

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

# Entorno Virtual de Aprendizaje (EVA), a la apropiación de la competencia digital en seguridad y privacidad de la información

Edith Cortés

William Camilo Rodríguez Mejía

Universidad Distrital Francisco José de Caldas

Facultad de Ciencias y Educación

Maestría en Educación en Tecnología

Bogotá, 2025

# Entorno Virtual de Aprendizaje (EVA), a la apropiación de la competencia digital en seguridad y privacidad de la información

Edith Cortés

William Camilo Rodríguez Mejía

Trabajo de Grado para optar por el título de Magister en Educación en Tecnología

Modalidad: Profundización

Director de Tesis

Carlos Augusto Osorio Marulanda Ph. D

Universidad Distrital Francisco José de Caldas

Facultad de Ciencias y Educación

Maestría en Educación en Tecnología

Bogotá, 2025

## Dedicatoria

A Dios, proveedor de virtudes, salud, sabiduría, fe y fortaleza, por ser mi guía constante.

A mi esposo Alexander e hijos Erika y Ricardo, por su amor, comprensión y apoyo incondicional, que me animaron en los momentos de cansancio y me recordaron siempre el valor de la perseverancia; y a mi madre, por su presencia constante, sus oraciones y su amor inagotable.

Y de manera muy especial, a mis estudiantes de las Líneas de Profundización por su esfuerzo, dedicación y compromiso con el aprendizaje. Su entusiasmo, responsabilidad y los recursos invertidos —de tiempo, energía y económicos— reflejan el espíritu de superación que inspira la labor docente.

**Edith Cortés**

A Dios, fuente de sabiduría y fortaleza, por guiar mis pasos en cada etapa de este camino y darme la luz necesaria para culminar este propósito.

A mi esposa, Laura Alejandra Guzmán, por su amor, comprensión y apoyo incondicional, que fueron mi mayor inspiración y compañía en cada desafío.

A mis hijos, Juan Camilo Rodríguez e Isabella Rodríguez Guzmán, por ser mi mayor motivo para perseverar y mi alegría constante. Que este logro sea un ejemplo de esfuerzo, fe y dedicación.

A mis padres, Pedro Ignacio Rodríguez y Miryam Mejía de Rodríguez, por su amor, enseñanzas y apoyo inquebrantable, y por haberme formado con valores que hoy guían mi vida personal y profesional.

**William Camilo Rodríguez Mejía**

**Agradecimientos**

A mi compañero William Camilo Rodríguez Mejía, quien fue el complemento ideal en este proceso. Su espíritu competitivo, organización, compromiso y dedicación se alinearon perfectamente con mi convicción de terminar las cosas de la manera adecuada. El tiempo compartido, el trabajo colaborativo y las reflexiones conjuntas fueron fundamentales para culminar con éxito este proyecto y las demás actividades desarrolladas durante la maestría.

A los docentes de la Maestría en Educación en Tecnología de la Universidad Distrital Francisco José de Caldas, por su entrega, paciencia y conocimiento, que se convirtieron en fuente de inspiración para fortalecer mi labor como educadora. En especial, mi más profundo agradecimiento al Dr. Carlos Augusto Osorio Marulanda, director de tesis, por su orientación, acompañamiento y valiosas sugerencias que guiaron el desarrollo de esta investigación.

A mis compañeras de trabajo, por sus aportes, motivación constante y disposición para colaborar, compartir ideas y mantener el entusiasmo durante todo el proceso.

Y al Colegio IED San Cayetano, por abrir las puertas al desarrollo de esta investigación y permitir que la propuesta se materializara en un entorno de aprendizaje real, donde la innovación pedagógica y la formación en ciudadanía digital cobraron sentido.

**Edith Cortés**

A mi compañera de lucha, Edith Cortés, por esas noches de tertulia, debate y reflexión en las que, con compromiso y paciencia, completamos y validamos cada una de las actividades que dieron vida a este trabajo. Su constancia y amistad fueron pilares fundamentales en la culminación de este proceso.

A todas las personas que, de una u otra manera, contribuyeron al desarrollo de esta investigación, brindando su tiempo, conocimiento y apoyo desinteresado.

A mis docentes, quienes me han enseñado el valor de la educación y la importancia de la preparación constante, y que con su ejemplo renovaron en mí, una y otra vez, el amor por esta hermosa profesión.

Finalmente, a mis amigos y familiares, quienes han creído en mí y me han acompañado con su cariño, comprensión y palabras de aliento en cada etapa de este camino académico. A todos ustedes, mi más sincero agradecimiento.

**William Camilo Rodríguez Mejía**

Mil gracias.

**Ficha Descriptiva de la Tesis**

| 1. Información general | |
|---|---|
| **Tipo de documento** | Trabajo de Grado para optar por el título de Magister en Educación en Tecnología |
| **Modalidad** | Profundización |
| **Acceso al documento** | Universidad Distrital Francisco José de Caldas – RIUD- |
| **Título del documento** | Entorno Virtual de Aprendizaje (EVA), a la apropiación de la competencia digital en seguridad y privacidad de la información. |
| **Autores** | Edith Cortés - William Camilo Rodríguez Mejía |
| **Director** | Dr. Carlos Augusto Osorio Marulanda |
| **Publicación** | Digital |
| **Programa** | Maestría en Educación en Tecnología |
| **Unidad patrocinante** | Edith Cortés - William Camilo Rodríguez Mejía |
| **Palabras clave** | Ciberseguridad, competencia digital, ciudadanía digital, educación rural, conectivismo, gamificación. |
| **Keywords** | Cybersecurity, digital competence, digital citizenship, rural education, connectivism, gamification. |

| 2. Descripción |
|---|
| La presente investigación tuvo como propósito evaluar, cómo una estrategia pedagógica fundamentada en los enfoques conectivista y constructivista, implementada mediante el Entorno Virtual de Aprendizaje (EVA) *Omniverso Digital*, favorece la |

apropiación de la competencia digital en seguridad y privacidad de la información en estudiantes de educación media de la IED Rural San Cayetano, ubicada en la localidad de Usme (Bogotá D.C.). El estudio se desarrolló bajo un **enfoque mixto con diseño dominante cualitativo**, en el cual el componente cuantitativo cumplió una función de apoyo interpretativo, articulado con un **diseño cuasi-experimental de pretest y postest en un solo grupo** y con la **Investigación-Acción Educativa (IAE)** de carácter pedagógico.

Los instrumentos aplicados fueron la *Escala de Competencias Digitales en Seguridad y Privacidad de la Información (ECDSPI)*, una encuesta abierta sobre ciberseguridad y el análisis de evidencias cualitativas derivadas del EVA, incluyendo los productos digitales elaborados por los estudiantes y las nubes de palabras construidas a partir de dichos productos. Los resultados evidenciaron un fortalecimiento significativo en la comprensión de los riesgos digitales, la gestión de la identidad en línea y la adopción de comportamientos seguros y éticos.

La estrategia pedagógica implementada, más que un recurso tecnológico, se consolidó como una propuesta educativa sostenible que integró las dimensiones cognitivas, ética y social de la competencia digital. El proyecto demostró que los entornos virtuales de aprendizaje, cuando se articulan con metodologías conectivistas y estrategias de gamificación, pueden transformar la enseñanza de la ciberseguridad en contextos rurales, fomentando una ciudadanía digital crítica, ética y responsable.

## 3. Abstract

The present research aimed to evaluate how a pedagogical strategy grounded in connectivist and constructivist approaches, implemented through the Virtual Learning Environment (VLE) *Omniverso Digital*, supports the development of digital competence in information security and privacy among upper-secondary students at IED Rural San Cayetano, located in the locality of Usme (Bogotá D.C.). The study was conducted under a mixed-methods approach with a qualitatively driven design, in which the quantitative component served an interpretative support function. This was integrated with a quasi-experimental pretest–posttest single-group design and Educational Action Research (EAR) of a pedagogical nature.

The instruments applied included the *Digital Competencies Scale in Information Security and Privacy (DCSISP*; *Spanish version: ECDSPI)*, an open-ended cybersecurity survey, and the analysis of qualitative evidence derived from the Virtual Learning Environments (VLE), including digital artifacts produced by the students and word clouds built from such products. The results showed a significant strengthening in the students' understanding of digital risks, management of online identity, and adoption of safe and ethical behaviors.

The implemented pedagogical strategy, beyond serving as a technological resource, consolidated itself as a sustainable educational proposal integrating the cognitive, ethical, and social dimensions of digital competence. The project demonstrated that virtual learning environments, when articulated with connectivist methodologies and gamification strategies, can transform cybersecurity teaching in rural contexts, fostering critical, ethical, and responsible digital citizenship.

## 4. Fuentes

Para la elaboración de esta investigación se consultaron 73 fuentes académicas entre libros, artículos científicos, informes institucionales y documentos normativos nacionales e internacionales. Las referencias abarcan un rango temporal comprendido entre 2000 y 2025, con especial énfasis en estudios recientes que abordan la educación digital, la ciberseguridad educativa y el desarrollo de competencias digitales desde una perspectiva pedagógica y tecnológica.

Las fuentes incluyen aportes teóricos de autores clásicos como Castells (2006) y Siemens (2005), junto con investigaciones actuales de organismos internacionales como la UNESCO (2019, 2022, 2023), el NIST (2024) y la ENISA (2025), que orientan la comprensión de la seguridad digital en el ámbito educativo. Asimismo, se destacan estudios contemporáneos que fundamentan el diseño del *Entorno Virtual de Aprendizaje Omniverso Digital*, entre ellos los de Zhao, Pinto y Cruz (2021) sobre competencias digitales, Barragán y Murta (2023) en torno a la seguridad en línea, Crompton y Burke (2024) respecto a los estándares ISTE, y Garmendia et al. (2024) sobre ciberseguridad y convivencia digital escolar.

En conjunto, las consultadas proporcionan un sustento teórico, metodológico y contextual sólido para el desarrollo de la investigación, garantizando actualidad, pertinencia y coherencia con los objetivos del estudio.

## 5. Contenido

El trabajo de grado da respuesta a la pregunta de investigación: ¿Cómo contribuye un Entorno Virtual de Aprendizaje (EVA) a la apropiación de la competencia digital en seguridad

y privacidad de la información en estudiantes de educación media de la Institución Educativa Distrital Rural San Cayetano?

El objetivo principal del estudio es evaluar la apropiación de la competencia digital en seguridad y privacidad de la información mediante la implementación del Entorno Virtual de Aprendizaje Omniverso Digital. La investigación se sustenta en un marco teórico que articula los enfoques de conectivismo, entornos virtuales de aprendizaje, tecnología, informática y sociedad, ciudadanía digital y competencias digitales, integrando de manera transversal la dimensión ética y ciudadana del aprendizaje digital.

Desde el punto de vista metodológico, el estudio se desarrolló bajo un enfoque mixto con diseño cuasi-experimental, complementado con investigación-acción educativa, en el que los datos cuantitativos cumplieron una función de apoyo interpretativo del análisis cualitativo. La intervención pedagógica incorporó la narrativa de gamificación CyberShield, estructurada a través de misiones, insignias y desafíos orientados a fortalecer la motivación, la autorregulación y el aprendizaje significativo.

El EVA Omniverso Digital fue diseñado a partir de esta narrativa, integrando actividades interactivas y colaborativas que promovieron en los estudiantes una comprensión crítica, técnica y ética sobre la protección de datos personales, la gestión de la identidad digital y la prevención de riesgos en línea, mediante el uso pedagógico de recursos digitales contextualizados.

Los resultados evidenciaron avances significativos en la autonomía digital, en la apropiación del lenguaje técnico de la ciberseguridad y en la adopción de comportamientos responsables frente a los riesgos digitales. De manera complementaria, el análisis cuantitativo mostró mejoras en los niveles de dominio de los ítems asociados a la dimensión de seguridad y privacidad de la información.

El estudio concluye que el Omniverso Digital fortaleció la competencia digital en seguridad y privacidad de la información al promover la comprensión y aplicación de principios propios de la ciberseguridad, como la gestión de riesgos digitales, la protección de la información personal, la autenticación segura y la respuesta ante incidentes. Este proceso formativo contribuyó a la consolidación de una cultura digital ética, crítica y responsable, alineada con los lineamientos del Ministerio de Educación Nacional (MEN, 2022) y los Estándares ISTE para Estudiantes (Crompton y Burke, 2024), orientados al desarrollo de ciudadanos digitales capaces de proteger su identidad y actuar con criterio en el entorno digital.

La tesis se estructura en seis capítulos:

*Capítulo I*, Planteamiento del problema, que presenta el contexto, el problema de investigación, los objetivos, la justificación y los antecedentes;

*Capítulo II*, Fundamentación teórica, que desarrolla los referentes conceptuales sobre conectivismo, ciudadanía digital, competencias digitales y ciberseguridad;

*Capítulo III*, Metodología, que describe el enfoque mixto, el diseño cuasi-experimental y la investigación-acción educativa;

*Capítulo IV*, Diseño del Entorno Virtual de Aprendizaje Omniverso Digital, basado en la narrativa de CyberShield y estrategias de gamificación;

*Capítulo V*, Resultados y análisis de resultados, que expone los hallazgos cualitativos y cuantitativos relacionados con la autonomía, el lenguaje técnico y la ética digital; y

*Capítulo VI,* Conclusiones, que presenta las conclusiones del estudio, sus limitaciones y recomendaciones, resaltando el valor del Omniverso Digital como una estrategia pedagógica para la apropiación de la competencia digital en seguridad y privacidad de la información en estudiantes de educación media de la IED Rural San Cayetano.

## 6. Metodología

La investigación se desarrolló bajo un enfoque mixto con diseño dominante cualitativo, en el cual los datos cuantitativos cumplieron una función de apoyo interpretativo. En el componente cualitativo se adoptó la Investigación-Acción Educativa (IAE) como marco metodológico, orientada a la reflexión sistemática sobre la práctica pedagógica y a la comprensión de los procesos formativos. De manera complementaria, en el componente cuantitativo se empleó un diseño cuasi-experimental de series temporales con pretest y postest en un solo grupo, con el propósito de identificar variaciones en la apropiación de la competencia digital en seguridad y privacidad de la información.

La investigación se desarrolló con estudiantes de educación media de la IED San Cayetano, colegio rural de Bogotá.

Para la recolección de la información se emplearon tres instrumentos: la Escala de Competencia Digital en Seguridad y Privacidad de la Información (ECDSPI), una encuesta

abierta de ciberseguridad y el análisis de evidencias cualitativas derivadas del Entorno Virtual de Aprendizaje (EVA) Omniverso Digital.

El procedimiento investigativo se desarrolló en cuatro fases:

- **Diagnóstico inicial**, mediante la aplicación del pretest y la identificación de los conocimientos previos de los estudiantes.
- **Diseño del EVA**, fundamentado en los principios del conectivismo, la gamificación educativa y el uso de contextos hipotético-reales.
- **Implementación progresiva**, a través de actividades interactivas desarrolladas en el Omniverso Digital.
- **Evaluación y análisis**, mediante la aplicación del postest y la triangulación de los resultados obtenidos.

El análisis de la información integró análisis de contenido de carácter inductivo para los datos cualitativos y estadística descriptiva para los datos cuantitativos, apoyado en un proceso de triangulación metodológica, teórica y temporal. Este enfoque permitió interpretar y evaluar los resultados de la intervención pedagógica, evidenciando el fortalecimiento de la competencia digital en seguridad y privacidad de la información.

## 7. Conclusiones

El Entorno Virtual de Aprendizaje (EVA) *Omniverso Digital*, fundamentado en el enfoque conectivista e integrado con estrategias de gamificación, favoreció de manera significativa la apropiación de la competencia digital en seguridad y privacidad de la información en los estudiantes de educación media de la IED San Cayetano. La intervención

pedagógica permitió no solo el fortalecimiento de conocimientos técnicos asociados a la ciberseguridad, sino también el desarrollo de procesos de reflexión crítica, autonomía y autorregulación frente al uso de la tecnología en contextos digitales.

Los resultados evidencian avances en la gestión responsable de la identidad digital, la protección de los datos personales y la adopción de prácticas seguras en línea, así como una apropiación progresiva del lenguaje técnico propio de la ciberseguridad. Desde una perspectiva ética y ciudadana, las producciones estudiantiles reflejaron una mayor conciencia sobre el impacto de las acciones en el entorno digital, consolidando aprendizajes que trascienden el ámbito escolar.

Asimismo, se identificó la necesidad de extender estas prácticas formativas al entorno familiar y comunitario, reconociendo la ciberseguridad y la ciudadanía digital como procesos colectivos que requieren corresponsabilidad social. En este sentido, el proyecto se alinea con los Estándares ISTE para Estudiantes (Crompton y Burke, 2024) y con las orientaciones del Ministerio de Educación Nacional (MEN, 2022), consolidándose como una estrategia pedagógica pertinente, ética y sostenible para el fortalecimiento de la ciudadanía digital en contextos rurales.

| | |
|---|---|
| **Elaborado** | Edith Cortés - William Camilo Rodríguez Mejía |
| **Revisado** | Dr. Carlos Augusto Osorio Marulanda |

| | | | |
|---|---|---|---|
| **Fecha de elaboración del resumen** | 06 | 11 | 2025 |

**Tabla de contenido**

Capítulo I. La Investigación ..... 25

Introducción ..... 25

Planteamiento del Problema ..... 26

La pregunta esencial que orienta esta investigación es ..... 28

Objetivo General ..... 28

Objetivos Específicos ..... 28

Contexto de la Investigación ..... 29

Contexto Macro ..... 29

Contexto Micro ..... 31

Contexto Tecnológico y de Infraestructura. ..... 31

Caracterización de los Estudiantes. ..... 33

Caracterización de los Cuidadores. ..... 34

Caracterización Socioeconómica. ..... 35

Justificación ..... 35

Antecedentes ..... 37

Conectivismo ..... 39

Entornos Virtuales de Aprendizaje - EVA ..... 42

Impacto de la tecnología en la apropiación de competencias de seguridad y privacidad digital ..... 47

Competencias Digitales ..... 49

Información y alfabetización de datos. ..... 49

Comunicación y colaboración. ..... 50

Crear contenidos digitales. ..... 51

Seguridad. ..... 51

Capítulo II. Marco Teórico ..... 55

Competencia Digital en Seguridad y Privacidad de la Información ..... 55

Definición Operacional de la Competencia Estudiada ..... 55

Relación entre Competencia Digital en Seguridad y Privacidad con Ciberseguridad ..... 57

Fundamentación en Marcos Normativos Internacionales y Nacionales ..... 58

*Síntesis: Competencia Integral* ..... 59

Desagregación Conceptual: Competencia Digital en Seguridad y Privacidad ..... 60

Nivel 1. Competencia (macrodimensión) ..... 60

Nivel 2. Ejes o dimensiones de la competencia ..... 61

Eje 1. Protección de datos personales ..... 61

Eje 2. Gestión de la identidad digital ..... 61

Eje 3. Reconocimiento y mitigación de amenazas digitales ..... 62

Nivel 3. Actitudes y valores (componente ético-social) ..... 62

Conectivismo ..... 64

Entorno Virtual de Aprendizaje EVA ..... 65

Tecnología, Informática y Sociedad ..... 68

Ciudadano digital ..... 69

Competencias Digitales ..... 71

Información y Alfabetización de Datos. ..... 72

Comunicación y Colaboración. ..... 73

Crear Contenidos Digitales. ..... 73

Seguridad. ..... 73

Capítulo III. Metodología ..... 76

Enfoque de la Investigación ..... 76

Diseño Metodológico ..... 77

Proceso Investigativo ..... 78

*Fase 1. Diagnóstico contextual* ..... 79

Fase 2. Adaptación y validación de instrumentos ..... 79

*Fase 3. Diseño e implementación del EVA* ..... 80

*Fase 4. Aplicación de instrumentos y recolección de evidencias* ..... 80

Fase 5. Análisis e interpretación de resultados ..... 80

Instrumentos de Observación ..... 81

*Escala de Competencia Digital en Seguridad y Privacidad de la Información (ECDSPI)* ..... 81

*Encuesta Abierta de Ciberseguridad* ..... 82

Entorno Virtual de Aprendizaje (EVA) – Omniverso Digital ..... 83

Recolección de Información ..... 85

Procesamiento y Análisis de la Información ..... 87

Análisis Cualitativo ..... 87

Análisis Cualitativo ..... 88

Triangulación de Resultados ..... 88

Triangulación de datos. 88

Triangulación de instrumentos. 89

Triangulación interpretativa 89

Capítulo IV. Diseño, Implementación del EVA Omniverso Digital y Recolección de Evidencias 91

Diseño Pedagógico y Tecnoeducativo del EVA 92

Metodología de Diseño Instruccional: Modelo ADDIE Adaptado 93

Fase 1. Análisis 93

Justificación del modelo ADDIE 94

Fase 2. Diseño 94

Fase 3. Desarrollo 94

Fase 4. Implementación 95

Fase 5. Evaluación 95

Evidencias Visuales del Entorno Virtual Omniverso Digital 96

Interfaz principal 96

Estructura de un Desafío de Salvaguardia 97

Sistema de Insignias y Gamificación 99

Foro de Discusión y Colaboración 100

Recursos Disponibles en Cada Desafío 102

Rutas de Aprendizaje y Secuenciación 103

Ejemplos de Actividades Específicas ..... 105

Diseño y Validación de los Instrumentos de Evaluación ..... 108

*Validación de la Escala ECDSPI* ..... 108

Ítems de la *ECDSPI*. ..... 109

- Competencia: Seguridad y Protección de Datos Personales. ..... 109
- Competencia: Gestión de Identidad Digital. ..... 109
- Competencia: Reconocimiento y Mitigación de Amenazas. ..... 110

*Validación de la Encuesta Abierta de Ciberseguridad* ..... 112

Preguntas Encuesta Abierta: ..... 112

*Validación del EVA Omniverso Digital* ..... 113

Implementación del EVA y Aplicación de los Instrumentos ..... 114

Capítulo V. Resultados y Análisis ..... 116

Etnografía de los estudiantes del IED San Cayetano ..... 116

Resultados cualitativos ..... 119

*Análisis de la Encuesta de Ciberseguridad* ..... 119

Presentación de Resultados Encuesta abierta Ciberseguridad ..... 120

*Evidencias del aprendizaje mediado por el EVA - Omniverso Digital* ..... 124

Nivel de compromiso y creatividad ..... 126

*Apropiación del lenguaje técnico de Ciberseguridad con la intervención de la EVA* ..... 126

Evidencias gráficas: Nubes de palabras por actividad ..... 128

Resultados cuantitativos (ECDSPI) ..... 134
*Comparativo Pretest–Postest* ..... 135

Triangulación de la información ..... 145
Integración de los tipos de triangulación en el análisis de resultados ..... 146

Triangulación de casos representativos ..... 146

*Interpretación pedagógica de los resultados* ..... 152

Síntesis del proceso investigativo ..... 152
Análisis e Interpretación de resultados triangulados ..... 153
Interpretación desde el modelo pedagógico ..... 154
Capítulo VI. Conclusiones ..... 155

Conclusiones ..... 155
Limitaciones del Estudio ..... 158
Recomendaciones ..... 158
Referencias ..... 160

## Tabla de Figuras

**Figura 1** *Mapa de ubicación y fotografías de la IED San Cayetano* ..... 31

**Figura 2** *Fotos de espacios de tecnología e informática en la IED san cayetano* ..... 33

**Figura 3** *Interfaz principal del EVA Omniverso Digital* ..... 97

**Figura 4** *Estructura pedagógica de un Desafío de Salvaguardia en el EVA Omniverso Digital* 98

**Figura 5** *Panel de insignias, logros y progreso del EVA Omniverso Digital* ..... 99

**Figura 6** *Interacción colaborativa en foros del EVA Omniverso Digital* ..... 101

**Figura 7** *Recursos educativos digitales del EVA Omniverso Digital* ..... 102

**Figura 8** *Rutas de aprendizaje y secuenciación pedagógica del EVA Omniverso Digital* ..... 104

**Figura 9** *Ejemplos de productos elaborados por pioneros en el desafío 3: carteles sobre consejos de seguridad digital* ..... 106

**Figura 10** *Carta reflexiva elaborada por pioneros en el desafío 6: mentoría entre pares* ..... 107

**Figura 11** *Estructura repositorio de evidencias desafío de salvaguardia.* ..... 125

**Figura 12** *Nube de palabras – Alianza de Responsabilidad***.** ..... 128

**Figura 13** *Nube de palabras – Conocimiento Seguro* ..... 129

**Figura 14** *Nube de palabras – Consejos de Seguridad.* ..... 131

**Figura 15** *Nube de palabras – Riesgos Tecnológicos* ..... 132

**Figura 16** *Nube de palabras – Protocolo de Seguridad* ..... 133

**Figura 17** *Nube de palabras – Reflexión Personal* ..... 134

## Tabla de tablas

**Tabla 1** *Ejes, descripción y habilidades específicas de la competencia digital en seguridad y privacidad de la información* ..... 56

**Tabla 2** *Correspondencia entre los componentes de la competencia digital en seguridad y privacidad de la información y los instrumentos de medición* ..... 63

**Tabla 3** *Articulación entre ECDSPI y encuesta abierta de ciberseguridad* ..... 108

**Tabla 4** *Escala de respuestas* ..... 110

**Tabla 5** *Comparativo pretest–postest: tipos de contenido compartido por los estudiantes en línea* ..... 120

**Tabla 6** *Comparativo pretest–postest: criterios que aplican antes de publicar información en línea* ..... 121

**Tabla 7** *Comparativo pretest–postest: percepción sobre publicar información o imágenes de otros sin permiso* ..... 122

**Tabla 8** *comparativo pretest–postest: conversaciones familiares o escolares sobre seguridad digital* ..... 122

**Tabla 9** *Comparativo pretest–postest: autopercepción sobre la preparación ante riesgos digitales* ..... 123

**Tabla 10** *Evolución del lenguaje técnico en ciberseguridad a partir de las actividades del EVA – Omniverso Digital. Reto 1* ..... 127

**Tabla 11** *Evolución del lenguaje técnico en ciberseguridad a partir de las actividades del EVA – Omniverso Digital. Reto 2* ..... 129

**Tabla 12** *Evolución del lenguaje técnico en ciberseguridad a partir de las actividades del EVA – Omniverso Digital. Reto 3* ..... 130

**Tabla 13** *Evolución del lenguaje técnico en ciberseguridad a partir de las actividades del EVA – Omniverso Digital. Reto 4* ..... 131

**Tabla 14** *Evolución del lenguaje técnico en ciberseguridad a partir de las actividades del EVA – Omniverso Digital. Reto 5* ..... 132

**Tabla 15** *Evolución del lenguaje técnico en ciberseguridad a partir de las actividades del EVA – Omniverso Digital. Reto 6* ..... 133

**Tabla 16** *Comparativo pretest–postest: "Puedo crear contraseñas seguras y complejas para proteger mi información personal"* ..... 136

**Tabla 17** *Comparativo pretest–postest: "Puedo verificar y modificar la configuración de privacidad en redes sociales y otras plataformas digitales"* ..... 136

**Tabla 18** *Comparativo pretest–postest: "Puedo identificar correos electrónicos o mensajes sospechosos (phishing) y evitar caer en estafas"* ..... 137

**Tabla 19** *Comparativo pretest–postest: "Puedo distinguir entre sitios web seguros y no seguros antes de ingresar mi información personal."* ..... 138

**Tabla 20** *Comparativo pretest–postest: "Puedo realizar copias de seguridad de mis archivos importantes para evitar su pérdida."* ..... 138

**Tabla 21** *Comparativo pretest–postest: "Puedo controlar qué información personal comparto en línea y en qué plataformas."* ..... 139

**Tabla 22** *Comparativo pretest–postest: "Puedo administrar de forma segura mis cuentas digitales y contraseñas."* ..... 140

**Tabla 23** *Comparativo pretest–postest: "Puedo reconocer intentos de suplantación de identidad o perfiles falsos en línea."* ..... 140

**Tabla 24** *Comparativo pretest–postest "Puedo identificar aplicaciones o sitios que solicitan permisos innecesarios o riesgosos."* ..... 141

**Tabla 25** *Comparativo pretest–postest "Puedo aplicar medidas de seguridad en mis dispositivos (como contraseñas, antivirus o bloqueo de pantalla)."* ..... 142

**Tabla 26** *Comparativo pretest–postest "Puedo mantener mis dispositivos y aplicaciones actualizados para protegerme de vulnerabilidades."* ..... 142

**Tabla 27** *Comparativo pretest–postest "Puedo reconocer y tomar medidas cuando siento que mi identidad en línea ha sido comprometida."* ..... 143

**Tabla 28** *Caso 1. Reconocimiento de riesgos digitales (Phishing y enlaces falsos)* ..... 147

**Tabla 29** *Caso 2. Protección de la identidad y los datos personales* ..... 148

**Tabla 30** *Caso 3. Ética y responsabilidad digital* ..... 149

**Tabla 31** *Caso 4. Autonomía y autorregulación tecnológica* ..... 150

**Tabla 32** *Caso 5. Comunicación y colaboración segura en línea* ..... 150

# Capítulo I. La Investigación

## Introducción

En la era digital, las Tecnologías de la Información y la Comunicación (TIC) son fundamentales en la vida cotidiana, lo cual genera oportunidades significativas de interacción y aprendizaje, pero también introduce desafíos en seguridad y privacidad. La adquisición de competencias digitales es esencial para que estudiantes y docentes interactúen de forma segura en entornos digitales, especialmente conforme aumenta el uso de Internet entre los jóvenes, lo cual incrementa la necesidad de formar ciudadanos digitales responsables capaces de navegar de forma ética y consciente, como lo referenciado por Crompton y Burke (2024). Este proyecto se enfoca en la apropiación de competencias digitales en seguridad y privacidad en estudiantes de media vocacional, mediante un Entorno Virtual de Aprendizaje (en adelante) EVA, basada en el conectivismo, un modelo pedagógico para la era digital (Siemens, 2005). Mediante esta estrategia, se buscó desarrollar la capacidad de los estudiantes para comprender y gestionar riesgos en línea y participar de manera segura en la red.

El marco de referencia incluye los Estándares The International Society for Technology in Education (ISTE), los cuales, como indican Crompton y Burke (2024), preparan a los estudiantes para desenvolverse en un entorno tecnológico dinámico. La competencia de Ciudadanía Digital impulsa a los estudiantes a gestionar su huella digital, fomentar interacciones inclusivas, proteger su bienestar y salvaguardar su privacidad en línea. Además, el Ministerio de Educación Nacional (en adelante MEN, 2022), establece para los grados décimo y once la competencia de actuar críticamente frente a las implicaciones éticas y sociales del uso de la tecnología, incluyendo la construcción de protocolos de seguridad y el uso ético de la tecnología para evitar riesgos personales y proteger la información. Esta investigación buscó analizar la

implementación de un EVA en la adquisición de competencias en seguridad digital, con el fin de estructurar un enfoque que guíe a los estudiantes de grados décimo y once de la Institución Educativa Distrital Rural San Cayetano en el uso responsable y seguro de las TIC. De esta manera, se busca fortalecer su formación integral.

