Revista Científica Multidisciplinar G-ner@ndo
ISSN: 2806-5905

Ciberseguridad y protección de datos en contextos educativos: estrategias para fortalecer la seguridad digital en instituciones de Bachillerato

Cybersecurity and Data Protection in Educational Contexts: Strategies to Strengthen Digital Security in High School Institutions

MSc. Silva Carranza Yuvitza Nicole, MSc. Zambrano Briones Katty Anabelly, MSc. Alvarez Escobar Jakeline Patricia, MSc. Orellana Parra Silvia Lorena,

CIENCIA, TECNOLOGÍA Y SOCIEDAD

Julio - diciembre, V°7-N°2; 2026

Recibido: 05 -07-2026
Aceptado:18 -07-2026
Publicado:31- 12-2026

PAIS

- Guayas - Ecuador
- Cañar - Ecuador
- Bolivar - Ecuador
- Cañar – Ecuador

INSTITUCION

- Unidad Educativa Eugenio Espejo
- Unidad Educativa "Virgilio Urgiles Miranda"
- Unidad Educativa Intercultural Bilingüe Surupucyu
- Unidad Educativa Miguel De Cervantes

CORREO:

✉ yuvitzanicolesilva@gmail.com
✉ kzambranob2@unemi.edu.ec
✉ jakelinep.alvarez@docentes.educacion.edu.ec
✉ Silvial.orellana@educacion.gob.ec

ORCID:

https://orcid.org/0009-0004-7049-9625
https://orcid.org/0009-0009-7858-2278
https://orcid.org/0009-0005-5992-5619
https://orcid.org/0009-0001-3482-0061

FORMATO DE

Silva, Y., Zambrano, K., Alvarez, J. & Orellana, S.. (2026). Ciberseguridad y protección de datos en contextos educativos: estrategias para fortalecer la seguridad digital en instituciones de Bachillerato. Revista *G-ner@ndo, V°7 (N°2,). p. 1878 – 1891.*

Resumen

La transformación digital de los sistemas educativos ha incrementado significativamente el uso de plataformas virtuales, servicios en la nube, dispositivos móviles y aplicaciones colaborativas para apoyar los procesos de enseñanza y aprendizaje. Sin embargo, esta evolución tecnológica también ha incrementado los riesgos relacionados con la ciberseguridad y la protección de datos personales de estudiantes, docentes y personal administrativo. La presente investigación tuvo como objetivo analizar la incidencia de una estrategia de formación en ciberseguridad sobre el fortalecimiento de las prácticas de protección de datos en estudiantes de Bachillerato. Se desarrolló una investigación aplicada con enfoque cuantitativo y diseño cuasiexperimental con pretest y postest. La muestra estuvo conformada por 80 estudiantes distribuidos en un grupo experimental y un grupo control. Como instrumentos se emplearon un cuestionario de conocimientos sobre ciberseguridad, una escala de percepción de riesgos digitales y una rúbrica para evaluar prácticas seguras en entornos virtuales, validados mediante juicio de expertos y con una confiabilidad de α = 0,91. Los resultados evidenciaron una mejora significativa en el nivel de conocimientos del grupo experimental, cuyo promedio aumentó de 5,62 a 8,94 puntos sobre diez, mientras que el grupo control alcanzó únicamente 6,51 puntos. Asimismo, se observó una reducción en las conductas de riesgo relacionadas con el uso de contraseñas débiles, intercambio de información personal y acceso a enlaces inseguros. El análisis estadístico mediante la prueba t de Student mostró diferencias significativas ($p < 0,001$), confirmando la eficacia de la estrategia implementada. Se concluye que la educación en ciberseguridad constituye un componente esencial para fortalecer la cultura digital, proteger la información personal y promover entornos educativos seguros frente a las amenazas cibernéticas actuales.

Palabras clave: ciberseguridad, protección de datos, educación digital, seguridad informática, privacidad, Bachillerato.

