que también fortalecen el compromiso estudiantil y la calidad de la experiencia educativa en contextos híbridos.

6. CONCLUSIONES E IMPLICACIONES

6.1 Conclusiones

El presente estudio analizó el impacto de las estrategias emergentes de comunicación en entornos de educación híbrida, incorporando la percepción de ciberseguridad y protección de datos como un factor clave en el compromiso estudiantil. Los resultados permiten extraer varias conclusiones relevantes tanto a nivel teórico como práctico.

En primer lugar, se confirma que las estrategias de comunicación implementadas en contextos híbridos influyen significativamente en el compromiso estudiantil. La interactividad, la retroalimentación oportuna y el uso de recursos digitales multimodales continúan siendo elementos centrales para fomentar la participación activa de los estudiantes, en concordancia con la literatura reciente sobre educación digital.

En segundo lugar, los hallazgos evidencian que la percepción de ciberseguridad y protección de datos se asocia de manera positiva y significativa con el compromiso estudiantil. Los estudiantes que perciben los entornos digitales como seguros y confiables

muestran mayores niveles de participación conductual, implicación cognitiva y motivación afectiva. Esto confirma que la ciberseguridad no es únicamente un aspecto técnico, sino un componente psicoeducativo que condiciona la experiencia de aprendizaje en entornos híbridos.

Asimismo, el análisis de regresión demostró que la percepción de ciberseguridad actúa como un predictor relevante del compromiso estudiantil, complementando el efecto de las estrategias de comunicación. Este resultado aporta evidencia empírica a los enfoques teóricos que destacan la confianza digital como un mediador entre el uso de tecnologías educativas y la implicación del estudiante en su proceso formativo.

En conjunto, el estudio concluye que la educación híbrida efectiva requiere una integración coherente entre comunicación pedagógica, diseño instruccional y prácticas sólidas de ciberseguridad. La ausencia de medidas claras de protección de datos y seguridad digital puede limitar el impacto positivo de las estrategias comunicativas, reduciendo la confianza y el compromiso de los estudiantes.

6.2 Implicaciones teóricas

Desde el punto de vista teórico, este estudio contribuye a la literatura sobre educación híbrida y compromiso estudiantil al incorporar explícitamente la ciberseguridad como una variable relevante en los modelos explicativos. Tradicionalmente, el compromiso estudiantil ha sido analizado desde perspectivas pedagógicas y psicológicas; sin embargo, los resultados sugieren que la percepción de seguridad digital debe ser considerada como un factor contextual clave en entornos educativos mediados por tecnología.

El estudio amplía los modelos de compromiso estudiantil al integrar el concepto de confianza digital, alineándose con enfoques contemporáneos sobre ética, gobernanza de datos y tecnología educativa. De este modo, se propone una visión más holística del compromiso estudiantil en contextos híbridos, que trasciende la mera interacción pedagógica e incorpora dimensiones de seguridad y privacidad.

6.3 Implicaciones prácticas

En términos prácticos, los resultados ofrecen orientaciones claras para las instituciones de educación superior. En primer lugar, se recomienda que las estrategias de comunicación educativa incluyan de manera explícita componentes relacionados con la ciberseguridad y la protección de datos, tales como políticas de privacidad claras, protocolos de acceso seguro y comunicación transparente sobre el uso de la información estudiantil.

En segundo lugar, se sugiere fortalecer la formación en alfabetización digital y ciberseguridad tanto para docentes como para estudiantes. El desarrollo de competencias en seguridad digital puede reducir la ansiedad tecnológica, incrementar la confianza en las plataformas institucionales y, en consecuencia, mejorar el compromiso estudiantil.

Finalmente, las instituciones deben considerar la ciberseguridad como un elemento estratégico de la calidad educativa en entornos híbridos, integrándola en la planificación académica, la gestión tecnológica y la evaluación de la experiencia del estudiante.