El presente documento se organiza en cinco capítulos. En el Capítulo I, La investigación, se presentan la introducción, el planteamiento del problema, la justificación y los antecedentes. El Capítulo II, Marco teórico, aborda los fundamentos conceptuales que sustentan el estudio, incluyendo el conectivismo, los EVA y el impacto de las TIC en la educación, con especial énfasis en las competencias digitales de seguridad y privacidad. El Capítulo III, Metodología, describe el enfoque de investigación, el diseño metodológico y los instrumentos empleados para recolectar y analizar de datos. En el Capítulo IV, Resultados y análisis de resultados, se exponen los hallazgos obtenidos durante la implementación del EVA, junto con su respectiva interpretación y análisis. Finalmente, el Capítulo V, Conclusiones, recoge los aportes de la investigación, estableciendo una reflexión integral que articula el planteamiento del problema con la evaluación y análisis de la propuesta desarrollada.

**Planteamiento del Problema**

El problema de la falta de competencias en seguridad y privacidad digital en jóvenes se ve agravado en contextos rurales, donde el acceso a la tecnología es limitado y las oportunidades de formación en el uso seguro de las TIC son escasas. En la Institución Educativa Distrital Rural San Cayetano, los estudiantes de media vocacional tienen acceso a tecnologías y redes sociales, pero carecen de una formación adecuada para navegar de forma segura y ética en el entorno digital. Esto los deja expuestos a riesgos como el ciberacoso, la manipulación de su información

personal, otros delitos tipificados y la creación de una huella digital negativa que podría perjudicarlos en el futuro.

Aunque existen programas como "*En TIC Confío +"* del Ministerio de Tecnologías de la Información y Comunicaciones de Colombia (MinTic, 2021), y otras iniciativas a nivel global, persiste una falta de integración estructurada de la seguridad digital en los currículos escolares, especialmente en entornos rurales. Según Muñoz y Mora (2021), las limitaciones en infraestructura y formación docente dificultan la implementación de programas de educación digital que aborden estos temas de manera efectiva. Los estudiantes, atraídos por las tendencias digitales, a menudo desconocen o subestiman los riesgos asociados, lo que incrementa su vulnerabilidad en línea.

El conectivismo, como modelo de aprendizaje basado en redes (Siemens, 2005), plantea un enfoque adecuado para enfrentar este problema, pues permite el aprendizaje autónomo y colaborativo y fomenta la reflexión crítica en los estudiantes sobre los riesgos y la protección en el entorno digital. Al participar activamente en redes de conocimiento, los estudiantes no solo acceden a la información, sino que se convierten en agentes en la construcción de su aprendizaje, lo cual es esencial para internalizar prácticas seguras y éticas en línea.

Este estudio plantea una propuesta basada en un EVA que permita a los estudiantes adquirir competencias prácticas en seguridad y privacidad digital. La intención es que esta propuesta contribuya a formar jóvenes más conscientes y críticos, capaces de gestionar su huella digital y de interactuar de manera responsable en entornos digitales, cerrando así la brecha formativa en seguridad digital en entornos rurales.

La falta de formación en seguridad digital deja a los estudiantes vulnerables a generar una huella digital negativa, lo que puede afectar tanto su reputación personal como sus oportunidades

académicas y profesionales. Es crucial que los estudiantes comprendan cómo gestionar su identidad en línea de manera consciente y ética para evitar futuras consecuencias adversas.

**La pregunta esencial que orienta esta investigación es**

¿Cómo contribuye un Entorno Virtual de Aprendizaje (EVA), a la apropiación de la competencia digital en seguridad y privacidad de la información en estudiantes de educación media de la Institución Educativa Distrital Rural San Cayetano?

**Objetivo General**

Evaluar la apropiación de la competencia digital en seguridad y privacidad de la información en la red por parte de los estudiantes de educación media de la Institución Educativa Distrital Rural San Cayetano, a través de un Entorno Virtual de Aprendizaje (EVA).

**Objetivos Específicos**

- **Diagnosticar** los conocimientos previos de la competencia digital en seguridad y privacidad de la información en estudiantes de educación media de la Institución Educativa Distrital Rural San Cayetano
- **Diseñar** un Entorno Virtual de Aprendizaje (EVA) fundamentado en contextos hipotético-reales para favorecer la apropiación de la competencia digital en seguridad y privacidad de la información.
- **Implementar** el EVA en un grupo de estudiantes de educación media de la Institución Educativa Distrital Rural San Cayetano.
- **Evaluar** los resultados del proceso de implementación del EVA, protocolos de seguridad y de uso ético de los productos tecnológicos para evitar diversos riesgos personales y de información personal en la red.

## Contexto de la Investigación

### *Contexto Macro*

El IED San Cayetano Rural, ubicado en la periferia de Bogotá, en la montaña Juan Rey, se construyó como un megacolegio durante la primera alcaldía de Enrique Peñalosa. Este colegio actúa como refugio en caso de emergencia en la zona. Accesible desde el centro de Bogotá, esta aproximadamente a una hora y cuarto en transporte público o a 45 minutos en vehículo particular.

Con un clima frío debido a su proximidad al páramo, el colegio ofrece una infraestructura amplia y moderna que incluye 31 aulas de clase, salones de artes y danzas, y una cabaña temática llamada "Mundos Mágicos" para el área de Humanidades. Además, dispone de un helipuerto, una estación meteorológica y un salón de biosfera, lo que complementa su enfoque en la educación integral.

El colegio IED San Cayetano (2023), cuenta con una biblioteca, un espacio para preescolar, una zona administrativa, y un área de orientación con tres oficinas y una sala de actividades de bienestar. Su diseño arquitectónico está adaptado a su entorno montañoso, con rampas que facilitan el desplazamiento. También posee un pozo de reserva de agua subterránea que proporciona agua circulante proveniente de la flora de la región.

Un dato curioso del IED San Cayetano Rural según la Secretaría de Educación (2021), fue el primer colegio rural que incorporó el programa "Al Colegio en Bici". Sin embargo, aunque las bicicletas proporcionadas por el Distrito no fueron adecuadas debido a las condiciones del terreno, se fabricaron bicicletas con características especiales para los estudiantes. Además, el colegio cuenta con rutas diseñadas para facilitar el transporte de estudiantes y docentes. Como colegio rural, desarrolla la Expedición Rural (2023), la cual está enfocado en el cuidado del agua

y la sostenibilidad en sus prácticas educativas. En las jornadas, el colegio atiende aproximadamente 1.700 estudiantes, de la siguiente manera:

- **Jornada única** para preescolar, con aproximadamente 120 estudiantes, y media vocacional, con alrededor de 270 estudiantes, en articulación con el SENA. Esta jornada cuenta con desayuno y almuerzo para cada estudiante.
- **Jornada de la mañana** para bachillerato, que atiende aproximadamente a 630 estudiantes, y que también cuenta con desayuno.
- **Jornada de la tarde** para primaria, con cerca de 650 estudiantes, donde se ofrece almuerzo.

La cocina del colegio, en colaboración con Compensar, se encarga de ofrecer comidas calientes a los estudiantes. Además, se proporcionan refrigerios a los participantes de diversos grupos de interés, como robótica, huerta, danza, banda, emisora, fútbol sala, entre otros, quienes asisten en horarios de contra jornada. Esta iniciativa no solo garantiza el bienestar nutricional de los estudiantes, sino que también contribuye a crear un ambiente favorable para el aprendizaje. En la Figura 1, se puede observar la localización e infraestructura de la IED San Cayetano

**Figura 1**

*Mapa de ubicación y fotografías de la IED San Cayetano*




*Nota.* La figura muestra en la parte superior la localización de la IED San Cayetano encontrada por Google Maps, en la parte inferior derecha se muestra una toma aérea de toda la infraestructura de la institución, en la parte derecha se observan 3 imágenes que muestran diferentes partes de la IED. Fuente: Google Maps y fotografías de la IED San Cayetano (2024). Ramírez (2023)

## *Contexto Micro*

### Contexto Tecnológico y de Infraestructura.

El Colegio IED Rural San Cayetano cuenta con recursos tecnológicos que facilitan el aprendizaje digital, aunque existen limitaciones en el acceso y la conectividad:

- **Salas de Informática:** La institución dispone de cinco salas de informática con aproximadamente 150 computadoras conectadas a internet, pantalla digital o videobeam, proporcionando un espacio dedicado al aprendizaje digital.
- **Biosferas Interactivas:** Equipadas con una pantalla digital interactiva, impresora en 3D, kits de robótica y elementos de realidad aumentada, estas biosferas ofrecen a los estudiantes un entorno moderno que fomenta la exploración de tecnologías emergentes.
- **Conectividad y Redes**: La conexión a internet depende de redes Wi-Fi, lo que presenta desafíos debido a las condiciones climáticas y la extensión del campus. Se están implementando mejoras en la infraestructura para pasar a un sistema de cableado estructurado que asegure una conectividad más estable.
- **Acceso a Dispositivos en el Hogar**: Un análisis revela que el 86% de los estudiantes de media vocacional cuenta con acceso a internet en sus hogares, lo que facilita el acceso a recursos en línea. Sin embargo, el 14% no tiene conectividad, lo que puede limitar su participación en actividades académicas que dependen del acceso a internet.

**Figura 2**

*Fotos de espacios de tecnología e informática en la IED San Cayetano*




*Nota*. La imagen muestra fotos de los espacios y recursos tecnológicos de la IED San Cayetano, en la imagen de arriba se ve una de las salas de informática y en la de abajo la biosfera interactiva. Fuente: IED San Cayetano. (2023), Fotos propias (2024)

### Caracterización de los Estudiantes.

La diversidad de condiciones y antecedentes de la población estudiantil influye en sus necesidades y formas de aprendizaje:

- **Disparidad de Género:** La cantidad de estudiantes hombres es el doble en comparación con mujeres.
- **Rango de Edades**: Los estudiantes de media vocacional tienen entre 14 y 17 años, un rango que abarca diferentes etapas de desarrollo cognitivo y emocional.
- **Entorno de hogar**: Aproximadamente la mitad de los estudiantes vive en un entorno rural, lo que implica un contexto de vida ligado a actividades agrícolas y costumbres locales.

**Caracterización de los Cuidadores.**

- **Nivel Educativo de los Cuidadores:** La formación académica de los cuidadores varía considerablemente. Muchos han completado la educación secundaria, mientras que otros no han finalizado este nivel o solo tienen estudios de primaria. Un pequeño grupo ha accedido a la educación superior, ya sea universitaria o técnica. Esta diversidad educativa puede afectar la capacidad de algunos cuidadores para brindar apoyo académico a sus hijos, lo que subraya la necesidad de contar con recursos accesibles que faciliten el aprendizaje independiente de los estudiantes.
- **Disponibilidad y Carga Laboral de los Cuidadores:** La mayoría de los cuidadores se encuentra en el mercado laboral, aunque un porcentaje significativo no trabaja. Entre aquellos que están empleados, muchos tienen jornadas laborales extensas, lo que puede limitar el tiempo que pueden dedicar a ayudar a sus hijos con sus estudios. Esta situación resalta la importancia de diseñar estrategias que consideren la disponibilidad de los cuidadores, de modo que puedan involucrarse más en el proceso educativo.
- **Sensibilidad Cultural, Social y Socioeconómica:** El Colegio IED Rural San Cayetano cuenta con una población estudiantil diversa que requiere sensibilidad en el diseño de los contenidos para garantizar su relevancia y conexión con la vida de los estudiantes:
- **Relevancia Cultural de los Contenidos**: Aproximadamente la mitad de los estudiantes proviene de un entorno rural. Esto destaca la importancia de adaptar los contenidos educativos a un contexto agrícola y a los valores de la comunidad, para lograr un aprendizaje más significativo.

**Caracterización Socioeconómica.**

- **Condición Socioeconómica**: La mayoría de los estudiantes pertenece a los estratos socioeconómicos más bajos. El 63% proviene de hogares en el estrato 1, mientras que el 14% pertenece al estrato 2, el 7% al estrato 3, y solo el 2% al estrato 4. No hay estudiantes en los estratos 5 y 6, que representan los niveles más altos. Un 14% no ha determinado su estrato, posiblemente viviendo en asentamientos informales. Esta situación enfatiza la necesidad de implementar estrategias educativas que atiendan las limitaciones económicas, promoviendo un entorno equitativo y accesible para todos.
- **Composición Familiar:** En la IED Rural San Cayetano, la mayoría de los estudiantes proviene de familias de tamaño mediano, generalmente de cuatro integrantes, aunque también hay hogares con dos integrantes y otros con hasta nueve integrantes. Esta diversidad en la composición familiar implica distintas dinámicas y necesidades que pueden influir en el apoyo educativo.
- **Prioridades de Gasto:** En términos de gasto, las familias suelen concentrarse en cubrir necesidades esenciales como alimentación, vivienda y servicios básicos. Para algunos hogares, el transporte representa un gasto considerable, mientras que la recreación y el ocio no suelen estar dentro de las prioridades, posiblemente debido a limitaciones económicas.

## Justificación

La formación en seguridad y privacidad digital adquiere una importancia crítica en los contextos educativos rurales, donde las limitaciones de conectividad y el acceso restringido a contenidos educativos actualizados dificultan la preparación de los estudiantes frente a los riesgos del entorno digital. En estos escenarios, los jóvenes de educación media suelen

conectarse a través de redes inestables o compartidas, sin contar con una orientación sistemática sobre cómo proteger su información personal ni sobre las implicaciones de su comportamiento en línea.

En su esfuerzo por integrarse a la vida digital —dado que participan de manera activa en redes sociales y plataformas de uso cotidiano— muchos estudiantes desconocen o subestiman las prácticas básicas de seguridad digital. Esta situación los expone a riesgos como el robo de identidad, el ciberacoso y la difusión no autorizada de información, y contribuye a la construcción de una huella digital negativa que puede afectar su bienestar personal, académico y social a corto y largo plazo.

Por ello, resulta fundamental no solo enseñar habilidades técnicas orientadas a la protección de la información digital, sino también promover una formación ética que permita a los estudiantes actuar de manera responsable, reflexiva y respetuosa consigo mismos y con los demás. Esta necesidad se acentúa en el contexto rural, donde la educación formal sobre estos temas suele ser limitada y los jóvenes carecen de referentes claros o de espacios de diálogo orientados a la comprensión de los riesgos y responsabilidades del entorno digital

El presente estudio se justifica, entonces, en dos sentidos fundamentales: por un lado, en la escasez de EVA diseñados específicamente para la formación en seguridad y privacidad digital en poblaciones escolares; y, por otro, en la urgencia de que los estudiantes desarrollen una comprensión integrada —técnica y ética— de su comportamiento en los entornos virtuales que habitan cotidianamente.

Desde esta perspectiva, la intervención educativa se desarrolla a través del EVA **Omniverso Digital**, concebido como un espacio pedagógico conectado que favorece la apropiación significativa de la competencia en seguridad y privacidad de la información

mediante actividades interactivas, análisis de casos reales y simulaciones. Su estructura se fundamenta en el enfoque conectivista, el cual concibe el aprendizaje como la capacidad de establecer conexiones entre diversas fuentes de información, experiencias digitales y actores sociales.

Asimismo, esta propuesta busca motivar a los estudiantes a aprender de forma autónoma y colaborativa, fortaleciendo su capacidad para identificar riesgos digitales, aplicar medidas de protección personal y reflexionar sobre el impacto de sus acciones en el ecosistema digital. De este modo, se promueve la construcción de una huella digital consciente, positiva y empática, que no solo resguarde la seguridad individual, sino también la de su entorno familiar, escolar y comunitario.

Finalmente, este proyecto aporta valor tanto a nivel local como académico, al presentar un EVA diseñado, implementado y evaluado en un contexto educativo real, susceptible de ser replicado y adaptado en otras instituciones educativas rurales del país. Su enfoque pedagógico, centrado en la articulación entre competencias digitales, ciudadanía y ética, constituye una herramienta relevante para avanzar hacia una educación más inclusiva, crítica y segura en la era digital.

## Antecedentes

En esta sección se exponen los antecedentes que respaldan la necesidad de desarrollar una EVA apoyada en contextos hipotético-reales y fundamentada en el conectivismo, en la competencia digital relacionada con la seguridad y la privacidad. Se mencionan estudios previos

que han demostrado una creciente preocupación por la falta de preparación de los estudiantes en cuanto a la protección de sus datos personales y la gestión ética de su identidad digital.

También se mencionan las diversas investigaciones que han abordado los desafíos relacionados con la seguridad en entornos digitales y la necesidad de estrategias didácticas efectivas que formen a los estudiantes en esta competencia crítica. En esta investigación, los antecedentes se centran en el uso de EVA como estrategia pedagógica conectivista para fortalecer competencias digitales en seguridad y privacidad.

Diversos estudios han evidenciado que los EVA, al estar basados en la colaboración, el aprendizaje autónomo y el uso de tecnologías digitales, favorecen la apropiación significativa de conocimientos en estudiantes de contextos rurales (Muñoz y Mora, 2021; Cueva et al., 2019). Asimismo, investigaciones recientes han resaltado que la integración de EVA permite superar barreras geográficas y de acceso a la información, especialmente cuando están diseñados con un enfoque contextualizado y gamificado.

Para esta investigación, se tendrá en cuenta documentos desde el año 2016 hasta la fecha, lo que incluye publicaciones en revistas y repositorios de universidades nacionales y extranjeras, como son investigaciones, artículos y revistas indexadas. Se encontraron 26 trabajos relacionados, entre ellos 1 libro, 3 tesis de maestría nacionales y 27 artículos académicos (6 de origen nacional y 21 internacionales), seleccionados por su pertinencia con los ejes temáticos del estudio.

A continuación, se presentan los antecedentes de esta investigación, estructurados en torno a cuatro grandes categorías: el conectivismo, los EVA, el impacto de la tecnología en la sociedad, y las competencias digitales con especial énfasis en la seguridad y la privacidad en

línea. Estas categorías permiten entender los fundamentos teóricos y prácticos sobre los cuales se basa esta investigación y cómo se relacionan con la problemática educativa actual.

### *Conectivismo*

Alvarez et al. (2022) investigan el conectivismo como paradigma para la educación en contextos postpandemia, señalando los retos y oportunidades que ofrece este modelo para transformar el sistema educativo tradicional. Su estudio analiza como el conectivismo puede transformar el aprendizaje tradicional en uno fundamentado en la colaboración, la autonomía y el acceso flexible a recursos digitales. Los autores presentan un análisis documental de estudios previos sobre educación en red y comparan los retos de conectividad y adaptación tecnológica en diversas instituciones educativas de América Latina y Estados Unidos.

La metodología documental y exploratoria de este trabajo permite un enfoque integral en el análisis de las barreras que limitan la implementación del conectivismo, incluyendo la brecha digital y el analfabetismo informático. Esta referencia es crucial, ya que ofrece un enfoque práctico para comprender cómo una EVA conectivista puede contribuir al desarrollo de competencias digitales en seguridad y privacidad. Asimismo, el estudio resalta la importancia de crear entornos conectados que fomenten el aprendizaje autónomo y la participación en redes de conocimiento.

Como explora Goldie (2016), el conectivismo constituye una teoría de aprendizaje relevante para la era digital. Goldie analiza cómo el conectivismo aborda el aprendizaje en red y cómo las conexiones entre nodos de información permiten la construcción del conocimiento en entornos digitales. Al utilizar un enfoque teórico, el autor revisa el papel de los educadores y estudiantes en la era de la información, destacando la importancia del aprendizaje autónomo y la colaboración en línea.

Este estudio de Goldie es importante para la tesis, ya que proporciona una base teórica para el diseño de una EVA basada en el conectivismo. Al entender cómo los estudiantes aprenden mediante la creación de redes de conocimiento, el EVA puede ser estructurada para promover la autonomía en el aprendizaje de competencias en seguridad y privacidad digital.

En su estudio Torres y Barnabé (2020) examinan cómo el conectivismo y las redes sociales pueden integrarse en la educación para crear ecologías de aprendizaje colaborativas y efectivas. Su estudio examina la creación de entornos de aprendizaje colaborativos y digitales, donde los estudiantes pueden intercambiar conocimiento y experiencias de manera autónoma. Los autores destacan que el conectivismo permite a los estudiantes participar activamente en redes de conocimiento y utilizar plataformas digitales para construir comunidades de aprendizaje en línea. Este análisis es fundamental para comprender cómo las redes y la colaboración en entornos digitales pueden apoyar el desarrollo de competencias específicas.

A través de una revisión sistemática de literatura, Torres y Barnabé enfatizan la importancia de los principios del conectivismo para fomentar una mayor interacción y participación en el aprendizaje. Este estudio es significativo, ya que respalda la idea de que una EVA conectivista puede mejorar las competencias en seguridad digital de los estudiantes. Este enfoque fomenta la colaboración y la autogestión en redes, en aspectos esenciales para que los estudiantes puedan enfrentar los riesgos de la privacidad en entornos digitales.

En la discusión que proponen Tumino y Bournissen (2016) sobre el conectivismo como un paradigma que promueve la enseñanza por competencias en entornos digitales, los autores analizan, a partir de un enfoque cualitativo, cómo aplicar el conectivismo en el aula para que los estudiantes asuman un rol activo en la construcción de su propio conocimiento.

La relevancia de este estudio radica en que proporciona una comprensión profunda de cómo el conectivismo fomenta la autonomía y la colaboración en entornos de aprendizaje en red, lo que es esencial para desarrollar competencias en seguridad digital. La propuesta de Tumino y Bournissen respalda la implementación de una EVA conectivista que permita a los estudiantes interactuar de forma segura y autónoma, utilizando recursos digitales para construir su conocimiento sobre la privacidad en línea.

De otro lado, Cueva et al. (2019) abordan cómo el conectivismo y las tecnologías de la información y la comunicación (TIC) transforman la educación al promover aprendizajes autónomos, colaborativos y significativos. Enfatizan en la necesidad de preparar tanto a estudiantes como a docentes en el uso crítico de las TIC para enfrentar entornos cambiantes y superar barreras como la brecha digital. Este enfoque destaca, que integrar el conectivismo con el uso estratégico de TIC facilita un aprendizaje activo y motivador, al desarrollar habilidades como la autoorganización y la toma de decisiones conscientes en escenarios educativos.

También Sanchez et al. (2019) analizan el conectivismo basado en la creación de redes de conocimiento y la interacción activa con nodos de información, en tanto se adapta a los retos de la era digital. La problemática radica en la necesidad de un paradigma que responda al aprendizaje distribuido y volátil, característico del mundo conectado actual, particularmente en contextos con limitaciones tecnológicas como los rurales. En su conclusión, los autores destacan que el conectivismo no solo complementa teorías pedagógicas previas, sino que es especialmente efectivo al integrar tecnologías digitales en ambientes de aprendizaje, al fomentar la autoorganización y la colaboración en red, principios esenciales para diseñar una EVA que desarrolle competencias digitales en seguridad y privacidad.

Bernal (2020), en su trabajo, ofrece una base sólida para estructurar una EVA destacando el conectivismo como enfoque pedagógico que promueve el aprendizaje en red y la construcción colaborativa del conocimiento. La problemática que aborda incluye la necesidad de adaptar las prácticas educativas a las demandas de la era digital, donde los estudiantes deben desarrollar habilidades para identificar, conectar y organizar información de manera autónoma. Este enfoque es particularmente relevante en contextos rurales, donde los recursos tecnológicos suelen ser limitados, al proponer estrategias como el uso de redes de aprendizaje y entornos personales que optimicen los recursos disponibles. En su conclusión, el autor resalta que el conectivismo facilita la consolidación de nuevos modelos instruccionales que fomentan la autoorganización, la colaboración y el aprendizaje significativo, proporcionando una metodología adaptable para el desarrollo de competencias digitales en seguridad y privacidad.

La teoría conectivista ofrece una base sólida para la creación de una EVA enfocada en la seguridad digital, al enfatizar la construcción del conocimiento a través de redes y la participación activa. Esta perspectiva es crucial en el desarrollo de competencias digitales que permitan a los estudiantes gestionar y proteger su información en un entorno digital.

Como se puede observar con estos antecedentes presentados en torno al conectivismo y el aprendizaje, en red, se refuerza la viabilidad de implementar una EVA que promueva la autonomía y la colaboración entre los estudiantes. Esta base teórica es esencial para desarrollar competencias digitales en seguridad, ya que fomenta la participación en la construcción de conocimientos y la concienciación sobre la importancia de una navegación segura en línea.

### *Entornos Virtuales de Aprendizaje - EVA*

Diversos estudios han explorado el impacto y los retos de los EVA en los procesos de aprendizaje. Cedeño y Murillo (2019) analizaron cómo estos entornos promueven procesos de

enseñanza innovadores y facilitan la integración de tecnologías que enriquecen la experiencia educativa. Su investigación enfatiza el rol transformador de los EVA en la educación superior y su potencial para ampliar el acceso a la educación de calidad.

En su trabajo, Restrepo (2023) destaca la importancia de estructurar ambientes de aprendizaje que combinen recursos físicos y digitales para el desarrollo progresivo de competencias específicas. Estos principios pueden ser adaptados al diseño de EVA, ya que permiten que los estudiantes transiten por experiencias formativas interactivas, desde el diagnóstico hasta la aplicación, especialmente en temas de seguridad y privacidad digital. La metodología de creación de espacios adaptados para desarrollar competencias específicas puede ser aplicada en la planificación de actividades secuenciales que guíen a los estudiantes en el aprendizaje seguro en internet.

Restrepo analiza cómo las actividades en bibliotecas escolares deben estructurarse de forma secuencial para permitir un desarrollo gradual de competencias, desde habilidades básicas de alfabetización digital hasta competencias más avanzadas en el manejo seguro de información. Este enfoque en la secuencialidad se alinea con la tesis, donde el EVA debe permitir a los estudiantes progresar en su comprensión y práctica de la seguridad en línea de manera ordenada.

También enfatiza el papel activo del facilitador en la biblioteca, quien guía y apoya a los estudiantes en la construcción de conocimiento digital. Esta investigación es aplicable al EVA del presente trabajo, en la cual el docente o facilitador desempeña un rol clave en la enseñanza de prácticas seguras en internet, asegurando que cada fase del EVA sea efectiva y alineada con los objetivos de seguridad digital.

Tal como concluye López (2017), que propone integrar el enfoque de aprendizaje basado en problemas y contextos significativos para promover la comprensión conceptual y el

aprendizaje activo; es posible considerar que este enfoque es aplicable en este proyecto, ya que sugiere estructurar actividades que aborden problemáticas cercanas a los estudiantes, como la seguridad y privacidad digital, integrando herramientas tecnológicas y fomentando el trabajo colaborativo bajo la guía de un docente facilitador. Además, destaca la importancia de evaluar continuamente las dificultades y avances de los estudiantes para ajustar las actividades y asegurar un aprendizaje progresivo y efectivo.

De otro lado, Marrón y Martínez (2023) resaltan cómo los programas de formación continua estructurados digitalmente fortalecen competencias en seguridad y privacidad en línea. Mediante un análisis documental, los autores revisan programas de acreditación que enfatizan la seguridad y privacidad en línea. Su investigación resalta que los EVA permiten un desarrollo progresivo de competencias, aspecto que es crucial para diseñar actividades que promuevan el aprendizaje seguro y la interacción ética en línea.

Esta referencia es útil, ya que destaca la importancia de la estructura y planificación en el aprendizaje de competencias digitales. Estos hallazgos son transferibles al contexto estudiantil, y permiten sustentar el uso del EVA como una herramienta eficaz para desarrollar habilidades digitales esenciales en entornos educativos rurales.

En su estudio Cagüeño y Cifuentes (2022) presentan estrategias para superar barreras tecnológicas mediante propuestas instruccionales adaptadas a contextos rurales. Se centra en el diagnóstico inicial de dificultades, el diseño de actividades prácticas y dinámicas mediadas por recursos concretos y tecnológicos, y la evaluación formativa y sumativa. El documento subraya cómo las estrategias fortalecen habilidades fundamentales al integrar contenidos educativos con la realidad cotidiana de los estudiantes. Sus aportes son clave en la implementación de un EVA

que utilice recursos digitales accesibles y fomente la construcción de competencias digitales vinculadas con la privacidad y la seguridad en línea.

Como señala Galbin (2011)el desarrollo de la competencia digital se ha convertido en una habilidad esencial dentro de los entornos de aprendizaje remoto y virtual, especialmente tras los cambios acelerados que experimentó la educación a partir de la pandemia. Su estudio evidencia que los procesos formativos mediados por tecnología requieren estrategias pedagógicas flexibles y contextualizadas que reduzcan las brechas de acceso y promuevan la equidad digital entre los estudiantes. Desde esta perspectiva, el fortalecimiento de las competencias digitales en seguridad y privacidad no solo depende de la infraestructura tecnológica, sino también de la capacidad docente para diseñar entornos virtuales inclusivos y éticos, que permitan a los estudiantes desenvolverse con autonomía y responsabilidad en la red. Estos planteamientos respaldan la pertinencia del *EVA Omniverso Digital,* al proponer un modelo pedagógico que articula conectividad, aprendizaje colaborativo y formación en ciudadanía digital segura.

Por su parte, Torres y Barnabé (2020) investigaron el enfoque conectivista aplicado a la educación digital, subrayando la importancia de las redes sociales y ecologías de aprendizaje como estructuras fundamentales para el desarrollo de competencias en entornos virtuales. Su trabajo aporta una base teórica sólida para entender los desafíos que enfrentan los docentes al incorporar EVA en sus prácticas pedagógicas.

Como explorarán Basurto et al. (2021) estructuran en su propuesta pedagógica conectivista mediante el uso de plataformas digitales, lo cual promueve el aprendizaje autónomo y la colaboración, elementos clave en el diseño instruccional del EVA. Utilizando una metodología cualitativa, el estudio se centra en la aplicación de actividades estructuradas en el

EVA que permiten a los estudiantes aprender a través de redes. Los autores encuentran que este modelo fomenta la autonomía del estudiante y su participación en la construcción del conocimiento, cualidades que son esenciales para el aprendizaje de competencias en entornos digitales.

La importancia de este estudio radica en su enfoque práctico sobre cómo estructurar EVA en un contexto que puede ser adaptado para el aprendizaje de competencias en seguridad y privacidad. Este enfoque permite a los estudiantes no solo acceder a información, sino también colaborar y aplicar conocimientos de manera autónoma en actividades prácticas, algo fundamental para desarrollar habilidades críticas en seguridad digital.

También se encontró en Gallego (2017), el análisis de cómo estructurar procesos de aprendizaje en entornos de e-learning, destacando la importancia de la comunicación digital, la organización progresiva del contenido y la reflexión crítica. Su metodología cualitativa explora el diseño de estrategias que integran el uso de herramientas digitales, facilitando un aprendizaje progresivo en los estudiantes. El estudio enfatiza que estas estrategias no solo organizan el contenido, sino que también promueven la interacción y la reflexión crítica, habilidades fundamentales en el entorno digital actual.

