UNIVERSIDAD NACIONAL DE CHIMBORAZO

VICERRECTORADO DE INVESTIGACIÓN, VINCULACION Y POSGRADO

DIRECCIÓN DE POSGRADO

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE:

MAGISTER EN EDUCACIÓN MENCIÓN GESTIÓN DEL APRENDIZAJE MEDIADO POR TIC.

TEMA:

DESAFÍOS ÉTICOS EN LA GESTIÓN DEL APRENDIZAJE MEDIADO POR TIC. PRIVACIDAD, SEGURIDAD Y EQUIDAD

AUTORA:

Lic. Mayra Araceli Villacrés Obregón

TUTOR:

Mgs. Leonardo Ayavaca Vallejo

Riobamba – Ecuador 2025

Certificación del Tutor

Certifico que el presente trabajo de titulación denominado: **DESAFÍOS ÉTICOS EN LA GESTIÓN DEL APRENDIZAJE MEDIADO POR TIC. PRIVACIDAD, SEGURIDAD Y EQUIDAD** ha sido elaborado por la maestrante **Mayra Araceli Villacrés Obregón**, el mismo que ha sido orientado y revisado con el asesoramiento permanente de mi persona en calidad de Tutor. Así mismo, refrendo que dicho trabajo de titulación ha sido revisado por la herramienta antiplagio institucional; por lo que certifico que se encuentra apto para su presentación y defensa respectiva.

Es todo cuanto puedo informar en honor a la verdad.

Riobamba, 24 de marzo de 2025.

Mgs. Leonardo Ayavaca Vallejo

TUTOR

Declaración de Autoría y Cesión de Derechos

Yo, **Mayra Araceli Villacrés Obregón**, con número único de identificación 0602141459, declaro y acepto ser responsable de las ideas, doctrinas, resultados y lineamientos alternativos realizados en el presente trabajo de titulación denominado: "**DESAFÍOS ÉTICOS EN LA GESTIÓN DEL APRENDIZAJE MEDIADO POR TIC. PRIVACIDAD, SEGURIDAD Y EQUIDAD"** previo a la obtención del grado de Magíster en Educación, mención Gestión del Aprendizaje mediado por TIC.

- Declaro que mi trabajo investigativo pertenece al patrimonio de la Universidad Nacional de Chimborazo de conformidad con lo establecido en el artículo 20 literal j) de la Ley Orgánica de Educación Superior LOES.
- Autorizo a la Universidad Nacional de Chimborazo que pueda hacer uso del referido trabajo de titulación y a difundirlo como estime conveniente por cualquier medio conocido, y para que sea integrado en formato digital al Sistema de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor, dando cumplimiento de esta manera a lo estipulado en el artículo 144 de la Ley Orgánica de Educación Superior LOES.

Riobamba, 24 de marzo de 2025

Lic. Mayra Araceli Villacrés Obregón

N.U.I. 060214145-9

Agradecimiento

En este momento de culminación académica, quiero expresar un agradecimiento profundo a mi tutor y mis docentes quienes, con sus orientaciones y conocimientos, además de su comprensión y confianza, han sido fundamentales para llevar a buen puerto este proceso formativo en mi vida.

Gracias por ser una guía constante en esta etapa. Gracias por enseñarme que la sabiduría se alcanza con suficiente paciencia, y que la educación debe mirar más allá de los paradigmas establecidos.

A cada uno de ellos, mi reconocimiento y absoluto respeto por su capacidad de transmitir no únicamente contenido académico, sino también, los valores éticos y principios que rigen al educador y al ser humano, Sus ideales han marcado para siempre mi crecimiento personal y profesional.

Al Mgs. Leonardo Ayavaca, mi Docente Tutor, mi gratitud constante por compartir su conocimiento de manera incondicional, y generar la confianza suficiente en mí, para aprender a creer y alcanzar mis metas. Espero que este logro sea el reflejo de su labor excepcional como educador.

Agradezco también a las instituciones que hicieron posible el desarrollo de esta investigación, facilitando los recursos y espacio necesarios para llevarla a cabo.

Finalmente, mi reconocimiento sincero a todas aquellas personas que, de manera directa o indirecta, aportaron con su conocimiento, apoyo y gestos de ánimo. Han sembrado de gratitud mi alma.

Dedicatoria

Quiero dedicar este logro a mi familia, mi mayor fortaleza. A mis padres, por inculcarme desde siempre el amor por el aprendizaje; a mis hermanos por creer en mí incluso en los momentos más inciertos y por enseñarme con su ejemplo que la perseverancia y el esfuerzo siempre rinden frutos. A mi esposo e hijos, quienes con su apoyo incondicional y palabras de ánimo hicieron que cada desafío pareciera más llevadero. Gracias por ser una fuente de inspiración y motivación, su apoyo ha sido clave para la culminación de este proyecto.

INDICE DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

Resumen

El rápido avance de las tecnologías de la información y comunicación (TIC) y su integración en la educación han transformado significativamente la forma de impartir clases, pero también han generado importantes desafíos éticos en su uso. El objetivo de esta investigación es la de examinar las amenazas y vulnerabilidades de seguridad en plataformas de aprendizaje, así como las pautas éticas y protocolos de uso para educadores y estudiantes en el acceso a las tecnologías educativas. La metodología utilizada en este estudio se basó en un enfoque cualitativo mediante el análisis bibliográfico a través de la recopilación de fuentes científicas relevantes sobre el tema. Se identifica que las plataformas de educación en línea tienen varios problemas relacionados con la privacidad y la seguridad de los datos, como el robo de información y la exposición de datos sensibles tanto de estudiantes como de profesores, así como la conciencia sobre las prácticas de seguridad informática es prácticamente inexistente.

Palabras Claves: Tecnologías de la Información y la Comunicación (TIC), Tecnología educativa, Éticas, Protocolos, Aprendizaje Digital, Metaverso.

Abstract

The rapid advancement of information and communication technologies (ICTs) and their integration into education have significantly transformed how classes are taught. However, they have also generated significant ethical challenges in their use. This research aims to examine security threats and vulnerabilities of learning platforms, as well as ethical guidelines and usage protocols for educators and students when accessing educational technologies. The methodology used in this study was based on a qualitative approach using bibliographic analysis through the collection of relevant scientific sources on the topic. It was identified that online education platforms have several issues related to privacy and data security, such as information theft and exposure of sensitive data of both students and teachers and awareness of cybersecurity practices is practically nonexistent. The digital transformation of education has been a major catalyst in how we teach and learn today.

Keywords: Information and communication technologies (ICT), educational technology, ethics, protocols, digital learning, metaverse.

Reviewed by:

Ms.C. Ana Maldonado León

ENGLISH PROFESSOR

C.I.0601975980

Introducción

La integración de las Tecnologías de la Información y la Comunicación (TIC) en la educación ha marcado un punto de inflexión en los procesos de enseñanza y aprendizaje. Desde su surgimiento, las TIC han sido promovidas no solo como herramientas complementarias, sino que transforman la experiencia educativa, ofreciendo nuevas oportunidades para la personalización de la enseñanza, el acceso a recursos globales y la interacción en tiempo real entre estudiantes y docentes. Plataformas de aprendizaje en línea, aplicaciones educativas, recursos multimedia interactivos y la inteligencia artificial son solo algunos ejemplos de cómo las TIC han reconfigurado el panorama educativo (Suárez Álvarez et al., 2020).

Cabe recalcar que ese fenómeno no está exento de controversias y preocupaciones, a medida que las TIC se integran más profundamente en los entornos educativos, emergen una serie de desafíos éticos que cuestionan la forma en que estas tecnologías deben ser utilizadas y gestionadas (Suárez-Guerrero y Lloret-Catalá, 2022). Uno de los principales desafíos es la privacidad y la protección de los datos personales de los estudiantes. Las plataformas de aprendizaje en línea recolectan grandes cantidades de información, desde datos demográficos hasta registros detallados de desempeño y comportamiento en línea. La gestión y protección de esta información es crítica, ya que cualquier brecha de seguridad podría tener graves consecuencias para los estudiantes y las instituciones (Suárez Álvarez et al., 2020).

Otro aspecto ético de gran relevancia es la equidad en el acceso a la tecnología, aunque las TIC tienen el potencial de democratizar la educación, también existe el riesgo de que amplíen las brechas existentes entre diferentes grupos socioeconómicos. La falta de acceso a dispositivos,

conectividad adecuada o competencias digitales pueden provocar exclusión educativa, perpetuando e incluso agravando desigualdades sociales (Paz Saavedra y Gisbert Cervera, 2020).

Hoy en día el uso de inteligencia artificial en la educación plantea también importantes dilemas éticos, si bien la inteligencia artificial brinda soluciones personalizadas y adaptativas, preocupa que su implementación pueda deshumanizar la educación, al depender excesivamente de algoritmos que podrían replicar o reforzar sesgos existentes. Además, se incluye la opacidad de algunos algoritmos y la falta de transparencia en cómo se toman decisiones basadas en inteligencia artificial generan desconfianza y dudas alrededor de la equidad y justicia de estos sistemas (Paz Saavedra y Gisbert Cervera, 2020).

La protección de la propiedad intelectual en un entorno digital es otro desafío que no puede ser ignorado. La facilidad con la que los recursos educativos digitales pueden ser compartidos y reproducidos plantea interrogantes sobre los derechos de autor y la justa compensación de los creadores de contenido, esto es particularmente relevante en un contexto donde la educación abierta y los recursos educativos abiertos (REA) ganan popularidad como herramientas de enseñanza (Castro Rodríguez, 2020). La relación entre tecnología y pedagogía también está en el centro de las preocupaciones éticas. La adopción de TIC en el ámbito educativo debe alinearse con objetivos pedagógicos claros en lugar de basarse únicamente por la disponibilidad tecnológica. Existe el riesgo de que, en la búsqueda de innovación, se implementen soluciones tecnológicas que no mejoren necesariamente la calidad educativa y, en algunos casos, desvíen la atención de lo que realmente importa: el aprendizaje significativo de los estudiantes (Novas, 2022).

En este contexto, la presente investigación propone analizar en profundidad los desafíos éticos que surgen en la gestión de la instrucción educativa mediada por las TIC. El análisis no se

centrará en identificar y categorizar los desafíos, sino que también explorará las posibles soluciones y buenas prácticas que deben adoptarse para mitigar los riesgos éticos, además, se evaluarán las políticas y normativas actuales que regulan el uso de TIC en la educación, con el fin de proponer recomendaciones que contribuyan a una gestión más ética y efectiva en la era digital (Novas, 2022).

Con este objetivo, la investigación se estructura en varios capítulos que abordarán el marco teórico y conceptual de los desafíos éticos de la problemática. Al final, se espera que los hallazgos de esta investigación no solo enriquezcan el entendimiento académico sobre el tema, sino que también ofrezcan herramientas prácticas para docentes, administradores educativos y responsables de políticas, en su esfuerzo por gestionar de manera ética el proceso educativo mediado por las TIC.

CAPÍTULO 1. Generalidades

1.1. Planteamiento del problema

Como lo expresa (Carissa, 2020), la privacidad es un concepto que abarca, entre otras cosas, el derecho a la libertad de pensamiento, control sobre nuestro cuerpo, soledad en nuestro hogar, control sobre la información personal, el derecho a no ser vigilado, protección a la reputación y protección de pesquisas e interrogatorios. A medida que las instituciones educativas adoptan plataformas digitales y herramientas tecnológicas para mejorar la experiencia de aprendizaje, surgen interrogantes sobre la privacidad de los datos de los estudiantes, la seguridad de la información y la equidad en el acceso y uso de estas tecnologías.

Este fenómeno ha generado un contexto en el cual se requiere una comprensión profunda de los dilemas éticos inherentes, así como la formulación de estrategias y protocolos que permitan abordar estos desafíos de manera efectiva. Ante este panorama, surge la necesidad de una investigación exhaustiva que analice de manera integral los aspectos éticos relacionados con la gestión del aprendizaje mediado por TIC, con el objetivo de proporcionar orientaciones sólidas y promover prácticas responsables en el ámbito educativo digital (Cortés-Nájera, 2022).

En este contexto este problema se origina debido a la rápida evolución de las prácticas educativas hacia entornos digitales y en línea, que plantean cuestiones éticas significativas que deben abordarse de manera efectiva para garantizar una educación inclusiva, segura y equitativa para todos los estudiantes. Si bien, no hay una receta que solucione la problemática y se erradiquen de tajo las prácticas de deshonestidad académica, si se pueden realizar acciones y estrategias que coadyuven con el fortalecimiento de los valores y las buenas prácticas académicas. La ética y los patrones morales adoptados en la conducta profesional serán en gran medida el resultado del cruce

de influencias provenientes de la educación familiar, de la cultura nacional y organizacional de tolerancia al fraude (Orozco y lamberto, 2022).

Estos desafíos incluyen preocupaciones sobre la protección de datos personales de los estudiantes, el riesgo de violaciones de privacidad y el uso indebido de la información, así como la seguridad de los sistemas de información educativa frente a amenazas cibernéticas. Además, surge la necesidad de garantizar un acceso equitativo a la tecnología educativa para todos los estudiantes, independientemente de su ubicación geográfica o situación socioeconómica.

Para abordar estos desafíos éticos de manera integral y proactiva, es fundamental desarrollar un marco normativo que proteja la privacidad de los datos de los estudiantes, garantice la seguridad de los sistemas de información educativa y promueva la equidad en el acceso y uso de la tecnología educativa. Esto permitirá una transformación digital educativa más ética, inclusiva y centrada en el estudiante, con beneficios tangibles para el aprendizaje y el desarrollo en la era digital, especialmente en un mundo donde la interconectividad y la acumulación de información son esenciales para el desenvolvimiento social (Rodríguez Samudio, 2019)..

1.2. Preguntas de investigación

¿Cuáles son las principales amenazas y vulnerabilidades de seguridad en las plataformas de aprendizaje en línea, y qué estrategias pueden implementarse para mitigar estos riesgos y proteger la integridad de la información?

¿Cuáles son los factores que impiden el acceso en el uso de las tecnologías educativas, y qué estrategias pueden implementarse para reducir las brechas digitales y promover la equidad en el aprendizaje digital?

¿Cuáles son las leyes vigentes para proteger la privacidad de los estudiantes en el contexto de la transformación digital educativa?

1.3. Contexto y justificación del estudio.

La implementación de las tecnologías de la comunicación ha transformado significativamente la forma en que hoy se imparten y reciben conocimientos a través de plataformas de aprendizaje y herramientas digitales en el aula, facilitando la participación y la expansión de la educación. Sin embargo, este avance trae consigo una serie de desafíos éticos que merecen una atención cuidadosa (Martín Fernández et al., 2022).