6.4 Limitaciones y líneas futuras de investigación

A pesar de sus aportes, el estudio presenta algunas limitaciones. El diseño transversal no permite establecer relaciones causales entre las variables analizadas, por lo que futuras investigaciones podrían emplear diseños longitudinales o experimentales. Asimismo, el

uso de muestreo no probabilístico limita la generalización de los resultados a otros contextos educativos.

Como líneas futuras de investigación, se sugiere profundizar en el rol mediador o moderador de la ciberseguridad entre las estrategias de comunicación y el compromiso estudiantil, así como explorar diferencias entre disciplinas académicas, niveles educativos y contextos culturales. Además, estudios cualitativos podrían aportar una comprensión más profunda de las percepciones estudiantiles sobre seguridad digital y su influencia en la experiencia de aprendizaje híbrido.

Referencias

1. Almeida, F., & Simões, J. (2023). The role of digital communication tools in hybrid learning environments. *Education and Information Technologies, 28*(2), 1785–1802. https://doi.org/10.1007/s10639-022-11123-6

2. Bond, M., Buntins, K., Bedenlier, S., Zawacki-Richter, O., & Kerres, M. (2024). Mapping research in student engagement and educational technology in higher education: A systematic evidence map. *International Journal of Educational Technology in Higher Education, 21*(1), 1–23. https://doi.org/10.1186/s41239-024-00437-9

3. ENISA. (2023). *Cybersecurity challenges in the education sector*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

4. Fredricks, J. A., Blumenfeld, P. C., & Paris, A. H. (2004). School engagement: Potential of the concept, state of the evidence. *Review of Educational Research, 74*(1), 59–109. https://doi.org/10.3102/00346543074001059

5. Graham, C. R., Henrie, C. R., & Gibbons, A. S. (2021). Developing models and theory for blended learning research. *Educational Technology Research and Development, 69*(2), 681–700. https://doi.org/10.1007/s11423-021-09987-5

6. Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). SAGE Publications.

7. Hernández-Sampieri, R., & Mendoza, C. (2022). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta* (7.ª ed.). McGraw-Hill.

8. Ifenthaler, D., & Yau, J. Y. K. (2020). Utilising learning analytics to support study success in higher education: A systematic review. *Educational Technology Research and Development, 68*(4), 1961–1990. https://doi.org/10.1007/s11423-020-09788-z

9. Kahu, E. R., & Nelson, K. (2018). Student engagement in the educational interface: Understanding the mechanisms of student success. *Higher Education Research & Development, 37*(1), 58–71. https://doi.org/10.1080/07294360.2017.1344197

10. OECD. (2023). *Education at a glance 2023: OECD indicators*. OECD Publishing. https://doi.org/10.1787/69096873-en

11. Ramos-Azcuy, F. J., Rodríguez-Gámez, M., Benavides-Bailón, J. M., Bonilla-Jiménez, M. M., & Arroba-Cárdenas, Á. E. (2025). Despertando el compromiso estudiantil: El poder transformador de H5P en la educación superior. *RIED. Revista Iberoamericana de Educación a Distancia, 28*(2), 379–400. https://doi.org/10.5944/ried.28.2.43542

12. Taddeo, M., & Floridi, L. (2021). The notion of trust in artificial intelligence. *Ethics and Information Technology, 23*(2), 1–14. https://doi.org/10.1007/s10676-020-09554-3

13. Tsai, C. C., Lin, O. P., Hong, J. C., & Tai, K. H. (2022). The effects of technology anxiety and digital trust on students' engagement in online learning. *Computers & Education, 182*, 104457. https://doi.org/10.1016/j.compedu.2022.104457
14. UNESCO. (2021). *Reimagining our futures together: A new social contract for education*. UNESCO Publishing. https://unesdoc.unesco.org
15. Zepke, N. (2021). Student engagement research in higher education: Questioning an academic orthodoxy. *Teaching in Higher Education, 26*(2), 257–269. https://doi.org/10.1080/13562517.2019.1637041