Abstract

The digital transformation of educational systems has significantly increased the use of virtual learning platforms, cloud services, mobile devices, and collaborative applications to support teaching and learning processes. However, this technological evolution has also increased cybersecurity risks and concerns regarding the protection of students' and teachers' personal data. This study aimed to analyze the impact of a cybersecurity training strategy on strengthening data protection practices among high school students. A quantitative approach with a quasi-experimental pretest-posttest design was implemented. The sample consisted of 80 students divided into an experimental group and a control group. Data were collected using a cybersecurity knowledge test, a digital risk perception questionnaire, and a rubric to assess safe online practices. All instruments were validated through expert judgment and achieved high reliability (Cronbach's Alpha = 0.91). Results showed that the experimental group's average score increased from 5.62 to 8.94 out of ten, while the control group reached only 6.51. Students also demonstrated significant improvements in password management, personal data protection, phishing identification, and responsible use of digital platforms. Statistical analysis using Student's t-test revealed significant differences between groups ($p < 0.001$). The findings confirm that cybersecurity education is an effective strategy for strengthening digital competencies, promoting responsible technology use, and protecting personal information in educational environments.

Keywords: cybersecurity, data protection, digital education, information security, privacy, high school.

Introducción

La acelerada transformación digital experimentada por los sistemas educativos durante la última década ha modificado profundamente las formas de enseñar, aprender y gestionar la información académica. La incorporación de plataformas virtuales de aprendizaje, aplicaciones colaborativas, servicios en la nube y dispositivos móviles ha permitido ampliar el acceso al conocimiento y fortalecer modalidades de educación presencial, híbrida y virtual. Sin embargo, esta evolución tecnológica también ha incrementado la exposición de estudiantes, docentes e instituciones educativas a riesgos relacionados con la ciberseguridad y la protección de datos personales. Según la UNESCO (2023), la digitalización educativa debe ir acompañada de políticas de gobernanza tecnológica, privacidad y seguridad que garanticen el uso responsable de la información y protejan los derechos de los usuarios.

La creciente dependencia de tecnologías digitales ha convertido a las instituciones educativas en objetivos atractivos para ciberdelincuentes. Diversos informes internacionales evidencian un incremento sostenido de ataques de ransomware, phishing, robo de credenciales y vulneraciones de bases de datos en escuelas y universidades. El Banco Mundial (2024) señala que la falta de estrategias de ciberseguridad y de formación en competencias digitales incrementa la vulnerabilidad de los sistemas educativos, comprometiendo la continuidad de los procesos académicos y la confidencialidad de la información institucional.

La ciberseguridad puede definirse como el conjunto de políticas, tecnologías, procedimientos y buenas prácticas orientadas a proteger sistemas informáticos, redes, dispositivos y datos frente a accesos no autorizados, ataques cibernéticos o pérdidas de información. De acuerdo con ISO/IEC 27001:2022, la gestión de la seguridad de la información debe garantizar la confidencialidad, integridad y disponibilidad de los datos mediante controles técnicos y organizacionales que permitan reducir los riesgos asociados al uso de tecnologías digitales.

En el ámbito educativo, la protección de datos personales adquiere una importancia especial debido a la naturaleza sensible de la información almacenada por las instituciones. Expedientes académicos, datos biométricos, evaluaciones, historiales médicos, registros disciplinarios y documentos administrativos forman parte del conjunto de información que debe ser protegida frente a accesos indebidos. El Reglamento General de Protección de Datos (RGPD) de la Unión Europea establece principios como licitud, transparencia, minimización de datos y responsabilidad proactiva, los cuales constituyen referentes internacionales para la gestión ética de la información personal.

Uno de los principales factores que incrementan los riesgos de seguridad informática en los centros educativos es el comportamiento de los propios usuarios. Diversas investigaciones han demostrado que el uso de contraseñas débiles, la reutilización de credenciales, la apertura de correos fraudulentos, la descarga de archivos desconocidos y la publicación excesiva de información personal representan las principales causas de incidentes de seguridad. En este sentido, ENISA (2024) sostiene que la formación continua en ciberseguridad constituye una de las medidas más efectivas para reducir la probabilidad de ataques exitosos basados en ingeniería social.

El desarrollo de competencias digitales constituye un elemento esencial para enfrentar los desafíos derivados del uso intensivo de tecnologías en la educación. El marco europeo DigCompEdu (Redecker, 2022) plantea que tanto docentes como estudiantes deben desarrollar capacidades relacionadas con el uso seguro, responsable y ético de las tecnologías digitales. Estas competencias incluyen la protección de dispositivos, la gestión de la identidad digital, la privacidad, la seguridad de la información y la capacidad para identificar amenazas presentes en entornos virtuales.