Desde la última década, la educación mediada por las TIC ha cobrado un protagonismo creciente, facilitando el acceso a recursos educativos, la personalización del aprendizaje y la colaboración en entornos virtuales. Sin embargo, esta evolución tecnológica también plantea una serie de desafíos éticos que requieren una atención particular. El plagio de trabajos académicos entre estudiantes es una problemática frecuente en casi todos los niveles educativos, esta acción lacera la adquisición de aprendizajes significativos porque interrumpe los procesos cognitivos más profundos para la asimilación y acomodación de los contenidos (Martín Fernández et al., 2022).

1.4. Objetivos

General

- Desarrollar pautas éticas y protocolos para educadores, estudiantes, y demás actores involucrados en la gestión del aprendizaje digital promoviendo prácticas responsables y transparentes.

Específicos

- Examinar las amenazas y vulnerabilidades de seguridad en plataformas de aprendizaje en línea, con el propósito de diseñar estrategias para mitigar riesgos y fortalecer la protección de la información.
- Analizar las disparidades en el acceso y uso de tecnologías educativas, con el fin de proponer estrategias para reducir brechas y fomentar la equidad en el aprendizaje digital.
- Examinar las leyes existentes en la protección de la información dentro de las diferentes plataformas de aprendizaje.

CAPITULO 2. Marco teórico

2.1. Desafíos Éticos Iniciales

Inicialmente los estudios sobre la implementación de las TIC en la educación se centraron en cuestiones de acceso y equidad. La brecha digital, que se refiere a la desigualdad en el acceso a dispositivos e internet, fueron identificadas como un problema ético significativo, particularmente en países en desarrollo y en comunidades marginadas. La falta de acceso adecuado no solo limita las oportunidades de aprendizaje, sino también exacerba las desigualdades existentes en la sociedad actual (Mariscal San Martin et al., 2022).

2.2. Privacidad y Seguridad de la Información

Con el avance de las plataformas educativas digitales, la privacidad y la seguridad de la información emergieron como preocupaciones críticas. Las instituciones educativas comenzaron a recopilar grandes cantidades de datos de los estudiantes a través de sistemas de gestión de aprendizaje (LMS) y otras herramientas tecnológicas, esto ha generado sobre la responsabilidad de las instituciones en la protección (Mariscal San Martin et al., 2022).

2.3. Deshumanización del Proceso Educativo

Otro tema relevante es el riesgo de deshumanización del proceso educativo. A medida que las interacciones se mediatizan a través de pantallas, surge la preocupación de que se pierdan aspectos cruciales de la educación, como la empatía, la comunicación no verbal y la conexión humana entre docentes y estudiantes. Este fenómeno ha sido especialmente notorio durante la pandemia de COVID-19, cuando el aprendizaje en línea se convirtió en norma, revelando las limitaciones de la educación completamente digital (Espinosa Cevallos, 2024).

La experiencia en la práctica educativa manifiesta que las acciones de plagio entre el estudiantado se dan con mayor regularidad en tareas didácticas designadas en cada clase. Esto se debe a que los estudiantes pueden acceder fácilmente a la información disponible en el ciberespacio, lo que a menudo se traduce en la habitual práctica del "copia y pega" (Espinosa Cevallos, 2024).

2.4. Plagio y Honestidad Académica

El acceso ilimitado a recursos en línea ha facilitado también la proliferación de casos de plagio y otras formas de deshonestidad académica, actualmente las TIC permiten a los estudiantes acceder a información y contenido de manera rápida y sencilla, lo que, si no se maneja adecuadamente, puede llevar a prácticas poco éticas en la presentación de trabajos académicos. Investigaciones recientes subrayan la necesidad de desarrollar herramientas más efectivas y políticas institucionales claras para combatir estas prácticas (Díaz Arce, 2023).

Se entiende como plagio al "robo de ideas, textos, métodos, mecanismos, diseños y, en general, de todo aquello que puede ser considerado como propiedad intelectual académica ajena (Díaz Arce, 2023).

Por lo tanto, plagio se define como la adjudicación de ideas académicas u obras o parte de ellas adjudicándolas como propias sin dar el crédito respectivo a quien las emitió.

Existen dos tipos de plagio académico: el involuntario y el intencional; en el primer caso este se presenta por falta de conocimiento y competencias del estudiante para referenciar las fuentes originales de donde toma la información, situación frecuente e incorrecta práctica del "copia y pega"; en el segundo caso se actúa consciente del fraude que se está cometiendo. Esta

clasificación coincide con la tipología propuesta por (Soto Rodríguez, 2021), que define el plagio accidental como: “Plagio accidental: el estudiante no entiende la definición de plagio o comete un error al citar o parafrasear. Es ocasionado por ignorancia, exceso de información y organización. Plagio oportunista: el estudiante sabe que es incorrecto plagiar, pero de igual forma lo hace debido a la desorganización, exceso de la información, fallos en la conducta ética, pereza o miedo”.

2.5. Educación Inclusiva y Accesibilidad

Recientemente, la atención se ha centrado en la necesidad de que las TIC en la educación sean inclusivas y accesibles para todos los estudiantes, incluidos aquellos con discapacidades. Aunque las TIC tienen el potencial de ofrecer soluciones innovadoras para mejorar la accesibilidad, también presentan desafíos éticos relacionados con el diseño inclusivo y la equidad en el acceso a recursos adaptados (Quintero Ayala, 2020).

Actualmente la privacidad se ha convertido en una de las grandes preocupaciones de la sociedad por tal motivo ha dado lugar a la cuarta generación de derechos humanos (Quintero Ayala, 2020).

2.6. Gestión del aprendizaje mediado por TIC

En la actualidad, la irrupción de las Tecnologías de la Información y la Comunicación (TIC) ha transformado profundamente el proceso educativo, ampliando las oportunidades de enseñanza y aprendizaje. Las TIC no solo facilitan el acceso a una vasta gama de recursos digitales, sino que también posibilitan la creación de entornos de aprendizaje más dinámicos, flexibles e interactivos. En este contexto, la gestión del aprendizaje mediado por TIC se ha convertido en un factor crucial para maximizar el potencial de estas herramientas tecnológicas (Espinoza Freire,

2018).

Un uso eficaz de las TIC en educación no solo permite la personalización de la enseñanza, sino que también garantiza el acceso a materiales educativos desde cualquier lugar y en cualquier momento, fomentando la colaboración entre estudiantes y docentes a través de plataformas virtuales. Asimismo, impulsa la innovación pedagógica, al adaptarse a los distintos ritmos y estilos de aprendizaje individuales. No obstante, gestionar eficazmente este tipo de aprendizaje implica no solo el dominio de las herramientas tecnológicas, sino también el diseño de estrategias pedagógicas que integren dichas tecnologías de manera coherente con los objetivos educativos (Espinoza Freire, 2018).

2.7. Evolución del TIC en la educación

Es indudable la evolución de las TIC pues se ha convertido en un viaje desde las primeras computadoras en el aula hasta la masiva adopción de plataformas en línea, la inteligencia artificial y la creación de entornos educativos que permiten la masificación de la educación, este proceso ha transformado no solo la forma en que se imparte y recibe la educación, sino también que ha permitido abrir un abanico de oportunidades y expectativas. Según (Arras Vota et al., 2021), (Salgado Reyes, 2023) y (Agnelli Faggioli , 2020) las etapas más importantes del tic en la educación son:

1. **Primeras Etapas (1960s - 1980s): Introducción de las Tecnologías Básicas**

- **1960s: Primeros Pasos con las Computadoras y la Tecnología Analógica**
    - Durante la década de 1960, las primeras computadoras comenzaron a integrarse en las universidades y centros de investigación. Estas máquinas, aunque primitivas en

comparación con los estándares actuales, marcaron el inicio de la informatización de la educación. Programas como PLATO (Programmed Logic for Automatic Teaching Operations), desarrollado en la Universidad de Illinois, fueron pioneros en el uso de computadoras para la enseñanza asistida, ofreciendo tutorías y ejercicios interactivos a los estudiantes.

  - Paralelamente, las tecnologías analógicas como los proyectores de transparencias y las grabadoras de audio y video fueron utilizados para mejorar la experiencia educativa y proporcionar a los docentes herramientas para ilustrar conceptos y compartir contenidos de manera más dinámica.

- **1970s: El Surgimiento del Software Educativo y la Educación a Distancia**
  - En la década de 1970, la aparición de las computadoras personales (PCs) dio lugar a una nueva era en la educación. El software educativo comenzó a desarrollarse con programas que ofrecían desde ejercicios de matemáticas hasta simulaciones científicas. Estas herramientas permitieron a los estudiantes interactuar de manera innovadora con los contenidos y facilitaron el estudio autodirigido.
  - La educación a distancia también comenzó a ganar terreno en esta época, utilizando la radio y la televisión para transmitir clases y contenidos educativos a zonas remotas. Estas iniciativas fueron precursoras de los sistemas de aprendizaje en línea, que más tarde se consolidarían con la llegada de Internet.

- **1980s: Expansión de las TIC en las Aulas**
  - Durante la década de 1980, las computadoras se convirtieron en una herramienta más común en las escuelas, especialmente en países desarrollados. Los programas

educativos se volvieron más sofisticados, integrando gráficos y multimedia que facilitaban la comprensión de conceptos complejos. Surgieron los primeros sistemas de gestión del aprendizaje (LMS) rudimentarios, que ayudaban a los docentes a organizar materiales educativos y realizar evaluaciones en línea.

- Se popularizaron los laboratorios de computación en las escuelas, donde los estudiantes aprendían a programar y a utilizar herramientas digitales. Este período sentó las bases para una integración más profunda de las TIC en el currículo escolar.

2. Expansión y Consolidación (1990s - 2000s): Internet y Aprendizaje en Línea

- **1990s: La Revolución de Internet y el Nacimiento del E-learning**
  - La llegada de Internet en la década de 1990 marcó un punto de inflexión en la educación, con la capacidad de acceder a una vasta cantidad de información y recursos educativos en línea, las TIC se convirtieron en un componente esencial del proceso educativo. Las instituciones educativas comenzaron a implementar proyectos de conectividad, proporcionando acceso a Internet a estudiantes y docentes.
  - Durante esta década, surgieron las primeras plataformas de e-learning, como Blackboard, que facilitaban la enseñanza y el aprendizaje a distancia de manera más estructurada e interactiva. Estas plataformas contenían foros de discusión, correo electrónico y sistemas de gestión de contenidos, lo que permitía a los docentes crear cursos en línea, y a los estudiantes acceder a materiales y tareas desde cualquier lugar con conexión de Internet.

- **2000s: La Explosión de las Plataformas Educativas y la Movilización del Aprendizaje**
  - Con el inicio del siglo XXI, la educación en línea se consolidó y expandió globalmente.

Las TIC comenzaron a desempeñar un papel central no solo en la educación superior, sino también en la educación primaria y secundaria, surgieron plataformas como Moodle, que permitían a los docentes y administradores educativos crear entornos de enseñanza personalizados, facilitando la interacción y el seguimiento del progreso académico.

- Esta década fue testigo del auge de los Recursos Educativos Abiertos (REA), que proporcionaban acceso gratuito a materiales educativos de alta calidad, fomentando a estudiantes de todo el mundo el aprendizaje autodidacta. Además, la introducción de dispositivos móviles y tabletas en el aula marcó el comienzo de la educación móvil (m-learning), permitiendo que la educación se llevara a cabo en cualquier momento y lugar.

3. La Era de la Innovación (2010s - 2020s): TIC, Big Data y Aprendizaje Personalizado

- **2010s: El Boom de los MOOCs y el Aprendizaje Basado en Datos**
  - La década de 2010 estuvo marcada por la explosión de los Massive Open Online Courses (MOOCs), que democratizaron el acceso a una educación de calidad a nivel global. Plataformas como Coursera, edX y Udacity facilitaron a millones de personas la oportunidad de participar en procesos educativos ofrecidos por universidades de élite de manera gratuita o a bajo costo. Estos cursos en línea abiertos a gran escala revolucionaron la educación continua y la formación profesional.
  - El uso de Big Data y analítica avanzada comenzó a transformar la educación, favoreciendo el desarrollo de sistemas de aprendizaje adaptativo que personalizaba la experiencia educativa en función del progreso y las necesidades individuales de los estudiantes. La gamificación, la realidad aumentada (AR) y la realidad virtual (VR) se integraron en los entornos de aprendizaje, ofreciendo experiencias inmersivas y

motivadoras.

- **2020s: La Educación en la Era de la Pandemia y la Expansión de la Inteligencia Artificial**
    - La pandemia de COVID-19 aceleró dramáticamente la adopción de tecnologías digitales en la educación, con un cambio casi universal hacia el aprendizaje en línea y a distancia, esto llevó a una mayor inversión en infraestructuras digitales y a un aumento en la dependencia de herramientas como videoconferencias, plataformas de gestión del aprendizaje y aplicaciones educativas. La crisis sanitaria global evidenció la necesidad de resiliencia en los sistemas educativos y subrayó el papel fundamental de las TIC para asegurar la continuidad educativa.
    - La inteligencia artificial (IA) comenzó a jugar un papel cada vez más relevante en la educación mediante la creación de sistemas de tutoría inteligente, análisis predictivo y automatización de procesos educativos. La IA ofrece recomendaciones personalizadas de aprendizaje, identifica brechas de conocimiento y adapta los contenidos a las necesidades individuales, optimizando los resultados educativos.

4. Tendencias Futuras (2020s en adelante): Hacia una Educación Digitalmente Integrada

- **Integración completa de las TIC:**
    - En el futuro se espera que las TIC se integren de manera aún más profunda y completa en todos los aspectos de la educación. Las aulas híbridas y virtuales se volverán más comunes, combinando lo mejor del aprendizaje presencial y en línea. La educación se verá cada vez más como un ecosistema digitalmente integrado, donde las TIC faciliten no solo la entrega de contenidos, sino también la evaluación, la interacción y el apoyo

emocional y social de los estudiantes.

- **Educación basada en datos:**
    - La recopilación y análisis de datos a gran escala siguen mejorando la personalización del aprendizaje. Las plataformas educativas emplean la inteligencia artificial para ofrecer recomendaciones de instrucción, identificar brechas de comprensión y adaptar los contenidos a las necesidades individuales, esta tendencia permite un enfoque más efectivo y centrado en el estudiante, alineado con sus intereses y metas.