Este enfoque proporciona un modelo de estructura didáctica aplicable a la enseñanza de competencias en seguridad digital. Al organizar el aprendizaje en fases progresivas, las estrategias propuestas en el estudio de Gallego (2017), permiten que los estudiantes no solo adquieran conocimiento teórico, sino que también apliquen y analicen prácticas seguras en línea, lo cual favorece una comprensión integral de la seguridad digital.

En el contexto de esta investigación, estos elementos son esenciales en el diseño de EVA, ya que permiten promover habilidades prácticas en seguridad digital a través de escenarios

virtuales. Ya que ayuda a los estudiantes a comprender y aplicar conceptos de protección de datos y privacidad de manera estructurada y práctica.

Los aportes de Aguilar et al. (2022) proponen una organización en fases que puede adaptarse a la estructura pedagógica del EVA, lo que permite un aprendizaje gradual de la seguridad digital mediante actividades virtuales y prácticas contextualizadas. Ellos indican que se deben estructurar las actividades en tres fases: preliminares, para identificar saberes previos; de aprendizaje, con ejercicios prácticos apoyados en recursos visuales, auditivos y kinestésicos; e integradoras, que evidencien el aprendizaje mediante la aplicación de conocimientos adquiridos en contextos reales. Además, sugiere el uso del modelo ADDIE para el diseño instruccional, enfatizando análisis, diseño, desarrollo, implementación y evaluación como etapas fundamentales. En su conclusión, resalta que los entornos virtuales promueven la autogestión y el aprendizaje autónomo, adaptando los contenidos a las necesidades del estudiante, lo cual es directamente aplicable para fomentar competencias digitales en seguridad y privacidad.

Finalmente, Cueva Delgado et al. (2019) abordaron la relación entre el conectivismo y las tecnologías de la información y la comunicación, resaltando cómo estas influyen en la transformación de los procesos educativos y en la formación de competencias para la era digital, lo que reafirma la relevancia de los EVA en el contexto educativo actual.

### *Impacto de la tecnología en la apropiación de competencias de seguridad y privacidad digital*

El impacto de la tecnología en el desarrollo de competencias digitales relacionadas con la seguridad y la privacidad se evidencia en diversos estudios recientes. Por ejemplo, Castillejos, Torres, y Lagunes (2016) destacan que la exposición constante de los estudiantes a entornos digitales exige fortalecer las competencias asociadas con la protección de la información personal, la gestión ética de datos y la autorregulación del comportamiento en línea. Su

investigación demuestra que los jóvenes tienden a utilizar las tecnologías de forma intuitiva, pero sin una conciencia clara de los riesgos vinculados con la seguridad digital. En este sentido, la integración pedagógica de EVA se convierte en una estrategia esencial para fomentar una ciudadanía digital crítica, responsable y capaz de salvaguardar su identidad digital. Así, el *EVA Omniverso Digital* se plantea como un espacio formativo que trasciende el uso instrumental de la tecnología y promueve la apropiación ética y consciente de las prácticas de seguridad y privacidad en la red.

En su libro Van Dirk (2020) examina cómo la brecha digital afecta el acceso y uso de la tecnología en la educación. Utilizando un enfoque cuantitativo, Van Dijk estudia las diferencias de acceso a las TIC y su impacto en la sociedad, especialmente en el ámbito educativo. El autor destaca que la desigualdad digital sigue siendo un desafío que limita las oportunidades educativas y el desarrollo de competencias digitales.

Esta investigación es útil para la tesis, ya que resalta la importancia de considerar el contexto socioeconómico en el desarrollo de EVA para el aprendizaje de seguridad digital. Al reconocer estas limitaciones, el entorno propuesto puede adaptarse para maximizar el acceso y comprensión de competencias digitales en seguridad y privacidad, incluso en contextos con acceso limitado a la tecnología.

En la investigación de Torres y Barnabé (2020) examinan el impacto de las redes sociales y las ecologías de aprendizaje en la educación, argumentando que la tecnología digital debe integrarse de manera responsable para crear entornos de aprendizaje seguros y colaborativos. Mediante una revisión sistemática de literatura, los autores destacan cómo el uso crítico de la tecnología puede mejorar las competencias digitales y facilitar la gestión de la identidad en línea.

Este enfoque es valioso, ya que resalta la importancia de un aprendizaje seguro y colaborativo en temas de seguridad digital.

Los hallazgos de Torres y Barnabé refuerzan la idea de que la interacción digital puede apoyar la formación de competencias éticas y seguras en los estudiantes. Esto permite comprender la importancia de utilizar redes digitales para promover la autonomía en la gestión de la privacidad, aspecto crucial en el EVA que se plantea en la tesis.

Crompton y Burke (2024) plantean un conjunto de normas internacionales que describen las competencias que deben tener tanto estudiantes como docentes en el uso de tecnología los ISTE Standars. Estos estándares promueven un uso seguro, ético y efectivo de la tecnología, lo que incluye la competencia en la gestión de la privacidad y la seguridad en línea. El enfoque del documento es fundamentalmente normativo y educativo, orientado a establecer prácticas seguras y responsables en el ámbito digital.

La relevancia de estos estándares es evidente, ya que proporcionan una guía sobre las habilidades específicas de seguridad digital que deberían desarrollarse en los estudiantes. Estos lineamientos permiten estructurar el EVA en la tesis, asegurando que las actividades propuestas respondan a estándares internacionales en el uso seguro y ético de las tecnologías.

### *Competencias Digitales*

#### Información y alfabetización de datos.

En el documento de la UNESCO (2019) se presenta un marco de competencias en materia de TIC, organizado en tres niveles: adquisición, profundización y creación de conocimientos. El marco abarca seis aspectos: comprensión del papel de las TIC en las políticas educativas, currículo y evaluación, pedagogía, aplicación de competencias digitales, organización y administración, y aprendizaje profesional de los docentes. También se incluyen

consideraciones sobre el desarrollo profesional continuo de los docentes en materia de TIC, todos estos son aspectos fundamentales de esta investigación, ya que son útiles para fortalecer la alfabetización de datos.

En estudiantes de secundaria, la alfabetización mediática e informacional (MIL) se relaciona fuertemente con factores socioformativos como el acceso a Internet, el tipo de institución y el contexto urbano–rural, lo que impacta directamente su capacidad para buscar, evaluar y gestionar información confiable. En un diagnóstico con 1.250 estudiantes de 9.º a 11.º en Arequipa (Perú), Turpo-Gebera et al. (2023) validan un instrumento basado en UNESCO y evidencian que mayores niveles de MIL se asocian con mejor disponibilidad de servicios y recursos tecnológicos, así como con la progresión por edad/curso; además, señalan brechas que requieren intervenciones curriculares para enfrentar la desinformación y fortalecer el pensamiento crítico en la escuela. Estos hallazgos respaldan el diseño del EVA Omniverso Digital para desarrollar, dentro del aula, rutinas explícitas de verificación de fuentes, curaduría crítica y uso ético de la información.

**Comunicación y colaboración.**

La competencia de comunicación y colaboración digital en estudiantes se potencia cuando las tareas en línea exigen coordinación real entre pares y diálogo académico de calidad. En un proyecto intercultural con estudiantes de secundaria, Aguilar-Cruz y Xiang (2023) evidencian que la escritura colaborativa en entornos virtuales favorece la empatía digital, la co-regulación y la responsabilidad compartida. De forma complementaria, Jurkowski, Mundelsee y Hänze (2024) muestran que un entrenamiento integrado en aula sobre comunicación transaccional (formular preguntas, argumentar y construir sobre las ideas de otros) eleva la eficacia del aprendizaje colaborativo. Estos resultados orientan el diseño del *EVA Omniverso*

*Digital* hacia actividades con roles claros, rúbricas de interacción y productos colectivos, asegurando interacciones respetuosas y seguras entre estudiantes.

Como ya se mencionó, UNESCO (2019) presenta un marco de competencias en materia de TIC y también puede utilizarse para la comunicación y colaboración, ya que destaca las competencias digitales necesarias para que docentes y estudiantes interactúen en entornos digitales.

**Crear contenidos digitales.**

En el ámbito de la creación de contenidos digitales, Pertegal y Lorenzo (2019) evidencian cómo la gamificación mediante herramientas TIC, como Kahoot, promueve la motivación y la participación activa de los estudiantes en el aula. Su estudio analiza la integración de videoclips y recursos interactivos como medios para dinamizar la enseñanza y favorecer la producción de contenidos por parte de los estudiantes. Los resultados revelan un alto nivel de satisfacción (81%) entre los participantes, quienes valoraron positivamente la experiencia gamificada frente a un 19% de valoración negativa, lo que demuestra la efectividad de estas estrategias para fortalecer el aprendizaje significativo y el compromiso estudiantil.

Esta competencia es fundamental en una EVA orientada a la seguridad digital, ya que ayuda a los estudiantes a tomar conciencia de su huella digital y de los efectos de su actividad en línea.

**Seguridad.**

De acuerdo con Barragán y Murta (2023), la seguridad en Internet constituye un componente esencial de la competencia digital ciudadana y debe abordarse desde una perspectiva educativa integral que combine el desarrollo técnico con la reflexión ética. En su revisión sistemática, los autores subrayan que la formación en ciberseguridad no puede limitarse al

conocimiento de herramientas, sino que debe promover actitudes críticas y comportamientos responsables frente al uso de la información personal, la interacción en redes sociales y la gestión de la identidad digital. Asimismo, advierten que el desconocimiento de los riesgos asociados al entorno virtual incrementa la vulnerabilidad de los estudiantes frente a prácticas de suplantación, acoso o exposición de datos.

Por su parte, Garmendia, Martínez, Larrañaga, y Jiménez (2024) señalan que la competencia digital en ciberseguridad constituye un componente esencial en la formación del alumnado, particularmente en los niveles de educación primaria y secundaria. Su estudio demuestra que la integración de la ciberseguridad en las prácticas pedagógicas favorece no solo la protección de datos personales, sino también la convivencia digital responsable, al promover comportamientos éticos y respetuosos en los entornos virtuales. Los autores enfatizan que las brechas en la alfabetización digital de seguridad de los estudiantes pueden limitar la eficacia de las estrategias formativas, lo que refuerza la necesidad de incorporar entornos virtuales que desarrollen competencias prácticas en la gestión de la privacidad, la huella digital y la prevención de riesgos en línea. Estos hallazgos respaldan el propósito del *EVA Omniverso Digital*, orientado a fortalecer la competencia de seguridad digital en contextos escolares mediante experiencias conectivistas y actividades interactivas.

Como plantean Zhao, Pinto, y Cruz (2021), la dimensión de seguridad dentro de la competencia digital continúa siendo una de las áreas menos desarrolladas en los procesos educativos, tanto en la educación superior como en los niveles básicos y medios. En su revisión sistemática, los autores identifican una brecha significativa entre el uso instrumental de la tecnología y la formación en prácticas seguras, éticas y responsables en el entorno digital. Subrayan que, aunque las instituciones educativas han avanzado en la integración de plataformas

virtuales y recursos tecnológicos, persiste una limitada incorporación de estrategias pedagógicas orientadas a la protección de datos personales, la gestión crítica de la información y la prevención de riesgos digitales. Asimismo, advierten que la falta de alfabetización en seguridad digital puede comprometer la autonomía del estudiante y su capacidad para actuar como ciudadano digital consciente. En este sentido, sus conclusiones respaldan la pertinencia del *EVA Omniverso Digital*, al proponer un modelo formativo que no solo promueve el aprendizaje técnico, sino también la construcción de valores y comportamientos responsables frente a la privacidad, la identidad digital y la convivencia en línea, contribuyendo al fortalecimiento integral de la competencia digital en contextos escolares.

Por otra parte, Castillejos et al. (2016) explora las prácticas de seguridad digital entre estudiantes universitarios de la generación millennial, evaluando su percepción y comportamiento en torno a la protección de datos personales, dispositivos, salud y el medio ambiente. Mediante un enfoque mixto que combina encuestas en línea y entrevistas semiestructuradas, el estudio analiza las competencias digitales de los estudiantes en relación con la seguridad. Los autores utilizan el marco del proyecto IKANOS del Instituto Vasco de Cualificaciones, que clasifica las competencias digitales en diversas áreas, incluidas la seguridad y la gestión de la privacidad, utilizando herramientas estadísticas para interpretar los datos obtenidos.

La investigación proporciona un análisis detallado de cómo los estudiantes millennials manejan aspectos de seguridad y privacidad en línea, el estudio ofrece información valiosa sobre las prácticas comunes de protección de datos personales y la gestión de la identidad digital. Esta referencia es relevante porque sustenta la importancia de desarrollar competencias digitales en

seguridad para enfrentar los riesgos de ciberseguridad, lo que coincide con el objetivo de la tesis de fortalecer estas competencias en entornos educativos.

Este aspecto de la competencia digital es esencial para el desarrollo de una EVA que prepare a los estudiantes para navegar de manera segura en un entorno digital cada vez más complejo.

# Capítulo II. Marco Teórico

En este apartado se aborda de manera preliminar la revisión teórica que fundamenta la propuesta, la cual se aborda desde cinco ejes fundamentales: conectivismo, EVA, tecnología, informática y sociedad, ciudadano digital, competencias digitales, de esta última se desprenden cuatro subcategorías que son información y alfabetización de datos, comunicación y colaboración, creación de contenidos digitales y seguridad esta última subcategoría es la que se enfatiza en este trabajo.

Estos ejes fundamentales y subcategorías serán revisadas según varios referentes representativos, para establecer los cimientos teóricos. Cada uno de estos ejes se complementa para sostener la propuesta de formar a los estudiantes en la gestión responsable de su seguridad y privacidad en línea.

En el contexto educativo, la integración de las tecnologías de la información y la comunicación (TIC) ha planteado nuevos desafíos para el aprendizaje. El desarrollo de competencias digitales en los estudiantes se ha vuelto fundamental, especialmente en lo relacionado con la seguridad y privacidad en entornos digitales. Este marco teórico explora varios enfoques y teorías que fundamentan este estudio.

## Competencia Digital en Seguridad y Privacidad de la Información

### *Definición Operacional de la Competencia Estudiada*

La Competencia Digital en Seguridad y Privacidad de la Información se define, en el marco de esta investigación, como el conjunto integrado de conocimientos, habilidades y actitudes que permiten a los usuarios desenvolverse de manera segura, responsable y ética en entornos digitales, mediante la protección de su información personal, la gestión consciente de su identidad digital y la prevención de riesgos asociados al uso de tecnologías de la información.

De manera específica, esta competencia posibilita que los estudiantes:

- Protejan la información personal y los datos sensibles en entornos digitales.
- Gestionen su identidad digital de forma segura y responsable.
- Reconozcan, prevengan y respondan ante amenazas y riesgos digitales.
- Actúen de manera ética y responsable en los espacios virtuales.

Esta definición operacional orienta tanto el diseño de los instrumentos de evaluación como la estructuración de las actividades pedagógicas desarrolladas en el EVA *Omniverso Digital*.

Dimensiones de la competencia digital en seguridad y privacidad de la información

A partir de la *Escala de Competencias Digitales en Seguridad y Privacidad de la Información* (en adelante ECDSPI,) la competencia se estructura en tres ejes fundamentales, los cuales permiten analizar su desarrollo de manera integral:

**Tabla 1**

*Ejes, descripción y habilidades específicas de la competencia digital en seguridad y privacidad de la información*

| Eje | Descripción | Habilidades específicas |
|---|---|---|
| Protección de datos personales | Capacidad para resguardar la información personal frente a accesos no autorizados y usos indebidos en entornos digitales. | Crear contraseñas seguras, configurar opciones de privacidad en redes sociales, reconocer intentos de phishing. |

| | | |
|---|---|---|
| Gestión de la identidad digital | Administración consciente de la huella digital y de la presencia en línea. | Controlar la información que se comparte, reconocer la suplantación de identidad, gestionar permisos y configuraciones de acceso. |
| Reconocimiento y mitigación de amenazas | Identificación de riesgos digitales y adopción de medidas preventivas y de respuesta. | Detectar malware, mantener sistemas actualizados, responder adecuadamente ante incidentes de seguridad. |

*Nota.* La tabla presenta los ejes que conforman la competencia digital en seguridad y privacidad de la información, junto con su descripción conceptual y las habilidades específicas asociadas a cada uno. Estos ejes orientan el diseño de los instrumentos de evaluación y la estructuración de las actividades pedagógicas del EVA Omniverso Digital, permitiendo analizar el desarrollo de prácticas seguras, responsables y éticas en el uso de las tecnologías digitales por parte de los estudiantes. Elaboración propia (2026).

### *Relación entre Competencia Digital en Seguridad y Privacidad con Ciberseguridad*

La *ciberseguridad* se entiende como un campo disciplinar de carácter técnico que abarca el conjunto de prácticas, tecnologías, normas y estrategias orientadas a la protección de sistemas, redes y datos frente a accesos no autorizados, ataques informáticos y amenazas digitales.

En el contexto educativo, la Competencia Digital en Seguridad y Privacidad de la Información representa la traducción pedagógica y formativa de los principios de la ciberseguridad, enfocada en el desarrollo de capacidades prácticas y éticas en los estudiantes. En este sentido:

- Ciberseguridad (enfoque técnico): se centra en sistemas, protocolos, infraestructuras y mecanismos tecnológicos de protección.

- Competencia digital en seguridad y privacidad (enfoque educativo): promueve en los estudiantes la capacidad de aplicar dichos principios técnicos en su vida digital cotidiana, tomando decisiones informadas, responsables y éticas.

En consecuencia, no se trata de dos competencias independientes, sino de una relación de complementariedad, donde la competencia digital en seguridad y privacidad constituye la expresión educativa, contextualizada y humanizada de la ciberseguridad, orientada a la formación de ciudadanos digitales responsables.

***Fundamentación en Marcos Normativos Internacionales y Nacionales***

Desde el marco normativo colombiano, el MEN, (2022) establece que, en los grados décimo y undécimo, los estudiantes deben desarrollar la capacidad de:

Actuar críticamente frente a las implicaciones éticas y sociales del uso de la tecnología, incluyendo la construcción de protocolos de seguridad y el uso ético de la tecnología para evitar riesgos personales y proteger la información.

Esta orientación normativa reconoce que la formación en tecnología debe trascender el aprendizaje instrumental, incorporando dimensiones *éticas, críticas y de autocuidado digital,* aspectos directamente relacionados con la competencia digital en seguridad y privacidad de la información.

De manera complementaria, los Estándares ISTE para Estudiantes (Crompton y Burke, 2024) reconocen la Ciudadanía Digital como una competencia clave que implica:

- Gestionar la huella digital.
- Proteger el bienestar en línea.
- Salvaguardar la privacidad.

- Fomentar interacciones seguras, responsables e inclusivas en entornos digitales.

Ambos marcos coinciden en que la competencia en seguridad digital trasciende el ámbito técnico, integrando dimensiones éticas, sociales y prácticas, lo cual respalda el enfoque adoptado en esta investigación.

***Síntesis: Competencia Integral***

Por tanto, en esta investigación, la *Competencia Digital en Seguridad y Privacidad de la Información* se concibe como un *constructo educativo integral*, de carácter ético, práctico y contextualizado, que articula distintas dimensiones del aprendizaje digital. Esta competencia comprende:

- **Saber técnico**, asociado a la comprensión de conceptos básicos de ciberseguridad (por ejemplo, virus informáticos, phishing y riesgos digitales).
- **Saber hacer**, relacionado con la aplicación de acciones concretas de protección, como la creación de contraseñas seguras, la configuración de opciones de privacidad y la identificación de situaciones de riesgo en entornos digitales.
- **Saber ser y pensar críticamente**, expresado en la reflexión ética, la autonomía en la toma de decisiones y la conciencia sobre las implicaciones del uso de la tecnología.
- **Saber convivir**, vinculado al respeto por la privacidad propia y ajena, la responsabilidad social y el acompañamiento a otros en prácticas digitales seguras.

Desde el punto de vista metodológico, esta competencia integral no se evalúa en su totalidad mediante un único instrumento. La medición cuantitativa del aprendizaje digital se realizó exclusivamente sobre los ítems correspondientes a la dimensión de seguridad y

privacidad, a través de la ECDSPI, la cual constituye una adaptación parcial de la *Escala de Competencias Digitales (*en adelante ECD) propuesta por Schwarz et al. (2024).

**Desagregación Conceptual: Competencia Digital en Seguridad y Privacidad**

Con el fin de precisar el alcance de la competencia digital en seguridad y privacidad de la información, en esta investigación se adopta una estructura de análisis organizada jerárquicamente, que facilita su comprensión desde una perspectiva educativa. Esta desagregación se fundamenta en la ECD propuesta por Schwarz et al. (2024), de la cual se adapta el dominio correspondiente a seguridad y privacidad de la información, dando lugar a la ECDSPI.

Es importante precisar que la ECD de Schwarz et al. (2024) se fundamenta en el Marco Europeo de Competencia Digital para la Ciudadanía (DigComp 2.1), desarrollado por Carretero et al., (2017), No obstante, en esta investigación dicho marco no se emplea de manera directa, sino que se asume mediado metodológicamente a través del instrumento validado por los autores, garantizando coherencia teórica y rigor metodológico.

Desde esta base, la competencia se analiza mediante una estructura jerárquica de tres niveles:

- La competencia como macrodimensión,
- Los ejes o dimensiones que la conforman, y
- El componente ético-actitudinal que orienta su aplicación en los entornos digitales escolares.

***Nivel 1. Competencia (macrodimensión)***

La competencia digital en seguridad y privacidad de la información se entiende como la capacidad del estudiante para proteger su información personal, gestionar de manera responsable

su identidad digital y actuar de forma segura, ética y autónoma frente a los riesgos presentes en los entornos digitales.

***Nivel 2. Ejes o dimensiones de la competencia***

Las habilidades asociadas a cada eje se derivan de los ítems operativos de la ECDSPI (ítems 1–12) y se presentan como una operacionalización pedagógica que permite hacer observable y evaluable la competencia en estudiantes de educación media. Estas habilidades no constituyen una taxonomía exhaustiva, sino un conjunto de desempeños representativos alineados con el dominio de seguridad y privacidad del instrumento adaptado.

**Eje 1. Protección de datos personales**

Este eje se refiere a la capacidad de reconocer qué información es sensible y de aplicar medidas preventivas para evitar su acceso no autorizado en entornos digitales.

Habilidades asociadas:

H1.1. Crear y gestionar contraseñas seguras y complejas.

H1.2. Identificar y evitar estafas en línea, como el phishing y la suplantación de identidad.

H1.3. Configurar adecuadamente las opciones de privacidad en plataformas digitales.

H1.4. Realizar copias de seguridad preventivas de la información.

H1.5. Distinguir sitios web seguros de aquellos que representan un riesgo.

**Eje 2. Gestión de la identidad digital**

Este eje aborda la administración consciente de la huella digital y la presencia en línea, considerando las implicaciones sociales, éticas y personales del intercambio de información en espacios virtuales.

Habilidades asociadas:

H2.1. Controlar qué información personal se comparte en la web.

H2.2. Administrar múltiples cuentas digitales de forma segura.

H2.3. Reconocer intentos de suplantación de identidad, como perfiles falsos.

H2.4. Evaluar los permisos solicitados por aplicaciones y sitios web.

H2.5. Comprender y gestionar la huella digital personal.

**Eje 3. Reconocimiento y mitigación de amenazas digitales**

Este eje se centra en la identificación de riesgos y amenazas digitales, así como en la aplicación de medidas preventivas y correctivas para reducir su impacto.

Habilidades asociadas:

H3.1. Reconocer distintos tipos de amenazas digitales, como malware, ransomware y virus.

H3.2. Aplicar medidas básicas de seguridad en dispositivos digitales, como contraseñas y antivirus.

H3.3. Mantener sistemas operativos y aplicaciones actualizados.

H3.4. Identificar situaciones en las que la identidad digital ha sido comprometida.

H3.5. Implementar acciones de respuesta ante incidentes de seguridad digital.

***Nivel 3. Actitudes y valores (componente ético-social)***

Además de los conocimientos y habilidades técnicas, la competencia digital en seguridad y privacidad de la información integra un componente ético-social fundamental, que se manifiesta en las siguientes actitudes y valores:

Ética digital, entendida como la comprensión de las implicaciones morales de las acciones realizadas en entornos digitales.

Responsabilidad social, orientada a la protección de los datos propios y al respeto por la privacidad de los demás.

Autonomía, que implica la capacidad de tomar decisiones informadas, críticas y conscientes frente a los riesgos digitales.

Ciudadanía digital, expresada en la participación segura, responsable y respetuosa dentro de las comunidades virtuales.

**Tabla 2**

*Correspondencia entre los componentes de la competencia digital en seguridad y privacidad de la información y los instrumentos de medición*

| Componente | Instrumento | Tipo de dato |
|---|---|---|
| **Conocimientos técnicos** | ECDSPI, ítems 1–12 (adaptada de la ECD de Schwarz et al., 2024) | Cuantitativo |
| **Habilidades prácticas** | ECDSPI y EVA *Omniverso Digital* (Desafíos de Salvaguardia) | Cuantitativo y cualitativo |
| **Reflexión ética** | Encuesta abierta de ciberseguridad y análisis de producciones mediante nubes de palabras | Cualitativo |
| **Autonomía y conciencia** | Encuesta abierta y análisis de casos representativos del EVA | Cualitativo |

*Nota*. La tabla presenta el mapeo entre los componentes que conforman la competencia digital en seguridad y privacidad de la información y los instrumentos utilizados para su medición en la investigación. Esta correspondencia permite articular datos cuantitativos y cualitativos, favoreciendo un análisis integral del desarrollo de la competencia desde los componentes cognitivo, procedimental y actitudinal (saber, saber hacer y saber ser). Elaboración propia. (2026)

**Conectivismo**

El conectivismo, teoría propuesta por Siemens (2005) y Downes (2007), plantea que el aprendizaje se lleva a cabo en redes de conocimiento, haciendo hincapié en la conexión entre nodos de información y en la colaboración en entornos digitales. Este enfoque es especialmente relevante en la educación actual, donde el acceso a la información y el aprendizaje autónomo son fundamentales. En el contexto de este estudio, el conectivismo ofrece una base teórica para el desarrollo de competencias digitales de seguridad, promoviendo una mayor responsabilidad y conciencia en la gestión de la privacidad y seguridad en línea.

Como analizan Altamirano et al. (2010), en el conectivismo como una teoría educativa emergente, adaptada a los entornos digitales, el aprendizaje ocurre a través de redes de conocimiento. Los autores exploran cómo el conectivismo rompe con las teorías tradicionales del aprendizaje, permitiendo una mayor flexibilidad y colaboración en el acceso a la información. Su investigación aborda específicamente el impacto de esta teoría en la educación media y superior, donde las herramientas TIC juegan un papel central en la formación de competencias.

Este estudio emplea una metodología cualitativa, basada en la revisión de literatura académica sobre teorías educativas y en el análisis de casos de implementación del conectivismo en instituciones educativas de América Latina. Esta investigación destaca cómo los estudiantes pueden aprender de manera autónoma, colaborando en redes de conocimiento, lo que es esencial para desarrollar competencias en seguridad digital dentro de un marco conectivista.

Gutiérrez (2012) resalta elementos aplicables al EVA, como el diseño de ecologías de aprendizaje mediante herramientas digitales (blogs, wikis y redes sociales) para fomentar la colaboración y la autonomía estudiantil. Propone un aprendizaje en red, donde los estudiantes interactúan con nodos de conocimiento en contextos prácticos y dinámicos, alineándose con un

enfoque basado en contextos hipotético-reales. Además, destaca la importancia de la flexibilidad y personalización del aprendizaje, permitiendo que los estudian tes definan sus objetivos y utilicen tecnologías como la Web 2.0 para desarrollar competencias digitales esenciales en seguridad y privacidad.

Tambien Alvarez et al. (2022) subrayan que el conectivismo surge como un paradigma educativo fundamental en la era postpandemia, se adapta a la interconexión y colaboración digital, lo cual fomenta el aprendizaje autónomo en entornos educativos virtuales.

Esta teoría es fundamental en el contexto de la educación digital, donde los estudiantes deben adquirir competencias para gestionar y evaluar la información de manera crítica y autónoma. En el marco de esta investigación, el conectivismo ofrece una base conceptual sólida para diseñar una EVA que fomente la colaboración en redes y el aprendizaje seguro en entornos digitales.

**Entorno Virtual de Aprendizaje EVA**

Un EVA es una plataforma digital estructurada para facilitar procesos formativos mediados por tecnologías de la información y la comunicación. Según Muñoz y Mora (2021), los EVA permiten diseñar experiencias de aprendizaje flexibles, personalizadas y centradas en el estudiante. Desde la perspectiva conectivista, los EVA se convierten en nodos dinámicos de interacción, donde los estudiantes construyen conocimiento mediante la colaboración, la navegación en red y la reflexión crítica. En esta investigación, el EVA se concibe como una herramienta clave para fomentar la competencia digital en seguridad y privacidad, integrando elementos de gamificación, actividades asincrónicas y evaluaciones formativas que promuevan la apropiación significativa del conocimiento.

Los EVA se han consolidado como una herramienta fundamental en la educación contemporánea, facilitan procesos de enseñanza-aprendizaje innovadores y adaptados a las necesidades del siglo XXI. Cedeño y Murillo (2019) destacan que los EVA no solo permiten el acceso a recursos digitales, sino que también promueven la interacción dinámica entre estudiantes y docentes, lo cual favorece el aprendizaje colaborativo y autónomo. Estos entornos se configuran como espacios flexibles que potencian la innovación pedagógica, facilitando la adaptación de contenidos y actividades a los diferentes estilos de aprendizaje.

Dentro del marco teórico del conectivismo, Torres y Barnabé (2020) plantean que el aprendizaje se concibe como la creación y navegación a través de redes de información y conocimiento, donde el papel del docente es guiar y facilitar la conexión entre nodos de aprendizaje. Este paradigma se adapta especialmente bien a los EVA, ya que promueven la construcción colectiva del conocimiento mediante redes sociales y ecologías del aprendizaje digitales.

Un EVA es una estructura que organiza de manera progresiva el proceso de enseñanza y aprendizaje. Zabala y Arnau (2007) proponen una organización progresiva del aprendizaje que puede adaptarse al diseño instruccional de un EVA, permitiendo que los estudiantes avancen en el desarrollo de competencias digitales mediante momentos formativos articulados, especialmente en temas de seguridad y privacidad. Ellos sostienen que este enfoque permite una mejor planificación y ejecución de actividades educativas, facilitando el desarrollo de competencias. En el contexto de la seguridad digital, los EVA deben diseñarse para guiar a los estudiantes a través de situaciones hipotéticas en las que puedan aplicar conocimientos sobre seguridad y privacidad en línea.

Galbin (2021), desde un estudio desarrollado en Rumania, plantea que el fortalecimiento de la competencia digital constituye un eje esencial de la educación remota y virtual, enfatizando la necesidad de metodologías inclusivas que promuevan la equidad digital.

Por su parte, Fernández y Jiménez (2023) señalan que los entornos de aprendizaje que siguen un enfoque conectivista fomentan la autonomía y la colaboración entre los estudiantes. Estas características pueden ser incorporadas en el diseño de un EVA, facilitando la apropiación significativa de competencias digitales críticas como la gestión de la privacidad.