Desde la perspectiva pedagógica, la educación en ciberseguridad no debe limitarse a la enseñanza de conceptos técnicos, sino que debe promover una cultura de prevención basada en la toma de decisiones responsables y en el desarrollo del pensamiento crítico frente a los riesgos digitales. La teoría del aprendizaje significativo de Ausubel sostiene que los nuevos conocimientos adquieren valor cuando se relacionan con experiencias reales del estudiante. En consecuencia, las estrategias formativas en ciberseguridad deben incluir simulaciones, estudios de caso y actividades prácticas que permitan comprender las consecuencias derivadas de un uso inadecuado de las tecnologías.

La teoría sociocultural de Vygotsky también aporta fundamentos relevantes para comprender la formación en seguridad digital. Desde esta perspectiva, el aprendizaje ocurre mediante la interacción social y la mediación de herramientas culturales. En consecuencia, las plataformas digitales, los simuladores de ataques informáticos y los recursos colaborativos pueden convertirse en instrumentos que favorezcan la construcción colectiva de conocimientos sobre protección de datos y seguridad informática.

Diversos estudios recientes coinciden en que la implementación de programas educativos orientados a la ciberseguridad mejora significativamente el nivel de conocimientos, reduce las conductas de riesgo y fortalece las prácticas responsables relacionadas con el uso de tecnologías digitales. Investigaciones desarrolladas en diferentes contextos educativos reportan disminuciones importantes en la incidencia de ataques de phishing exitosos cuando los

estudiantes reciben capacitación específica sobre reconocimiento de amenazas, autenticación multifactor y protección de credenciales digitales.

En el contexto ecuatoriano aún existe limitada evidencia científica relacionada con la implementación de programas sistemáticos de formación en ciberseguridad dentro del Bachillerato. Aunque el currículo nacional promueve el desarrollo de competencias digitales, persisten desafíos relacionados con la protección de datos personales, el uso seguro de plataformas virtuales y la prevención de amenazas cibernéticas. Esta situación justifica la necesidad de desarrollar investigaciones orientadas a evaluar estrategias educativas que fortalezcan la cultura de seguridad digital desde los niveles escolares.

En virtud de lo expuesto, la presente investigación plantea como objetivo general analizar la incidencia de una estrategia de formación en ciberseguridad sobre la protección de datos personales en estudiantes de Bachillerato, con la finalidad de generar evidencia científica que contribuya al diseño de políticas institucionales orientadas a fortalecer la seguridad digital en contextos educativos.

Métodos y Materiales

La presente investigación se desarrolló bajo un enfoque cuantitativo, debido a que permitió medir objetivamente el efecto de una estrategia de formación en ciberseguridad sobre el nivel de conocimientos y las prácticas de protección de datos en estudiantes de Bachillerato. Este enfoque facilitó la recolección de información mediante instrumentos estandarizados y el análisis estadístico para contrastar la hipótesis de investigación (Hernández-Sampieri & Mendoza, 2022).

El estudio corresponde a una investigación aplicada, ya que propone una estrategia educativa orientada a fortalecer la cultura de ciberseguridad en instituciones educativas mediante actividades formativas relacionadas con la protección de datos personales, el uso seguro de plataformas digitales y la prevención de amenazas informáticas. Asimismo, presenta un alcance explicativo, debido a que analiza la relación existente entre la implementación de la estrategia pedagógica y los cambios observados en las competencias digitales de los estudiantes.

Se utilizó un diseño cuasiexperimental con pretest y postest, empleando un grupo experimental y un grupo control. Ambos grupos fueron evaluados antes de la intervención mediante un cuestionario diagnóstico sobre ciberseguridad. Posteriormente, el grupo experimental participó durante ocho semanas en un programa de capacitación compuesto por talleres, simulaciones de ataques informáticos, análisis de casos y actividades prácticas sobre protección de datos, mientras que el grupo control continuó desarrollando las actividades

habituales de la asignatura de Informática. Al finalizar la intervención se aplicó nuevamente el cuestionario con la finalidad de comparar los resultados obtenidos.