- **Inclusión y accesibilidad:**
    - Las TIC desempeñan un papel crucial en reducir la brecha digital, asegurando que todos los estudiantes, independientemente de ubicación geográfica o situación socioeconómica, tengan acceso una educación de calidad, esto requerirá políticas educativas y esfuerzos coordinados para proporcionar acceso a tecnologías y recursos, así como para desarrollar competencias digitales en toda la población estudiantil.

- **Ética y privacidad**
    - A medida que las TIC se integren más en la educación se revelan las preocupaciones sobre la ética, la privacidad y la seguridad de los datos, los cuales se volverán más relevantes. Las instituciones educativas deben establecer políticas claras y efectivas para proteger los derechos de los estudiantes y garantizar un uso responsable de la tecnología. Esto incluirá la regulación del uso de datos personales y la implementación de medidas de ciberseguridad para salvaguardar información sensible.

- **Aprendizaje permanente (Lifelong Learning):**
    - La naturaleza cambiante del mercado laboral, impulsada por la automatización y la globalización, incrementará la demanda de oportunidades de aprendizaje de forma constante la demanda de aprendizaje a lo largo de la vida. Las TIC facilitan el acceso a la educación continua y la capacitación profesional, permitiendo que las personas actualicen sus habilidades y conocimientos de manera flexible y adaptada a sus necesidades individuales.

2.8. Plataformas de aprendizaje en línea

Una plataforma virtual de aprendizaje es un sistema que gestiona el proceso educativo, actuando como intermediario entre el estudiante y el profesor. Estas plataformas permiten que los estudiantes accedan, visualicen, descarguen e interactúen con recursos educativos a través de un navegador web, brindando flexibilidad y accesibilidad en el proceso de aprendizaje (Vital Carrillo, 2021).

Existen diversas plataformas virtuales de aprendizaje diseñadas para diferentes arquitecturas computacionales, incluidas versiones optimizadas para dispositivos móviles. Estas plataformas pueden ser de tipo propietario o de uso comercial, diferenciándose principalmente por su acceso gratuito o tarifado. Inicialmente, las plataformas virtuales de aprendizaje se utilizaron como un complemento para la entrega de actividades académicas. Sin embargo, debido a su rápida expansión y evolución, su uso se ha ampliado, aprovechando al máximo sus múltiples funcionalidades para facilitar y enriquecer el logro de los objetivos educativos (Vital Carrillo, 2021).

Las principales plataformas de aprendizaje se presentan en la **Tabla 1.**

Tabla 1: Principales plataformas de aprendizaje

Plataforma educativa	Ventajas	Desventajas
Moodle	• Herramienta efectiva que permite crear y gestionar cursos, temas y contenidos de forma sencilla. • Permite crear a los docentes EVA para el desarrollo de cursos on-line o como apoyo a la enseñanza presencial.	• Los docentes necesitan ser capacitados para poder editar sus cursos y subir los recursos. • Si el docente quiere tener su propia aula virtual con dominio propio es necesario pagar por la licencia.
Educativa	• Flexibilidad para Diversos Estilos de Aprendizaje • Amplia Gama de Recursos y Contenidos.	• Limitaciones en la Evaluación y Retroalimentación • Barreras de Acceso para Algunos Usuarios
Platzi	• Posee una única metodología de enseñanza para todos los cursos y se esfuerzan para que los contenidos sean dinámicos y entretenidos.	• No tiene cursos por niveles, es decir, principiante, intermedio o avanzado • Tiene características simples que están limitadas, por ejemplo, el control del avance de un curso no es tan preciso.
Google Classroom	• Se integra perfectamente con otras herramientas de Google como Docs, Drive y Calendar, lo que facilita la colaboración y la gestión del tiempo. • Classroom permite a los estudiantes y profesores acceder fácilmente a materiales, tareas y anuncios en un solo lugar, manteniendo todo organizado y accesible.	• Requiere una conexión a Internet constante, lo que puede ser un problema en áreas con conectividad limitada. • Como cualquier herramienta en línea, existe el riesgo de problemas de privacidad y seguridad de datos.
Microsoft Teams	• Facilita la colaboración en documentos compartidos y proyectos en tiempo real, permitiendo a los usuarios editar archivos de Office	• Aunque Microsoft Teams ofrece una versión gratuita, esta tiene algunas limitaciones en cuanto a almacenamiento, número de usuarios y

	simultáneamente y ver las actualizaciones en tiempo real. • Microsoft Teams se integra perfectamente con otras herramientas de Microsoft, como Office 365, SharePoint y Outlook, lo que facilita la colaboración y el flujo de trabajo dentro de un entorno familiar.	funcionalidades avanzadas, lo que puede no ser adecuado para todas las empresas. • Microsoft Teams puede consumir una cantidad significativa de recursos del sistema, especialmente durante llamadas de videoconferencia o al compartir archivos grandes, lo que puede afectar el rendimiento de dispositivos más antiguos o con recursos limitados.
Chamilo	• Soporte multi idiomas • Seguimiento de cursos y usuarios mediante detallados informes de actividad	• Necesidad de contar con alumnos motivados y participativos

Fuente: (Espinosa Izquierdo et al., 2021)

2.9. Amenazas de las plataformas digitales

Las amenazas de las plataformas digitales se refieren a las diversas amenazas y peligros que pueden surgir al utilizar herramientas en línea, abarcando desde la privacidad de los usuarios hasta la seguridad de la información. Estas amenazas tienen un impacto en una variedad de áreas, como la educación, el comercio, las redes sociales, el entretenimiento y cualquier otro servicio basado en la web. A medida que la digitalización crece y más personas e instituciones utilizan plataformas en línea para sus actividades diarias, también aumentan los riesgos asociados (Ordóñez Pineda y Calva Jiménez, 2020).

2.10. Vulnerabilidades de las plataformas digitales

Las vulnerabilidades de las plataformas digitales son debilidades, fallas o puntos ciegos en el diseño, la implementación o la gestión de sistemas en línea que los atacantes pueden aprovechar para comprometer la seguridad, la privacidad e la integridad de los datos, así como el correcto funcionamiento de la plataforma. Estas fallas permiten que los ciberdelincuentes accedan a datos confidenciales, modifiquen el comportamiento del sistema, interrumpan servicios o realicen actividades ilegales sin permiso (Carmona Vásquez y Monsalve Giraldo, 2024).

2.11. Seguridades de las plataformas digitales

Las medidas y prácticas conocidas como seguridades de las plataformas digitales están destinadas a proteger la integridad, confidencialidad y disponibilidad de los datos y recursos en línea. Estas medidas tienen como objetivo evitar accesos no autorizados, garantizar la protección de los datos personales y prevenir ataques cibernéticos que puedan afectar el funcionamiento adecuado de las plataformas (Carmona Vásquez y Monsalve Giraldo, 2024).

A continuación, se da a conocer las principales medidas y prácticas de seguridad de plataformas digitales:

- Cifrado de datos
- Control de acceso y privilegios
- Protección contra amenazas externas
- Gestión de vulnerabilidades
- Protección de privacidad

2.12. Triada de la CIA

La triada de la CIA (Confidentiality, Integrity, Availability) en el mundo de la ciberseguridad representan los principios fundamentales de seguridad informática: Confidencialidad, Integridad y Disponibilidad, conocidos colectivamente como la tríada CIA (Fortine, 2024).

La tríada de la CIA es fundamental para proteger la información. Cada vez que ocurre un incidente de ciberseguridad, al menos uno de sus principios se ve comprometido (confidencialidad, integridad o disponibilidad). Los profesionales de ciberseguridad evalúan las amenazas y las vulnerabilidades en función de estos principios, luego implementan controles para reducir el riesgo (Fortine, 2024).

En la Triada de la CIA interactúan tres aspectos importantes de los cuales se debe tratar individualmente tales como:

- **Confidencialidad:** La confidencialidad se refiere a los esfuerzos de una organización para garantizar que los datos sean privados y protegidos. Controlando el acceso a la información para evitar su divulgación no autorizada, ya sea deliberada o accidental, y preservar su integridad. Una tarea crucial es evitar que personas no autorizadas accedan a bienes esenciales para el usuario. Un sistema efectivo debe asegurarse de que aquellos que necesitan acceso tengan los privilegios adecuados para llevar a cabo sus funciones. Para lograr esto se debe aplicar los siguientes procesos.
    - Implementar políticas internas de seguridad que minimicen los riesgos, como pautas para establecer accesos seguros y el uso de canales confidenciales para transmitir información confidencial.

- Cifrar la información, lo que dificulta que los atacantes accedan a la información confidencial.
- Procedimientos de control de acceso y autenticación que impiden que usuarios no autorizados ingresen al sistema.
- Almacenar datos con una buena gestión y herramientas especializadas para protegerlos.

Un ejemplo de cómo se puede ver comprometida la confidencialidad es cuando un atacante puede acceder a nuestros sistemas e infraestructura a través de fallas en las aplicaciones, perder una computadora portátil con datos sensibles, alguien espiando mientras ingresamos una contraseña, o enviar archivos adjuntos accidentalmente a la persona equivocada (Fuenmayor Tobar et al., 2024).

- **Integridad:** La integridad garantiza que los datos sean precisos y no hayan sido modificados. Cuando la información es auténtica, precisa y consistente, se mantiene. Para lograr esto se debe aplicar los siguientes procesos:
  - Es fundamental administrar el control de acceso para que solo los perfiles autorizados puedan modificar los datos, evitando accidentes o eliminaciones indeseables.
  - En caso de alteraciones accidentales o malintencionadas, deben implementarse contramedidas para restaurar los datos.
  - Además, el uso de firmas digitales y procedimientos de verificación puede garantizar que cualquier modificación sea auténtica y realizada por personal autorizado.

Un ejemplo de cómo se puede ver comprometida la integridad es cuando un atacante ingresa a nuestra base de datos y logra modificar o eliminar forma no autorizada los datos, o incluso una alteración autorizada pero no deseada. Es por esto por lo que es sumamente importante tener un proceso de respaldo constante para que en caso de suceda este proceso sean capaces de volver a restaurar la información (Fuenmayor Tobar et al., 2024).

- **Disponibilidad:** A pesar de mantener la privacidad y la integridad de los datos, pueden ser inútiles si no están disponibles para quienes los necesitan, ya sea dentro de la organización o para los clientes a los que se brinda servicio. Esto significa que los sistemas, las redes y las aplicaciones deben funcionar correctamente y de manera eficiente. Además, es esencial que las personas autorizadas tengan la capacidad de acceder a la información requerida de manera oportuna y sin demoras excesivas. Para lograr esto se debe aplicar los siguientes procesos:
    - Para evitar caídas y fallas técnicas, es esencial crear sistemas ágiles que garanticen una rápida capacidad de respuesta y una alta disponibilidad de los servidores.
    - Implementar medidas para proteger contra ataques de denegación de servicio (DoS), que son utilizados por piratas informáticos para interrumpir el servicio web al llenar un servidor con solicitudes innecesarias, lo que reduce la disponibilidad para los usuarios legítimos.
    - Los sistemas que tienen altos requisitos de tiempo de actividad continuo deben tener redundancia de hardware y mantener copias de seguridad y almacenamiento de datos actualizados y fácilmente accesibles.

Un ejemplo de cómo se puede ver comprometida la disponibilidad es cuando los sistemas críticos se ven afectados en caso de un corte de energía sin un sistema de recuperación ante desastres. Además, eventos naturales como inundaciones o tormentas graves pueden impedir el acceso a la oficina y los dispositivos esenciales para el negocio (Fuenmayor Tobar et al., 2024).

2.12.1. Aplicación de la triada de la CIA

Según (Caballero et al., 2022) existe un modelo estándar de ciberseguridad, su aplicación varía según las necesidades específicas de cada organización. Es por esto por lo que lo más conveniente en el caso de que se deba aplicar la triada de la CIA es:

- Realiza un análisis exhaustivo de la organización: Evalúa el equipo, los sistemas, los accesos y clasifica los datos para su adecuada protección.
- Capacita al personal: No todos necesitan conocer a fondo la tríada CIA, pero es crucial que el equipo esté formado en políticas de seguridad para reducir riesgos de filtraciones y accesos no autorizados.
- Actualiza regularmente controles, accesos y contraseñas: Asegúrate de que, si los agentes externos obtienen esta información, se vuelva obsoleta y no permita su entrada.
- Implementa estrategias de gestión de riesgos: Detecta y fortalece vulnerabilidades potenciales para anticipar y mitigar posibles ataques."

2.13. Plataformas virtuales

Las plataformas virtuales son entornos en Internet diseñados para alojar y ejecutar múltiples aplicaciones y programas en un solo espacio. Ofrecen una variedad de funciones que

permiten a los usuarios abordar diversos problemas de manera eficiente y automática, al tiempo que optimizan el uso de los recursos. El principal objetivo de las plataformas digitales es simplificar la ejecución de tareas al centralizar diversos programas y aplicaciones en un único lugar en la web (Copola, 2023).

Existen una variedad de plataformas virtuales por nombrar algunas tenemos:

- Educativas
- Sociales
- Networking
- Trabajo Remoto
- Videoconferencias
- De pagos digitales
- Música y etc.

2.13.1. Amenazas y vulnerabilidades de plataformas virtuales

Las plataformas se enfrentan a numerosas vulnerabilidades y amenazas informáticas, lo que ha provocado un aumento significativo de la inversión en ciberseguridad y sistemas de protección. Como resultado, los profesionales de la ciberseguridad se han convertido en uno de los talentos más buscados de la industria. Estas son las principales amenazas y vulnerabilidades que enfrentan las plataformas en la actualidad:

- **Amenazas de malware**

Según (Garcia y Pesantez, 2023) , las amenazas de malware son:

- **Virus**: Los virus informáticos son programas diseñados para interferir con el funcionamiento de un dispositivo.
- **Gusanos:** Es uno de los tipos de malware más comunes en empresas, ya que puede infectar equipos sin necesidad de intervención del usuario ni modificación de archivos.
- **Troyanos**: Son programas que se ocultan en un equipo para permitir la instalación de otro software malicioso.
- **Ransoware**: Es el malware más temido hoy en día, ya que encripta toda la información de una empresa, bloqueando el acceso a datos y sistemas, y exige un rescate para liberarlos.
- **Keylogers**: Estos programas maliciosos se infiltran mediante troyanos y están diseñados para robar credenciales de acceso a plataformas web, sitios bancarios y otros servicios en línea similares.

- **Amenazas de ataques de denegación de servicio**
  - Un ataque DDoS ocurre cuando un servidor es inundado con solicitudes simultáneas de múltiples computadoras (bots), sobrecargando el sistema y provocando su caída o funcionamiento incorrecto (Garcia y Pesantez, 2023).
- **Vulnerabilidades**

Según (Garcia y Pesantez, 2023) , las vulnerabilidades que existen son:

- Errores de configuración.
- Errores en la gestión y asignación de permisos.