Basurto et al. (2021) destacan que las estrategias de enseñanza basadas en plataformas digitales pueden fomentar la construcción autónoma del conocimiento. Esto respalda el uso del EVA como un entorno ideal para que los estudiantes adquieran competencias digitales relacionadas con la seguridad.

En particular, Cagüeño y Cifuentes (2022) subrayan la importancia de estructurar entornos de aprendizaje con una secuencia lógica adaptada al contexto rural. En un EVA, estos principios pueden traducirse en módulos formativos digitales que respeten los ritmos de aprendizaje y las condiciones tecnológicas del estudiantado.

Además, Marrón y Martínez (2023) destacan que el desarrollo de competencias digitales puede fortalecerse mediante estrategias formativas estructuradas en entornos virtuales. Estos hallazgos apoyan el diseño del EVA como espacios que promueven el aprendizaje seguro y ético de la tecnología en estudiantes de media vocacional.

Finalmente, Cueva et al. (2019) señalan que el conectivismo y las TIC representan un paradigma que transforma radicalmente el proceso de enseñanza-aprendizaje. La integración de las tecnologías digitales, en especial a través del EVA, permite no solo la transmisión de

conocimientos, sino también el desarrollo de competencias digitales, pensamiento crítico y habilidades para el aprendizaje permanente.

**Tecnología, Informática y Sociedad**

La relación entre la tecnología, la informática y la sociedad constituye un eje esencial para comprender las transformaciones culturales, comunicativas y educativas de la era digital. La tecnología, entendida no solo como instrumento, sino como sistema sociotécnico, ha modificado las formas de pensar, aprender y relacionarse, generando nuevas prácticas de socialización y producción de conocimiento. Como plantea Tejada (2000), la tecnología no solo transforma los procesos educativos, sino también los modos de interacción social y los entornos de aprendizaje, demandando una reflexión constante sobre su uso ético y pedagógico.

En la denominada sociedad red, la digitalización ha configurado una estructura social basada en la conectividad, en la cual el acceso a la información y la capacidad de gestionarla constituyen factores de inclusión o exclusión (Castells, 2006, pp. 21–78). Desde esta perspectiva, las TIC no deben ser comprendidas únicamente como mediadores técnicos del aprendizaje, sino como espacios de construcción identitaria y ciudadana. El desarrollo de la competencia digital, por tanto, implica preparar a los estudiantes para desenvolverse de manera crítica, segura y responsable en entornos digitales cada vez más complejos.

Por su parte, Van Dijk (2020) señala que la desigualdad digital no se limita al acceso a los dispositivos, sino que incluye las diferencias en habilidades, uso y beneficios derivados de la tecnología. Este autor enfatiza la importancia de abordar la brecha digital como un fenómeno multidimensional que repercute en las oportunidades de aprendizaje, en especial en contextos escolares (pp. 1–22, 23–45, 127–155). En esta misma línea, Selwyn, (2021) advierte que la educación digital no debe enfocarse únicamente en el dominio técnico, sino en la comprensión

de las implicaciones sociales, políticas y éticas del uso de la tecnología (pp. 1–23, 191–210). Ello implica reconocer que los entornos digitales también pueden reproducir desigualdades y riesgos, como la desinformación, la pérdida de privacidad o la exposición a contenidos dañinos.

Finalmente, organismos internacionales como la UNESCO (2019, 2023) subrayan que la integración de la tecnología en la educación debe promover una ciudadanía digital activa y ética. En sus marcos de competencia digital, la UNESCO resalta la importancia de la seguridad, la privacidad y la protección de datos personales como dimensiones centrales de la alfabetización digital. Estas orientaciones refuerzan la pertinencia de iniciativas como el *EVA Omniverso Digital*, concebido para fortalecer la competencia digital del estudiantado mediante experiencias conectivistas, colaborativas y seguras, orientadas al desarrollo de una cultura tecnológica responsable y crítica.

La interacción entre la tecnología, la informática y la sociedad ha transformado la forma en que las personas aprenden e interactúan, generando tanto beneficios como riesgos. En el ámbito educativo, el uso de tecnologías requiere un enfoque crítico que permita a los estudiantes utilizar estos recursos de manera ética y segura. Esta sección examina cómo las TIC influyen en las competencias digitales y la importancia de formar a los estudiantes en prácticas seguras en línea.

**Ciudadano digital**

En la sociedad digital contemporánea, el ciudadano no solo accede a la información, sino que participa activamente en su producción y circulación, asumiendo un papel protagónico en la construcción de la cultura digital. Desde esta perspectiva, el ciudadano digital se concibe como una persona capaz de actuar con pensamiento crítico, autonomía y responsabilidad en los entornos tecnológicos, ejerciendo sus derechos y deberes en el ciberespacio. La UNESCO (2023)

plantea que la educación para la ciudadanía digital debe promover la participación ética, segura y solidaria, garantizando que los estudiantes comprendan las implicaciones sociales y morales del uso de las tecnologías de la información y la comunicación.

Una de las principales amenazas a la práctica de la ciudadanía digital es la *ingeniería social*, entendida como el conjunto de estrategias psicológicas y comunicativas utilizadas para manipular a las personas con el fin de obtener datos o inducir acciones que comprometen su seguridad. De acuerdo con la Agencia Europea de Ciberseguridad (European Union Agency for Cybersecurity (ENISA), 2025), más del 60 % de los incidentes informáticos se originan mediante tácticas de engaño como el *phishing* o la suplantación de identidad. En el contexto educativo, abordar este fenómeno implica formar en pensamiento crítico, verificación de información y autogestión de la seguridad digital, de modo que los estudiantes puedan reconocer y resistir los intentos de manipulación en línea.

El uso ético, seguro y responsable de internet constituye la base del comportamiento ciudadano en los entornos digitales. Los Estándares ISTE para Estudiantes (Crompton y Burke, 2024) señalan que un ciudadano digital reconoce sus responsabilidades y oportunidades de contribuir a las comunidades digitales de manera positiva. En este sentido, los estudiantes deben gestionar su identidad digital y comprender el impacto duradero de sus comportamientos en línea sobre sí mismos y los demás, tomando decisiones seguras, legales y éticas; demostrar interacciones empáticas e inclusivas y utilizar la tecnología de forma responsable para contribuir al bienestar colectivo; salvaguardar su bienestar siendo conscientes del tiempo y las actividades que realizan en línea; y proteger su privacidad digital y sus datos personales mientras navegan o utilizan dispositivos conectados. Estos principios orientan la formación de una ciudadanía digital

consciente, empática y crítica, centrada en la responsabilidad, la seguridad y la ética en la vida digital contemporánea.

La *seguridad digital*, la *gestión de la identidad* y la *mitigación de riesgos* son competencias interdependientes que refuerzan la autonomía del usuario en el entorno digital. El *Cybersecurity Framework 2.0* del (National Institute of Standards and Technology (NIST), 2024) propone que toda persona debe ser capaz de identificar, proteger, detectar, responder y recuperarse frente a incidentes de seguridad, aplicando principios básicos de prevención y resiliencia. En el ámbito escolar, ello implica enseñar a los estudiantes a configurar su privacidad, detectar amenazas, proteger sus dispositivos y actuar con prudencia ante solicitudes de información sospechosas. La gestión consciente de la identidad digital, por su parte, permite construir una reputación positiva y proteger la información personal frente a riesgos como la suplantación o el robo de datos.

Finalmente, la ciudadanía digital ética y responsable integra todas las dimensiones anteriores y representa el horizonte formativo del ciudadano contemporáneo. La UNESCO (2023) sostiene que la ciudadanía digital implica el desarrollo de actitudes y valores que articulan lo técnico, lo ético y lo social, promoviendo la comunicación responsable, la convivencia digital, el bienestar tecnológico y la participación cívica en entornos digitales.

**Competencias Digitales**

Las competencias digitales son habilidades fundamentales para interactuar de manera segura y responsable en entornos digitales. En esta investigación, se abordan cuatro áreas esenciales: información y alfabetización de datos, comunicación y colaboración, creación de contenidos digitales y seguridad. Cada una de estas subcategorías contribuye a la formación de

ciudadanos digitales responsables, con habilidades prácticas y éticas para gestionar su presencia en línea.

***Información y Alfabetización de Datos.***

La alfabetización de datos constituye un eje central dentro de las competencias digitales, pues permite comprender, evaluar y utilizar la información de manera crítica, ética y significativa en entornos digitales. Este concepto tiene una evolución histórica que parte de la alfabetización informacional (information literacy) promovida en la década de 1970 por Paul Zurkowski, quien la definió como la capacidad de reconocer cuándo se necesita información y de localizarla, evaluarla y usarla eficazmente. Posteriormente, con el auge de internet y las tecnologías de la información, este enfoque se amplió hacia la alfabetización digital y mediática, integrando dimensiones técnicas, comunicativas y sociales del uso de la información (Bawden, 2008; Area y Guarro, 2012).

En el contexto contemporáneo, la alfabetización de datos se concibe como la capacidad de interpretar, gestionar y comunicar información basada en datos de manera responsable. Según Calzada-Prado y Marzal (2013), implica no solo acceder a la información, sino también comprender su origen, fiabilidad, estructura y finalidad, fomentando la toma de decisiones fundamentadas en evidencia. Esta perspectiva promueve una ciudadanía crítica y consciente en el ecosistema digital, al tiempo que refuerza la seguridad y la privacidad en el manejo de datos personales.

De acuerdo con la UNESCO (2019), la competencia de alfabetización en información y datos forma parte de las habilidades clave para el siglo XXI, integrando los principios de búsqueda, evaluación, uso ético y comunicación responsable de la información. En el marco del

DigComp 2.2 (Vuorikari et al., 2022), esta competencia se clasifica como la primera área de la competencia digital, denominada *alfabetización en información y datos*, que abarca el tratamiento responsable de la información y el reconocimiento de los riesgos asociados a su uso inadecuado. En este sentido, promover la alfabetización de datos en el ámbito escolar no solo fortalece el pensamiento crítico, sino que también prepara a los estudiantes para desenvolverse de forma segura y ética en entornos digitales donde la información circula de manera masiva y constante.

***Comunicación y Colaboración.***

La competencia de comunicación y colaboración es esencial en la era digital, ya que permite a los estudiantes trabajar en equipo de manera efectiva, interactuar en entornos digitales y respetar la privacidad de los demás. Estas habilidades son fundamentales para la convivencia digital segura y el trabajo colaborativo en línea. Marrón y Martínez (2023) destacan la importancia de fomentar la colaboración y el aprendizaje autónomo en entornos digitales.

***Crear Contenidos Digitales.***

Crear contenido digital de manera ética y segura es fundamental para el desarrollo de competencias digitales. Esta habilidad permite a los estudiantes aprender a expresarse y a compartir información en línea, respetando la privacidad y los derechos de autor. Pertegal y Lorenzo (2019) sugieren que los docentes pueden utilizar herramientas como videoclips y aplicaciones interactivas para fomentar la creatividad y el pensamiento crítico de los estudiantes.

***Seguridad.***

La competencia en seguridad digital implica la protección de la privacidad y la información personal, así como la capacidad de gestionar de forma responsable la identidad en

línea y reconocer los posibles riesgos en entornos digitales. La UNESCO (2019) subraya la necesidad de educar a los estudiantes para que comprendan cómo administrar sus datos personales y cómo identificar y evitar situaciones de riesgo en Internet. Esta competencia se considera esencial para promover la autonomía, la responsabilidad y el comportamiento ético en el uso de la tecnología.

De acuerdo con Crompton y Burke (2024) en los Estándares ISTE para estudiantes preparan a los jóvenes para desenvolverse en un entorno tecnológico dinámico, fomentando el aprendizaje autodirigido y la participación ética en comunidades digitales. En la competencia de *Ciudadanía Digital*, los estudiantes aprenden a gestionar su huella digital mediante el desarrollo de una identidad en línea responsable y la toma de decisiones seguras; a promover interacciones inclusivas y empáticas que reflejen respeto y ética en los entornos virtuales; a proteger su bienestar mediante un uso equilibrado e intencional de la tecnología; y a salvaguardar su privacidad digital garantizando la seguridad de sus datos personales. Estos estándares contribuyen al fortalecimiento de competencias que permiten a los estudiantes participar de manera segura, ética y positiva a sus comunidades digitales.

Por su parte Muñoz y Mora (2021) destacan la relevancia de formar competencias en seguridad digital en el estudiantado, señalando que el EVA proporcionan herramientas esenciales para la protección de datos y la gestión ética de la identidad en línea. De manera complementaria, Marrón y Martínez (2023) subrayan la importancia de que los docentes desarrollen estas competencias para poder transferirlas a sus estudiantes, lo cual favorece prácticas responsables en la administración de la información personal y refuerza la ética en los contextos digitales.

En síntesis, la competencia en seguridad digital capacita a los estudiantes para identificar y mitigar riesgos en línea, proteger su información personal y gestionar su identidad digital de forma crítica y responsable. Esta competencia abarca acciones concretas, como el uso de contraseñas seguras, la configuración adecuada de la privacidad en redes sociales y el reconocimiento oportuno de amenazas digitales. Su desarrollo fortalece la autonomía y la conciencia ética del estudiante, preparándolo para interactuar en entornos digitales cada vez más complejos y desafiantes.

# Capítulo III. Metodología

El presente capítulo describe el proceso metodológico que orientó el desarrollo de la investigación, detallando las estrategias y procedimientos empleados para alcanzar los objetivos propuestos. Su propósito es exponer de manera clara la ruta seguida desde el diseño metodológico hasta la evaluación de los resultados, asegurando la coherencia y rigurosidad del estudio.

El marco metodológico constituye la estrategia que guía la obtención y el análisis de la información, definiendo los métodos, técnicas y criterios que sustentan el proceso investigativo (Hernández et al., 2014). En este sentido, el capítulo presenta el enfoque de la investigación, el diseño metodológico, el proceso investigativo, los instrumentos de recolección de información, así como los procedimientos empleados para el análisis y la evaluación de los resultados.

## Enfoque de la Investigación

La presente investigación se desarrolla bajo un *enfoque mixto*, con un *diseño dominante cualitativo*, en el cual los datos cuantitativos cumplen una *función de apoyo interpretativo* (Cueva et al., 2023). Este enfoque se adopta considerando que el interés central del estudio se orienta a analizar la apropiación de la competencia digital en seguridad y privacidad de la información en estudiantes de educación media, a partir de la implementación de un EVA.

El *componente cualitativo* constituye el eje principal de la investigación, ya que permite interpretar las prácticas, percepciones y reflexiones de los estudiantes frente al uso seguro, ético y responsable de la tecnología, así como comprender los significados que atribuyen a la seguridad y la privacidad de la información en entornos digitales. Este análisis se apoya en la información obtenida mediante la encuesta abierta y en las evidencias generadas durante el desarrollo de las actividades pedagógicas del EVA.

De manera complementaria, se incorpora un *componente cuantitativo,* representado por la aplicación de la ECDSPI en modalidad de pretest y postest. Los datos obtenidos permiten identificar variaciones en la apropiación de la competencia antes y después de la intervención. En este sentido, la información cuantitativa se integra como un recurso que fortalece y respalda la interpretación cualitativa del fenómeno estudiado.

La articulación de ambos enfoques permite *presentar los resultados de la intervención del EVA*, integrando el análisis de las prácticas, percepciones y cambios observados en la apropiación de la competencia digital, en coherencia con los objetivos del estudio y con la naturaleza educativa de la competencia analizada.

**Diseño Metodológico**

El estudio se desarrolla bajo un diseño metodológico de carácter educativo, enmarcado en un enfoque mixto con un diseño dominante cualitativo, en el cual los datos cuantitativos cumplen una función de apoyo interpretativo, orientado a la evaluación de los resultados de una intervención pedagógica mediada por un EVA para el fortalecimiento de la competencia digital en seguridad y privacidad de la información en estudiantes de educación media.

En el *componente cualitativo,* que constituye el eje central del estudio, se adopta el enfoque de *Investigación-Acción Educativa (IAE)*, entendido como un proceso de reflexión sistemática sobre la práctica docente que busca transformar y mejorar de manera continua los entornos de aprendizaje. De acuerdo con Rodríguez (2005), la investigación-acción educativa se orienta al análisis y la resolución de problemáticas concretas de la práctica pedagógica, promoviendo una acción reflexiva y transformadora que contribuye al cambio educativo desde la experiencia docente. Este componente permite interpretar las prácticas, percepciones y

reflexiones de los estudiantes frente al uso seguro, ético y responsable de la tecnología durante la implementación del EVA.

De manera complementaria, dentro del componente cuantitativo, se incorpora un diseño cuasi-experimental de series temporales como estrategia metodológica de apoyo, apropiada para contextos educativos en los cuales los grupos ya están conformados y no es posible realizar una asignación aleatoria. Este diseño permite comparar los resultados obtenidos antes y después de la intervención pedagógica, con el fin de identificar variaciones en la apropiación de la competencia digital asociadas a la experiencia educativa implementada (DeCarlo, 2018; Hernández et al., 2014).

La articulación de ambos componentes metodológicos permite evaluar los resultados de la intervención pedagógica integrando el análisis cualitativo con los datos obtenidos a través del diseño cuasi-experimental de series temporales. De este modo, el estudio conjuga la reflexión crítica propia de la Investigación-Acción Educativa con la información cuantitativa de apoyo, fortaleciendo la interpretación de los resultados y aportando a la mejora de la práctica docente.

**Proceso Investigativo**

El proceso investigativo se desarrolló en **c***inco fases secuenciales y articuladas*, integrando los principios del *enfoque mixto con diseño dominante cualitativo* y los del modelo de *Investigación-Acción Educativa (IAE):*

En este proceso, los docentes-investigadores asumieron un *rol dual de facilitadores y observadores*, orientando las actividades del EVA *Omniverso Digital*, acompañando a los estudiantes en el desarrollo de los desafíos y registrando de manera sistemática las evidencias de aprendizaje y las transformaciones en las prácticas digitales. Este rol activo permitió mantener una *reflexión constante sobre la práctica pedagógica* y retroalimentar las decisiones

metodológicas a lo largo del estudio. El proceso investigativo contempló cinco fases, descritas a continuación:

***Fase 1. Diagnóstico contextual***

En la primera fase se realizó un *diagnóstico etnográfico*, orientado a comprender las dinámicas institucionales, socioculturales y tecnológicas de la Institución Educativa Distrital Rural San Cayetano. Este diagnóstico permitió identificar las prácticas digitales, el nivel de acceso a las TIC y las percepciones de los estudiantes en torno a la seguridad y la privacidad de la información. Los resultados de esta fase sirvieron de base para el diseño de la intervención pedagógica y la adecuación de los instrumentos de observación.

***Fase 2. Adaptación y validación de instrumentos***

La segunda fase correspondió a la *adaptación y validación de los instrumentos de observación*, con el fin de garantizar su coherencia y pertinencia en el contexto educativo. En este estudio se utilizaron dos instrumentos principales:

- *(ECDSPI)*, adaptación de la (ECD) de Schwarz et al. (2024), centrada exclusivamente en las dimensiones de seguridad digital e identidad en línea.
- *Encuesta Abierta de Ciberseguridad,* diseñada para explorar percepciones, reflexiones y prácticas relacionadas con el uso ético, seguro y responsable de internet, aplicada como instrumento cualitativo complementario para apoyar la interpretación de los resultados obtenidos con la ECDSPI.

La descripción detallada del proceso de adaptación, validación y aplicación de ambos instrumentos se presenta en el apartado Instrumentos de Observación.

***Fase 3. Diseño e implementación del EVA***

En la tercera fase se diseñó e implementó el *EVA Omniverso Digital*, alojado en la plataforma Moodle de la Universidad Distrital Francisco José de Caldas. Este entorno fue concebido como el *núcleo de la intervención pedagógica*, fundamentado en los principios del conectivismo y la gamificación, con el objetivo de fortalecer la competencia digital en seguridad y privacidad de la información mediante actividades contextualizadas y situaciones hipotético-reales.

***Fase 4. Aplicación de instrumentos y recolección de evidencias***

La cuarta fase comprendió la *aplicación de los instrumentos de observación en dos momentos: pretest y postest.* En el pretest se aplicaron la ECDSPI y la Encuesta Abierta de Ciberseguridad para establecer la línea base de las competencias y percepciones de los estudiantes. Durante la implementación del EVA se recolectaron diversos *productos digitales elaborados por los participantes*, tales como cartas, foros, organizadores gráficos, recursos multimedia y reflexiones personales. Posteriormente, en el postest se aplicaron nuevamente ambos instrumentos, lo que permitió identificar variaciones y cambios asociados a la intervención pedagógica.

**Fase 5. Análisis e interpretación de resultados**

Finalmente, la quinta fase consistió en el *análisis e interpretación de los resultados*, priorizando el **c**omponente cualitativo del estudio, en coherencia con el **e**nfoque mixto con diseño dominante cualitativo adoptado en la investigación. Este análisis se centró en la interpretación de las percepciones, reflexiones y evidencias producidas por los estudiantes durante la implementación del EVA, a partir de la información obtenida mediante la encuesta abierta y los productos digitales elaborados.

De manera complementaria, se integraron los datos cuantitativos provenientes de la ECDSPI, los cuales cumplieron una función de apoyo interpretativo, permitiendo identificar variaciones en la apropiación de la competencia digital antes y después de la intervención pedagógica.

La integración de ambos tipos de datos se realizó mediante un proceso de triangulación metodológica, que permitió evaluar los resultados de la intervención, identificando avances en la apropiación de la competencia digital, en el uso del lenguaje técnico asociado a la ciberseguridad.

## Instrumentos de Observación

En esta investigación se emplearon *tres instrumentos de observación,* articulados de manera coherente con el enfoque mixto con diseño dominante cualitativo adoptado en el estudio: la *ECDSPI, la Encuesta Abierta de Ciberseguridad* y el *EVA Omniverso Digital*. La integración de estos instrumentos permitió recolectar y triangular información cualitativa y cuantitativa, priorizando la interpretación de las prácticas, percepciones y producciones de los estudiantes, mientras que los datos cuantitativos cumplieron una función de apoyo interpretativo para la evaluación de los resultados de la intervención pedagógica.

### *Escala de Competencia Digital en Seguridad y Privacidad de la Información (ECDSPI)*

La ECDSPI corresponde a una *adaptación de la ECD* desarrollada por Schwarz et al. (2024), en la cual se seleccionaron y ajustaron exclusivamente los ítems relacionados con la *seguridad digital y la identidad en línea*, conformando una escala unidimensional aplicada en este estudio. Su propósito fue identificar variaciones en la apropiación de la competencia digital en seguridad y privacidad de la información antes y después de la implementación del EVA.

El instrumento permitió reconocer niveles de desempeño en aspectos asociados a la protección de datos personales, la gestión ética de la identidad digital y la adopción de prácticas seguras en entornos digitales, aportando información cuantitativa que respaldó la interpretación cualitativa de los resultados.

- **Adaptación.** La escala original fue concebida como un instrumento de 12 ítems para medir la competencia digital en sentido amplio. En la presente investigación, se adaptaron y ampliaron los ítems vinculados a seguridad y privacidad, ajustando la redacción y los niveles de respuesta al contexto educativo local y a la población participante.
- **Alcance.** Este instrumento no evalúa la competencia digital general, sino de manera específica la dimensión de seguridad y privacidad de la información, por lo cual los resultados deben interpretarse dentro de este marco delimitado.
- **Instrucciones.** Los estudiantes respondieron a un conjunto de afirmaciones relacionadas con competencias digitales en seguridad y privacidad, seleccionando el nivel de logro que mejor describía su desempeño percibido.

***Encuesta Abierta de Ciberseguridad***

La *Encuesta Abierta de Ciberseguridad* se diseñó como un *instrumento cualitativo complementario,* orientado a explorar las percepciones, reflexiones y prácticas de los estudiantes en relación con el uso ético, seguro y responsable de internet. Su función principal fue profundizar e interpretar los resultados obtenidos a través de la ECDSPI, aportando una mirada contextual y reflexiva sobre la apropiación de la competencia digital.

Las preguntas, formuladas en formato de respuesta abierta, se aplicaron en dos momentos (pretest y postest). Las respuestas obtenidas fueron analizadas mediante *categorías emergentes*,

lo que permitió interpretar las percepciones, reflexiones y prácticas de los estudiantes en relación con el uso ético, seguro y responsable de internet, así como identificar cambios en la apropiación de la competencia digital a lo largo de la intervención.

La articulación entre la ECDSPI y la Encuesta Abierta de Ciberseguridad se presenta de manera detallada en el Capítulo IV. Diseño e Implementación del EVA y de los Instrumentos de Evaluación, específicamente en el apartado Diseño y Validación de los Instrumentos de Evaluación, donde se incluye la Tabla 3. Articulación entre la ECDSPI y la Encuesta Abierta de Ciberseguridad, que evidencia la correspondencia entre los ejes de la competencia y los componentes cualitativos y cuantitativos del estudio.

**Entorno Virtual de Aprendizaje (EVA) – Omniverso Digital**

El Omniverso Digital fue concebido como un *EVA de* carácter transmedia y gamificado, diseñado tanto como *estrategia de intervención pedagógica* como *fuente de evidencias cualitativas* para el análisis del estudio. Su propósito fue fortalecer la competencia digital en seguridad y privacidad de la información en estudiantes de educación media rural.

La narrativa del EVA se articuló en torno a *CyberShield*, un guardián digital que acompañó a los estudiantes —denominados *Pioneros*— en su proceso de formación hacia una ciudadanía digital crítica, ética y responsable. A través de retos cooperativos y competitivos, los participantes enfrentaron situaciones simuladas relacionadas con riesgos digitales y protección de datos, favoreciendo la motivación y la apropiación progresiva de la competencia en ciberseguridad, en coherencia con los lineamientos del MEN (2022).

Implementado en la plataforma Moodle de la Universidad Distrital Francisco José de Caldas, el EVA integró recursos interactivos, actividades colaborativas y productos digitales que

posibilitaron el aprendizaje autónomo y la reflexión ética sobre el uso responsable de la tecnología.

La estructura del EVA se visualizó a partir de un **mapa de navegación**, que orientó la ruta de los *Pioneros* dentro del entorno virtual. La experiencia inició con una bienvenida narrativa y condujo a los apartados principales: *Documentos de Autor, Mapa Conceptual, Mapa de Navegación, Planeador y Perfil Docente*. El punto de partida pedagógico fue *Start Now*, desde donde los estudiantes accedieron a los *Desafíos de Salvaguardia.*

Los *Desafíos de Salvaguardia* se estructuraron en tres momentos pedagógicos progresivos:

- **Exploración y compromiso**, que incluyó la firma de la *Alianza de Responsabilidad* y la actividad *Conocimiento Seguro*, centrada en el análisis crítico de la desinformación (fake news) y la ingeniería social.
- **Colaboración y aplicación**, con actividades como los *Consejos de Seguridad* y el desafío *Riesgos Tecnológicos*, un juego tipo carrera de obstáculos orientado a la identificación de amenazas digitales.
- **Evaluación de la competencia digital**, enfocada en la elaboración de un *Protocolo de Seguridad* (producto multimedia) y una *Reflexión Personal*, expresada en una carta dirigida a estudiantes de grados inferiores.

El diseño del Omniverso Digital integró principios del *conectivismo* y la *gamificación educativa*, favoreciendo el aprendizaje en red, la interacción constante y la construcción colaborativa del conocimiento. El sistema de recompensas simbólicas, la narrativa inmersiva y la autonomía en la toma de decisiones pedagógicas contribuyeron a consolidar una experiencia significativa centrada en el desarrollo de la competencia digital en ciberseguridad.

El diseño y la implementación del EVA se fundamentaron en una adaptación del modelo *ADDIE* (Analysis, Design, Development, Implementation, Evaluation), ampliamente reconocido en el ámbito del diseño instruccional para la planificación, desarrollo y evaluación de ambientes de aprendizaje mediados por tecnologías digitales. La adopción de este modelo permitió estructurar el proceso de diseño de forma sistemática, flexible y contextualizada, atendiendo a las particularidades del contexto educativo rural y a los objetivos formativos de la investigación. Tanto los instrumentos como el entorno de aprendizaje fueron revisados y ajustados para garantizar su coherencia con los objetivos del estudio y la población participante.

**Recolección de Información**

La recolección de la información se realizó siguiendo el principio de *complementariedad del enfoque mixto con diseño dominante cualitativo,* integrando instrumentos *cualitativos, cuantitativos y observacionales* para comprender y evaluar los resultados de la intervención pedagógica. Cada instrumento fue aplicado en momentos estratégicos del proceso investigativo, garantizando la coherencia entre los objetivos, los métodos y las técnicas empleadas, así como la función de apoyo interpretativo de los datos cuantitativos.

En primer lugar, se aplicó la *Encuesta Abierta de Ciberseguridad,* en dos momentos (pretest y postest), con el propósito de explorar las *percepciones, reflexiones y prácticas* de los estudiantes frente al uso ético, seguro y responsable de internet. Este instrumento cualitativo permitió interpretar los significados atribuidos por los participantes a la seguridad digital y contextualizar los cambios observados a lo largo de la implementación del EVA.

De manera complementaria, se administró la *ECDSPI*, adaptación de la Escala de Competencia Digital de Schwarz et al. (2024), también en modalidad de pretest y postest. Este instrumento cuantitativo tuvo como finalidad identificar variaciones en los niveles de

apropiación de la competencia digital relacionadas con la protección de datos personales y la gestión de la identidad en línea. La escala se estructuró como una herramienta unidimensional centrada exclusivamente en la dimensión de seguridad y privacidad digital, y sus resultados fueron interpretados dentro de este marco delimitado, cumpliendo una función de *apoyo interpretativo* al análisis cualitativo.

Adicionalmente, se recolectaron *registros de participación y productos digitales* generados por los estudiantes en la plataforma Moodle, espacio principal del EVA *Omniverso Digital*. En este entorno se alojaron los recursos, se desarrollaron los *Desafíos de Salvaguardia* y se recopilaron las evidencias de aprendizaje. En algunos casos, debido a limitaciones de conectividad, las entregas se realizaron mediante Classroom, garantizando la continuidad del proceso formativo y la inclusión de todos los participantes.

Asimismo, se emplearon *rúbricas de evaluación* para valorar los productos elaborados por los estudiantes —cartas, foros, organizadores gráficos, juegos, protocolos multimedia y reflexiones individuales—, con el fin de asegurar criterios de coherencia, equidad y transparencia en la valoración del desempeño y facilitar el análisis cualitativo de los aprendizajes evidenciados.

Finalmente, se utilizaron herramientas tecnológicas de apoyo para la organización y el análisis preliminar de la información cualitativa. Mediante el uso de inteligencia artificial (ChatGPT-5 y TurboScribe) se realizó el conteo de palabras frecuentes en los textos producidos por los estudiantes, incluyendo transcripciones de productos multimedia. Posteriormente, los resultados fueron visualizados a través de nubes de palabras elaboradas con WordArt.com, lo que permitió evidenciar la apropiación progresiva del vocabulario técnico asociado a la ciberseguridad.