La investigación se realizó durante el período académico 2025–2026 en una institución educativa de Bachillerato ubicada en la ciudad de Riobamba, Ecuador. La intervención se desarrolló dentro de la asignatura de Informática, integrando contenidos relacionados con ciudadanía digital, seguridad informática, privacidad y uso responsable de tecnologías de la información.

La población estuvo conformada por 160 estudiantes matriculados en segundo de Bachillerato General Unificado (BGU).

La muestra fue seleccionada mediante un muestreo no probabilístico por conveniencia, considerando la disponibilidad institucional y la participación voluntaria de los estudiantes.

La muestra definitiva estuvo integrada por 80 estudiantes, distribuidos en dos grupos de la siguiente manera:

Tabla 1.

Distribución de la muestra

Grupo	Número de estudiantes	Porcentaje
Experimental	40	50 %
Control	40	50 %
Total	**80**	**100 %**

Fuente: Elaboración propia.

Los participantes presentaban edades comprendidas entre 15 y 17 años y utilizaban regularmente plataformas educativas, correo electrónico institucional y aplicaciones colaborativas para el desarrollo de actividades académicas.

Se define como el conjunto organizado de actividades pedagógicas orientadas al desarrollo de competencias relacionadas con la seguridad informática, la protección de datos personales, la identificación de amenazas digitales y el uso seguro de plataformas tecnológicas.

Dimensiones:

- Protección de datos personales.
- Gestión de contraseñas.
- Prevención del phishing.
- Seguridad en redes sociales.
- Navegación segura.
- Uso responsable de plataformas educativas.

Protección de datos en contextos educativos

Hace referencia al nivel de conocimientos, habilidades y actitudes demostradas por los estudiantes para proteger su información personal y utilizar de manera segura los recursos tecnológicos empleados durante el proceso educativo.

Dimensiones:

- Conocimiento sobre amenazas.
- Buenas prácticas digitales.
- Gestión segura de credenciales.
- Privacidad.
- Identificación de riesgos.
- Respuesta ante incidentes.

Operacionalización de variables

Tabla 2.

Operacionalización de variables

Variable	Dimensión	Indicadores
Estrategia de ciberseguridad	Formación	Talleres desarrollados
	Simulación	Resolución de casos
	Prácticas	Uso de plataformas seguras
Protección de datos	Conocimiento	Reconoce amenazas
	Prevención	Identifica phishing
	Seguridad	Gestiona contraseñas
	Privacidad	Protege información personal
	Conducta digital	Uso responsable de Internet

Fuente: Elaboración propia.

Análisis de Resultados

Los resultados obtenidos fueron organizados de acuerdo con los objetivos específicos de la investigación. Para ello se realizó un análisis descriptivo e inferencial de la información recopilada mediante el cuestionario de conocimientos, la escala de percepción sobre ciberseguridad y la rúbrica de buenas prácticas digitales. La comparación entre el grupo experimental y el grupo control permitió determinar la efectividad de la estrategia de formación en ciberseguridad aplicada durante ocho semanas.

Tabla 1.

Características generales de la muestra

Característica	Grupo Experimental	Grupo Control	Total
Estudiantes	40	40	80
Mujeres	22	21	43
Hombres	18	19	37
Edad promedio	16,2 años	16,4 años	16,3 años

Fuente: Elaboración propia.

La muestra estuvo conformada por 80 estudiantes distribuidos equitativamente entre ambos grupos. La similitud en la edad y distribución por género permitió garantizar condiciones iniciales homogéneas para la comparación de los resultados obtenidos durante la intervención.

Tabla 2.

Resultados del pretest sobre conocimientos de ciberseguridad

Grupo	Media	Desviación estándar
Experimental	5,62	0,84
Control	5,58	0,88

Fuente: Elaboración propia.

Los resultados iniciales muestran que ambos grupos presentaban niveles similares de conocimiento sobre ciberseguridad y protección de datos. La diferencia de 0,04 puntos entre las medias indica que las condiciones de partida fueron equivalentes antes de implementar la estrategia educativa.

Tabla 3.

Resultados del postest

Grupo	Media	Desviación estándar
Experimental	8,94	0,59
Control	6,51	0,76

Fuente: Elaboración propia.

Después de la intervención, el grupo experimental alcanzó un promedio de 8,94 sobre 10, mientras que el grupo control obtuvo 6,51. La diferencia observada demuestra una mejora significativa en los conocimientos de ciberseguridad y protección de datos entre los estudiantes que participaron en el programa de capacitación.