- **Vulnerabilidades producidas por contraseñas**
  - Con el auge del teletrabajo y el cloud computing, la gestión de contraseñas se

ha vuelto crucial en ciberseguridad. El uso de contraseñas débiles crea vulnerabilidades que pueden permitir a terceros no autorizados acceder a sistemas, robar o alterar información, y modificar configuraciones o apagar equipos si tienen los privilegios adecuados.

En la **Tabla 2** se presentan las amenazas y vulnerabilidades identificadas, caracterizadas según la triada de la CIA (Confidencialidad, Integridad y Disponibilidad) en el caso de plataformas educativas, lo que permite un análisis estructurado y detallado de los riesgos asociados.

Tabla 2: Amenazas y Vulnerabilidades de plataformas educativas

PLATAFORMAS EDUCATIVAS		
AMENAZAS	**VULNERABILIDADES**	**AFECTACIÓN CIA**
Ransomware: Software malicioso que ingresa a tu sistema y roba información y luego pedir rescate.	**Pérdida o Robo de Dispositivos**: Es un riesgo significativo ya la información puede quedar expuesta.	Confidencialidad
Phishing: Ciberataque en el cual se hacen pasar por entidades confiables para engañar al usuario y robar su información.	**Uso de Dispositivos Personales**: Es una mala práctica de seguridad informática, ya que en estos se encuentra información personal que al momento de que exista un ciberataque corre el riesgo de ser robada.	Integridad
Ataques DDoS: Ciberataque donde se satura una red con una gran cantidad de tráfico malicioso para que sea inaccesible.	**Reutilización de Contraseñas**: Es una mala práctica en seguridad informática porque se debe utilizar contraseñas diferentes para cada sitio así mejoramos la seguridad de nuestra información.	Disponibilidad
Spyware: Es un software malicioso diseñado para espiar al usuario.	**Falta de Presupuesto para IT**: Es un gran problema, ya que no se puede implementar una buena seguridad informática por lo que estaríamos expuestos a ciberataques.	Confidencialidad

Fuente: (Navarro , 2022)

En la **Tabla 3** se presentan las amenazas y vulnerabilidades identificadas, caracterizadas según la triada de la CIA (Confidencialidad, Integridad y Disponibilidad) en el caso de plataformas sociales, lo que permite un análisis estructurado y detallado de los riesgos asociados

Tabla 3: Amenazas y Vulnerabilidades de plataformas sociales

PLATAFORMAS SOCIALES		
AMENAZAS	**VULNERABILIDADES**	**AFECTACIÓN CIA**
Ransomware: Software malicioso que ingresa a tu sistema y roba información y luego pedir rescate.	**Configuraciones de Privacidad Inadecuadas**: Este tipo de configuraciones expone la seguridad de los usuarios	Confidencialidad
Phishing: Ciberataque en el cual se hacen pasar por entidades confiables para engañar al usuario y robar su información.	**APIs Vulnerables**: Estas representar un riesgo significativo para la seguridad es por esto por lo que es sumamente importante su correcta configuración.	Integridad
Suplantación de identidad: Es el robo de información para suplantar tu identidad para cometer acciones ilícitas.	**Mal Configuración de Controles de Acceso**: Esto trae como resultado errores en la implementación de la seguridad de la plataforma	Confidencialidad
Robo de datos personales: Ingresar a tu sistema para captar información personal y tomarla sin tu consentimiento.	**Software Desactualizado**: Al no contar con un software actualizado su seguridad está desactualizada por lo que está sujeta a ciberataques	Integridad
Malware y enlaces maliciosos: Es un software malicioso diseñado para espiar al usuario.	**Autenticación Débil**: Siempre es importante contar con un proceso de autentificación fuerte ya sea de huella o con un pin que llegue únicamente a dispositivos del usuario.	Integridad

Fuente: (Navarro , 2022).

En la **Tabla 4** se presentan las amenazas y vulnerabilidades identificadas, caracterizadas según la triada de la CIA (Confidencialidad, Integridad y Disponibilidad) en el caso de plataformas de trabajo remoto, lo que permite un análisis estructurado y detallado de los riesgos asociados.

Tabla 4: Amenazas y Vulnerabilidades de plataformas de trabajo remoto

PLATAFORMAS TRABAJO REMOTO		
AMENAZAS	**VULNERABILIDADES**	**AFECTACIÓN CIA**
Phishing: Ciberataque en el cual se hacen pasar por entidades confiables para engañar al usuario y robar su información.	Redes no seguras: La conexión a redes no seguras es una de las principales razones por las cuales la información puede ser robada.	Integridad
Ransomware: Software malicioso que ingresa a tu sistema y roba información y luego pedir rescate.	**Contraseñas débiles**: Las contraseñas deben de tener diferentes caracteres esto es una medida de seguridad informática.	Confidencialidad
Acceso no autorizado: Ingreso de individuos a recursos e información que no le pertenece.	**Falta de Autenticación Multifactor**: Es la capacidad de tener dos o más autentificaciones de usuario para mayor seguridad.	Integridad
Fuga de datos: Es la exposición de información de manera no autorizada.	**Software Desactualizado**: Al no contar con un software actualizado su seguridad está desactualizada por lo que está sujeta a ciberataques	Confidencialidad
Ataques DDoS: Ciberataque donde se satura una red con una gran cantidad de tráfico malicioso para que sea inaccesible.	**Configuraciones de Seguridad Inadecuadas**: El tener malas configuraciones de seguridad informática siempre da como resultado que nuestra información no se encuentre segura.	Disponibilidad

Fuente: **(Navarro , 2022)**

En la **Tabla 5** se presentan las amenazas y vulnerabilidades identificadas, caracterizadas según la triada de la CIA (Confidencialidad, Integridad y Disponibilidad) en el caso de plataformas de pagos digitales, lo que permite un análisis estructurado y detallado de los riesgos asociados.

Tabla 5: Amenazas y Vulnerabilidades de plataformas de pagos digitales

PLATAFORMAS PAGOS DIGITALES		
AMENAZAS	**VULNERABILIDADES**	**AFECTACIÓN CIA**
Phishing: Ciberataque en el cual se hacen pasar por entidades confiables para engañar al usuario y robar su información.	**Exposición de datos en tránsito**: Esto ocurre cuando nuestra información es interceptada y robada.	Integridad

Ransomware: Software malicioso que ingresa a tu sistema y roba información y luego pedir rescate.	**Vulneraciones en el software**: Al no contar con una correcta configuración en el software su seguridad esta desactualizada por lo que está sujeta a ciberataques.	Confidencialidad
Accesos no autorizados: Ingreso de individuos a recursos e información que no le pertenece.	**Gestión deficiente de sesiones**: se refiere a prácticas inadecuadas en la administración de sesiones de usuario en las plataformas de trabajo.	Integridad
Exposición de datos: Es la exposición de información de manera no autorizada.	**Fuga de datos**: Es la exposición de información de manera no autorizada.	Confidencialidad
Spyware: Es un software malicioso diseñado para espiar al usuario.	**Autenticación Débil**: Se refiere a mecanismos de autentificación débil para el inicio de sesiones en las plataformas de trabajo.	Confidencialidad

Fuente: (Navarro , 2022)

2.14. Disparidades en el acceso y uso de la tecnología educativa

El acceso y el uso de las tecnologías educativas son una problemática importante en el sistema educativo en todo el mundo. Esto se debe a factores sociales y económicos, la falta de docentes formados para este medio y la infraestructura tecnológica deficiente. Mientras que en algunas regiones se integran herramientas avanzadas como plataformas de aprendizaje en línea y entornos virtuales interactivos, en otras, el acceso a dispositivos básicos y una conexión estable a internet sigue siendo un obstáculo crítico. Todo esto no solo limita la capacidad de las personas de adquirir hábitos digitales que son cada vez más importantes, sino que hace que las divisiones en la educación continúen existiendo, afectando el desempeño escolar. Por esas razones, es muy importante que se elaboren políticas que sean inclusivas para garantizar que se tenga un acceso adecuado en la educación y que se logre usar de forma efectiva (Cajamarca-Correa et al., 2024).

El primer factor para analizar es el caso de comunidades rurales las cuales enfrentan barreras significativas para acceder a recursos tecnológicos esenciales, como internet, computadoras y tabletas. En estos contextos, las familias con recursos económicos limitados no invierten en tecnología educativa ya que se ven obligadas a priorizar necesidades básicas como alimentación, vivienda y salud. Esta situación no solo arrebata las oportunidades de aprendizaje en línea, sino que también amplifica la brecha digital y educativa, dificultando que los estudiantes de estas comunidades adquieran las competencias digitales necesarias para competir en un mundo cada vez más tecnológico (Solano-Gutiérrez, 2024).

El segundo factor para analizar es que, en algunas regiones, las escuelas enfrentan una gran carencia de recursos tecnológicos, como laboratorios de informática, plataformas de aprendizaje en línea y servicios de soporte técnico que garanticen el mantenimiento, incluso no cuentan con servicio de internet. Estas limitaciones suelen verse agravadas por falta de inversión por parte de los gobiernos en infraestructura tecnológica. Como resultado, los estudiantes y docentes se ven privados de oportunidades clave para integrar la tecnología en los procesos de enseñanza y aprendizaje (Solano-Gutiérrez, 2024).

2.14.1. Impacto de las disparidades en el acceso y uso de la tecnología educativa

Según (Cajamarca-Correa et al., 2024), las disparidades en el acceso y uso de la tecnología educativa generan desigualdad creando impactos tales como:

- **Desigualdad en el ámbito educativos**: Los estudiantes con acceso limitado a la tecnología tienen menos oportunidades para desarrollar competencias tecnológicas, siendo una desventaja en un mundo con auge tecnológico.
- **Exclusión social**: El poco acceso a herramientas tecnológicas amplia las brechas

sociales y limita la integración en entornos educativos, laborales y sociales.

- **Baja efectividad en la enseñanza**: La falta de formación docente que maneje la tecnología da como resultado que baja calidad de la enseñanza en la actualidad la tecnología es uno de los materiales de apoyo más importante que debe manejar el docente.

2.14.2. Propuestas para mitigar las disparidades

La equidad en el acceso y uso de la tecnología educativa es sumamente importante ya implica garantizar que todos los estudiantes, independientemente de su origen socioeconómico, ubicación geográfica o condición cultural, tengan las mismas oportunidades para aprovechar las herramientas tecnológicas (Solano-Gutiérrez, 2024). Es por esto por lo que se propone ciertas acciones para mitigar este problema tales como:

- **Invertir en infraestructura tecnológica:** Realizar una inversión acorde a esta problemática para que exista una equidad en el acceso tecnológica en las instituciones esto con el fin de disminuir las brechas tecnológicas que existen en la actualidad (Solano-Gutiérrez, 2024).
- **Formación docente:** Aumentar los programas de capacitación para educadores y así estos puedan utilizar la tecnología de manera efectiva e inclusiva (Solano-Gutiérrez, 2024).
- **Desarrollar políticas inclusivas:** Diseñar estrategias educativas que prioricen a las comunidades que no cuenten con acceso tecnológico con el fin de promover la equidad tecnológica (Solano-Gutiérrez, 2024).

2.15. Seguridad en plataformas educativas

La seguridad y privacidad en plataformas educativas buscan proteger los datos personales, contenido académico y la identidad digital de los usuarios. Esto incluye medidas técnicas, como cifrado y autenticación, y el cumplimiento de normativas legales de protección de datos y propiedad intelectual (Morales Paredes y Chicaiza, 2021). Son esenciales para asegurar confianza, calidad y eficacia en la educación online, y prevenir amenazas que puedan comprometer la integridad o rendimiento de los usuarios. Para mitigar las amenazas, es fundamental abordar dos aspectos clave: por un lado, garantizar la seguridad robusta de la plataforma mediante medidas técnicas; por otro, fomentar que los usuarios sigan prácticas de ciberseguridad adecuadas para protegerse eficazmente (Rodríguez, 2021).

Según (Gaviria Lopera et al., 2023) los aspectos de seguridad informática de las plataformas educativas son:

- **Implementar sistemas de autenticación multifactor (MFA):** Es un tipo de seguridad donde se requiere dos o más códigos de verificación por parte de los usuarios. Una plataforma que tiene esta seguridad es Microsoft Teams al activar esta opción una vez que el usuario haya introducido su contraseña personal la aplicación le envía un código de verificación ya sea a su teléfono o correo electrónica como medida de seguridad.
- **Encriptar los datos de los usuarios:** es un proceso en el que se transforma información sensible en un formato codificado que únicamente puede ser leído por sistemas autorizados. Una plataforma que realiza este tipo de seguridad es Moodle en la cual se almacena información educativa y tiene encriptación en el tránsito de datos y acceso restringido para que únicamente el usuario real sea capaz de manejar su información.

- **Ofrecer herramientas de control parental:** Es un control para que padres o tutores tengan acceso a la plataforma y les lleguen las notificaciones de los avances y tareas que realizan los estudiantes. Una plataforma que utiliza este tipo de seguridad es Khan Academy.
- **Mantener activas actualizaciones y los broches de seguridad:** Tener activos las actualizaciones y los parches de seguridad de manera automática es sumamente importante ya que estas traen continuamente mejoras en la seguridad informática. Una plataforma que permite realizar esto es Blackboard el cual es un programa de actualizaciones automáticas para asegurar las plataformas educativas.
- **Copias de seguridad regulares y cifradas:** se refiere a la copia de archivos físicos o virtuales o bases de datos de un sitio. Una plataforma que realiza este tipo de proceso es Edmodo.

Según (Gaviria Lopera et al., 2023), los aspectos de seguridad informática que deben seguir los usuarios:

- Elegir una plataforma educativa con una sólida reputación en materia de seguridad y privacidad. Al momento de trabajar en plataformas educativas virtuales es importante elegir una plataforma que ofrezca la seguridad adecuada para el manejo de la información ejemplos de estas plataformas se encuentran en el tema anterior.
- Leer atentamente las políticas de seguridad y privacidad de la plataforma antes de crear una cuenta. Se debe ser consciente de que el leer los términos y políticas de las páginas que visitamos es de suma importancia, ya que entre estos términos y condiciones pueden existir cláusulas en las cuales nuestra información puede ser robada.

- Utilizar contraseñas seguras y únicas para cada cuenta. El utilizar contraseñas complejas y con diferentes caracteres siempre ayuda a que los usuarios en las plataformas tengan una mayor seguridad.