En conjunto, estos instrumentos y procedimientos permitieron recolectar información pertinente, sistemática y coherente con el enfoque metodológico adoptado, garantizando insumos suficientes para la evaluación e interpretación integral de los resultados de la intervención del EVA Omniverso Digital en el desarrollo de la competencia digital en seguridad y privacidad de la información.

**Procesamiento y Análisis de la Información**

El procesamiento y análisis de la información se desarrollaron en coherencia con el *enfoque mixto con diseño dominante cualitativo* adoptado en el estudio, integrando procedimientos cualitativos y cuantitativos que permitieron **i**nterpretar y evaluar los resultados de la intervención pedagógica mediante un proceso de triangulación metodológica.

**Análisis Cualitativo**

Es el *eje central del proceso analítico*. Las respuestas obtenidas en la **E**ncuesta Abierta de Ciberseguridad, junto con los productos digitales elaborados por los estudiantes durante la implementación del EVA —cartas, foros, protocolos de seguridad, organizadores gráficos y reflexiones—, fueron analizados mediante análisis de contenido de carácter inductivo, a partir de la identificación de categorías emergentes.

Este procedimiento permitió interpretar los significados construidos por los estudiantes en relación con el uso del lenguaje técnico, la adopción de prácticas digitales seguras y la reflexión ética sobre la ciudadanía digital, así como identificar transformaciones en sus percepciones y comportamientos a lo largo del proceso formativo.

Como apoyo al análisis cualitativo, se utilizaron *herramientas tecnológicas* como ChatGPT-5 y TurboScribe para el procesamiento textual y la organización de la información, y WordArt.com para la elaboración de nubes de palabras a partir de los textos producidos en las

actividades del EVA. Estas representaciones visuales facilitaron la identificación de patrones léxicos y evidenciaron la apropiación progresiva del vocabulario técnico asociado a la ciberseguridad.

**Análisis Cualitativo**

De manera complementaria, los datos provenientes de la *ECDSPI* fueron tabulados y procesados mediante con la herramienta informática *Microsoft Excel*, calculando porcentajes de avance, niveles de competencia y diferencias entre los resultados del pretest y el postest.

Este análisis permitió identificar variaciones en la apropiación de la competencia digital en las dimensiones de seguridad digital, gestión de la identidad y reconocimiento de riesgos, cumpliendo una función de apoyo interpretativo al análisis cualitativo, sin pretender establecer relaciones causales ni generalizar los resultados.

**Triangulación de Resultados**

La triangulación metodológica constituyó una fase fundamental del análisis, al permitir integrar y contrastar la información obtenida desde diferentes fuentes, instrumentos y perspectivas analíticas, fortaleciendo la validez interna del estudio y la coherencia interpretativa de los resultados.

Se desarrollaron tres niveles de triangulación:

**Triangulación de datos.**

Se contrastaron los resultados cuantitativos de la ECDSPI con los hallazgos cualitativos derivados de la Encuesta Abierta de Ciberseguridad y de los productos elaborados por los estudiantes en el EVA. Este cruce permitió identificar correspondencias entre los avances observados en la competencia digital y las transformaciones en las percepciones, prácticas y discursos de los estudiantes.

**Triangulación de instrumentos.**

La integración de la ECDSPI, la encuesta abierta, las rúbricas de evaluación y las evidencias del EVA permitió analizar el fenómeno educativo desde perspectivas complementarias: la autoevaluación, la reflexión cualitativa y la observación pedagógica. En este nivel se incorporó el análisis de *nubes de palabras elaboradas a partir de los textos producidos en las actividades del EVA*, lo que permitió visualizar la evolución del lenguaje técnico empleado por los estudiantes, evidenciando la apropiación progresiva de términos asociados a la ciberseguridad, en coherencia con las competencias establecidas por el MEN (2022).

**Triangulación interpretativa**

Se realizó una revisión conjunta de los datos cuantitativos, cualitativos y observacionales, considerando el rol de los docentes-investigadores como facilitadores y analistas del proceso formativo. Esta triangulación permitió interpretar los resultados de manera integral, contrastando los datos numéricos con las evidencias pedagógicas y las reflexiones surgidas durante el acompañamiento en el entorno virtual.

En conjunto, el proceso de triangulación permitió establecer una relación consistente entre la apropiación del vocabulario técnico, la consolidación de prácticas digitales seguras y el fortalecimiento de la reflexión crítica sobre la ciudadanía digital. De este modo, la triangulación no solo validó los resultados obtenidos, sino que también fortaleció el componente formativo y reflexivo de la *Investigación-Acción Educativa (IAE)*, reafirmando el valor del *Omniverso Digital* como estrategia pedagógica transformadora.

En síntesis, el capítulo metodológico presentó la ruta seguida para el desarrollo del estudio, fundamentada en un enfoque mixto con diseño dominante cualitativo, en el cual el diseño cuasi-experimental de series temporales se incorporó como estrategia de apoyo, articulado

con el modelo de Investigación-Acción Educativa. Esta integración permitió vincular la evaluación de la competencia digital con la reflexión pedagógica sobre la práctica docente, proporcionando las bases para el análisis de los resultados presentados en el siguiente capítulo.

# Capítulo IV. Diseño, Implementación del EVA Omniverso Digital y Recolección de Evidencias

Este capítulo presenta el diseño pedagógico y tecnológico del Entorno Virtual de Aprendizaje Omniverso Digital, y su implementación en el contexto educativo seleccionado y el proceso de recolección de la información. El EVA constituyó el escenario principal de intervención y, simultáneamente, la fuente de obtención de evidencias cualitativas y cuantitativas, a partir de las actividades desarrolladas por los estudiantes, los instrumentos aplicados y los productos generados durante la experiencia formativa.

El propósito general fue fortalecer la *competencia digital en seguridad y privacidad de la información*, conforme a los lineamientos del *MEN, 2022* que orientan la formación de ciudadanos digitales éticos y responsables.

El *Omniverso Digital* se concibió como un *EVA transmedia y gamificado*, basado en los principios del *conectivismo* y de la *Investigación-Acción Educativa (IAE)*. Su estructura, alojada en la plataforma Moodle de la Universidad Distrital Francisco José de Caldas, integró actividades colaborativas, recursos interactivos y rúbricas de evaluación que aseguraron la coherencia entre los objetivos pedagógicos y la valoración de los aprendizajes.

Este capítulo se desarrolla en coherencia con un enfoque mixto con diseño dominante cualitativo, en el cual los datos cuantitativos cumplen una función de apoyo interpretativo en la evaluación de la intervención pedagógica.

Antes de su implementación, tanto el EVA como los instrumentos de medición fueron validados por expertos y pares académicos de la Maestría en Educación en Tecnología, cuyos aportes permitieron mejorar la redacción, pertinencia y coherencia metodológica. Las

valoraciones completas pueden consultarse en el Repositorio de Valoraciones y Percepciones – Universidad Distrital Francisco José de Caldas.

**Diseño Pedagógico y Tecnoeducativo del EVA**

El *Omniverso Digital* fue diseñado como un entorno de aprendizaje transmedia que integra los principios del conectivismo (Siemens, 2004) y la gamificación educativa (Deterding et al., 2011). Desde el conectivismo, el aprendizaje se concibe como la creación de redes de conocimiento a través de la interacción entre estudiantes, docentes, recursos y comunidades digitales. Por su parte, la gamificación —entendida como el uso de elementos del diseño de los juegos en contextos no lúdicos— incorpora mecánicas como niveles, insignias y recompensas simbólicas que fomentan la motivación, la cooperación y la autorregulación en los procesos educativos.

La narrativa del EVA gira en torno a *CyberShield*, un guardián digital que acompaña a los estudiantes —denominados *Pioneros*— en su formación como ciudadanos digitales críticos y éticos. El entorno se articula en tres *Desafíos de Salvaguardia*, progresivos y secuenciales, que orientan el desarrollo de la competencia digital en seguridad y privacidad.

El *mapa de navegación* del *Omniverso Digital* estructura la experiencia a través de secciones que incluyen *Documentos de Autor*, *Mapa Conceptual*, *Planeador*, *Perfil Docente* y *Recursos del Omniverso*. Estos últimos reúnen materiales teóricos y los elementos de gamificación: *Puntos de Integridad* y *Medallones de Virtud*, que simbolizan el avance y la apropiación de los aprendizajes.

Cada desafío y actividad cuenta con una *rúbrica de evaluación* que establece criterios claros para valorar la comprensión conceptual, la aplicación práctica y la reflexión ética, garantizando la coherencia entre el diseño pedagógico y la evaluación formativa.

## Metodología de Diseño Instruccional: Modelo ADDIE Adaptado

El diseño del EVA *Omniverso Digital* se fundamentó en una adaptación del modelo ADDIE (Analysis, Design, Development, Implementation, Evaluation), ampliamente reconocido en el ámbito del diseño instruccional para la planificación, desarrollo y evaluación de ambientes de aprendizaje mediados por tecnologías digitales. La adopción de este modelo permitió estructurar el proceso de diseño de manera sistemática, flexible y contextualizada, atendiendo a las particularidades del entorno educativo rural y a los objetivos formativos de la investigación.

### *Fase 1. Análisis*

En la fase de análisis se identificaron las características de la población objetivo, conformada por estudiantes de los grados décimos y undécimos pertenecientes a contextos rurales de instituciones educativas oficiales de Bogotá. Se diagnosticaron las principales necesidades de aprendizaje, centradas en el fortalecimiento de la competencia digital en seguridad y privacidad de la información, así como las restricciones técnicas asociadas al acceso limitado a Internet, la variabilidad en el ancho de banda y la disponibilidad intermitente de dispositivos tecnológicos.

Asimismo, se analizó el contexto pedagógico institucional, considerando las orientaciones curriculares del (MEN, 2022) y los Estándares ISTE para estudiantes, con el fin de garantizar la pertinencia y alineación del EVA con los lineamientos educativos vigentes. Como resultado de esta fase, se definieron los objetivos de aprendizaje que orientaron el diseño pedagógico y tecnológico del entorno virtual, este desarrollo sigue el modelo ADDIE, como se justifica a continuación.

### Justificación del modelo ADDIE

La adopción del modelo ADDIE permitió garantizar la coherencia entre los objetivos pedagógicos, el diseño del EVA, la implementación de las actividades y la evaluación de los resultados. Su carácter sistemático y flexible facilitó la adaptación del proceso de diseño a las condiciones del contexto rural, fortaleciendo la rigurosidad metodológica y la consistencia teórico-práctica de la investigación.

#### *Fase 2. Diseño*

Durante la fase de diseño se estructuraron los objetivos específicos del EVA a partir de los tres ejes de la competencia digital en seguridad y privacidad de la información: protección de datos personales, gestión de la identidad digital y reconocimiento y mitigación de amenazas digitales. Se seleccionaron estrategias pedagógicas coherentes con el enfoque teórico de la investigación, integrando el conectivismo (Siemens, 2005), el constructivismo social y la gamificación, mediante una narrativa transmedia denominada *CyberShield*, orientada al aprendizaje basado en desafíos.

La estructura de contenidos se organizó en seis "Desafíos de Salvaguardia", diseñados con una progresión gradual de complejidad que permitió el desarrollo incremental de conocimientos, habilidades y actitudes. En esta fase también se planificó el proceso de evaluación, incorporando un pretest, instancias de evaluación formativa durante el desarrollo de los desafíos y un postest, con el propósito de medir el impacto del EVA. El resultado de esta fase fue el diseño pedagógico y tecnológico documentado del *Omniverso Digital*.

#### *Fase 3. Desarrollo*

En la fase de desarrollo se implementaron los diseños previamente definidos utilizando la plataforma Moodle, un sistema de gestión de aprendizaje (LMS) de código abierto, seleccionado

por su flexibilidad y accesibilidad en contextos educativos rurales. Se elaboraron y adaptaron diversos recursos educativos digitales, entre ellos simulaciones, videos, foros de discusión y tareas interactivas, ajustados al lenguaje y a las características de los estudiantes de educación media vocacional.

Los contenidos y actividades del EVA fueron sometidos a un proceso de validación mediante revisión por pares académicos, contando con el acompañamiento de la Dra. Ruth Molina, Javier Adames y el equipo del Programa de Acompañamiento Educativo y Tecnológico (PAET). Como resultado de esta fase, se obtuvo una versión del *Omniverso Digital* lista para su implementación.

***Fase 4. Implementación***

La fase de implementación correspondió a la puesta en marcha del EVA en el contexto educativo seleccionado, durante un periodo previamente definido de ejecución. En esta etapa participaron estudiantes de los grados décimo y undécimo, quienes desarrollaron las actividades propuestas, incluyendo desafíos, foros de discusión, reflexiones escritas y cartas dirigidas a sus pares.

El proceso estuvo acompañado por un monitoreo continuo y una retroalimentación semanal, con el fin de orientar el aprendizaje, resolver dificultades técnicas y pedagógicas, y favorecer la prácticas participación activa de los estudiantes. Como resultado de esta fase se recopilaron evidencias de aprendizaje, interacción y participación en el entorno virtual.

***Fase 5. Evaluación***

La fase de evaluación integró un enfoque mixto, combinando estrategias cuantitativas y cualitativas. La evaluación formativa se realizó a partir del desempeño de los estudiantes en cada

uno de los desafíos, mientras que la evaluación sumativa se llevó a cabo mediante la aplicación de la (ECDSPI) en modalidad de pretest y postest.

Adicionalmente, se desarrolló una evaluación cualitativa a través de la encuesta abierta, el análisis de los productos elaborados en el EVA y el estudio de casos representativos, lo que permitió profundizar en las percepciones, actitudes y reflexiones éticas del estudiantado.

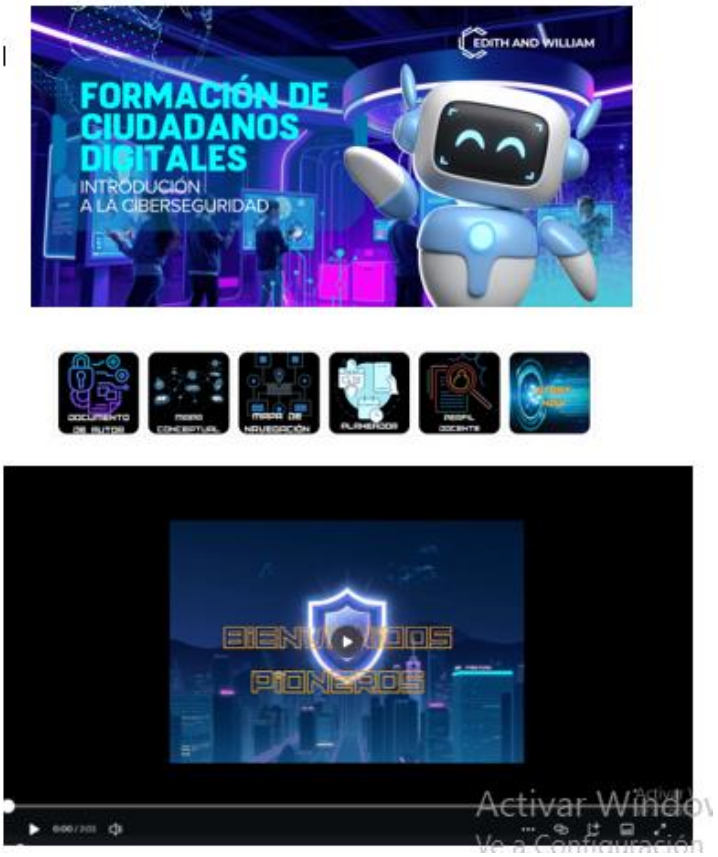
Finalmente, se incluyó una evaluación de usabilidad del EVA basada en la retroalimentación del equipo PAET. El resultado de esta fase fue un análisis triangulado del impacto del *Omniverso Digital* y la identificación de oportunidades de mejora para futuras versiones.

## Evidencias Visuales del Entorno Virtual Omniverso Digital

### *Interfaz principal*

La interfaz principal del EVA Omniverso Digital fue diseñada como un espacio de acceso central que articula la narrativa pedagógica, los contenidos formativos y las herramientas de interacción del entorno. Desde esta interfaz, el estudiantado puede orientarse de manera autónoma dentro del ecosistema digital, visualizar su progreso y acceder a los diferentes recursos y actividades propuestas. Su diseño responde a criterios de usabilidad, accesibilidad y coherencia pedagógica, con el propósito de facilitar la experiencia de aprendizaje y promover una participación activa, consciente y responsable en el desarrollo de la competencia digital en seguridad y privacidad de la información.

**Figura 3**
Interfaz principal del EVA Omniverso Digital




*Nota*. La figura presenta la interfaz principal del EVA Omniverso Digital, en la cual se observa el banner inicial con la narrativa de CyberShield, el menú de navegación que da acceso a los desafíos, recursos, foros e insignias, así como el listado de los seis Desafíos de Salvaguardia organizados de forma progresiva. También se incluye un indicador de avance que permite al estudiante visualizar las actividades completadas y un acceso al perfil y configuración del usuario. El diseño del entorno prioriza criterios de accesibilidad, como el uso de colores de alto contraste, tipografías legibles y una navegación intuitiva, con el fin de garantizar una experiencia inclusiva y facilitar el aprendizaje autónomo. Elaboración propia. (2024)

### *Estructura de un Desafío de Salvaguardia*

Los *Desafíos de Salvaguardia* constituyen la unidad pedagógica central del EVA *Omniverso Digital*, ya que en ellos se integran la narrativa, los contenidos conceptuales, las actividades y los criterios de evaluación. Cada desafío ha sido diseñado para guiar al estudiante a

través de una experiencia de aprendizaje progresiva, significativa y contextualizada, orientada al fortalecimiento de la competencia digital en seguridad y privacidad de la información. La estructura de los desafíos favorece la comprensión del propósito formativo, la autonomía del estudiante y la reflexión ética sobre el uso responsable de la tecnología.

**Figura 4**

*Estructura pedagógica de un Desafío de Salvaguardia en el EVA Omniverso Digital*




*Nota.* La figura muestra un ejemplo de la estructura de un Desafío de Salvaguardia correspondiente al Desafío 1: Alianza de Responsabilidad. En la interfaz se evidencian los componentes que conforman cada desafío: la contextualización narrativa mediante la historia de CyberShield, los objetivos de aprendizaje, la sección de recursos (videos, lecturas e infografías), la actividad principal a desarrollar, la rúbrica de evaluación con criterios explícitos de logro, el área de entrega de evidencias y el espacio de retroalimentación docente y entre pares. La organización visual y funcional de los desafíos responde a un diseño pedagógico progresivo, en el cual cada reto incrementa su

nivel de complejidad y profundiza en los aprendizajes desarrollados previamente, favoreciendo la construcción gradual de la competencia digital en seguridad y privacidad de la información. Elaboración propia. (2024)

### *Sistema de Insignias y Gamificación*

El sistema de insignias y logros del EVA *Omniverso Digital* cumple una función pedagógica y motivacional fundamental dentro de la estrategia didáctica gamificada. A través de este sistema, el estudiantado puede visualizar de manera inmediata su progreso, reconocer los aprendizajes alcanzados y fortalecer su compromiso con las actividades propuestas. Las insignias operan como mecanismos de retroalimentación positiva que estimulan la autorregulación, la persistencia y la participación activa, favoreciendo el aprendizaje significativo y la consolidación de la competencia digital en seguridad y privacidad de la información.

**Figura 5**

*Panel de insignias, logros y progreso del EVA Omniverso Digital*




*Nota.* La figura presenta el panel de insignias y logros del EVA Omniverso Digital, donde se visualizan las insignias obtenidas por el estudiante, acompañadas de su nombre, representación gráfica y descripción del logro

alcanzado. Asimismo, se incluye una barra de progreso general, la diferenciación entre logros desbloqueados y pendientes, un ranking de clase de carácter opcional con fines motivacionales y estadísticas personales de participación. Este sistema de gamificación permite ofrecer retroalimentación inmediata y visual sobre el avance del estudiante, promoviendo la motivación intrínseca, la autonomía y el seguimiento consciente del proceso de aprendizaje. Elaboración propia. (2024)

### *Foro de Discusión y Colaboración*

Los foros de discusión en el EVA *Omniverso Digital* constituyen un espacio central para la construcción colaborativa del conocimiento y la reflexión crítica en torno a la seguridad y la privacidad de la información. A través de estos escenarios de interacción asincrónica, los estudiantes comparten experiencias, argumentan sus posturas y dialogan con sus pares y el docente, fortaleciendo procesos de aprendizaje social, pensamiento crítico y ciudadanía digital. La participación en los foros permite evidenciar no solo la apropiación conceptual, sino también el desarrollo de actitudes éticas, comunicativas y reflexivas propias de la competencia digital.

**Figura 6**

*Interacción colaborativa en foros del EVA Omniverso Digital*




*Nota.* La figura muestra uno de los foros del EVA Omniverso Digital, en el que se observa la pregunta desencadenante planteada por el docente, y las respuestas de los estudiantes son organizadas en orden cronológico, la estructura de hilos de respuesta anidados y las opciones de edición o eliminación de mensajes propios. Esta configuración favorece la participación activa, el respeto por la opinión de los demás y la autorregulación comunicativa, promoviendo el aprendizaje colaborativo y el fortalecimiento de la competencia digital en comunicación, ética y seguridad en entornos virtuales. Elaboración propia. (2024)

### *Recursos Disponibles en Cada Desafío*

El EVA *Omniverso Digital* integra una variedad de recursos educativos digitales diseñadas para facilitar la comprensión de conceptos relacionados con la seguridad y la privacidad de la información desde enfoques visuales, interactivos y experienciales. Estos recursos cumplen una función mediadora del aprendizaje, permitiendo a los estudiantes acceder a los contenidos de manera flexible y significativa, reforzar los conceptos clave y desarrollar habilidades prácticas mediante la experimentación guiada. La diversidad de formatos favorece la atención a distintos ritmos y estilos de aprendizaje, fortaleciendo la autonomía y el compromiso del estudiantado con su proceso formativo.

**Figura 7**

*Recursos educativos digitales del EVA Omniverso Digital*




*Nota.* La figura presenta la sección de los recursos educativos digitales disponibles en el EVA Omniverso Digital, entre los que se incluyen videos explicativos de corta duración (entre tres y cinco minutos) con lenguaje

accesible, infografías que sintetizan visualmente conceptos clave sobre seguridad digital, simuladores interactivos —como el simulador de phishing— que permiten al estudiante identificar correos electrónicos fraudulentos en un entorno controlado, lecturas breves con palabras clave resaltadas y enlaces externos a herramientas de seguridad digital (gestores de contraseñas, redes privadas virtuales, entre otros). La selección y organización de estos recursos responde a criterios pedagógicos de claridad, pertinencia y aplicabilidad, orientados al desarrollo progresivo de la competencia digital en seguridad y privacidad de la información. Elaboración propia. (2024)

### *Rutas de Aprendizaje y Secuenciación*

La estructura del EVA *Omniverso Digital* se organizó a partir de rutas de aprendizaje secuenciadas que orientan el progreso cognitivo y formativo del estudiantado. Estas rutas responden a una progresión intencional de los objetivos de aprendizaje, fundamentada en la Taxonomía de Bloom revisada, lo que permite transitar desde niveles básicos de reconocimiento conceptual hasta niveles superiores de análisis, evaluación y creación. La secuenciación de los *Desafíos de Salvaguardia* garantiza que los estudiantes consoliden los aprendizajes esenciales antes de abordar tareas de mayor complejidad, favoreciendo un desarrollo gradual, significativo y reflexivo de la competencia digital en seguridad y privacidad de la información.

**Figura 8**

*Rutas de aprendizaje y secuenciación pedagógica del EVA Omniverso Digital*




*Nota.* La figura representa la estructura general del EVA Omniverso Digital y la secuenciación de sus seis Desafíos de Salvaguardia, organizada según los niveles de la Taxonomía de Bloom. El Desafío 1 (Recordar) introduce los conceptos básicos de seguridad digital y el lenguaje fundamental mediante la Alianza de Responsabilidad; el Desafío 2 (Comprender) profundiza en la identificación de riesgos como phishing y malware en contextos simples; el Desafío 3 (Aplicar) promueve la implementación de medidas de seguridad en situaciones reales; el Desafío 4 (Analizar) orienta al análisis de escenarios complejos con múltiples riesgos; el Desafío 5 (Evaluar) implica la valoración del nivel de seguridad de un entorno y la justificación de decisiones de protección; y el Desafío 6 (Crear) favorece la síntesis del aprendizaje mediante la elaboración de una reflexión personal y una carta de mentoría dirigida a compañeros de grados inferiores. Esta progresión asegura la coherencia entre objetivos, actividades y evaluación, fortaleciendo el desarrollo integral de la competencia digital en seguridad y privacidad de la información. Elaboración propia. (2024)

### *Ejemplos de Actividades Específicas*

Las actividades desarrolladas por los estudiantes dentro de los *Desafíos de Salvaguardia* constituyen evidencias concretas del proceso de apropiación de la competencia digital en seguridad y privacidad de la información. En particular, las producciones elaboradas en el Desafío 3, orientado a la aplicación de medidas de seguridad digital, permiten observar la integración de conocimientos conceptuales, habilidades prácticas y creatividad comunicativa. Estas actividades favorecen la transferencia del aprendizaje al contexto comunitario y fortalecen la capacidad del estudiantado para comunicar de manera clara y responsable recomendaciones de seguridad en entornos digitales.

El Desafío 6, orientado a la reflexión personal y la mentoría entre pares, permitió evidenciar niveles superiores de apropiación de la competencia digital en seguridad y privacidad de la información. A través de la escritura de cartas dirigidas a estudiantes de grados inferiores, los participantes no solo sintetizaron los aprendizajes adquiridos, sino que asumieron un rol pedagógico y ético al orientar a otros sobre prácticas seguras en el entorno digital. Esta actividad favoreció la consolidación del pensamiento reflexivo, la empatía y la responsabilidad social.

**Figura 9**

*Ejemplos de productos elaborados por pioneros en el Desafío 3: Carteles sobre consejos de seguridad digital*

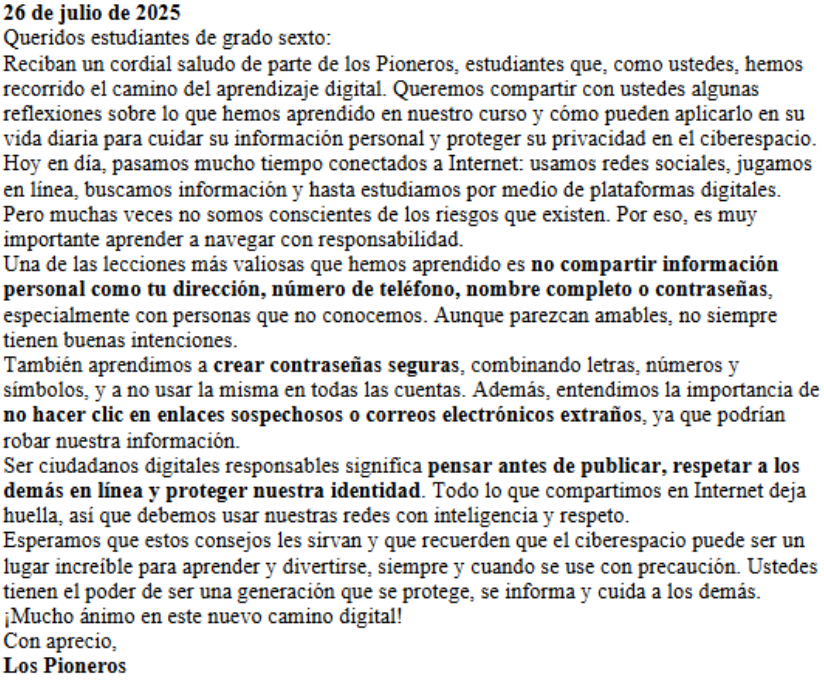



*Nota.* La figura presenta un ejemplo de los carteles e infografías diseñados por los estudiantes como parte del Desafío 3: Consejos de Seguridad, en los cuales se proponen cinco recomendaciones orientadas a la protección de la información personal y la prevención de riesgos digitales en su comunidad. Estas producciones evidencian la apropiación de conceptos clave de seguridad digital, la capacidad para aplicar los aprendizajes en contextos reales y

el desarrollo de habilidades comunicativas y creativas. Asimismo, reflejan el tránsito del estudiante desde la comprensión teórica hacia la aplicación práctica del conocimiento, fortaleciendo la competencia digital desde una perspectiva técnica, ética y social. Elaborado por grupo de pioneros de líneas de profundización de tecnología de la IED Rural San Cayetano. (2025)

**Figura 10**

*Carta reflexiva elaborada por pioneros en el Desafío 6: Mentoría entre pares*



**26 de julio de 2025**

Queridos estudiantes de grado sexto:

Reciban un cordial saludo de parte de los Pioneros, estudiantes que, como ustedes, hemos recorrido el camino del aprendizaje digital. Queremos compartir con ustedes algunas reflexiones sobre lo que hemos aprendido en nuestro curso y cómo pueden aplicarlo en su vida diaria para cuidar su información personal y proteger su privacidad en el ciberespacio.

Hoy en día, pasamos mucho tiempo conectados a Internet: usamos redes sociales, jugamos en línea, buscamos información y hasta estudiamos por medio de plataformas digitales. Pero muchas veces no somos conscientes de los riesgos que existen. Por eso, es muy importante aprender a navegar con responsabilidad.

Una de las lecciones más valiosas que hemos aprendido es **no compartir información personal como tu dirección, número de teléfono, nombre completo o contraseñas**, especialmente con personas que no conocemos. Aunque parezcan amables, no siempre tienen buenas intenciones.

También aprendimos a **crear contraseñas seguras**, combinando letras, números y símbolos, y a no usar la misma en todas las cuentas. Además, entendimos la importancia de **no hacer clic en enlaces sospechosos o correos electrónicos extraños**, ya que podrían robar nuestra información.

Ser ciudadanos digitales responsables significa **pensar antes de publicar, respetar a los demás en línea y proteger nuestra identidad**. Todo lo que compartimos en Internet deja huella, así que debemos usar nuestras redes con inteligencia y respeto.

Esperamos que estos consejos les sirvan y que recuerden que el ciberespacio puede ser un lugar increíble para aprender y divertirse, siempre y cuando se use con precaución. Ustedes tienen el poder de ser una generación que se protege, se informa y cuida a los demás.

¡Mucho ánimo en este nuevo camino digital!

Con aprecio,

**Los Pioneros**

*Nota.* La figura muestra una carta reflexiva elaborada por un estudiante de grado undécimo, dirigida a compañeros de grados inferiores, en la que se ofrecen recomendaciones sobre el uso seguro de contraseñas y la protección de la información personal. El texto evidencia la apropiación de lenguaje técnico propio de la seguridad digital, la capacidad para explicar conceptos de manera didáctica y accesible, y un compromiso ético con la formación de otros. Esta producción refleja el nivel de creación y síntesis del aprendizaje, correspondiente a los niveles superiores de la Taxonomía de Bloom, así como el fortalecimiento de la ciudadanía digital y la mentoría solidaria entre pares. Elaborado por uno de los pioneros de líneas de profundización de tecnología de la IED San Cayetano. (2025)

## Diseño y Validación de los Instrumentos de Evaluación

### *Validación de la Escala ECDSPI*

Para evaluar el impacto del *Omniverso Digital* se utilizaron dos instrumentos complementarios: la *ECDSPI* y la *Encuesta Abierta de Ciberseguridad*.