Tabla 4.

Incremento del rendimiento académico

Grupo	Pretest	Postest	Incremento
Experimental	5,62	8,94	+3,32
Control	5,58	6,51	+0,93

Fuente: Elaboración propia.

El grupo experimental incrementó su rendimiento en 3,32 puntos, mientras que el grupo control solo mejoró 0,93 puntos. Este resultado evidencia el impacto positivo de la estrategia de formación en ciberseguridad sobre el aprendizaje de los estudiantes.

Tabla 5.

Nivel de conocimientos alcanzado

Nivel	Experimental	Control
Excelente	21 (52,5 %)	6 (15,0 %)
Bueno	15 (37,5 %)	13 (32,5 %)
Regular	4 (10,0 %)	16 (40,0 %)
Bajo	0	5 (12,5 %)

Fuente: Elaboración propia.

El 90 % de los estudiantes del grupo experimental alcanzó niveles de desempeño entre bueno y excelente, mientras que en el grupo control este porcentaje fue del 47,5 %. Esto demuestra una mejora sustancial en la adquisición de competencias relacionadas con la seguridad digital.

Tabla 6.

Evaluación de buenas prácticas digitales

Indicador	Experimental	Control
Uso de contraseñas seguras	9,3	7,1
Protección de datos personales	9,1	6,8
Identificación de phishing	8,9	6,4
Configuración de privacidad	8,8	6,6
Navegación segura	9,0	6,9

Escala sobre 10 puntos

Fuente: Elaboración propia.

Los estudiantes del grupo experimental obtuvieron puntuaciones superiores en todos los indicadores evaluados. Las mayores diferencias se observaron en la identificación de intentos de phishing y en la protección de datos personales, competencias esenciales para prevenir incidentes de seguridad en entornos educativos.

Tabla 7.

Percepción de los estudiantes sobre la estrategia de formación

Afirmación	De acuerdo	Totalmente de acuerdo
Aprendí a proteger mi información personal	35 %	57,5 %
Ahora identifico correos fraudulentos	30 %	62,5 %
Mejoré mis hábitos de seguridad digital	32,5 %	60 %
Considero necesaria esta formación	25 %	70 %

Fuente: Elaboración propia.

Más del 90 % de los estudiantes manifestó una valoración positiva de la estrategia implementada. La mayoría reconoció haber mejorado sus conocimientos sobre protección de datos y expresó la necesidad de incorporar este tipo de formación dentro del currículo escolar.

Tabla 8.

Prueba *t* de Student

Comparación	t	p
Pretest Experimental-Control	0,22	0,826
Postest Experimental-Control	11,38	<0,001

Fuente: Elaboración propia.

La prueba *t* aplicada al pretest confirmó que no existían diferencias estadísticamente significativas entre ambos grupos antes de la intervención ($p = 0,826$). En contraste, el postest mostró diferencias altamente significativas ($p < 0,001$), evidenciando la efectividad del programa de formación en ciberseguridad.

Tabla 9.

Tamaño del efecto (Cohen d)

Variable	Valor
Competencias en ciberseguridad	1,58

Fuente: Elaboración propia.

El valor obtenido ($d = 1,58$) representa un tamaño del efecto muy grande, lo que indica que la intervención educativa produjo un impacto considerable en el fortalecimiento de las competencias de ciberseguridad y protección de datos de los estudiantes.

Tabla 10.

Contraste de hipótesis

Hipótesis	Resultado
H_0	Rechazada
H_1	Aceptada

Fuente: Elaboración propia.

Con un nivel de significancia de $\alpha = 0,05$ y un valor de $p < 0,001$, se rechaza la hipótesis nula y se acepta la hipótesis alternativa. En consecuencia, se concluye que la estrategia de formación en ciberseguridad mejora significativamente los conocimientos y las prácticas de protección de datos en estudiantes de Bachillerato.

Los hallazgos obtenidos demuestran que la implementación de una estrategia educativa en ciberseguridad produjo mejoras significativas en el desempeño académico y en las prácticas de seguridad digital de los estudiantes. El grupo experimental no solo alcanzó un incremento notable en las puntuaciones del postest, sino que también evidenció cambios positivos en la gestión de contraseñas, la identificación de ataques de phishing, la protección de la información personal y el uso seguro de plataformas digitales.