2.16. Ámbito Jurídico que regula la protección de datos

La protección de datos personales es crucial hoy en día. El Reglamento General de Protección de Datos (RGPD), entro en vigor desde mayo de 2018, ha transformado Internet al imponer requisitos a instituciones globales. Su alcance extraterritorial obliga a organizaciones de todo el mundo a cumplir con sus normas, y muchos países latinoamericanos están reformando sus leyes para alinearse con el RGPD. En este contexto, el Ecuador aprobó su Ley Orgánica de Protección de Datos el 10 de mayo de 2021, con muchas disposiciones similares al RGPD. El principal objetivo de este reglamento es regular, prever y desarrollar principios, obligaciones para garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos; y su protección (Asamblea Nacional del Ecuador, 2021).

Según (Gascón Marcén, 2021) en ámbito internacional existen otros reglamentos para la protección de información en plataformas digitales entre las importantes se encuentran tales como:

- Reglamento General de protección de datos (UE) 2016/679 (Unión Europea- 2016)
- Ley de Servicios Digitales (DSA)
- California Consumer Privacy Act (California-2018)
- Convenio 108 del Consejo de Europa
- Regulaciones de la ONU sobre privacidad de datos
- Iniciativa de las normas de privacidad transfronteriza (CBPR)-AEPC

2.17. Plataformas de aprendizaje en línea

En la **Tabla 6** se presentan las leyes de protección de la información que regulan el funcionamiento de las plataformas de aprendizaje

Tabla 6: Plataformas de aprendizaje y leyes que rigen la protección de los datos.

NOMBRE	LEYES EXISTENTES EN PROTEGER LA PRIVACIDAD
Moodle	• Reglamento General de Protección de Datos (GDPR) • Ley de Privacidad del Consumidor de California (CCPA)
Educativa	• Reglamento General de Protección de Datos (GDPR) - Unión Europea • Ley de Privacidad del Consumidor de California (CCPA) - Estados Unidos
Platzi	• Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) – México • Ley General de Protección de Datos (LGPD) – Brasil
Google Classroom	• Ley de Protección de la Privacidad en Línea para Niños (COPPA) - Estados Unidos • Ley de Protección de la Privacidad en Línea para Niños (COPPA) - Estados Unidos
Microsoft Teams	• Reglamento General de Protección de Datos (GDPR) - Unión Europea • Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) – México
Chamilo	• Reglamento General de Protección de Datos (GDPR) - Unión Europea • Ley de Privacidad del Consumidor de California (CCPA) - Estados Unidos
Schoology	• Ley General de Protección de Datos (LGPD) – Brasil • Ley de Derechos Educativos y Privacidad Familiar (FERPA) - Estados Unidos

Fuente: (Gascón Marcén, 2021)

CAPITULO 3. Marco metodológico

3.1. Enfoque de la investigación

El enfoque de esta investigación es mixta (cualitativo - cuantitativo), a nivel cualitativo ya que se centra en comprender y analizar fenómenos culturales y tecnológicos desde una perspectiva interpretativa y descriptiva; a nivel cuantitativo, porque se emplea una encuesta que permite obtener datos medibles sobre información de los estudiantes en prácticas de seguridad informática. La combinación de ambos enfoques permite contrastar descripciones con resultados numéricos, enriqueciendo el análisis y proporcionando una visión integral sobre los desafíos de la gestión del aprendizaje mediado por tic en los estudiantes.

3.2. Tipo de investigación

La investigación es de tipo descriptivo y bibliográfico. Siendo descriptivo porque se busca detallar el estado actual de las TIC en relación con aspectos de privacidad, seguridad y equidad y así poder plantear soluciones y bibliográfico por que el objetivo es explorar el campo de estudio a través de una revisión de fuentes bibliográficas que permitan obtener una visión global del tema.

3.3.Diseño de la investigación

El diseño de la investigación es no experimental ya que no se manipulan variables ni se realizan experimentos.

3.4.Técnicas e instrumentos para la recolección de datos.

Según la naturaleza de la investigación se aplicaron las siguientes técnicas e instrumentos:

3.6.1 Técnicas

- **Encuesta:** Esta técnica se utilizó para recopilar datos sobre las actitudes, opiniones y experiencias de los estudiantes en relación sobre los desafíos éticos que surgen en la gestión del aprendizaje mediado por tecnologías de la información y la comunicación (TIC).

3.6.2 Instrumentos

- Como instrumento se utilizó el cuestionario, el cual se ha diseñado para recopilar información clave sobre el conocimiento básico de los estudiantes en buenas prácticas de ciberseguridad y en la identificación de distintos tipos de ataques cibernéticos. Asimismo, se pretende explorar la percepción que tienen los estudiantes sobre la ciberseguridad al navegar y acceder a plataformas virtuales. Los datos obtenidos permitirán identificar patrones, tendencias y correlaciones relevantes, proporcionando una visión integral de las competencias y actitudes de los estudiantes frente a la ciberseguridad del Colegio Cap. Edmundo Chiriboga de primero de bachillerato. Las preguntas estarán organizadas en tres fases específicas como se puede observar en la **Figura 1.**

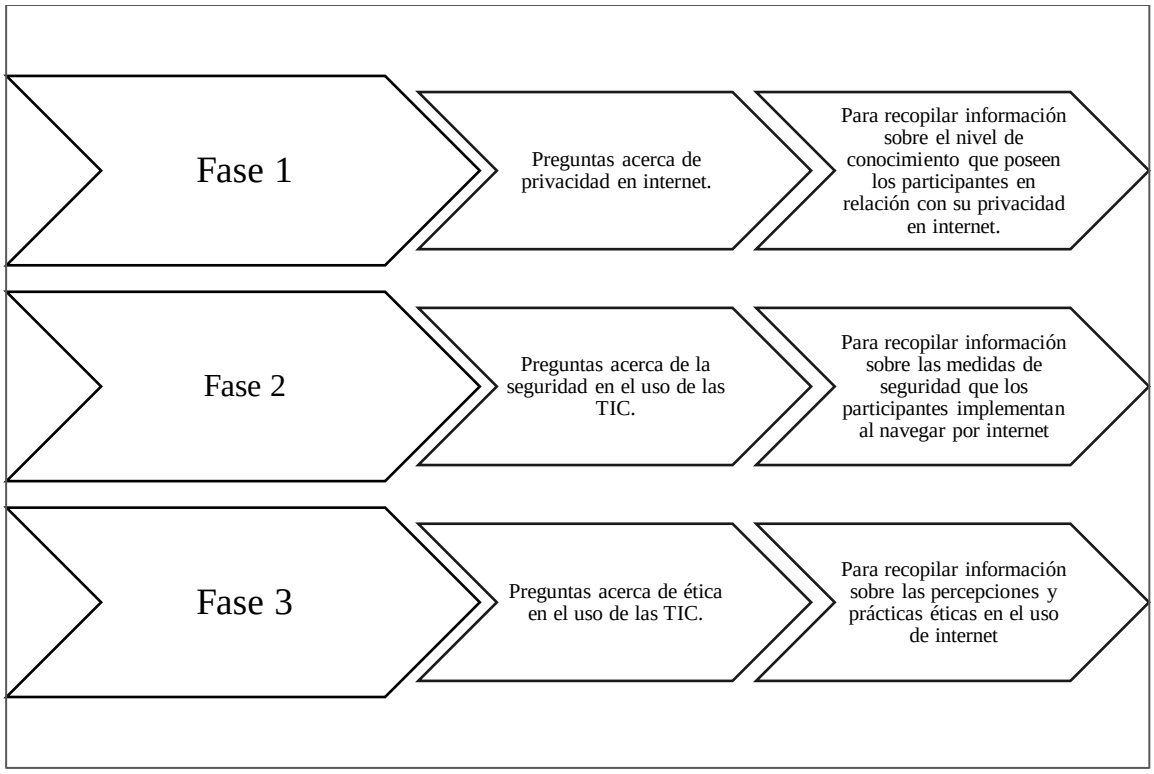


Figura 1. Fases del desarrollo de preguntas para la encuesta

3.5. Definición de población y muestra

Se determinó una población finita de 43 estudiantes del Colegio Cap. Edmundo Chiriboga de primero de bachillerato, sobre la cual se centrará el estudio. A partir de esta población, se calculará el porcentaje y el número de encuestas necesarias utilizando la fórmula de muestreo para poblaciones finitas, con el fin de asegurar la representatividad de los resultados en el contexto estudiantil.

$$\boldsymbol{n = \frac{N * Z_{\propto}^{2} * P * Q}{e^{2} * (N - 1) + Z_{\propto}^{2} * P * Q}} \qquad \textbf{(1)}$$

En la **ecuación (1)** podemos encontrar la fórmula para el cálculo de la muestra de una población conocida (finita), donde:

$\boldsymbol{n}$ = Es el tamaño de muestra que deseamos obtener, es decir, la cantidad de encuestas a realizar.

$\boldsymbol{N}$= Representa el tamaño de la población, es decir, el número total de estudiantes en ambos campus.

$\boldsymbol{Z\alpha}$ = Este parámetro estadístico se relaciona con el nivel de confianza que buscamos al estimar un valor utilizando una muestra previamente recolectada, el nivel de confianza (NC) representa la certeza o probabilidad expresada en porcentaje con la que realizamos esta estimación.

$\boldsymbol{P}$= Es la probabilidad de que la muestra finita de estudiantes participe en la encuesta.

$\boldsymbol{Q}$= Es la probabilidad de que la muestra finita de estudiantes no participe en la encuesta. Dado que no se conoce la probabilidad exacta (P), se le asigna el mismo peso que (Q). es decir, ambos parámetros se establecen en un 50%.

$\boldsymbol{e}$ = Representa la cantidad de error de muestreo aleatorio, este valor también será determinado por los investigadores y estará relacionado con el nivel de certeza que deseas en un estudio.

Tabla 7. Formula aplicada de la muestra finita a la población

Cálculo de muestra Finita

$$\boldsymbol{n} = \frac{43 * 1.96^2 * 0.5 * 05}{0.05^{2*}(43-1) + 1.96^2 * 0.5 * 0.5}$$

$$\boldsymbol{n} = \frac{29498}{761}$$

n=39

Una vez obtenidas las muestras, se procedió a distribuir la encuesta entre los estudiantes de primero de bachillerato del Colegio Cap. Edmundo Chiriboga. Este proceso de distribución fue cuidadosamente planificado para garantizar una alta tasa de respuesta y una representatividad adecuada de la población estudiantil. La información recopilada a través de las encuestas fue luego sistemáticamente tabulada, permitiendo así una organización clara y precisa de los datos para su posterior análisis.

CAPÍTULO 4. Análisis de resultados

En esta sección se presentan los resultados derivados de la recopilación y análisis exhaustivo de los datos obtenidos, con el objetivo de ofrecer una visión integral sobre los conocimientos, percepciones y prácticas de los estudiantes en relación con la ciberseguridad y la ética en el uso de internet A través del procesamiento detallado y la tabulación de las respuestas, se lograrán identificar patrones, tendencias y correlaciones claves que reflejan el nivel de conciencia, las actitudes y el grado de preparación de los estudiantes frente a los retos éticos y de seguridad que plantean. el entorno digital estos hallazgos proporcionan una base sólida no solo para entender la situación actual de los estudiantes en cuanto a su formación en ciberseguridad y ética digital, sino también para fundamentar propuestas y recomendaciones orientadas a fortalecer estos aspectos dentro del ámbito educativo con ello se espera contribuir al desarrollo de competencias digitales que promuevan un uso responsable y seguro de la tecnología.

4.1.Resultados del cuestionario

Mediante la encuesta realizada a los estudiantes del Colegio Cap. Edmundo Chiriboga de primero de bachillerato se obtuvieron los siguientes resultados.

P1. ¿Con qué frecuencia lees las políticas de privacidad antes de usar un servicio en línea o aplicación?

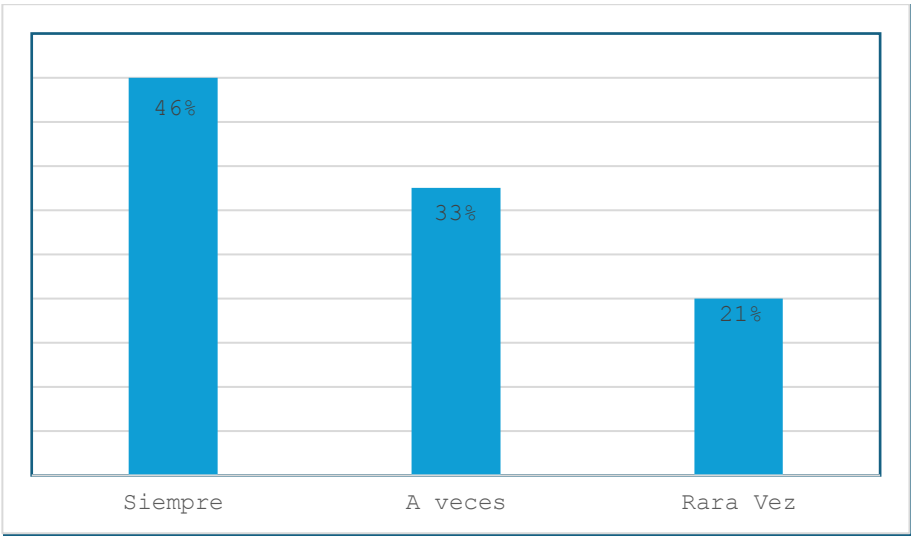


Figura 2. Diagrama de barras de los resultados de la P1.

La **Figura 2** muestra que el 46% de los estudiantes afirman que siempre leen las políticas de privacidad al utilizar un servicio en línea, demostrando un nivel alto de conciencia sobre la gestión de sus datos personales. En contraste, un 33% indica que solo revisa estas políticas a veces, mientras que el 21% rara vez lo hace, lo que sugiere una falta de consistencia en la práctica. Estos resultados revelan una variabilidad significativa en el grado de atención que los estudiantes prestan a la privacidad de sus datos.

P2. ¿Cuán preocupado/a estás por la privacidad de tus datos personales cuando navegas en línea?