La *ECDSPI*, adaptada de Schwarz et al. (2024), constituye el instrumento central de medición cuantitativa. Evalúa tres ejes: *protección de datos personales*, *gestión de identidad digital* y *reconocimiento y mitigación de amenazas*.

Fue aplicada en los momentos pretest y postest con el propósito de identificar variaciones en el progreso de los estudiantes en las dimensiones de seguridad y privacidad digital.

**Tabla 3**

*Articulación entre ECDSPI y encuesta abierta de ciberseguridad*

| Eje de la Competencia (ECDSPI) | Preguntas Cuantitativas (ECDSPI) | Preguntas Cualitativas Complementarias (Encuesta Abierta) | Objetivo de Articulación |
|---|---|---|---|
| **Protección de Datos Personales** | • Crear contraseñas seguras.<br>• Modificar la configuración de privacidad.<br>• Identificar intentos de phishing.<br>• Distinguir sitios web seguros.<br>• Realizar copias de seguridad | ¿Qué tipo de contenido sueles publicar en internet?<br>¿Cómo decides si ese contenido es apropiado para compartir?<br>¿Cómo crees que tus publicaciones afectan tu huella digital? | Medir de manera conjunta la capacidad técnica del estudiantado (ECDSPI) y su nivel de reflexión ética y conciencia sobre la información personal que comparte en entornos digitales (encuesta abierta). |
| **Gestión de Identidad Digital** | •Controlar la información personal compartida.<br>•Administrar cuentas y contraseñas. •Reconocer suplantación de identidad.<br>•Identificar permisos riesgosos en aplicaciones. | ¿Has observado que alguien publique información de otra persona sin su permiso? ¿Qué opinas sobre esa situación?<br>¿Has conversado en casa sobre el cuidado de la privacidad digital? | Validar la comprensión técnica de la gestión de la identidad digital junto con la percepción de responsabilidad social y respeto por los datos personales propios y de otros. |
| **Reconocimiento y Mitigación de Amenazas** | •Identificar aplicaciones o enlaces riesgosos.<br>•Aplicar medidas básicas de seguridad digital.<br>•Mantener dispositivos y aplicaciones actualizadas.<br>•Reconocer situaciones de compromiso de identidad | ¿Qué tan preparado te sientes para actuar de manera responsable en internet?<br>¿Qué has aprendido sobre los riesgos digitales y cómo prevenirlos? | Evaluar la autonomía, la confianza y la actitud del estudiante frente a la aplicación de medidas de seguridad digital, integrando el componente actitudinal de la competencia. |

*Nota.* La tabla presenta la articulación entre los ejes de la competencia digital en seguridad y privacidad de la información evaluados mediante la ECDSPI y las preguntas cualitativas complementarias de la encuesta abierta. Esta integración metodológica permite analizar de manera integral el desarrollo de la competencia desde los componentes cognitivo, procedimental y actitudinal (saber, saber hacer y saber ser), fortaleciendo la coherencia entre los instrumentos de recolección de información y los objetivos del estudio. Elaboración propia (2026).

**Ítems de la *ECDSPI*.**

- ***Competencia: Seguridad y Protección de Datos Personales.***

1. Puedo crear contraseñas seguras y complejas para proteger mi información personal.
2. Puedo verificar y modificar la configuración de privacidad en redes sociales y otras plataformas digitales.
3. Puedo identificar correos electrónicos o mensajes sospechosos (phishing) y evitar caer en estafas.
4. Puedo distinguir entre sitios web seguros y no seguros antes de ingresar mi información personal.
5. Puedo realizar copias de seguridad de mis archivos importantes para evitar su pérdida.

- ***Competencia: Gestión de Identidad Digital.***

6. Puedo controlar qué información personal comparto en línea y en qué plataformas.
7. Puedo administrar múltiples cuentas y proteger cada una con diferentes contraseñas seguras.
8. Puedo reconocer y tomar medidas cuando siento que mi identidad en línea ha sido comprometida.

- ***Competencia: Reconocimiento y Mitigación de Amenazas.***

9. Puedo reconocer intentos de suplantación de identidad en redes sociales o en correos electrónicos.
10. Puedo identificar aplicaciones o sitios web que solicitan permisos innecesarios o excesivos.
11. Puedo implementar medidas de seguridad básicas en mis dispositivos, como el bloqueo de pantalla y el cifrado de datos.
12. Puedo actualizar mis dispositivos y aplicaciones para mantenerme protegido contra las últimas amenazas de seguridad.

**Tabla 4**

*Escala de respuestas*

| Escala de Respuesta | Descripción de Nivel de Competencia |
|---|---|
| No puedo hacer esto | Sin competencia en la tarea |
| Puedo hacerlo solo con ayuda | Competencia básica con guía |
| Puedo hacerlo parcialmente solo | Competencia básica, algunas partes requieren apoyo |
| Puedo hacerlo en su mayoría solo | Competencia intermedia, autonomía en tareas rutinarias |
| Puedo hacerlo completamente solo | Competencia intermedia, autonomía total en tareas no rutinarias |
| Puedo explicarlo a otros | Competencia avanzada, habilidad para guiar a otros |
| Soy experto en esto | Competencia avanzada, optimización de soluciones |

*Nota.* Adaptado de Schwarz et al. (2024). Escala de Competencia Digital. Traducción y adaptación propia. (2024)

La validación de la escala fue realizada por jueces expertos, quienes valoraron la coherencia con los objetivos de investigación, la claridad de los ítems, la adecuación del lenguaje

y la pertinencia para estudiantes de educación media. Los resultados detallados se presentan en el driver Validaciones instrumentos "Valoración de la adaptación del instrumento ECDSPI".

Entre los evaluadores se destacan *Harold Andrés Ortiz Pinzón*, *César Mauricio Peña Martínez*, *Luis Leonardo Delgado Beltrán*, *Juan Pablo Martínez* e *Ingrid Cabezas*, quienes valoraron las dimensiones de pertinencia pedagógica, claridad semántica y coherencia con los objetivos de la investigación.

Las calificaciones oscilaron entre *4.5 y 5.0*, evidenciando una alta coherencia del instrumento. Las principales sugerencias se centraron en:

- Precisar el lenguaje técnico de términos como *huella digital* y *privacidad en línea*.
- Adecuar el nivel lingüístico a los estudiantes de educación media.
- Reforzar el componente reflexivo de las preguntas para promover pensamiento crítico y autorregulación digital.

Estas observaciones fueron incorporadas en la versión final de la encuesta, consolidando su validez de contenido y fortaleciendo su rol como instrumento cualitativo complementario de la *ECDSPI*.

No obstante, la *ECDSPI*, por su carácter estructurado, ofrece información exclusivamente cuantitativa, lo cual impide captar percepciones, reflexiones o cambios actitudinales. Por esta razón, se diseñó la *Encuesta Abierta de Ciberseguridad* como instrumento complementario para obtener información cualitativa que permitiera contextualizar e interpretar los resultados numéricos de la escala.

De esta manera, la encuesta posibilitó identificar procesos de *autorreflexión*, *ética digital* y *conciencia ciudadana*, permitiendo comprender de manera integral las transformaciones en las

competencias digitales antes y después de la intervención. La combinación de ambos instrumentos fortaleció la validez interpretativa del estudio y permitió triangular los resultados desde perspectivas complementarias.

### *Validación de la Encuesta Abierta de Ciberseguridad*

La Encuesta Abierta de Ciberseguridad se diseñó como un instrumento cualitativo complementario para explorar las percepciones, reflexiones y prácticas de los estudiantes sobre el uso ético, seguro y responsable de internet. Su función fue validar y complementar las respuestas obtenidas con la ECDSPI, aportando una mirada interpretativa a los resultados cuantitativos.

Las preguntas, formuladas en formato de respuesta abierta, fueron aplicadas en dos momentos: pretest y postest. Las respuestas obtenidas se analizaron mediante categorías emergentes, lo que permitió interpretar las percepciones, reflexiones y prácticas de los estudiantes frente al uso ético, seguro y responsable de internet.

**Preguntas Encuesta Abierta:**

1. ¿Qué tipo de contenido sueles publicar o compartir en redes sociales? ¿Cómo decides si es apropiado o no hacerlo?
2. ¿Alguna vez has visto que alguien publique algo sin el permiso de otra persona? ¿Qué opinas de eso?
3. ¿Crees que lo que publicas en internet puede afectar tu reputación o la de otros? ¿Por qué?
4. ¿Has hablado en tu casa o en el colegio sobre temas como ciberacoso, privacidad o huella digital? ¿Qué te han dicho?

5. ¿Qué tan preparado(a) te sientes para actuar de manera responsable en internet y proteger tus derechos y los de tus compañeros?

La *Encuesta Abierta de Ciberseguridad* fue revisada por docentes e investigadores de la Maestría en Educación en Tecnología de la Universidad Distrital y por profesionales del área educativa con experiencia en innovación pedagógica y mediación digital.

***Validación del EVA Omniverso Digital***

El diseño del *Omniverso Digital* fue sometido a un proceso de validación académica y técnica con el fin de garantizar su coherencia pedagógica, comunicativa y funcional.

*Dra. Ruth Molina Vásquez (Universidad Distrital Francisco José de Caldas):* Evaluó la estructura pedagógica, la accesibilidad, la coherencia narrativa y el diseño visual del entorno. Destacó la claridad de la navegación, la pertinencia de la gamificación y la integración entre teoría y práctica. Su calificación global fue de *5.0*.

*Javier Mauricio Adames (Par académico):* Revisó la integración de los componentes pedagógicos y tecnológicos, resaltando la relevancia de los *Desafíos de Salvaguardia* como ejes articuladores de la experiencia. Su evaluación general se ubicó entre *4.5 y 5.0*, destacando la solidez del diseño instruccional.

*Equipo PAET – Plataforma de Apoyo a Entornos de Aprendizaje y Tecnología Educativa:* Realizó una valoración institucional centrada en la usabilidad, navegabilidad y desempeño técnico del entorno. El informe concluyó que el EVA cumple con los estándares de calidad de la Universidad Distrital y es pertinente para contextos rurales. Su evaluación global se ubicó entre *4.5 y 5.0*.

Las observaciones conjuntas permitieron ajustar instrucciones, mejorar la redacción y optimizar recursos audiovisuales y enlaces interactivos, garantizando la accesibilidad y coherencia del diseño final.

**Implementación del EVA y Aplicación de los Instrumentos**

Tras la validación, se implementó el *Omniverso Digital* con los estudiantes de educación media del colegio rural *IED San Cayetano*, bajo la orientación de los docentes-investigadores en su rol de facilitadores y observadores.

La aplicación se desarrolló en tres etapas:

*Pretest:* aplicación inicial de la *ECDSPI* y la *Encuesta Abierta de Ciberseguridad* para establecer la línea base.

*Intervención:* desarrollo de los *Desafíos de Salvaguardia* en Moodle, combinando actividades individuales y colaborativas.

*Postest:* re-aplicación de los instrumentos para comparar los resultados y analizar los avances obtenidos.

Cada producto elaborado en el EVA —cartas, foros, juegos, protocolos multimedia y reflexiones personales— fue evaluado mediante rúbricas específicas, que aseguraron la objetividad, coherencia y equidad en la valoración del desempeño. El presente capítulo expuso el proceso de diseño, validación e implementación del *EVA Omniverso Digital* y de los instrumentos empleados para su evaluación. Las valoraciones realizadas por pares y expertos confirmaron la coherencia pedagógica y técnica de la propuesta, así como su pertinencia en el fortalecimiento de la competencia digital en seguridad y privacidad de la información.

La integración de la *ECDSPI* y la *Encuesta Abierta de Ciberseguridad* permitió combinar la medición objetiva con la reflexión crítica, proporcionando una comprensión más completa del aprendizaje.

A partir de esta base, el siguiente capitulo abordará el análisis e interpretación de los resultados obtenidos, evidenciando los avances, cambios y aprendizajes significativos logrados por los estudiantes.

# Capítulo V. Resultados y Análisis

El presente capítulo expone los resultados y el análisis del proceso investigativo desarrollado con los estudiantes de educación media del Instituto Educativo Distrital Rural San Cayetano, en el marco de la implementación del EVA *Omniverso Digital*. A partir de una mirada etnográfica, se presentan las características sociales, culturales y tecnológicas del grupo participante, junto con los hallazgos obtenidos a partir de los instrumentos aplicados. El análisis se desarrolla desde un enfoque mixto con diseño dominante cualitativo, en el cual los resultados cuantitativos cumplen una función de apoyo interpretativo, permitiendo una comprensión integral de los procesos formativos y de los cambios evidenciados en la competencia digital en seguridad y privacidad de la información.

El análisis se orienta al fortalecimiento de la competencia ciudadana digital en seguridad y privacidad de la información, en coherencia con la competencia del MEN (2022), que promueve la actuación crítica y argumentada frente a las implicaciones éticas del uso de la tecnología, y con el estándar del Ciudadano Digital de los ISTE para Estudiantes (2d), enfocado en la gestión responsable de los datos personales y la seguridad digital.

Estos resultados permiten evidenciar los avances en el desarrollo de prácticas éticas, reflexivas y seguras en el entorno digital, consolidando en los estudiantes una conciencia crítica frente al uso responsable de la información y la tecnología.

## Etnografía de los estudiantes del IED San Cayetano

El punto de partida de este proceso investigativo se sitúa en el reconocimiento del contexto sociocultural y educativo del *Instituto Educativo Distrital Rural San Cayetano*, ubicado en la localidad de *Usme*, barrio *Juan Rey*, en la periferia suroriental de Bogotá D.C. La institución se caracteriza por su entorno *rural–urbano de montaña*, donde convergen familias

con diversas condiciones socioeconómicas y culturales. Actualmente, el colegio cuenta con una población aproximada de *1.700 estudiantes distribuidos en tres jornadas*: preescolar y media vocacional en la jornada única, bachillerato en la mañana y primaria en la tarde. Su infraestructura incluye *31 aulas, biblioteca, laboratorios de informática, zonas artísticas, biosfera ambiental y espacios deportivos*, lo que facilita experiencias pedagógicas integrales orientadas al desarrollo humano, tecnológico y ambiental.

En cuanto al *perfil etnográfico de los estudiantes de educación media*, participantes en esta investigación, se evidencia que el *70% tiene entre 16 y 17 años*, el *25% entre 14 y 15*, y un pequeño grupo del *5% entre 18 y 19 años*, con una composición de *60% hombres y 40% mujeres*. La mayoría pertenece al *estrato socioeconómico 1 (85%)*, seguido de un *10% en estrato 2* y *5% en estrato 3*, lo que refleja un contexto de vulnerabilidad económica. De ellos, un número significativo reside en zonas rurales, enfrentando dificultades de transporte y conectividad. Esta condición incide directamente en las dinámicas de acceso al conocimiento y en la apropiación de las tecnologías digitales.

El *núcleo familiar* está constituido, en su mayoría, por entre *3 y 6 miembros*. El *75% de los cuidadores principales son madres* que, en su mayoría, tienen *nivel de escolaridad secundaria completa o incompleta*, y trabajan fuera del hogar en jornadas de más de ocho horas diarias, lo que limita el acompañamiento académico. Esta estructura familiar revela la relevancia de la escuela como espacio protector, formativo y mediador en el proceso de construcción de ciudadanía digital y ética.

Desde el punto de vista *tecnológico*, el *90% de los estudiantes cuenta con acceso a internet*, pero solo el *55% dispone de un computador propio o familiar*, lo que representa una brecha digital significativa. En este sentido, la escuela se convierte en el principal espacio de

interacción con las tecnologías, favoreciendo el desarrollo de competencias digitales a través de las salas de informática y del *EVA Omniverso Digital*. Este último ha permitido compensar, en parte, las desigualdades tecnológicas mediante la creación de experiencias gamificadas, colaborativas y críticas en torno a la ciberseguridad y la ética digital.

En el aspecto *académico y motivacional*, las asignaturas más apreciadas por los estudiantes son *Artes, Educación Física e Inglés*, lo cual revela una inclinación hacia expresiones comunicativas, creativas y culturales. El *80% considera su rendimiento académico como bueno*, aunque la autopercepción de excelencia es baja, lo que sugiere una necesidad de fortalecer la confianza y la autorregulación en el aprendizaje.

En cuanto a la *vida social y cultural*, los datos reflejan que *la mitad de los estudiantes no participa en actividades extracurriculares*, y un porcentaje significativo destina su tiempo libre a *ver televisión o practicar deportes*. Solo el *45% manifiesta sentirse identificado con la cultura local o nacional*, predominando el gusto por la música (60%) como principal expresión cultural. Esto evidencia la necesidad de potenciar espacios escolares donde los jóvenes puedan vincular sus identidades locales con la cultura digital global de forma crítica y significativa.

De acuerdo con el *Proyecto Educativo Institucional (PEI)* del colegio, la institución busca fortalecer la formación integral, la convivencia, el pensamiento crítico y el uso responsable de las tecnologías. En coherencia con ello, la etnografía de los estudiantes muestra una población resiliente, diversa y consciente de sus desafíos sociales y digitales, lo que justifica la pertinencia de la implementación del *Omniverso Digital* como estrategia pedagógica orientada a fortalecer las *competencias ciudadanas digitales en seguridad, privacidad y ética tecnológica*.

En síntesis, esta caracterización etnográfica permite comprender el contexto de partida desde el cual se construyó la propuesta educativa y tecnológica. Los estudiantes del *IED Rural*

*San Cayetano* no solo representan una comunidad educativa con limitaciones de acceso y recursos, sino también un grupo con alto potencial de aprendizaje, creatividad y sentido de comunidad, capaz de desarrollar habilidades digitales y reflexivas que los preparen para actuar como *ciudadanos digitales críticos, éticos y responsables*.

**Resultados cualitativos**

Este apartado presenta los resultados cualitativos obtenidos a partir de la Encuesta Abierta de Ciberseguridad y del análisis de las evidencias producidas por los estudiantes en el EVA Omniverso Digital. Desde un análisis de contenido de carácter inductivo, se identificaron categorías emergentes relacionadas con las prácticas digitales, la reflexión ética y la apropiación progresiva del lenguaje técnico en ciberseguridad.

Estos resultados permiten comprender en profundidad las transformaciones en las percepciones, actitudes y comportamientos de los estudiantes frente al uso seguro y responsable de la tecnología, constituyéndose en el eje central para la interpretación del impacto pedagógico de la intervención.

***Análisis de la Encuesta de Ciberseguridad***

El presente análisis corresponde a la *Encuesta de Ciberseguridad*, aplicada a los estudiantes de media de la *Institución de Educación Distrital (IED) San Cayetano* como complemento cualitativo de la *ECDSPI*. Este instrumento permitió profundizar en las percepciones, hábitos y actitudes de los estudiantes frente al uso seguro de la tecnología, la protección de los datos personales y la convivencia digital responsable.

La encuesta se aplicó en dos momentos —*pretest* y *postest*—, con el propósito de identificar los cambios en las prácticas y reflexiones de los participantes tras la implementación del *EVA Omniverso Digital*. Los ítems abordaron dimensiones como el tipo de contenido

compartido en línea, los criterios de publicación, la protección de la información personal, el diálogo familiar y escolar sobre ciberseguridad y la percepción de preparación ante riesgos digitales.

Los resultados comparativos evidencian un fortalecimiento de la conciencia crítica, la autorregulación y la práctica de comportamientos seguros en línea. Además, reflejan un avance en la comprensión ética del respeto, la privacidad y la responsabilidad compartida en el ecosistema digital, en coherencia con los lineamientos del *Ministerio de Educación Nacional (MEN, 2022)* y los *Estándares ISTE para Estudiantes (2024)*.

**Presentación de Resultados Encuesta abierta Ciberseguridad**

A continuación, se presentan los resultados comparativos del *pretest* y *postest* de la *Encuesta de Ciberseguridad*. Cada tabla muestra los porcentajes de respuesta agrupados por categoría, acompañados de una *nota seguida* que indica el número y enunciado de la pregunta, así como un *hallazgo interpretativo* que sintetiza las principales transformaciones observadas en los estudiantes después del proceso formativo en el *EVA Omniverso Digital*.

**Tabla 5**

*Comparativo pretest–postest: tipos de contenido compartido por los estudiantes en línea*

| Tipo de contenido compartido | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| Fotografías personales | 43.4 | 26.0 | –17.4 |
| Publicaciones familiares o de amigos | 56.5 | 39.1 | –17.4 |
| Opiniones o comentarios en redes | 34.8 | 26.0 | –8.8 |
| Contenidos escolares | 30.4 | 39.1 | +8.7 |
| Información personal (nombre, dirección, etc.) | 17.4 | 0 | –17.4 |

| | | | |
|---|---|---|---|
| No suelo compartir contenido en línea | 4.3 | 17.4 | +13.1 |
| **Total** | **100** | **100** | — |

*Nota.* Pregunta 1 del instrumento *Encuesta de Ciberseguridad*: "¿Qué tipo de contenido sueles compartir en redes sociales o plataformas digitales?". Comparativo *pretest–postest* con variaciones expresadas en porcentajes (%).

*Hallazgo:* Tras la intervención educativa, disminuyó la publicación de información personal y fotografías, mientras aumentó la tendencia a compartir contenido académico. Este cambio refleja una mayor conciencia sobre la huella digital y la gestión responsable de la información en línea, fortalecida por las actividades del *EVA Omniverso Digital*.

**Tabla 6**

*Comparativo pretest–postest: criterios que aplican antes de publicar información en línea*

| Criterio considerado antes de publicar | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| Verifico si afecta mi privacidad o reputación | 43.4 | 69.6 | +26.2 |
| Pienso en cómo puede interpretarse | 34.8 | 52.1 | +17.3 |
| Consulto con alguien antes de publicar | 21.7 | 26.0 | +4.3 |
| No reflexiono antes de publicar | 17.4 | 0 | –17.4 |
| No publico nada en redes | 4.3 | 8.7 | +4.4 |
| **Total** | **100** | **100** | — |

*Nota.* Pregunta 2 del instrumento *Encuesta de Ciberseguridad*: "Antes de publicar algo en redes o en línea, ¿qué sueles tener en cuenta?". Comparativo *pretest–postest* con variaciones expresadas en porcentajes (%).

*Hallazgo:* Se observa un incremento en la reflexión previa a la publicación y en la autorregulación digital. Los estudiantes desarrollaron pensamiento crítico frente a la privacidad, la reputación y las implicaciones de sus acciones en entornos virtuales, en coherencia con la *Competencia Digital Ciudadana* promovida por el *MEN (2022)* y los *Estándares ISTE (2024)*.

**Tabla 7**

*Comparativo pretest–postest: percepción sobre publicar información o imágenes de otros sin permiso*

| Opinión sobre publicar sin permiso | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| Lo he hecho alguna vez | 17.4 | 4.3 | –13.1 |
| Nunca lo he hecho | 56.5 | 78.3 | +21.8 |
| No estoy seguro(a) si eso está mal | 21.7 | 8.7 | –13.0 |
| No lo considero importante | 4.4 | 0 | –4.4 |
| **Total** | **100** | **100** | — |

*Nota.* Pregunta 3 del instrumento *Encuesta de Ciberseguridad*: "¿Has publicado o compartirías fotos, videos o información de otras personas sin su permiso?". Comparativo *pretest–postest* con variaciones expresadas en porcentajes (%).

*Hallazgo:* Tras la intervención, aumentó significativamente el número de estudiantes que reconocen la importancia del consentimiento antes de publicar contenido ajeno. El resultado refleja una consolidación de la ética digital y el respeto por la privacidad en el entorno virtual, promovidos en el *EVA Omniverso Digital*.

**Tabla 8**

*Comparativo pretest–postest: conversaciones familiares o escolares sobre seguridad digital*

| Frecuencia de conversaciones sobre seguridad digital | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| Hablo frecuentemente con mi familia o profesores | 26.1 | 47.8 | +21.7 |
| A veces se habla del tema | 39.1 | 39.1 | 0 |
| Casi nunca se habla del tema | 30.4 | 13.0 | –17.4 |
| Nunca se habla del tema | 4.4 | 0 | –4.4 |
| **Total** | **100** | **100** | — |

*Nota.* Pregunta 4 del instrumento *Encuesta de Ciberseguridad*: "¿Con qué frecuencia hablas en tu casa o en el colegio sobre seguridad digital o riesgos en internet?". Comparativo *pretest–postest* con variaciones expresadas en porcentajes (%).

*Hallazgo:* Se evidencia un aumento en el diálogo familiar y escolar sobre ciberseguridad, lo cual demuestra una apropiación del tema más allá del aula. Este resultado sugiere que el *EVA Omniverso Digital* fomentó la comunicación intergeneracional sobre el uso seguro y responsable de la tecnología.

**Tabla 9**

*Comparativo pretest–postest: autopercepción sobre la preparación ante riesgos digitales*

| Nivel de preparación ante riesgos digitales | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| **No sé cómo actuar ante riesgos o ataques** | 21.7 | 0 | –21.7 |
| **Tengo nociones básicas de protección** | 52.2 | 34.8 | –17.4 |
| **Me siento preparado(a) para actuar correctamente** | 26.1 | 65.2 | +39.1 |
| **Total** | **100** | **100** | — |

*Nota.* Pregunta 5 del instrumento *Encuestade Ciberseguridad*: "¿Qué tan preparado(a) te consideras para enfrentar un riesgo digital o un intento de fraude?". Comparativo *pretest–postest* con variaciones expresadas en porcentajes (%).

*Hallazgo:* El porcentaje de estudiantes que se consideran preparados para responder ante incidentes digitales aumentó del 26,1 % al 65,2 %. Este avance evidencia un fortalecimiento de la autonomía digital y la aplicación práctica de conocimientos de ciberseguridad desarrollados en el *EVA Omniverso Digital*.

En conjunto, los resultados de la Encuesta Abierta de Ciberseguridad evidencian transformaciones significativas en las prácticas, percepciones y actitudes de los estudiantes frente al uso de la tecnología y la gestión de la información personal. Los cambios observados entre el pretest y el postest reflejan un fortalecimiento progresivo de la reflexión ética, la autorregulación digital y la conciencia sobre la huella digital, así como una mayor disposición para actuar de

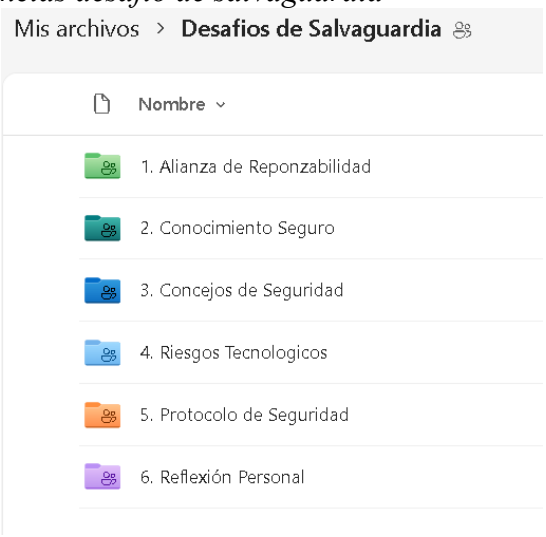
manera responsable ante los riesgos del entorno virtual. Estas transformaciones, promovidas a través de las actividades desarrolladas en el EVA *Omniverso Digital*, confirman el papel de la intervención pedagógica como un espacio formativo que trasciende el aprendizaje técnico, favoreciendo la construcción de una ciudadanía digital crítica, ética y comprometida con la protección de la información propia y ajena.

***Evidencias del aprendizaje mediado por el EVA - Omniverso Digital***

Las actividades desarrolladas en el EVA – Omniverso Digital se estructuraron en seis *Desafíos de Salvaguardia*, cada uno con entregables específicos que permitieron evidenciar el compromiso y la creatividad de los estudiantes. Las evidencias fueron recopiladas y organizadas en carpetas digitales (cartas, foros, organizadores, juegos, protocolos y reflexiones), disponibles en el repositorio institucional de la Universidad Distrital. Estas evidencias pueden ser consultadas en el siguiente enlace:

Repositorio de evidencias – Desafíos de Salvaguardia. https://udistritaleduco-my.sharepoint.com/:f:/g/personal/ecortes_udistrital_edu_co/Eurlkp5yrjNNq_1usCYm08IBe4m-OLYoKW9XER9mvLRxlQ?e=2n7uo2

**Figura 11**.
*Estructura repositorio de evidencias desafío de salvaguardia*




*Nota*. La imagen muestra las carpetas en OneDrive, en donde está el repositorio de trabajos entregados por los estudiantes de los desafíos de salvaguardia. Fuente: elaboración propia (2025)

- **Alianza de Responsabilidad (individual):** Los estudiantes redactaron cartas de compromiso en las que manifestaron su disposición a participar en las actividades de la EVA de forma ética y responsable. Este ejercicio permitió generar un sentido de pertenencia y establecer acuerdos iniciales de participación.
- **Conocimiento Seguro (individual):** Se implementó un foro académico en el cual los estudiantes analizaron noticias falsas y casos de ingeniería social. Las respuestas evidenciaron una evolución desde percepciones generales hacia argumentaciones críticas sobre la importancia de validar fuentes y reconocer intentos de manipulación digital.
- **Consejos de Seguridad (grupal):** Los estudiantes elaboraron organizadores gráficos que integraban riesgos tecnológicos y sus posibles medidas de mitigación. Esta actividad promovió la colaboración y fomentó la capacidad de sintetizar información técnica en un formato visual.

- **Riesgos Tecnológicos (grupal):** Se adaptó un artefacto tecnológico educativo (ATE) en forma de juego de carreras, en el cual los estudiantes construyeron circuitos con materiales reciclables. El juego simulaba amenazas del ciberespacio como obstáculos a esquivar, generando aprendizajes significativos mediante la gamificación.
- **Protocolo de Seguridad (grupal):** Para validar la competencia exigida por el MEN, los estudiantes diseñaron protocolos de seguridad digital. Estos no se limitaron a un documento formal, sino que incluyeron creaciones multimedia como podcasts, animaciones, canciones y videos, demostrando creatividad y apropiación del tema.
- **Reflexión Personal (individual):** Finalmente, los estudiantes redactaron cartas reflexivas dirigidas a sus pares de grados sexto y séptimo, en las que compartieron aprendizajes y recomendaciones para proteger la información personal y practicar una ciudadanía digital responsable. Estas cartas evidencian un progreso en el uso de un lenguaje técnico y ético en ciberseguridad.