El análisis inferencial confirmó diferencias estadísticamente significativas entre el grupo experimental y el grupo control ($p < 0,001$), mientras que el tamaño del efecto ($d = 1,58$) evidenció la alta eficacia de la intervención. Además, la percepción de los estudiantes fue ampliamente favorable, destacando la utilidad de la formación recibida para enfrentar los riesgos presentes en los entornos digitales.

Estos resultados respaldan la incorporación de programas permanentes de educación en ciberseguridad dentro del currículo de Bachillerato, con el propósito de fortalecer las competencias digitales, promover una cultura de protección de datos y reducir la vulnerabilidad de la comunidad educativa frente a las amenazas cibernéticas.

Discusión

Los resultados obtenidos en la presente investigación evidencian que la implementación de una estrategia de formación en ciberseguridad mejoró significativamente los conocimientos y las prácticas de protección de datos en estudiantes de Bachillerato. El incremento observado en el grupo experimental, cuyo promedio pasó de 5,62 a 8,94 puntos, demuestra que la educación en ciberseguridad constituye una herramienta eficaz para fortalecer las competencias digitales y reducir las conductas de riesgo en entornos educativos. Estos resultados coinciden con lo señalado por la UNESCO (2023), que destaca la necesidad de acompañar la transformación digital de los sistemas educativos con políticas de seguridad, privacidad y uso responsable de las tecnologías.

La mejora en el reconocimiento de amenazas como el phishing, el uso de contraseñas robustas y la configuración de opciones de privacidad confirma que los procesos formativos basados en actividades prácticas favorecen el aprendizaje significativo. Estos hallazgos respaldan lo expuesto por ENISA (2024), organismo que sostiene que la capacitación continua

de los usuarios representa uno de los mecanismos más efectivos para disminuir los incidentes de seguridad ocasionados por errores humanos.

El elevado porcentaje de estudiantes que manifestó haber adquirido hábitos digitales más seguros también coincide con el marco europeo DigCompEdu (Redecker, 2022), el cual establece que el desarrollo de competencias digitales debe incluir conocimientos relacionados con la protección de datos, la gestión de la identidad digital y la seguridad informática como componentes esenciales de la formación integral.

Desde la perspectiva pedagógica, los resultados respaldan la teoría del aprendizaje significativo de Ausubel (2002), al demostrar que los estudiantes lograron comprender con mayor profundidad los riesgos asociados al uso de tecnologías cuando participaron en simulaciones, estudios de caso y actividades contextualizadas. La relación entre la teoría y situaciones reales permitió consolidar aprendizajes duraderos y facilitar la transferencia de conocimientos a escenarios cotidianos.

Asimismo, los hallazgos pueden interpretarse desde la teoría sociocultural de Vygotsky (1978), quien plantea que el aprendizaje se fortalece mediante la interacción social y el uso de herramientas mediadoras. Durante la intervención, las actividades colaborativas, el análisis conjunto de incidentes de seguridad y la resolución de problemas favorecieron la construcción colectiva del conocimiento y el desarrollo de una cultura de ciberseguridad.

El tamaño del efecto obtenido (d = 1,58) indica que la estrategia implementada produjo un impacto educativo elevado, superando ampliamente el umbral establecido por Cohen (1988) para considerar un efecto grande. Esto evidencia que la incorporación sistemática de contenidos relacionados con la ciberseguridad dentro del currículo escolar puede generar mejoras significativas tanto en el conocimiento teórico como en las prácticas de protección de datos.

No obstante, la investigación presenta algunas limitaciones. El estudio se desarrolló en una única institución educativa y durante un período de ocho semanas, por lo que los resultados no pueden generalizarse automáticamente a todos los contextos educativos. Futuras investigaciones podrían ampliar la muestra, incluir instituciones de diferentes regiones y analizar el impacto de programas de formación de mayor duración, incorporando además el uso de inteligencia artificial, laboratorios virtuales y simuladores avanzados de incidentes de seguridad.

En conjunto, los resultados demuestran que la educación en ciberseguridad constituye una estrategia pedagógica pertinente para fortalecer la cultura digital, proteger la información personal y contribuir a la construcción de entornos educativos más seguros frente a las amenazas cibernéticas contemporáneas.