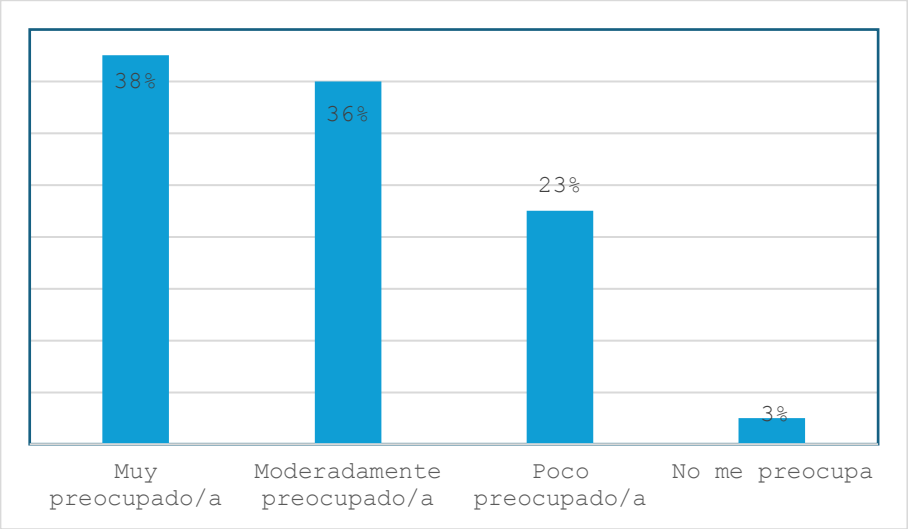


Figura 3. Diagrama de barras de los resultados de la P2.

En la **Figura 3** se observa que un 38% de los estudiantes se muestra muy preocupado por la seguridad de sus datos personales mientras navega por internet, lo que indica un alto nivel de conciencia sobre los riesgos asociados con la privacidad en línea. Por otro lado, un 36% expresa una preocupación moderada, sugiriendo que, aunque reconocen la importancia de la seguridad de sus datos, tal vez no se sientan completamente informados o capacitados para actuar en consecuencia. En contraste, un 23% de los encuestados se manifiestan poco preocupados, y un 3% afirma no preocuparse en absoluto, lo que refleja una posible desinformación o desinterés en relación con la protección de su información personal. Estos resultados destacan la necesidad de implementar estrategias educativas que aborden y refuercen la importancia de la ciberseguridad, promoviendo una cultura de responsabilidad y cuidado en el manejo de datos personales en el entorno digital.

P3. ¿Alguna vez has experimentado una vulneración de privacidad en línea (por ejemplo, robo de información personal)?

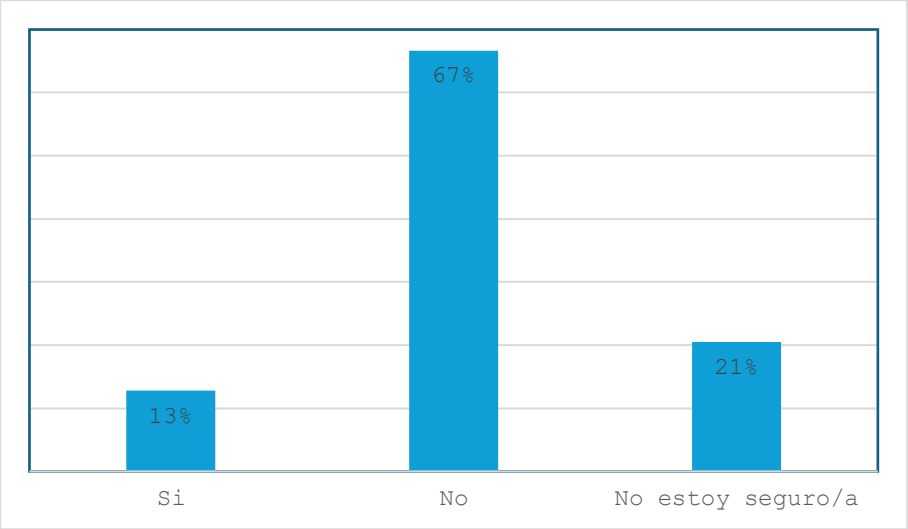


Figura 4. Diagrama de barras de los resultados de la P3.

La **Figura 4** muestra que el 13% de los estudiantes ha experimentado una vulneración de su privacidad en línea, mientras que el 67% no ha tenido tales experiencias. No obstante, un 21% no está seguro de si ha sido víctima de alguna vulneración, lo que indica una falta de claridad sobre los riesgos en el entorno digital. Estos resultados destacan la urgencia de proporcionar educación y recursos que capaciten a los estudiantes a reconocer y prevenir brechas de privacidad, así como a mejorar su confianza en la gestión de su información personal.

P4. ¿Crees que las empresas tecnológicas respetan adecuadamente la privacidad de sus usuarios?

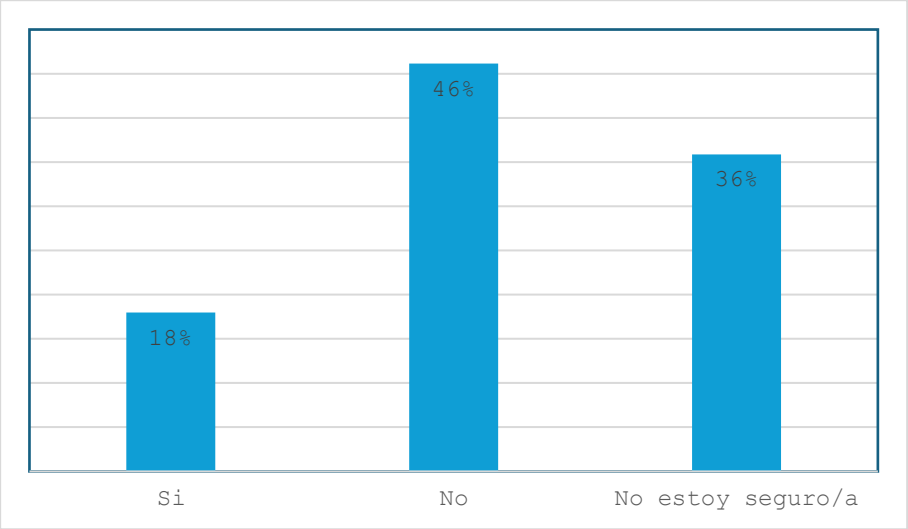


Figura 5. Diagrama de barras de los resultados de la P4.

La **Figura 5** indica que el 46 % de los encuestados desconfía de que las empresas tecnológicas respetan la privacidad de los usuarios, mientras que un 36% no está seguro y solo un 18% confía en que sí lo hacen. Estos resultados resaltan la necesidad de mayor transparencia y educación sobre las prácticas de privacidad de las empresas tecnológicas para fortalecer la confianza y comprensión de los usuarios.

P5. ¿Con qué frecuencia usas contraseñas seguras (combinación de letras, números y símbolos) para tus cuentas en línea?

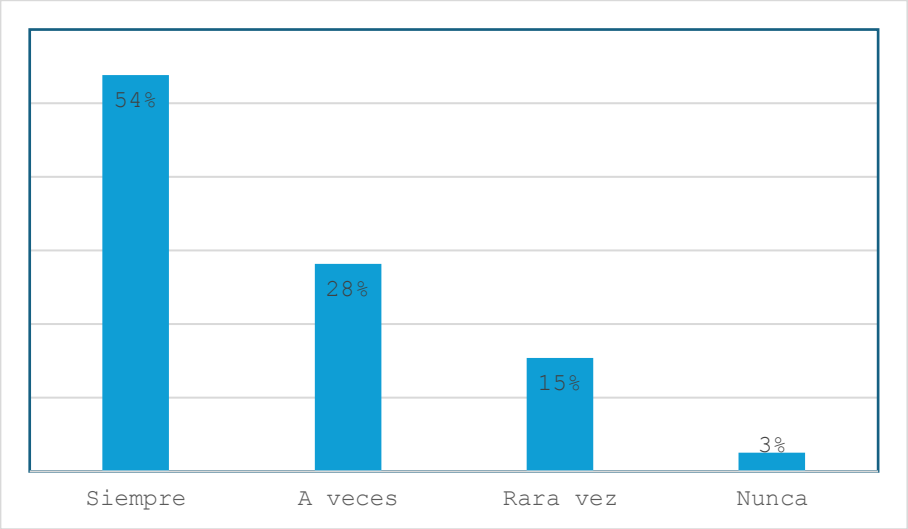


Figura 6. Diagrama de barras de los resultados de la P5.

En la **Figura 6** se observa que el 54% de los encuestados afirma utilizar contraseñas seguras con frecuencia para proteger sus cuentas en línea, lo que sugiere una conciencia relativamente alta sobre la importancia de esta medida de seguridad. En contraste, un 28% solo emplea contraseñas seguras de forma ocasional, mientras que un 15% lo hace rara vez y un 3% nunca utiliza contraseñas seguras. Estos resultados destacan la necesidad de reforzar la educación en prácticas de seguridad digital para fomentar una adopción más consistente de contraseñas robustas.

P6. ¿Alguna vez has recibido mensajes sospechosos o enlaces desconocidos que te hayan hecho sentir inseguro en línea?

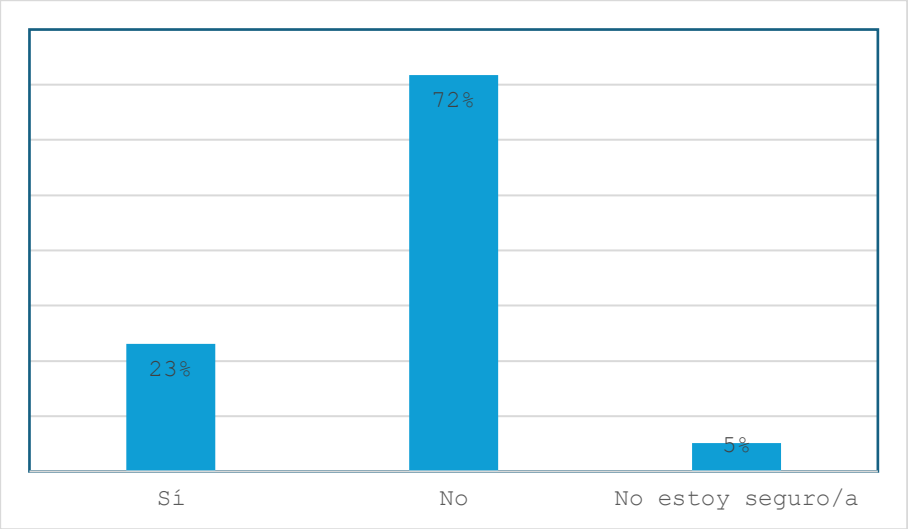


Figura 7. Diagrama de barras de los resultados de la P6.

La **Figura 7** indica que un 72% de los encuestados no ha recibido mensajes o enlaces desconocidos que les hayan generado inseguridad en línea, mientras que un 23% sí ha tenido esta experiencia y un 5% no está seguro. Estos resultados subrayan la importancia de promover la educación en ciberseguridad para ayudar a los usuarios a identificar y gestionar adecuadamente contenido sospechoso.

P7. ¿Te sientes seguro/a usando redes públicas de Wi-Fi para acceder a cuentas personales (correo, redes sociales, banca en línea)?

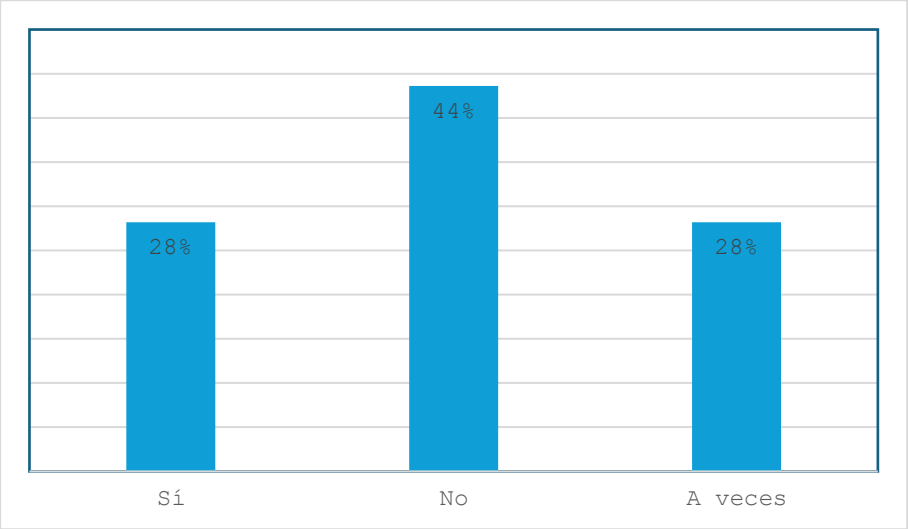


Figura 8. Diagrama de barras de los resultados de la P7.

La **Figura 8** muestra que un 44% de los encuestados no se siente seguro al usar sus cuentas personales en redes públicas, mientras que un 28% sí se siente seguro y un 28% solo a veces. Estos resultados resaltan la importancia de educar sobre los riesgos en redes públicas y fomentar prácticas seguras, como el uso de VPN y autenticación en dos pasos.

P8. ¿Qué tan importante consideras que es la seguridad en línea para tu vida diaria?

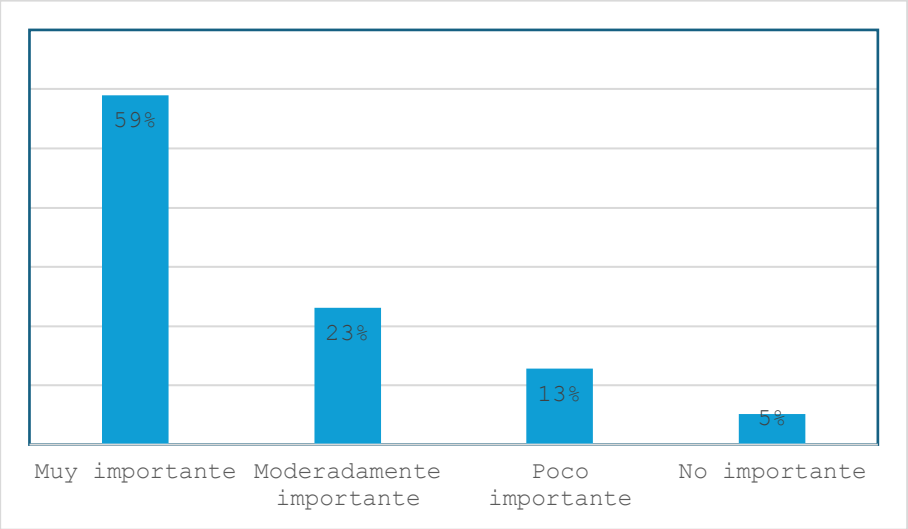


Figura 9. Diagrama de barras de los resultados de la P8.