**Nivel de compromiso y creatividad**

La participación de los estudiantes se caracterizó por un alto grado de creatividad y esfuerzo en la elaboración de productos digitales y escritos. A pesar de las dificultades de conectividad y acceso a la plataforma Moodle, los estudiantes buscaron alternativas de entrega en Classroom, garantizando la continuidad del proceso. Los productos finales muestran no solo comprensión conceptual, sino también apropiación crítica y ética de la competencia digital en seguridad y privacidad de la información.

***Apropiación del lenguaje técnico de Ciberseguridad con la intervención de la EVA***

Un propósito central de la implementación del EVA – Omniverso Digital consistió en promover la apropiación progresiva de un lenguaje técnico en ciberseguridad, articulado con el

desarrollo de la competencia digital en seguridad y privacidad.

Para cada una de las seis actividades del EVA, como lo fueron (cartas, foros, organizadores, protocolos, reflexiones, se realizó un conteo de las palabras más frecuentes vinculadas con la ciberseguridad, apoyado en la inteligencia artificial ChatGPT-5. Posteriormente, se construyeron *nubes de palabras* con la herramienta en línea WordArt (https://wordart.com/), De manera particular, para la actividad de Protocolo de Seguridad se utilizó la herramienta TurboScribe (https://turboscribe.ai/) con el fin de transcribir las entregas multimedia a texto

Los resultados evidencian una evolución clara: en las primeras actividades predominó un lenguaje cotidiano y descriptivo, mientras que en las últimas se incorporaron términos técnicos, reflexiones críticas y expresiones éticas propias de la competencia digital en seguridad y privacidad.

**Tabla 10**

*Evolución del lenguaje técnico en ciberseguridad a partir de las actividades del EVA – Omniverso Digital. Reto 1*

| **Actividad** | **Lenguaje predominante** | **Frecuencia de palabras clave de ciberseguridad más repetidas** | **Evidencia de evolución** |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1. Alianza de Responsabilidad (carta individual) | Expresiones generales: “responsabilidad”, “cuidar la información”, “uso correcto del internet”. | responsabilidad (15), información (12), internet (10), cuidado (8), compromiso (7) | Se reconoce la importancia de la seguridad, pero sin tecnicismos. |

*Nota*. Elaboración propia (2025) a partir del análisis de las cartas de compromiso estudiantiles

***Evidencias gráficas: Nubes de palabras por actividad***

**Figura 12.**

*Nube de palabras – Alianza de Responsabilidad.*




*Nota*. Fuente: Elaboración propia a partir de los productos estudiantiles, procesados con IA (ChatGPT-5) y representados en WordArt (2025).

**Tabla 11**

*Evolución del lenguaje técnico en ciberseguridad a partir de las actividades del EVA – Omniverso Digital. Reto 2*

| Actividad | Lenguaje predominante | Frecuencia de palabras clave de ciberseguridad más repetidas | Evidencia de evolución |
|---|---|---|---|
| 2. Conocimiento Seguro (foro individual sobre noticias falsas e ingeniería social) | Incorporación de nociones como noticias falsas, engaños, redes sociales. | noticias falsas (8), redes sociales (6), privacidad (5), engaño (5), seguridad (4) | Aparecen las primeras referencias a conceptos propios de la ciberseguridad. |

*Nota*. Elaboración propia (2025) construida a partir del foro académico sobre noticias falsas e ingeniería social, con categorización de palabras clave de ciberseguridad.

**Figura 13**

*Nube de palabras – Conocimiento Seguro*




*Nota*. Imagen generada a partir de los productos estudiantiles, procesados con IA (ChatGPT-5) y representados en WordArt (2025) Fuente: Elaboración propia (2025)

**Tabla 12**

*Evolución del lenguaje técnico en ciberseguridad a partir de las actividades del EVA – Omniverso Digital. Reto 3*

| **Actividad** | **Lenguaje predominante** | **Frecuencia de palabras clave de ciberseguridad más repetidas** | **Evidencia de evolución** |
|---|---|---|---|
| **3. Consejos de Seguridad (organizador gráfico grupal)** | Vocabulario más técnico: riesgos tecnológicos, contraseñas seguras, privacidad, verificación | Datos (10), Seguridad (8), Privacidad (7), Contraseñas (6), Robo de información/identidad (6), Malware/Virus (5), Phishing (4), Autenticación (4), Ciberacoso (3), Redes sociales (3) | Mayor claridad en la identificación de riesgos y medidas de mitigación |

*Nota*. Elaboración propia (2025) basada en la sistematización de los organizadores gráficos grupales elaborados por los estudiantes para identificar riesgos y medidas de seguridad digital.

**Figura 14**

*Nube de palabras – Consejos de Seguridad.*




*Nota*. Imagen elaborada a partir de los productos estudiantiles, procesados con IA (ChatGPT-5) y representados en WordArt (2025). Fuente: Elaboración propia (2025)

**Tabla 13**

*Evolución del lenguaje técnico en ciberseguridad a partir de las actividades del EVA – Omniverso Digital. Reto 4*

| Actividad | Lenguaje predominante | Frecuencia de palabras clave de ciberseguridad más repetidas | Evidencia de evolución |
|---|---|---|---|
| 4. Riesgos Tecnológicos (juego educativo tipo carrera de obstáculos) | Uso de términos como malware, nube, phishing, acceso seguro. | malware (6), nube (5), phishing (4), acceso (3), ataques (3), ciberespacio (2) | Se afianza un lenguaje más técnico al integrar amenazas concretas. |

*Nota*. Elaboración propia (2025) a partir de la adaptación del juego educativo de carreras de obstáculos, en el que se incorporaron amenazas y vocabulario técnico en ciberseguridad.

**Figura 15**
*Nube de palabras – Riesgos Tecnológicos*




*Nota*. Imagen generada a partir de los productos estudiantiles, procesados con IA (ChatGPT-5) y representados en WordArt (2025). Fuente: Elaboración propia (2025).

**Tabla 14**
*Evolución del lenguaje técnico en ciberseguridad a partir de las actividades del EVA – Omniverso Digital. Reto 5*

| Actividad | Lenguaje predominante | Frecuencia de palabras clave de ciberseguridad más repetidas | Evidencia de evolución |
|---|---|---|---|
| 5. Protocolo de Seguridad (creación multimedia) | Consolidación de expresiones técnicas: protocolo de seguridad, | protocolo (9), autenticación (6), huella digital (5), ciudadanía digital (5), | Se valida la competencia del MEN mediante creaciones críticas y |

| | | | |
|---|---|---|---|
| | autenticación, huella digital, ciudadanía digital. | protección (4), identidad digital (3), ética (3) | variadas (podcasts, videos, canciones). |

*Nota*. Elaboración propia (2025) construida a partir de los protocolos de seguridad digital creados por los estudiantes, con integración de expresiones técnicas y reflexiones críticas.

**Figura 16**

*Nube de palabras – Protocolo de Seguridad.*




*Nota*. Imagen generada a partir de los productos estudiantiles, transcriben el video a texto con TurboScribe, para procesados con IA (ChatGPT-5) y representados en WordArt (2025). Fuente: Elaboración propia (2025)

**Tabla 15**

*Evolución del lenguaje técnico en ciberseguridad a partir de las actividades del EVA – Omniverso Digital. Reto 6*

| Actividad | Lenguaje predominante | Frecuencia de palabras clave de ciberseguridad más repetidas | Evidencia de evolución |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 6. Reflexión Personal (carta a estudiantes de grados menores) | Lenguaje crítico y ético: protección de datos, riesgos personales, reputación digital, ética, ciudadanía digital. | protección de datos (8), riesgos (7), reputación digital (6), ética (6), ciudadanía digital (5), sospechoso (3), redes sociales (3) | Evidencia de apropiación técnica y de un discurso formativo hacia otros estudiantes. |

*Nota*. Elaboración propia (2025) a partir del análisis de cartas reflexivas escritas por los estudiantes para sus pares de grados menores, donde se evidencia apropiación crítica del lenguaje de ciberseguridad.

**Figura 17**

*Nube de palabras – Reflexión Personal.*




*Nota*. Imagen generada a partir de los productos estudiantiles, procesados con IA (ChatGPT-5) y representados en WordArt (2025). Fuente: Elaboración propia (2025)

**Resultados cuantitativos (ECDSPI)**

Los resultados cuantitativos obtenidos a través de la ECDSPI se presentan a continuación como un insumo complementario para la interpretación de los hallazgos cualitativos. Su

finalidad es identificar las variaciones en los niveles de competencia digital de los estudiantes antes y después de la intervención pedagógica desarrollada mediante el EVA Omniverso Digital.

El análisis se orientó a reconocer los avances en la competencia ciudadana digital relacionada con la seguridad, la privacidad y la gestión ética de la información en los estudiantes de educación media de la Institución Educativa Distrital San Cayetano, aportando evidencia cuantitativa que respalda y dialoga con los resultados cualitativos del estudio.

Los resultados, representados en doce tablas comparativas, evidencian que la categoría *"No puedo hacer esto"* descendió a cero, mientras que se redujeron las respuestas *"Puedo hacerlo con ayuda"* y *"Puedo hacerlo parcialmente solo"*. En contraste, las categorías *"Puedo hacerlo en su mayoría solo"*, *"Puedo hacerlo completamente solo"* y *"Soy experto en esto"* mostraron incrementos notables, reflejando un fortalecimiento progresivo de la autonomía y el pensamiento crítico en el manejo de la información digital.

Estos avances reafirman el desarrollo de la competencia digital ciudadana en seguridad y privacidad de la información, en coherencia con los lineamientos del *Ministerio de Educación Nacional (MEN, 2022)* y con los *Estándares ISTE para Estudiantes (2024)*, que promueven la gestión responsable, ética y segura de los datos personales. En conjunto, los resultados confirman el impacto positivo del *EVA Omniverso Digital* como una experiencia pedagógica que integra la gamificación, el aprendizaje activo y la reflexión ética, orientada a un uso crítico y seguro de la tecnología.

***Comparativo Pretest–Postest***

A continuación, se presentan los resultados del *postest* de la *ECDSPI*. Cada tabla compara los porcentajes del *pretest* y *postest*, e incluye una nota y un hallazgo interpretativo que resumen los avances observados en cada indicador.

**Tabla 16**

*Comparativo pretest–postest: "Puedo crear contraseñas seguras y complejas para proteger mi información personal"*

| Escala de respuesta | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| No puedo hacer esto | 8.7% | 0% | -8.7% |
| Puedo hacerlo con ayuda | 17.4% | 4.3% | -13.1% |
| Puedo hacerlo parcialmente solo | 17.4% | 8.7% | -8.7% |
| Puedo hacerlo en su mayoría solo | 30.4% | 30.4% | 0% |
| Puedo hacerlo completamente solo | 21.7% | 39.1% | +17.4% |
| Soy experto en esto | 4.3% | 17.4% | +13.1% |
| **Total** | **100%** | **100%** | — |

*Nota.* Pregunta 1 del instrumento *ECDSPI*: "Puedo crear contraseñas seguras y complejas para proteger mi información personal". Comparativo *Pretest–Postest*, con variaciones expresadas en porcentajes (%).

***Hallazgo**:* El número de estudiantes con dominio autónomo o experto en la creación de contraseñas aumentó del 26% al 56.5%. Este resultado **respalda** los cambios observados en las prácticas y reflexiones desarrolladas durante las actividades del EVA *Omniverso Digital*.

**Tabla 17**

*Comparativo pretest–postest: "Puedo verificar y modificar la configuración de privacidad en redes sociales y otras plataformas digitales"*

| Escala de respuesta | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| No puedo hacer esto | 13.0% | 0% | -13.0% |
| Puedo hacerlo con ayuda | 26.1% | 8.7% | -17.4% |
| Puedo hacerlo parcialmente solo | 21.7% | 8.7% | -13.0% |
| Puedo hacerlo en su mayoría solo | 26.1% | 30.4% | +4.3% |
| Puedo hacerlo completamente solo | 8.7% | 39.1% | +30.4% |

| | | | |
|---|---|---|---|
| Soy experto en esto | 4.3% | 13.0% | +8.7% |
| **Total** | **100%** | **100%** | — |

*Nota.* Pregunta 2 del instrumento *ECDSPI*: "Puedo verificar y modificar la configuración de privacidad en redes sociales y otras plataformas digitales". Comparativo *Pretest–Postest*, con variaciones expresadas en porcentajes (%).

*Hallazgo:* Los resultados muestran un avance sustancial en la autonomía para configurar la privacidad digital. El aumento del 39.1 % en la categoría *"Puedo hacerlo completamente solo"* y del 13 % en *"Soy experto en esto"* evidencia una apropiación más crítica de las herramientas de protección de datos personales y un mayor dominio técnico derivado de las actividades del *EVA Omniverso Digital*.

**Tabla 18**

*Comparativo pretest–postest: "Puedo identificar correos electrónicos o mensajes sospechosos (phishing) y evitar caer en estafas"*

| Escala de respuesta | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| No puedo hacer esto | 13.0% | 0% | -13.0% |
| Puedo hacerlo con ayuda | 21.7% | 4.3% | -17.4% |
| Puedo hacerlo parcialmente solo | 26.1% | 17.4% | -8.7% |
| Puedo hacerlo en su mayoría solo | 26.1% | 30.4% | +4.3% |
| Puedo hacerlo completamente solo | 13.0% | 34.8% | +21.8% |
| Soy experto en esto | 0% | 13.0% | +13.0% |
| Total | **100** | **100** | — |

*Nota.* Pregunta 3 del instrumento *ECDSPI*: "Puedo identificar correos electrónicos o mensajes sospechosos (phishing) y evitar caer en estafas". Comparativo *Pretest–Postest*, con variaciones expresadas en porcentajes (%).

*Hallazgo:* El dominio autónomo en la identificación de mensajes fraudulentos aumentó del 39 % al 78,2 %, mostrando un fortalecimiento importante en la detección de riesgos digitales y la conciencia sobre ciberfraudes.

**Tabla 19**

*Comparativo pretest–postest: "Puedo distinguir entre sitios web seguros y no seguros antes de ingresar mi información personal."*

| Escala de respuesta | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| No puedo hacer esto | 8.7 | 0 | -8.7 |
| Puedo hacerlo con ayuda | 21.7 | 4.3 | -17.4 |
| Puedo hacerlo parcialmente solo | 17.4 | 8.7 | -8.7 |
| Puedo hacerlo en su mayoría solo | 30.4 | 30.4 | 0 |
| Puedo hacerlo completamente solo | 17.4 | 34.8 | +17.4 |
| Soy experto en esto | 4.3 | 21.7 | +17.4 |
| **Total** | **100** | **100** | — |

*Nota.* Pregunta 4 del instrumento *ECDSPI*: "Puedo distinguir entre sitios web seguros y no seguros antes de ingresar mi información personal". Comparativo *Pretest–Postest* con variaciones expresadas en porcentajes (%).

*Hallazgo:* La capacidad de distinguir entre sitios web confiables y riesgosos aumentó del 43% al 86.9%, evidenciando un dominio más crítico de la navegación segura (uso de candado, HTTPS y verificación de URL).

**Tabla 20**

*Comparativo pretest–postest: "Puedo realizar copias de seguridad de mis archivos importantes para evitar su pérdida."*

| Escala de respuesta | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| No puedo hacer esto | 8.7% | 0% | -8.7% |
| Puedo hacerlo con ayuda | 21.7% | 8.7% | -13.0% |
| Puedo hacerlo parcialmente solo | 21.7% | 13.0% | -8.7% |
| Puedo hacerlo en su mayoría solo | 26.1% | 30.4% | +4.3% |

| | | | |
|---|---|---|---|
| Puedo hacerlo completamente solo | 17.4% | 26.1% | +8.7% |
| Soy experto en esto | 4.3% | 21.7% | +17.4% |
| **Total** | **100%** | **100%** | — |

*Nota.* Pregunta 5 del instrumento *ECDSPI*: "Puedo realizar copias de seguridad de mis archivos importantes para evitar su pérdida". Comparativo *Pretest–Postest* con variaciones expresadas en porcentajes (%).

*Hallazgo:* El grupo que respalda información con autonomía o dominio experto pasó de 47.8% a 78.2%, consolidando una práctica preventiva clave de gestión de la información personal.

**Tabla 21**

*Comparativo pretest–postest: "Puedo controlar qué información personal comparto en línea y en qué plataformas."*

| Escala de respuesta | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| No puedo hacer esto | 4.3% | 0% | -4.3% |
| Puedo hacerlo con ayuda | 13.0% | 4.3% | -8.7% |
| Puedo hacerlo parcialmente solo | 17.4% | 8.7% | -8.7% |
| Puedo hacerlo en su mayoría solo | 30.4% | 26.1% | -4.3% |
| Puedo hacerlo completamente solo | 26.1% | 39.1% | +13.0% |
| Soy experto en esto | 8.7% | 21.7% | +13.0% |
| **Total** | **100%** | **100%** | — |

*Nota.* Pregunta 6 del instrumento *ECDSPI*: "Puedo controlar qué información personal comparto en línea y en qué plataformas". Comparativo *Pretest–Postest* con variaciones expresadas en porcentajes (%).

*Hallazgo:* La autonomía para decidir qué compartir y con quién subió de 65.2% a 87%, reforzando conciencia de huella digital y criterios éticos en el *EVA Omniverso Seguro*.

***Tabla 22***

*Comparativo pretest–postest: "Puedo administrar de forma segura mis cuentas digitales y contraseñas."*

| Escala de respuesta | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| No puedo hacer esto | 8.7 | 0 | -8.7 |
| Puedo hacerlo con ayuda | 21.7 | 8.7 | -13.0 |
| Puedo hacerlo parcialmente solo | 21.7 | 13.0 | -8.7 |
| Puedo hacerlo en su mayoría solo | 26.1 | 34.8 | +8.7 |
| Puedo hacerlo completamente solo | 17.4 | 30.4 | +13.0 |
| Soy experto en esto | 4.3 | 13.0 | +8.7 |
| Total | **100** | **100** | — |

*Nota.* Pregunta 7 del instrumento *ECDSPI*: "Puedo administrar de forma segura mis cuentas digitales y contraseñas". Comparativo *Pretest–Postest*, con variaciones expresadas en porcentajes (%).

*Hallazgo:* El dominio autónomo en la administración de contraseñas pasó de 47,8 % a 78,2 %, consolidando la competencia de gestión segura de identidad digital, reforzada mediante prácticas guiadas en el *EVA Omniverso Seguro*.

**Tabla 23**

*Comparativo pretest–postest: "Puedo reconocer intentos de suplantación de identidad o perfiles falsos en línea."*

| Escala de respuesta | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| No puedo hacer esto | 8.7 | 0 | -8.7 |
| Puedo hacerlo con ayuda | 21.7 | 8.7 | -13.0 |
| Puedo hacerlo parcialmente solo | 26.1 | 13.0 | -13.1 |
| Puedo hacerlo en su mayoría solo | 26.1 | 30.4 | +4.3 |

| | | | |
|---|---|---|---|
| Puedo hacerlo completamente solo | 13.0 | 34.8 | +21.8 |
| Soy experto en esto | 4.3 | 13.0 | +8.7 |
| **Total** | **100** | **100** | — |

*Nota.* Pregunta 8 del instrumento *ECDSPI*: "Puedo reconocer intentos de suplantación de identidad o perfiles falsos en línea". Comparativo *Pretest–Postest*, con variaciones expresadas en porcentajes (%).

*Hallazgo:* El reconocimiento de perfiles falsos y suplantación aumentó de 43,4 % a 78 %, mostrando avances notables en el análisis crítico y la verificación de identidad digital. Los estudiantes fortalecieron su visión preventiva ante amenazas de *phishing social* y robo de identidad.

**Tabla 24**

*Comparativo pretest–postest "Puedo identificar aplicaciones o sitios que solicitan permisos innecesarios o riesgosos."*

| Escala de respuesta | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| No puedo hacer esto | 4.3 | 0 | -4.3 |
| Puedo hacerlo con ayuda | 17.4 | 4.3 | -13.1 |
| Puedo hacerlo parcialmente solo | 21.7 | 8.7 | -13.0 |
| Puedo hacerlo en su mayoría solo | 26.1 | 26.1 | 0 |
| Puedo hacerlo completamente solo | 21.7 | 39.1 | +17.4 |
| Soy experto en esto | 8.7 | 21.7 | +13.0 |
| **Total** | **100** | **100** | — |

*Nota.* Pregunta 9 del instrumento *ECDSPI*: "Puedo identificar aplicaciones o sitios web que solicitan permisos innecesarios o excesivos". Comparativo *Pretest–Postest*, con variaciones expresadas en porcentajes (%).

*Hallazgo:* El porcentaje de estudiantes capaces de identificar permisos innecesarios aumentó de 56,5 % a 87 %, evidenciando pensamiento crítico y lectura atenta de condiciones de

privacidad. Esta habilidad refleja la apropiación de estrategias de ciberseguridad práctica dentro del *EVA Omniverso Digital*.

***Tabla 25***

*Comparativo pretest–postest "Puedo aplicar medidas de seguridad en mis dispositivos (como contraseñas, antivirus o bloqueo de pantalla)."*

| Escala de respuesta | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| No puedo hacer esto | 4.3 | 0 | -4.3 |
| Puedo hacerlo con ayuda | 17.4 | 4.3 | -13.1 |
| Puedo hacerlo parcialmente solo | 21.7 | 8.7 | -13.0 |
| Puedo hacerlo en su mayoría solo | 26.1 | 26.1 | 0 |
| Puedo hacerlo completamente solo | 21.7 | 39.1 | +17.4 |
| Soy experto en esto | 8.7 | 21.7 | +13.0 |
| **Total** | **100** | **100** | — |

*Nota.* Pregunta 10 del instrumento *ECDSPI*: "Puedo implementar medidas de seguridad básicas en mis dispositivos, como el bloqueo de pantalla y el cifrado de datos.". Comparativo *Pretest–Postest*, con variaciones expresadas en porcentajes (%).

*Hallazgo:* El dominio autónomo en la aplicación de medidas de seguridad pasó de 56,5 % a 87 %, consolidando la protección activa de los dispositivos digitales. Los estudiantes interiorizaron rutinas de seguridad que fortalecen la prevención frente a ataques o pérdida de información.

**Tabla 26**

*Comparativo pretest–postest "Puedo mantener mis dispositivos y aplicaciones actualizados para protegerme de vulnerabilidades."*

| Escala de respuesta | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| No puedo hacer esto | 4.3 | 0 | -4.3 |
| Puedo hacerlo con ayuda | 17.4 | 8.7 | -8.7 |

| | | | |
|---|---|---|---|
| Puedo hacerlo parcialmente solo | 21.7 | 13.0 | -8.7 |
| Puedo hacerlo en su mayoría solo | 26.1 | 30.4 | +4.3 |
| Puedo hacerlo completamente solo | 21.7 | 30.4 | +8.7 |
| Soy experto en esto | 8.7 | 17.4 | +8.7 |
| **Total** | **100** | **100** | — |

*Nota.* Pregunta 11 del instrumento *ECDSPI*: "Puedo actualizar mis dispositivos y aplicaciones para mantenerme protegido contra las últimas amenazas de seguridad.". Comparativo *Pretest–Postest*, con variaciones expresadas en porcentajes (%).

*Hallazgo:* El porcentaje de estudiantes que actualiza sus dispositivos pasó del 56,5 % al 78 %, mostrando apropiación de prácticas de mantenimiento preventivo digital y fortalecimiento de la conciencia sobre vulnerabilidades tecnológicas.

**Tabla 27**

*Comparativo pretest–postest "Puedo reconocer y tomar medidas cuando siento que mi identidad en línea ha sido comprometida."*

| Escala de respuesta | Pretest (%) | Postest (%) | Variación (%) |
|---|---|---|---|
| No puedo hacer esto | 19 | 0 | -19 |
| Puedo hacerlo con ayuda | 19 | 5.6 | -13.4 |
| Puedo hacerlo parcialmente solo | 19 | 0 | -19 |
| Puedo hacerlo en su mayoría solo | 24 | 22.2 | -1.8 |
| Puedo hacerlo completamente solo | 5 | 33.3 | +28.3 |
| Soy experto en esto | 10 | 16.7 | +6.7 |
| **Total** | **100** | **100** | — |

*Nota.* Pregunta 12 del instrumento *ECDSPI*: *"Puedo reconocer y tomar medidas cuando siento que mi identidad en línea ha sido comprometida."*. Comparativo *Pretest–Postest*, con variaciones expresadas en porcentajes (%).

*Hallazgo:* La capacidad de reacción y autonomía ante incidentes de seguridad aumentó del 39 % al 72,2 %, evidenciando avances significativos en la gestión ética de la información, la seguridad digital y la acción responsable frente a las amenazas la gestión ética y la acción responsable frente a amenazas. Este avance refleja el impacto del *EVA Omniverso Seguro* como entorno formativo en ciberseguridad práctica y reflexión ética.

El análisis comparativo de los resultados del *pretest* y *postest* de la *ECDSPI* evidencia avances significativos en los estudiantes de media de la *Institución de Educación Distrital (IED) San Cayetano* tras la implementación del *EVA Omniverso Digital*.

Los resultados reflejan un incremento sostenido en las categorías *"Puedo hacerlo completamente solo"* y *"Soy experto(a) en esto"*, con variaciones positivas entre +13 % y +35 %. Este progreso confirma el impacto pedagógico del *EVA Omniverso Digital* en el fortalecimiento de la *Competencia Digital Ciudadana en Seguridad y Privacidad de la Información*, entendida por el *Ministerio de Educación Nacional (MEN, 2022)* y los *Estándares ISTE para Estudiantes (2024)* como la capacidad de comprender los riesgos del entorno digital, proteger la información propia y ajena, y actuar con ética, responsabilidad y pensamiento crítico en los entornos virtuales.

Tras la intervención, los estudiantes demostraron mayor autonomía en la gestión de contraseñas y cuentas, en la identificación de sitios confiables, en la aplicación de medidas de protección en dispositivos y en la respuesta ante incidentes digitales. Asimismo, se fortaleció la reflexión ética sobre el respeto, la privacidad y la responsabilidad compartida en el ecosistema digital.

En conjunto, estos resultados cuantitativos no se interpretan de manera aislada, sino que adquieren sentido al ser contrastados con las evidencias cualitativas del EVA, las reflexiones

estudiantiles y las nubes de palabras generadas a partir de las actividades desarrolladas, lo cual se profundiza en los apartados de triangulación. Desde esta integración, el EVA *Omniverso Digital* se consolida como una estrategia educativa innovadora que articula la tecnología con la formación ética y ciudadana, permitiendo que los estudiantes evolucionen de un conocimiento instrumental hacia una comprensión integral de la ciberseguridad y la privacidad digital, en coherencia con los lineamientos del Ministerio de Educación Nacional (MEN, 2022), los Estándares ISTE para Estudiantes (2024) y las demandas del mundo digital contemporáneo.

**Triangulación de la información**

La triangulación se constituyó en una estrategia metodológica clave para verificar la coherencia, complementariedad y validez de los datos obtenidos durante la investigación. De acuerdo con Benavides y Restrepo (2005), la triangulación se refiere al uso de diversos métodos, fuentes, teorías, momentos o expertos para analizar un fenómeno desde diferentes perspectivas, con el propósito de contrastar resultados y fortalecer la interpretación.

En la investigación *Omniverso Digital*, se implementaron cinco tipos de triangulación: de métodos, de sujetos, de momentos, de expertos y teórica; todas integradas en una triangulación múltiple.

El diseño metodológico combinó la información cuantitativa proveniente de la *ECDSPI* y la información cualitativa obtenida a través de la encuesta abierta de ciberseguridad y las evidencias generadas en el *EVA*, las cuales fueron representadas mediante nubes de palabras que sintetizaron las reflexiones y el lenguaje técnico de los estudiantes.

Este proceso permitió contrastar resultados, identificar coincidencias y diferencias, y comprender con mayor profundidad cómo se fortalecieron las competencias digitales en seguridad, privacidad y ética de los estudiantes de educación media.

***Integración de los tipos de triangulación en el análisis de resultados***

La triangulación de *métodos* contrastó los resultados numéricos de la *ECDSPI* con las respuestas cualitativas y las nubes de palabras del EVA, mostrando coherencia entre las mejoras porcentuales y el uso del lenguaje técnico.

La triangulación de *sujetos* integró las percepciones de estudiantes, docentes e investigadores, evidenciando consenso sobre los avances en ciberseguridad.

La triangulación de *momentos* permitió comparar los resultados del pretest y postest, mostrando progreso en la autonomía digital y en la comprensión de los riesgos.

La triangulación de *expertos* aseguró la validez de los instrumentos y los resultados mediante la revisión Inter pares, en la que los jueces académicos validaron tanto la *ECDSPI* como la estructura pedagógica y los contenidos del *EVA Omniverso Digital*.

Finalmente, la triangulación *teórica* articuló los marcos de competencia digital (MEN, 2022) y ciudadanía digital (Crompton y Burke, 2024), permitiendo interpretar los hallazgos desde un enfoque ético y social. En conjunto, estas modalidades configuran una triangulación múltiple que refuerza la validez metodológica y la coherencia interpretativa del estudio.

***Triangulación de casos representativos***

El análisis de la triangulación de casos representativos tiene como propósito integrar los resultados obtenidos desde diversas fuentes de información, con el fin de validar y enriquecer la interpretación de los hallazgos. A través de este proceso se contrastaron los datos cuantitativos de la *ECDSPI* con la información cualitativa proveniente de las encuestas abiertas, las nubes de palabras y las evidencias del EVA *Omniverso Digital*.

Cada tabla presentada a continuación sintetiza la relación entre las *fuentes de triangulación,* los *instrumentos o evidencias utilizadas,* los *resultados específicos observados* y

la *interpretación integrada de los hallazgos.* De esta manera, la triangulación de casos permite identificar la coherencia entre los datos y ofrecer una visión holística del impacto pedagógico del EVA en el fortalecimiento de la competencia digital en seguridad y privacidad de la información.

**Tabla 28**

*Caso 1. Reconocimiento de riesgos digitales (Phishing y enlaces falsos)*

| Fuente de triangulación | Fuente de información | Evidencia o resultado específico | Hallazgo |
|---|---|---|---|
| **Métodos** | Escala ECDSPI y encuesta abierta de ciberseguridad | Incremento del 33 % al 45 % en el reconocimiento de enlaces falsos; respuestas como “Verifico si el sitio tiene candado” y “No abro mensajes sospechosos”. | Coherencia entre el avance porcentual y las conductas preventivas descritas. Se evidencia apropiación del conocimiento sobre riesgos digitales. |
| **Datos** | Nubes de palabras generadas en el EVA | Predominan términos como *phishing*, *verificar*, *enlace*, *seguridad*. | Representación visual del cambio semántico y conceptual hacia un lenguaje técnico. |
| **Teórica** | Categorías de ciudadanía digital y seguridad en línea | Los estudiantes asocian la seguridad con la responsabilidad personal. | La teoría se refleja en la práctica: comprensión ética del riesgo digital. |

*Nota***.** Triangulación metodológica, de datos y teórica aplicada a la competencia de detección de riesgos digitales. Las evidencias del EVA se representaron mediante nubes de palabras que reflejan la evolución conceptual de los participantes.