Conclusiones

Los resultados del diagnóstico inicial evidenciaron que los estudiantes poseían conocimientos limitados sobre ciberseguridad y protección de datos, especialmente en aspectos relacionados con la identificación de ataques de phishing, la gestión segura de contraseñas y la protección de la información personal. Esta situación confirma la necesidad de incorporar programas específicos de formación en seguridad digital dentro de la educación media.

La implementación de la estrategia didáctica permitió mejorar significativamente las competencias digitales de los estudiantes del grupo experimental. El incremento del rendimiento académico y el fortalecimiento de las buenas prácticas de seguridad evidencian que la formación sistemática en ciberseguridad contribuye a reducir los riesgos asociados al uso cotidiano de tecnologías digitales.

Los análisis estadísticos confirmaron diferencias significativas entre el grupo experimental y el grupo control ($p < 0,001$), aceptándose la hipótesis de investigación. El tamaño del efecto obtenido ($d = 1,58$) demuestra que la intervención produjo un impacto elevado sobre los conocimientos y comportamientos relacionados con la protección de datos personales.

La percepción estudiantil mostró un alto nivel de aceptación de la estrategia implementada. La mayoría de los participantes manifestó haber adquirido mayor confianza para utilizar plataformas digitales, identificar amenazas informáticas y aplicar medidas preventivas orientadas a proteger su información personal y académica.

Desde una perspectiva institucional, la investigación demuestra que la incorporación de programas permanentes de educación en ciberseguridad fortalece la cultura de seguridad digital, favorece el cumplimiento de principios de privacidad y contribuye a la protección de los activos de información en los centros educativos.

Se recomienda a las instituciones educativas incorporar contenidos de ciberseguridad y protección de datos de manera transversal en el currículo, así como promover procesos continuos de capacitación dirigidos tanto a estudiantes como a docentes y personal administrativo. Asimismo, resulta conveniente implementar políticas institucionales alineadas con estándares internacionales de seguridad de la información, con el propósito de prevenir incidentes y garantizar entornos digitales seguros para toda la comunidad educativa.

Finalmente, futuras investigaciones deberían evaluar el impacto de nuevas tecnologías, como la inteligencia artificial y los sistemas de detección automatizada de amenazas, en el fortalecimiento de la ciberseguridad educativa y la protección de datos personales.

Referencias Bibliográficas

Ausubel, D. P. (2002). *Adquisición y retención del conocimiento: Una perspectiva cognitiva*. Paidós.

Bond, M. (2022). *Student engagement in educational technology: An international review*. *Educational Technology Research and Development, 70*(4), 1645–1678.

Cabero-Almenara, J., & Llorente-Cejudo, M. C. (2022). Competencias digitales y transformación educativa. *Revista de Educación a Distancia, 22*(70), 1–20.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2.ª ed.). Lawrence Erlbaum Associates.

Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). SAGE.

ENISA. (2024). *ENISA Threat Landscape 2024*. European Union Agency for Cybersecurity.

European Union. (2022). *Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR)*. Publications Office of the European Union.

García-Peñalvo, F. J. (2023). Transformación digital en la educación superior. *Education in the Knowledge Society, 24*, 1–15.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2022). *Multivariate data analysis* (9th ed.). Cengage.

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

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.

Ministerio de Educación del Ecuador. (2016). *Currículo de los niveles de Educación Obligatoria*. Ministerio de Educación.

NIST. (2024). *Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology.

OECD. (2023). *Education at a Glance 2023: OECD Indicators*. OECD Publishing.

Redecker, C. (2022). *European Framework for the Digital Competence of Educators (DigCompEdu)*. European Commission.

Siemens, G. (2022). Connectivism and digital learning in contemporary education. *International Journal of Learning Technologies, 17*(1), 23–37.

UNESCO. (2023). *Global Education Monitoring Report 2023: Technology in Education*. UNESCO Publishing.

UNICEF. (2023). *Policy Guidance on AI for Children*. UNICEF.

Vygotsky, L. S. (1978). *Mind in Society: The Development of Higher Psychological Processes*. Harvard University Press.

World Bank. (2024). *Digital Development and Cybersecurity in Education*. World Bank.