La **Figura 9** indica que el 59% de los encuestados considera que su seguridad en línea es altamente importante en su vida diaria, lo que demuestra una conciencia significativa sobre la protección de su información personal. Por otro lado, un 23% la percibe como moderadamente importante, mientras que un 13% le otorga poca importancia y un 5% no la considera relevante. Estos resultados destacan la necesidad de reforzar la educación en ciberseguridad para fomentar una mayor valoración de la seguridad en línea, especialmente.

P9. ¿Crees que es ético compartir información o imágenes de otras personas en redes sociales sin su consentimiento?

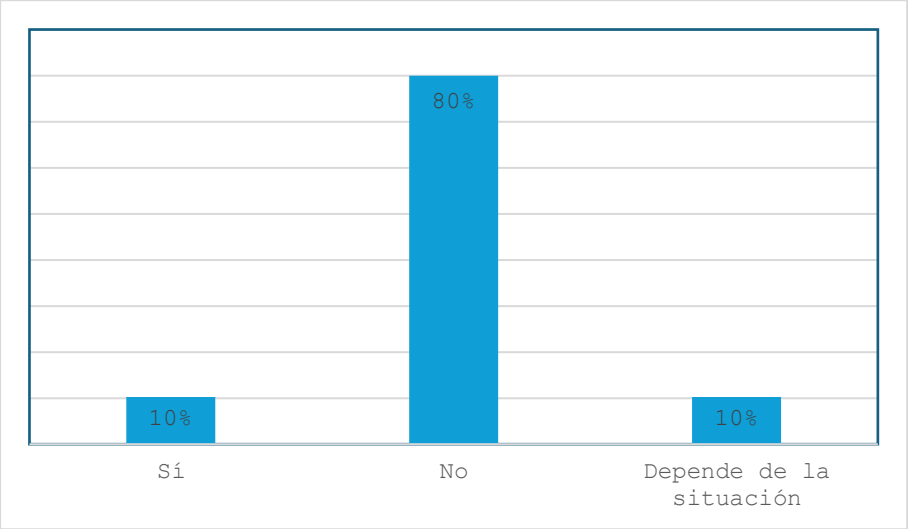


Figura 10. Diagrama de barras de los resultados de la P9.

En la **Figura 10** se observa que el 80% de los encuestados considera que compartir información personal de otras personas sin su permiso no es ético, lo que refleja un alto nivel de respeto por la privacidad ajena. Sin embargo, un 10% opina que la ética de esta acción depende de la situación específica, mientras que un 10% cree que sí es ético hacerlo. Estos resultados subrayan la importancia de fortalecer la educación en ética digital y privacidad, promoviendo una mayor conciencia sobre el respeto a la confidencialidad y el consentimiento en el manejo de la información personal de terceros.

P10. ¿Alguna vez has sido testigo de ciberacoso o comportamiento no ético en línea (como la difusión de noticias falsas o comentarios ofensivos)?

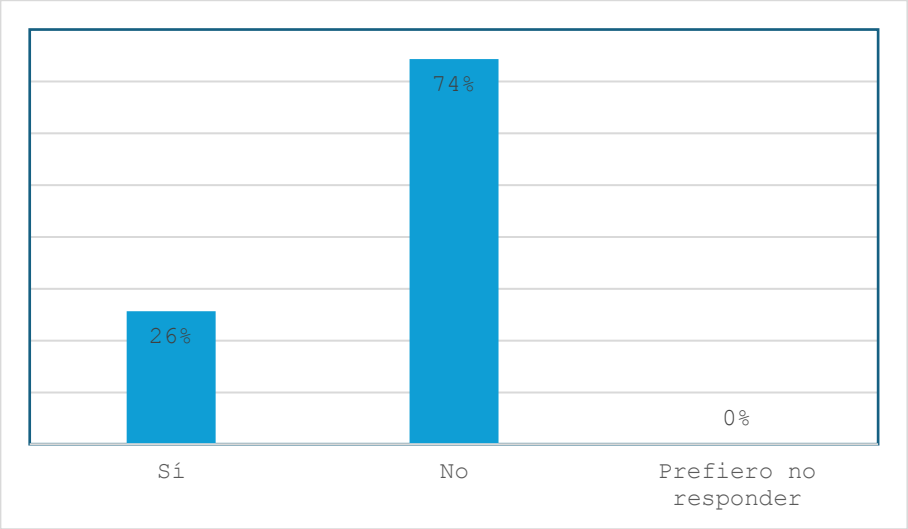


Figura 11. Diagrama de barras de los resultados de la P10.

La **Figura 11** indica que el 74% de los encuestados no ha sido testigo de comportamientos no éticos en línea, mientras que el 26% sí los ha presenciado. Aunque la mayoría no ha observado conductas inapropiadas, una parte significativa ha estado expuesta a ellas, lo que subraya la necesidad de fomentar una cultura de ética y responsabilidad en el uso de tecnologías digitales para reducir la normalización de estas conductas.

P11. ¿Consideras que los desarrolladores de tecnologías deben ser responsables de la aplicación de las leyes existentes que permitan proteger la privacidad de los usuarios?

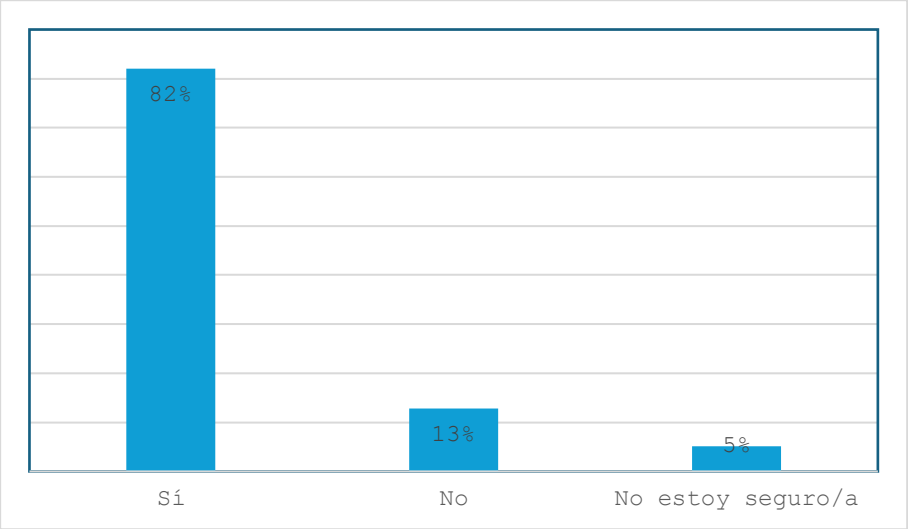


Figura 12. Diagrama de barras de los resultados de la P11.

La **Figura 12** revela que el 82% de los encuestados cree que los desarrolladores de tecnologías deben ser responsables de las implicaciones éticas de sus productos, indicando una alta expectativa de responsabilidad social en el sector. En contraste, el 13% opina que no deberían tener dicha responsabilidad y el 5% prefirió no responder. Estos resultados destacan la necesidad de que las empresas tecnológicas adopten políticas y prácticas éticas en el desarrollo de sus productos.

P12. ¿Qué tan informado/a te sientes sobre las implicaciones éticas del uso de la inteligencia artificial (IA) y otras tecnologías emergentes?

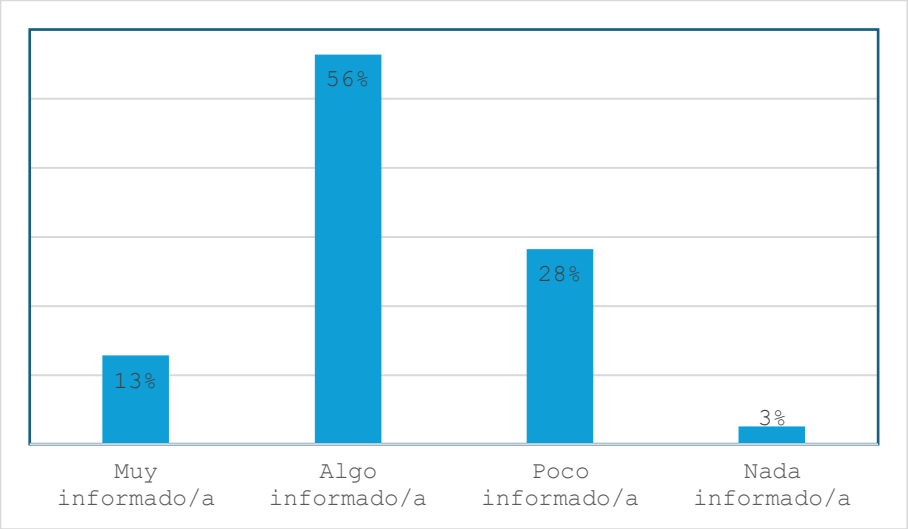


Figura 13. Diagrama de barras de los resultados de la P12

La **Figura 13** indica que un 56% de los encuestados se considera algo informado sobre las implicaciones éticas del uso de la inteligencia artificial y otras tecnologías emergentes, lo que sugiere un nivel moderado de conciencia en este ámbito. Por otro lado, un 28% se siente poco informado, un 13% se considera muy informado y un 3% afirma no estar informado en absoluto. Estos resultados indican la necesidad de incrementar la educación y la divulgación sobre la ética en el uso de tecnologías emergentes, para garantizar que más personas comprendan los desafíos y responsabilidades asociados con su implementación y uso.

CAPÍTULO 5. Marco Propositivo

5.1.Planificación de la actividad propositiva

Tras analizar los resultados obtenidos a partir de la encuesta y la revisión literaria, se propone el siguiente plan estratégico, diseñado como una herramienta clave para reducir la desinformación sobre seguridad informática entre los estudiantes de primero de bachillerato del Colegio Cap. Edmundo Chiriboga.

5.1.1. Datos informativos de la propuesta

Título de la propuesta: Plataforma Educativa Virtual de Aprendizaje sobre Seguridad Informática **(PEVASI)** para estudiantes del Colegio Cap. Edmundo Chiriboga.

Beneficiarios principales: Docente y estudiantes de primero de bachillerato del Colegio Cap. Edmundo Chiriboga.

5.1.2. Introducción

La presente propuesta “PEVASI” , tiene como objetivo principal desarrollar una actividad educativa e informativa a través de una plataforma virtual, centrada en la seguridad informática. Su finalidad es reducir la desinformación existente entre los estudiantes de primero de bachillerato del Colegio Cap. Edmundo Chiriboga.

Esta propuesta se fundamenta en los resultados obtenidos durante la investigación, identificando y abordando necesidades clave relacionadas con la **privacidad en Internet**, la **seguridad en el uso de las TIC** y la **ética en el manejo de herramientas tecnológicas**. Estas áreas han sido seleccionadas por su relevancia para fomentar hábitos seguros y responsables en el

uso cotidiano de Internet y de las plataformas digitales.

En definitiva, **PEVASI** busca no solo informar, sino también transformar las prácticas digitales de los estudiantes, promoviendo un entorno educativo más seguro y ético acorde a las demandas de la era digital.

5.1.3. Objetivos de la propuesta

Objetivo Principal

Desarrollar una actividad educativa e informativa a través de una plataforma virtual, centrada en la seguridad informática en los estudiantes de primero de bachillerato del Colegio Cap. Edmundo Chiriboga.

Objetivos específicos

- Promover la importancia de mantenerse informado sobre temas relacionados con la seguridad informática.
- Fortalecer las competencias digitales del docente y estudiantes a través del uso integrado de las TIC.
- Diseñar contenidos educativos enfocados en la privacidad en Internet y la seguridad informática, adaptados al nivel de comprensión de los estudiantes de primero de bachillerato.

5.1.4. Marco Teórico

Metaverso

El Metaverso es un mundo virtual inmersivo al que podremos acceder mediante una

variedad de dispositivos diseñados para hacernos sentir que estamos realmente dentro de él, interactuando con sus elementos como si formaran parte de nuestra realidad. A través de gafas de realidad virtual y otros complementos tecnológicos, será posible experimentar una auténtica sensación de teletransportación a un universo completamente nuevo (Alcívar-Cedeño et al., 2023).

Metaverso en la educación

Recientes investigaciones han analizado el impacto y las aplicaciones del metaverso en entornos educativos, centrándose en el diseño de metodologías para integrar tecnologías 3D en la docencia. Estos estudios incluyen el análisis de herramientas del metaverso y su influencia en la educación, destacando un creciente interés y aplicaciones prácticas en plataformas como *Second Life*, *Spatial* y *OpenSim*. Los hallazgos sugieren que el metaverso tiene el potencial de promover un aprendizaje más interactivo y colaborativo. Sin embargo, su implementación efectiva exige una comprensión profunda del entorno y el desarrollo de competencias específicas por parte de los educadores (Ordoñez Valencia et al., 2022).

5.2.Desarrollo de la propuesta propositiva

5.2.1. Criterios para proponer una actividad educativa mediante un metaverso

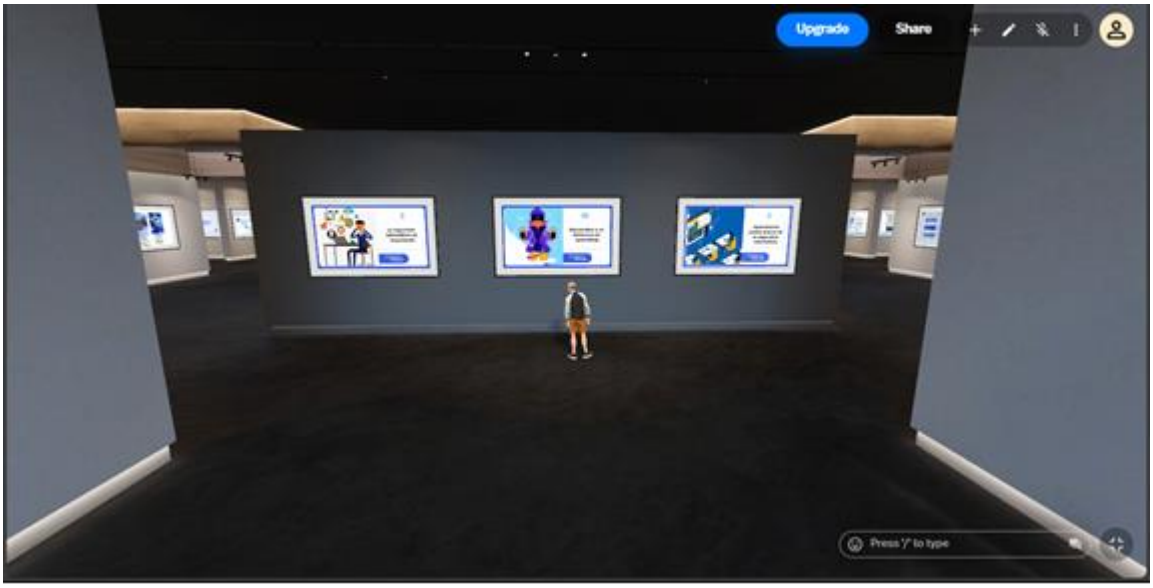


Figura 14. Entorno educativo para el aprendizaje de la seguridad Informática.