**Tabla 29**

*Caso 2. Protección de la identidad y los datos personales*

| Fuente de triangulación | Fuente de información | Evidencia o resultado específico | Hallazgo |
|---|---|---|---|
| **Métodos** | Escala ECDSPI (ítem 4 y 6) y encuesta abierta | Incremento del 41 % al 62 % en "Mantengo mi información personal segura". Respuestas: "Uso autenticación doble" y "No comparto mis datos". | Coherencia entre la autoevaluación cuantitativa y las acciones concretas de protección de identidad. |
| **Datos** | Nubes de palabras del EVA | Términos frecuentes: *privacidad*, *identidad*, *contraseña*, *control*. | Evidencia visual del fortalecimiento conceptual en torno a la protección de la identidad digital. |
| **Investigadores** | Validación entre docentes coinvestigadores | Consenso en la categoría "protección de identidad digital". | Refuerzo de la confiabilidad interpretativa mediante revisión entre pares. |

***Nota*.** Triangulación de métodos, datos e investigadores. Las nubes de palabras del EVA sirvieron como representación semántica del aprendizaje y de las prácticas seguras en línea.

**Tabla 30**

*Caso 3. Ética y responsabilidad digital*

| Fuente de triangulación | Fuente de información | Evidencia o resultado específico | Hallazgo |
|---|---|---|---|
| **Métodos** | Escala ECDSPI y encuesta abierta | Mejora del 29 % al 58 % en "Reflexiono sobre el impacto de mis acciones en línea". Frases como "Pienso antes de publicar" o "Verifico antes de reenviar". | Evidencia de interiorización ética y pensamiento reflexivo sobre la huella digital. |
| **Datos** | Nubes de palabras del EVA | Palabras destacadas: *ética*, *responsabilidad*, *publicar*, *respeto*, *empatía*. | Representación del cambio discursivo hacia la responsabilidad y el respeto digital. |
| **Teórica** | Ciudadanía digital y ética del dato | Se integran valores de respeto, empatía y cuidado digital. | Coherencia entre el marco teórico y las prácticas observadas en el entorno virtual. |

***Nota*.** Triangulación metodológica, de datos y teórica. Las nubes de palabras evidencian la consolidación del discurso ético y la reflexión crítica sobre el comportamiento en línea.

**Tabla 31**

*Caso 4. Autonomía y autorregulación tecnológica*

| Fuente de triangulación | Fuente de información | Evidencia o resultado específico | Hallazgo |
|---|---|---|---|
| **Métodos** | Escala ECDSPI y observaciones docentes | Incremento del 38 % al 63 % en "Actúo con autonomía ante incidentes digitales". Las observaciones muestran resolución independiente de problemas. | Convergencia entre el desempeño medido y la actuación autónoma evidenciada. |
| **Datos** | Nubes de palabras del EVA | Conceptos frecuentes: *autonomía*, *resolver*, *decisión*, *seguridad*. | Representación semántica del desarrollo de la autonomía digital. |
| **Investigadores** | Revisión del equipo docente | Coincidencia en la categoría "autonomía digital responsable". | Reducción de sesgos interpretativos mediante revisión conjunta. |

***Nota.*** Triangulación de métodos, datos e investigadores. Las nubes de palabras reflejan la apropiación del concepto de autorregulación tecnológica y su práctica autónoma.

**Tabla 32**

*Caso 5. Comunicación y colaboración segura en línea*

| Fuente de triangulación | Fuente de información | Evidencia o resultado específico | Hallazgo |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **Métodos** | Escala ECDSPI y foros colaborativos | Incremento del 35 % al 57 % en “Trabajo colaborativamente en línea con respeto y seguridad”; se observó un lenguaje respetuoso y uso ético de recursos. | Correlación entre la percepción autoevaluada y la práctica comunicativa responsable. |
| **Datos** | Nubes de palabras del EVA | Términos destacados: *colaboración*, *respeto*, *equipo*, *comunicación*. | Reflejo visual del fortalecimiento de la *netiqueta* y la ética comunicativa. |
| **Teórica** | Ciudadanía digital y aprendizaje colaborativo | La colaboración en red se asocia con la responsabilidad colectiva y la convivencia ética. | Integración entre aprendizaje técnico, ético y social. |

***Nota*.** Triangulación de métodos, datos y teórica. Las nubes de palabras confirman la apropiación de competencias comunicativas seguras y colaborativas.

Los cinco casos triangulados confirman la coherencia transversal entre los resultados cuantitativos obtenidos mediante la *ECDSPI* y las evidencias cualitativas representadas en las nubes de palabras del EVA, de la encuesta de *Ciberseguridad*.

Los hallazgos reflejan un progreso integral en las dimensiones cognitiva, ética y actitudinal de la competencia digital, evidenciando la efectividad del *Omniverso Digital* como una estrategia formativa que promueve la seguridad, la autonomía y la ética digital.

La triangulación permitió consolidar una visión integral del aprendizaje, donde los datos

numéricos, los discursos reflexivos y las representaciones semánticas convergen en la formación de ciudadanos digitales conscientes, críticos y responsables.

***Interpretación pedagógica de los resultados***

Este capítulo presenta la *interpretación de los hallazgos obtenidos tras la implementación del proceso pedagógico* orientado al fortalecimiento de las *competencias digitales en seguridad y privacidad de la información* de los estudiantes de educación media de la *IED San Cayetano, colegio rural*.

El análisis se centra en *cómo el trabajo desarrollado en el EVA Omniverso Digital contribuyó a transformar las prácticas, actitudes y conocimientos digitales* de los participantes. Este entorno actuó como una *herramienta mediadora de aprendizaje*, que integró la gamificación, la reflexión ética y la autonomía digital para promover experiencias significativas de formación en ciberseguridad.

Los apartados siguientes presentan la *síntesis del proceso investigativo*, el *análisis de los resultados triangulados*, la *interpretación desde el modelo pedagógico* y las *limitaciones y desafíos* encontrados durante la implementación.

**Síntesis del proceso investigativo**

La investigación se desarrolló en un contexto rural que presenta desafíos particulares en materia de conectividad y acceso a la tecnología. En este escenario, el *EVA Omniverso Digital* se diseñó como una alternativa de aprendizaje que combina componentes de gamificación, reflexión ética y autonomía digital.

El proceso investigativo transitó desde un diagnóstico inicial —basado en la *ECDSPI* y la encuesta abierta de ciberseguridad— hacia la implementación de la propuesta educativa. Los resultados iniciales permitieron identificar brechas significativas entre la autopercepción de los

estudiantes y sus competencias técnicas reales en temas de seguridad digital. Mientras la mayoría manifestaba sentirse preparada para actuar con responsabilidad en línea, se evidenciaron vacíos en la detección de amenazas, la gestión de la identidad digital y la navegación segura.

Asimismo, se constató que el componente ético de la ciudadanía digital requería fortalecerse. Muchos estudiantes mostraron una disposición positiva frente a la responsabilidad y el respeto en entornos digitales, pero no siempre reconocían la importancia del consentimiento, la reputación o la privacidad como criterios esenciales para su comportamiento en línea. Estas observaciones sirvieron de base para orientar el diseño de la intervención educativa implementada en el *EVA Omniverso Digital*.

**Análisis e Interpretación de resultados triangulados**

La triangulación de métodos y fuentes permitió observar una evolución significativa en el pensamiento y las prácticas digitales de los estudiantes. El análisis comparativo entre el pretest y el postest mostró avances claros en la comprensión de conceptos de ciberseguridad y en la adopción de comportamientos más responsables en el entorno digital.

En el ámbito técnico, los resultados evidenciaron una mejora en la capacidad para reconocer intentos de *phishing*, enlaces falsos y suplantaciones de identidad. El porcentaje de estudiantes que afirmaron poder identificar por sí mismos mensajes fraudulentos pasó del 33 % al 45 %, mientras que la respuesta autónoma ante incidentes de identidad digital aumentó del 38 % al 63 %. Estos datos confirman un fortalecimiento de la competencia para la gestión de riesgos digitales.

En el plano ético y reflexivo, las respuestas cualitativas y las nubes de palabras generadas en el *EVA* reflejaron un cambio notable en el discurso de los estudiantes. Palabras como *ética*,

*responsabilidad*, *privacidad*, *colaboración* y *respeto* adquirieron mayor presencia, indicando la interiorización de un lenguaje técnico y moral vinculado a la ciudadanía digital.

La triangulación de momentos permitió evidenciar cómo, a lo largo del proceso, los estudiantes pasaron de un reconocimiento superficial del riesgo a una comprensión crítica del mismo. De igual forma, la triangulación de expertos —que incluyó la revisión Inter pares de los instrumentos y del *EVA Omniverso Digital*— aseguró la validez de los resultados y reforzó la coherencia metodológica de la investigación.

**Interpretación desde el modelo pedagógico**

La implementación del *EVA Omniverso Digital* se sustentó en el enfoque *conectivista*, el cual concibe el aprendizaje como un proceso distribuido, colaborativo y sustentado en redes de conocimiento. En este entorno, las misiones y desafíos propuestos en torno a la ciberseguridad favorecieron la exploración, la autonomía y la reflexión ética.

El uso de la gamificación permitió mantener altos niveles de motivación y compromiso entre los participantes, generando experiencias significativas de aprendizaje a través del juego, el error y la superación progresiva de retos. Este enfoque, combinado con los recursos interactivos del *EVA*, promovió un aprendizaje situado, contextualizado y pertinente para el contexto rural, en el que los estudiantes lograron apropiarse de nociones técnicas sin perder de vista el componente humano y social del uso de la tecnología.

Las evidencias del *EVA* —particularmente las nubes de palabras y los productos reflexivos— confirman que los estudiantes no solo adquirieron vocabulario técnico, sino que transformaron su manera de pensar sobre la seguridad, la privacidad y la ética digital, vinculando el conocimiento con su vida cotidiana.

# Capítulo VI. Conclusiones

Este capítulo presenta las conclusiones derivadas del proceso investigativo, construidas a partir del análisis integrado de los resultados obtenidos tras la implementación del EVA Omniverso Digital. De igual manera, se describen las principales limitaciones del estudio y se plantean recomendaciones orientadas a la mejora, proyección y sostenibilidad de la propuesta pedagógica en contextos educativos rurales.

## Conclusiones

La presente investigación analizó cómo una estrategia pedagógica fundamentada en el enfoque conectivista, implementada mediante el *EVA Omniverso Digital*, favoreció la apropiación de la competencia digital en seguridad y privacidad de la información en estudiantes de educación media de la *IED San Cayetano*, colegio rural de Bogotá. El proceso investigativo permitió articular la práctica docente con la reflexión crítica, el aprendizaje colaborativo y la exploración autónoma de los riesgos, responsabilidades y posibilidades que emergen en el entorno digital contemporáneo.

Desde el punto de vista metodológico, el estudio se desarrolló bajo un enfoque mixto con diseño dominante cualitativo, en el cual los resultados cuantitativos cumplieron una función de apoyo interpretativo. La aplicación del diseño cuasi-experimental de pretest y postest en un solo grupo, complementado con la Investigación-Acción Educativa de carácter etnográfico, posibilitó una comprensión integral del fenómeno educativo, permitiendo identificar transformaciones tanto en los niveles de competencia técnica como en las percepciones, actitudes y comportamientos de los estudiantes frente a la ciberseguridad y la ciudadanía digital.

En primer lugar, los resultados cuantitativos obtenidos mediante la Escala de Competencia Digital en Seguridad y Privacidad de la Información (ECDSPI) evidenciaron

avances significativos en los doce ítems evaluados. Las variaciones positivas registradas entre el pretest y el postest reflejan un fortalecimiento sostenido en las dimensiones de protección de datos personales, gestión de la identidad digital y reconocimiento y mitigación de amenazas. Estos resultados indican un incremento en los niveles de autonomía, confianza y dominio técnico de los estudiantes para actuar de manera segura y responsable en entornos digitales, validando el impacto pedagógico de la intervención desarrollada a través del EVA Omniverso Digital.

Más allá del dominio técnico, el análisis cualitativo permitió evidenciar una evolución progresiva en la conciencia ética y la responsabilidad social de los estudiantes. Esta transformación se manifestó en la apropiación de un lenguaje técnico vinculado a la privacidad, la huella digital, la autenticación y la seguridad de la información, así como en reflexiones críticas sobre el impacto de sus acciones en línea. Las producciones estudiantiles —cartas, foros, organizadores gráficos, protocolos y reflexiones— mostraron una mayor sensibilidad frente al respeto por la privacidad propia y ajena, y una creciente capacidad para transferir los aprendizajes adquiridos a situaciones reales de su vida cotidiana, evidenciando la apropiación de la competencia desde la dimensión del *saber ser*.

Asimismo, la investigación permitió constatar un fortalecimiento de la autonomía y la autorregulación digital, reflejado en una mayor seguridad para tomar decisiones informadas sobre qué información compartir, cómo protegerla y cómo actuar frente a situaciones de riesgo. Este tránsito desde un uso reactivo e intuitivo de la tecnología hacia prácticas digitales conscientes, críticas y responsables confirma que la competencia digital en seguridad y privacidad trasciende el manejo instrumental de herramientas y se configura como una construcción ética, social y ciudadana.

En este proceso, la gamificación, incorporada mediante la narrativa transmedia de *CyberShield* con desafíos, misiones e insignias, se consolidó como un mediador clave del aprendizaje significativo. Estas dinámicas promovieron la motivación, la cooperación y la autorregulación, favoreciendo la comprensión técnica, crítica y ética de la protección de los datos personales, la gestión de la identidad digital y los riesgos en línea. El Omniverso Digital no funcionó únicamente como un recurso tecnológico, sino como una herramienta formativa integral que articuló la reflexión ética con la práctica autónoma y colaborativa, permitiendo a los estudiantes transitar de un conocimiento intuitivo de la seguridad digital hacia una comprensión crítica y responsable de su participación en la red.

Desde una perspectiva pedagógica, el EVA Omniverso Digital, fundamentado en el conectivismo, la gamificación y la construcción colaborativa del conocimiento, demostró ser una estrategia pertinente, ética y sostenible para el desarrollo de competencias digitales en contextos rurales. Su diseño, alineado con los lineamientos del Ministerio de Educación Nacional (MEN, 2022) y los Estándares ISTE para Estudiantes, permitió integrar de manera **co**herente las dimensiones técnicas, éticas y sociales de la competencia digital, adaptando principios de la ciberseguridad —tradicionalmente asociados a ámbitos especializados— al contexto educativo escolar.

La efectividad del EVA en un entorno rural evidenció que las limitaciones de conectividad, acceso a dispositivos y condiciones socioculturales no constituyen impedimentos insalvables para el desarrollo de experiencias educativas significativas. El uso de estrategias flexibles, recursos accesibles y una narrativa cercana a la realidad del estudiantado posibilitó resultados relevantes, reafirmando el derecho de las comunidades rurales a una formación de calidad en ciberseguridad y ciudadanía digital.

## Limitaciones del Estudio

Durante la implementación del proyecto se presentaron diversas limitaciones de carácter tecnológico y sociocomunitario, como la conectividad irregular, la disponibilidad limitada de equipos y situaciones de tensión propias del contexto escolar. Estas circunstancias exigieron ajustes pedagógicos, estrategias mixtas y un acompañamiento constante para restablecer la motivación y el bienestar emocional de los estudiantes. Lejos de invalidar la experiencia, este contexto puso de manifiesto el papel de la escuela como espacio de resiliencia, reconstrucción del tejido social y promoción de una cultura de paz apoyada en la educación digital.

## Recomendaciones

A partir de los resultados obtenidos, se recomienda fortalecer el EVA Omniverso Digital como una herramienta institucional de aprendizaje en la IED San Cayetano, integrando de manera transversal la formación en ciberseguridad, ciudadanía digital y ética tecnológica en los diferentes niveles educativos. Asimismo, resulta pertinente ampliar la formación docente en competencias digitales y en enfoques pedagógicos basados en el conectivismo y la gamificación educativa, con el fin de garantizar la sostenibilidad y proyección del proyecto. A nivel investigativo, se sugiere extender la experiencia a otras instituciones rurales, evaluar su impacto a mediano y largo plazo, y analizar la transferencia de los aprendizajes al contexto familiar y comunitario.

En síntesis, el Omniverso Digital se consolida como una experiencia pedagógica transformadora que demuestra que la innovación educativa, cuando se fundamenta en la ética, la cooperación y la reflexión crítica, puede resignificar la relación entre tecnología, conocimiento y vida. Esta investigación evidencia que es posible habitar el ciberespacio desde la educación rural

colombiana con sentido humano, crítico y esperanzador, fortaleciendo la autonomía, la empatía y la responsabilidad social de los estudiantes en los entornos digitales contemporáneos.

## Referencias

Aguilar, G., Romero, A., García, L., y Núñez, A. (2022). Diseño de una secuencia didáctica y su virtualización. *Revista Boletín Redipe, 11*(12), 64-68. doi:https://doi.org/10.36260/rbr.v11i12.1923

Aguilar-Cruz, P., y Xiang, Z. (2023). Online Collaborative Learning: Connecting Classrooms Between China and Colombia in pandemic times. *Academia y Virtualidad, 16*(1), 91-105. doi:https://doi.org/10.18359/ravi.5929

Altamirano, A., Becerra, N., y Nava, A. (2010). Hacia una educación conectivista. *Revista Alternativa*(22), 22-32. Obtenido de https://www.researchgate.net/publication/264790115_Hacia_una_educacion_conectivista

Alvarez, E., Alvarez, B., Maycock, N., y Alvarez, K. (2022). El conectivismo, un nuevo paradigma para la educación. *South Florida Journal of Development, 3*, 361-379. doi:https://doi.org/10.46932/sfjdv3n1-028

Area, M., y Guarro, A. (2012). La alfabetización informacional y digital: fundamentos pedagógicos para la enseñanza y el aprendizaje competente. *Revista Española De Documentación Científica, 35 (Monográfico)*(1), 46-74. doi:https://doi.org/10.3989/redc.2012.mono.977

Barragán, R., y Murta, L. (2023). La seguridad en Internet como parte de la competencia digital ciudadana: Revisión sistemática. *Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología (TEyET), 36*, 1-12. doi:https://doi.org/10.1590/1983-3652.2024.51787

Basurto, S., Moreira, J., Velásquez, A., y Rodríguez, M. (2021). El conectivismo como teoría innovadora en el proceso de enseñanza-aprendizaje del idioma inglés. *Polo del*

*Conocimiento, 6*(1), 234-252. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=9438794

Bawden, D. (2008). Origins and concepts of digital literacy. En C. Lankshear, M. Knobel, C. Lankshear, y M. Knobel (Edits.), *Digital Literacies: Concepts, Policies and Practices* (págs. 17-32). Nueva York: Peter Lang Publishing.

Benavides, M., y Restrepo, C. (2005). Métodos en investigación cualitativa: Triangulación. *Revista Colombiana de Psicología, XXXIV*(1), 118-124. doi:https://www.redalyc.org/pdf/806/80628403009.pdf

Bernal, E. (2020). Aportes a la consolidación del conectivismo como enfoque pedagógico para el desarrollo de procesos de aprendizaje. *Revista Innova Educación, 2*(3), 394-412. doi:https://doi.org/10.35622/j.rie.2020.03.002

Cagüeño, D., y Cifuentes, J. (2022). Fortalecimiento del pensamiento geométrico mediante secuencia didáctica en el modelo educativo Escuela Nueva. *Revista Criterios, 29*(2), 143-160. doi:https://doi.org/10.31948/rev.criterios/29.2-art9

Calzada-Prado, J., y Marzal, M. (2013). Incorporating data literacy into information literacy programs: Core competencies and contents. *Libri, 63*(2), 123–134. doi:https://doi.org/10.1515/libri-2013-0010

Carretero, S., Vuorikari, R., y Punie, Y. (2017). *DigComp 2.1: El Marco de Competencia Digital para Ciudadanos con ocho niveles de competencia y ejemplos de uso.* Luxemburgo: Oficina de Publicaciones de la Unión Europea. EUR 28558 EN. doi:https://doi.org/10.2760/38842

Castells, M. (2006). *La sociedad red: Una visión global.* Madrid, España: Alianza Editorial.

Castillejos, B., Torres, C., y Lagunes, A. (2016). La seguridad en las competencias digitales de los millennials. *Apertura: Revista de Innovación Educativa, 8*(2), 54–69. doi:http://dx.doi.org/10.32870/Ap.v8n2.914

Cedeño, E., y Murillo, J. (2019). Entornos virtuales de aprendizaje y su rol innovador den el proceso de enseñanza. *Rehuso, 4*(1), 119-127. Obtenido de https://revistas.utm.edu.ec/index.php/Rehuso/workflow/submission/2156

Crompton, H., y Burke, D. (2024). The Nexus of ISTE Standards and Academic Progress: A Mapping. *TechTrends*(68), 711-722. doi:https://doi.org/10.1007/s11528-024-00973-y

Cueva, J., García, A., y Martínez, O. (2019). El conectivismo y las TIC: Un paradigma que impacta el proceso enseñanza aprendizaje. *Revista Scientific, 4*(14), 205-227. doi:https://doi.org/10.29394/Scientific.issn.2542-2987.2019.4.14.10.205-227

Cueva, T., Jara, O., Arias, J., Flores, F., y Balmaceda, C. (2023). *Métodos mixtos de investigación para principiantes.* Puno: Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú. doi:https://doi.org/10.35622/inudi.b.106

DeCarlo, M. (2018). *Investigación científica en trabajo social.* Richmond, VA: Open Social Work Education. Obtenido de https://pressbooks.pub/scientificinquiryinsocialwork/

Deterding, S., Dixon, D., Khaled, R., y Nacke, L. (2011). From game design elements to gamefulness: Defining "gamification". *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, 9-15. Obtenido de https://uwaterloo.ca/scholar/sites/ca.scholar/files/lnacke/files/From_game_design_elements_to_gamefulness-_defining_gamification.pdf

Downes, S. (03 de Febrero de 2007). *What Connectivism Is.* Obtenido de Half An Hour: https://halfanhour.blogspot.com/2007/02/what-connectivism-is.html

European Union Agency for Cybersecurity (ENISA). (2025). *ENISA Threat Landscape.* Brussels: European Union Agency for Cybersecurity. doi: 10.2824/2445233

Expedición Rural. (2023). MURALISTAS Colegio San Cayetano (IED) "San Cayetano, cuidemos el agua, cultivemos nuestra mente.". *Expedición Rural 2023*. Obtenido de https://educacionruralbogota.org/index.php/colegio-san-cayetano-ied/

Galbin, A. (2011). Developing digital competence: An essential skill in remote learning. *Journal of Educational and Social Research, 11*(4), 74-83. doi:https://doi.org/10.20472/IAC.2020.056.002

Gallego, R. (2017). Antecedentes para el diseño de una nueva estrategia didáctica y de comunicación para el e-learning. *Razón y Palabra, 21*(98), 51-65. Obtenido de http://www.redalyc.org/articulo.oa?id=199553113005

Garmendia, M., Martínez, G., Larrañaga, N., y Jiménez, E. (2024). *Competencia digital docente, ciberseguridad y convivencia digital del alumnado en Educación Primaria y Secundaria.* Bilbao (España): SIC□Spain 3.0. (UE) y Universidad del País Vasco (UPV/EHU). Obtenido de https://www.researchgate.net/publication/381160011_Competencia_digital_docente_ciberseguridad_y_convivencia_digital_del_alumnado_en_Educacion_Primaria_y_Secundaria

Goldie, J. (2016). Connectivism: A knowledge learning theory for the digital age? *Medical Teacher, 38*(10), 1064-1069. doi: https://doi.org/10.3109/0142159X.2016.1173661

Gutiérrez, L. (2012). Conectivismo como teoría de aprendizaje: conceptos, ideas, y posibles limitaciones. *Educación y Tecnología*(1), 111-122. doi:https://revistas.umce.cl/index.php/edytec/article/view/39

Hernández, R., Fernández, C., y Baptista, P. (2014). *Metodología de la investigación (6.ª ed.).* México D.F: McGraw-Hill Education. Obtenido de https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf

IED San Cayetano (Dirección). (2023). *San Cayetano, formando seres sensibles, críticos y competentes* [Película]. Obtenido de https://youtu.be/x4QAjZ-Oqrc?si=KgnIHRbOlxWGHXbF

Jurkowski, S., Mundelsee, L., y Hänze, M. (2024). Strengthening collaborative learning in secondary school: Development and evaluation of a lesson-integrated training approach for transactive communication. *Learning and Instruction, 92*, 101934. doi:https://doi.org/10.1016/j.learninstruc.2024.101934

Katz, J., y Rice, R. (2002). Consecuencias sociales del uso de Internet. *Athenea Digital*, 276-278. Obtenido de https://www.researchgate.net/publication/30067182_KatzJ_E_y_RiceR_E_Consecuencias_sociales_del_uso_de_Internet

López, D. (2017). Diseño e implementación de una secuencia didáctica para la enseñanza del concepto de elemento químico. *Praxis y Saber, 11*(27). doi:https://doi.org/10.19053/22160159.v11.n27.2020.11116

Marrón, Y., y Martínez, M. (2023). Características de la acreditación de la Competencia Digital Docente. Relaciones con la Competencia Digital del alumnado. *Edutec, Revista Electrónica De Tecnología Educativa*(86), 184-202. doi:https://doi.org/10.21556/edutec.2023.86.2943

Ministerio de Educación Nacional. (2022). Orientaciones curriculares para el área de tecnología e informática en educación media y básica.

Ministerio de Tecnologías de la Información y Comunicaciones de Colombia - MinTic. (2021). 'En TIC Confío+': una década informando a niños y jóvenes sobre los riesgos en Internet. Obtenido de https://mintic.gov.co/portal/inicio/Sala-de-prensa/182632:En-TIC-Confio+-una-decada-informando-a-ninos-y-jovenes-sobre-los-riesgos-en-Internet

Muñoz, D., y Mora, M. (2021). Consolidación de competencias digitales en docentes de la IED MIGUEL SAMPER AGUDELO a través de un entorno virtual de aprendizaje en modalidad e-learning. Obtenido de http://hdl.handle.net/11349/29381

National Institute of Standards and Technology (NIST). (2024). *The NIST Cybersecurity Framework (CSF) 2.0* . Gaithersburg: U.S. Department of Commerce. doi:https://doi.org/10.6028/NIST.CSWP.29

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (2019). *Marco de competencias de los docentes enmateria de TIC UNESCO* (Vol. Versión 3). Paris: UNESCO. Obtenido de https://unesdoc.unesco.org/ark:/48223/pf0000371024

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (2022). Competencias TIC para docentes según UNESCO. *Profuturo*. Obtenido de https://profuturo.education/observatorio/competencias-xxi/competencias-tic-para-docentes-segun-unesco/

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (2023). *Reimagining Our Futures Together: A New Social Contract for Education.* París,

Francia: UNESCO Publishing. Obtenido de https://unesdoc.unesco.org/ark:/48223/pf0000379707

Pertegal, M., y Lorenzo, G. (2019). Gamificación en el aula a través de las TIC. *International Journal of Developmental and Educational Psychology INFAD Revista de Psicología, 3*(1), 553-562. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7376150

Restrepo, M. (2023). Ambientes de Aprendizaje desde la Biblioteca Escolar para el Siglo XXI: Retos y Desafíos. Obtenido de http://hdl.handle.net/10554/66530

Rodríguez, J. (2005). *La investigación-acción educativa: Paradigmas y enfoques en la investigación educativa.* Lima: ali arte gráfico publicaciones s.r.l. (auspiciado por DOXA). Obtenido de https://hdl.handle.net/20.500.14005/1358

Sanchez, R., Costa, Ó., Mañoso, L., Novillo, M., y Pericacho, F. (2019). Orígenes del conectivismo como nuevo paradigma del aprendizaje en la era digital. *Educación y Humanismo, 21*(36), 113-136. doi:https://doi.org/10.17081/eduhum.21.36.3265

Schwarz, S., Bieg, T., Svecnik, E., Schmölz, A., Geppert, C., y Gerdenitsch, C. (2024). Digital Competence Scale (DCS), A Short Self-Assessment Instrument for Measuring Digital Competences. *Nordic Journal of Digital Literacy, 19*(3), 126-143. doi:https://www.idunn.no/doi/10.18261/njdl.19.3.2

Secretaria de Educación. (2021). Por primera vez, ‘Al colegio en bici’ operará en una zona rural de Bogotá. Obtenido de https://www.educacionbogota.edu.co/portal_institucional/index.php/noticia/por-primera-vez-al-colegio-en-bici-operara-en-una-zona-rural-de-bogota

Selwyn, N. (2021). *Education and Technology: Key Issues and Debates (3rd ed.).* Londres: Bloomsbury Academic.

Siemens, G. (2005). Connectivism: A learning theory for the digital age. *International Journal of Instructional Technology and Distance Learning, 2*(1), 3-10. Obtenido de http://www.itdl.org/Journal/Jan_05/article01.htm

Tejada, J. (2000). La Educación en el Marco de una Sociedad Global: Algunos Principios y Nuevas Exigencias. *Profesorado. Revista de Currículum y Formación de Profesorado, 4*(1), 1-13. Obtenido de http://www.redalyc.org/articulo.oa?id=56751266002

Torres, J., y Barnabé, T. (2020). Aspectos pedagógicos del conectivismo y su relación con redes sociales y ecologías del aprendizaje. *Revista Brasilera de Educação, 25*(1), 1-22. doi:https://doi.org/10.1590/S1413-24782020250026

Tumino, M., y Bournissen, J. (2016). Conectivismo: Hacia el nuevo paradigma de la enseñanza por competencias. *European Scientific Journal, 12*(10), 112-125. doi:https://doi.org/10.19044/esj.2016.v12n10p112

Turpo-Gebera, O., Zea-Urviola, M., Huamaní-Portilla, F., Girón-Pizarro, M., Pérez-Zea, A., y Aguaded-Gómez, I. (2023). Media and information literacy in secondary students: Diagnosis and assessment. *Journal of Technology and Science Education (JOTSE), 13*(2), 514–531. doi:https://doi.org/10.3926/jotse.1746

UNICEF. (2016). Estado mundial de la infancia 2016: Una oportunidad para cada niño. Obtenido de https://www.unicef.org/reports/state-worlds-children-2016

Van Dirk, J. (2020). *The digital divide.* Cambridge, Reino Unido: Polity Press.

Vuorikari, R., Kluzer, S., y Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens – With new examples of knowledge, skills and attitudes.* Luxemburgo: Publications Office of the European Union. doi:https://doi.org/10.2760/115376

Zabala, A., y Arnau, L. (2007). La enseñanza de las competencias. *Innivación Educativa*(161), 40-46. Obtenido de https://biblioteca.marco.edu.mx/files/Educacion%20Basada%20en%20Competencias/8-Formaci%C3%B3n%20por%20Competencias/La%20ensenanza%20de%20las%20Competencias.pdf

Zhao, A., Pinto, A., y Cruz, M. (2021). Digital competence in higher education research: A systematic literature review. *Computers y Education, 168*, 104212. doi:https://doi.org/10.1016/j.compedu.2021.104212