En la **Figura 14** se ilustra el entorno en el que se llevará a cabo la actividad de aprendizaje sobre seguridad informática, utilizando un metaverso como plataforma principal. Este enfoque representa una forma innovadora de enseñanza que combina inmersión, interacción y tecnología avanzada para facilitar la comprensión y aplicación de conceptos complejos en un entorno virtual dinámico.

La evolución acelerada de la tecnología continúa sorprendiendo a diario, enfocándose en mejorar la calidad de vida de las personas. El ámbito educativo no es una excepción, ya que actualmente se dispone de diversos materiales didácticos que apoyan a los docentes en sus clases. Entre estas herramientas destacan las plataformas digitales, que ofrecen una amplia gama de actividades adaptables al proceso de enseñanza-aprendizaje. Un ejemplo innovador son las plataformas que permiten crear espacios en 3D, donde se puede alojar información clave para que

los estudiantes aprendan mientras se divierten, integrando entretenimiento y educación de manera efectiva. La propuesta de integrar un espacio virtual para la enseñanza tuvo que considerar diferentes aspectos importantes, tales como:

- **Plataforma novedosa:** En la actualidad, existe una amplia variedad de plataformas que pueden servir como material de apoyo para la enseñanza. En este caso, se propone utilizar la plataforma "Spatial.io", que ofrece numerosas ventajas en el ámbito educativo.
- **Inclusión de recursos visuales:** Se propone la incorporación de recursos multimedia como imágenes, gráficos y videos, complementados con el uso de un avatar personalizable que el estudiante pueda controlar. Esta estrategia tiene como objetivo fomentar una interacción más dinámica y atractiva, potenciando la experiencia de aprendizaje mediante el uso de tecnología avanzada.
- **Información novedosa:** Se buscó incorporar una amplia cantidad de información y recursos sobre seguridad informática, privacidad en Internet y los desafíos éticos de las TIC, con el objetivo de motivar a los estudiantes al explorar y revisar el contenido.
- **Retroalimentación:** Es fundamental evaluar todas las observaciones y sugerencias de los usuarios para generar un proceso de retroalimentación efectivo, lo que permitirá mejorar de manera continua el recurso propuesto.

5.2.2. Contenido de la plataforma virtual educativa

Con base en los resultados obtenidos, se propuso una estrategia para mitigar la desinformación sobre seguridad informática, integrando el uso de objetos de aprendizaje. El objetivo fue crear un recurso virtual atractivo que responda de manera efectiva a las necesidades educativas actuales.

- **Bloques del metaverso educativo**

En la **Tabla 8** se presenta una distribución detallada de la plataforma de aprendizaje sobre seguridad informática, organizada por secciones clave de información. Cada sección está diseñada para abordar aspectos específicos del tema, facilitando así una comprensión estructurada y accesible de los contenidos relevantes para los estudiantes."

Tabla 8. División de contenido del metaverso educativo

Sección	Contenido	Objetivo	Recursos
Bloque 1 Privacidad en Internet	Información acerca de la privacidad en internet	Fomentar el aprendizaje acerca de la privacidad en internet	Metaverso Diapositivas Imágenes Videos
Bloque 2 Seguridad en el Uso de las TIC	Información acerca de la seguridad en el uso de las TIC.	Fomentar el aprendizaje hacer de la seguridad en el de las TIC	
Bloque 3 Ética en el Uso de las TIC	Información acerca de la ética en el uso de las TIC	Fomentar el aprendizaje acerca de la ética en el uso de las TIC	

5.2.3. Uso del metaverso educativo

El metaverso ofrece la posibilidad de realizar una amplia variedad de actividades mientras se aprende de manera interactiva. En la **Figura 15** se ilustra cómo los usuarios pueden interactuar con otros avatares, representando a compañeros estudiantes, fomentando la colaboración y el aprendizaje en un entorno virtual inmersivo.

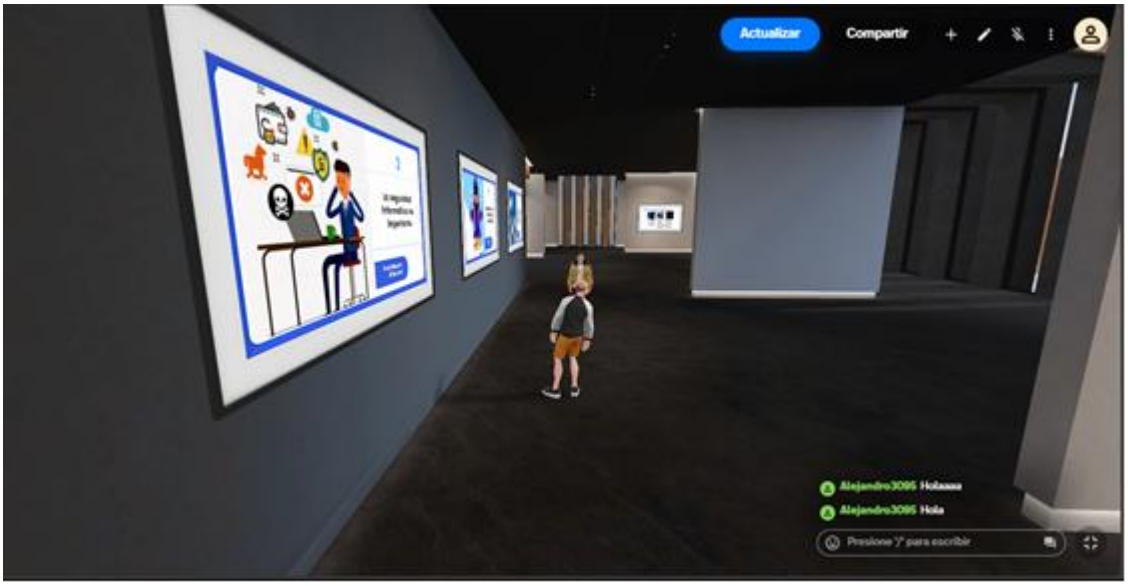


Figura 15. Interacción con otros avatares (estudiantes) en la plataforma.

En la Fig**ura 16** se muestra cómo la plataforma permite visualizar imágenes informativas en un tamaño adecuado, optimizado para facilitar la comprensión y captar con claridad la información presentada. En la **Figura 17** se puede observar de forma más general el metaverso educativo, cabe recalcar que hasta se puede utilizar esta plataforma desde tu teléfono celular esto da un plus ya que puedes ingresar a la plataforma a cualquier hora y educarte acerca de la seguridad informática.

Figura 16. Información para la enseñanza de la seguridad informática.

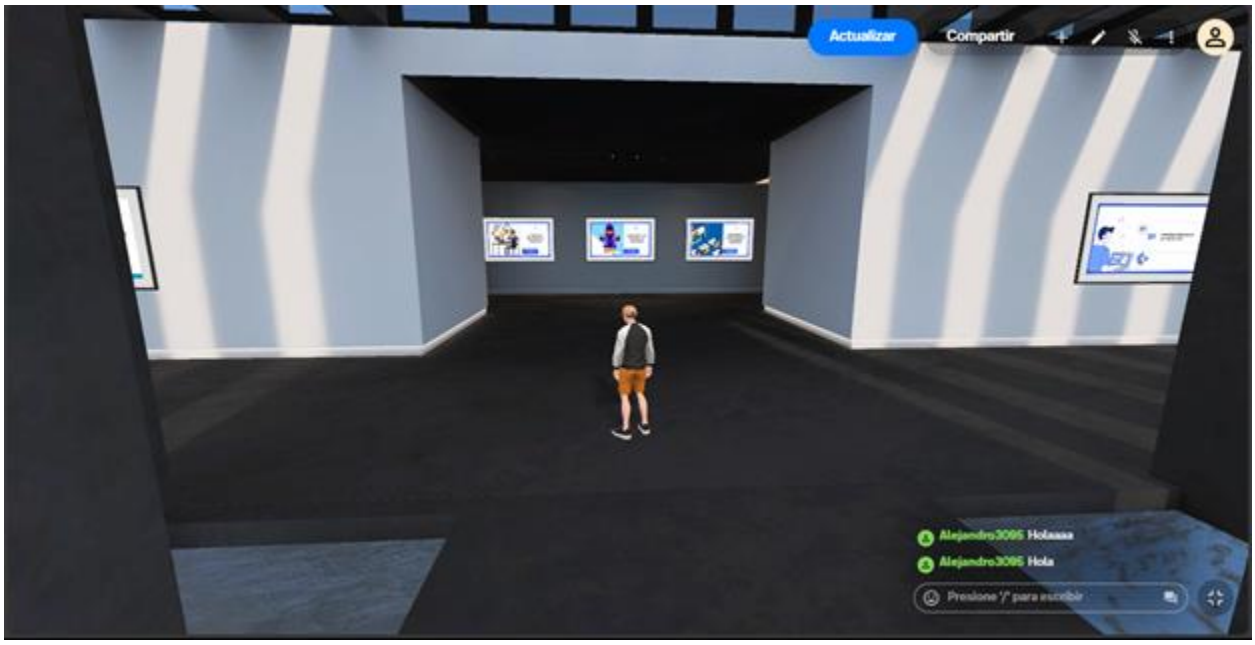


Figura 17. Multiverso educativo

- **Link de ingreso a la plataforma:** https://www.spatial.io/s/Profe_Mayras-3D-Hangout-6754d04bbb9cba0d7e045409?share=24146326800606365

CAPÍTULO 6:

Conclusiones

- Las plataformas educativas en línea presentan múltiples vulnerabilidades en términos de privacidad y seguridad de los datos. Es común el robo de información y la exposición de datos sensibles de estudiantes y docentes. Los resultados de la encuesta aplicada evidencian una falta de conciencia sobre prácticas de seguridad informática, lo que incrementa los riesgos de ataques cibernéticos.
- Las brechas de seguridad en estas plataformas están relacionadas, en gran medida, con errores humanos como el uso de contraseñas débiles, el intercambio de credenciales y la descarga de archivos sospechosos. Para mitigar estos riesgos, es fundamental capacitar a docentes, estudiantes y demás actores educativos en ciberseguridad, promoviendo una cultura de autoprotección digital.
- La implementación de estrategias diseñadas a partir de la evaluación de amenazas permite reducir significativamente los riesgos en las plataformas digitales. Entre las medidas más efectivas se encuentran la encriptación avanzada de datos, la autenticación multifactorial, el uso de firewalls robustos y la actualización constante del software. Asimismo, la realización de auditorías de seguridad periódicas resulta clave para detectar y corregir nuevas vulnerabilidades antes de que sean explotadas. Estas acciones no solo fortalecen la protección de la información, sino que también incrementan la confianza de los usuarios en los entornos educativos digitales.
- Promover la prevención de amenazas digitales ayuda a mitigar problemas como el ciberacoso, la desinformación y la invasión a la privacidad. Un enfoque proactivo en seguridad digital contribuye a la creación de un entorno de aprendizaje seguro, equitativo y confiable para todos

los usuarios.

- Existen marcadas disparidades en el acceso y uso de la tecnología educativa, siendo los principales factores limitantes de tipo económico, geográfico y social. Estas barreras dificultan el desarrollo de competencias tecnológicas, lo que representa una desventaja significativa en un mundo cada vez más digitalizado.
- La brecha digital no solo limita el acceso a herramientas tecnológicas, sino que también amplía la desigualdad en la adquisición de conocimientos y habilidades digitales, afectando el desempeño académico y las oportunidades laborales futuras.
- Para promover la equidad en el aprendizaje digital, es crucial diseñar políticas y programas que faciliten el acceso a tecnología de calidad, capacitación en competencias digitales y recursos educativos inclusivos. Estas estrategias deben considerar un enfoque integral que aborde tanto la infraestructura como la formación de docentes y estudiantes en el uso adecuado de las herramientas digitales.
- Las leyes vigentes presentan diversas inconsistencias en la protección de la privacidad de los datos de estudiantes y docentes frente al uso creciente de plataformas educativas gestionadas por terceros. Además, los datos obtenidos de la encuesta subrayan un bajo conocimiento de estas normativas por parte de los estudiantes, lo que agrava la vulnerabilidad de sus datos personales.
- En Ecuador, la protección de datos se encuentra enmarcada en el artículo 66, numeral 19, el cual reconoce y garantiza el derecho a la protección de datos personales. A pesar de los avances en la creación de un marco legal, la eficacia de estas leyes depende de su correcta aplicación y de la adopción de una cultura de protección de datos dentro del ámbito educativo.
- Los protocolos éticos en el uso de plataformas digitales no solo regulan el comportamiento de

los usuarios, sino que también fomentan la convivencia en línea y el respeto mutuo. Una adecuada formación en ética digital ayuda a prevenir malas prácticas y promueve el desarrollo de competencias digitales responsables.

- La enseñanza de principios éticos en entornos digitales es fundamental para que docentes, estudiantes y otros actores adopten prácticas responsables en el uso de la tecnología. La capacitación continua en competencias digitales y ética tecnológica permite fortalecer la cultura de respeto, seguridad y responsabilidad en el ecosistema educativo digital.

Recomendaciones

- Implementar talleres dirigidos a estudiantes, docentes y familias para concienciar sobre la seguridad informática, enfatizando buenas prácticas como el uso de contraseñas seguras, la protección de datos personales y la identificación de amenazas cibernéticas en plataformas educativas.
- Expandir el metaverso educativo con escenarios interactivos que simulen ciberataques comunes, permitiendo a los usuarios aprender estrategias de protección de manera práctica y dinámica.
- Implementar campañas educativas sobre derechos digitales y políticas de seguridad de datos, utilizando herramientas innovadoras como entornos virtuales inmersivos para reforzar el aprendizaje.
- Fomentar la creación de un marco regulatorio que exija a las plataformas educativas el cumplimiento de estándares de protección de datos, estableciendo sanciones económicas para aquellas que incumplan las normativas.
- Promover alianzas entre el sector público y privado para facilitar la inversión en infraestructura tecnológica, conectividad gratuita y equipamiento básico, asegurando que todos los estudiantes tengan acceso equitativo a la educación digital.
- Evaluar el nivel de alfabetización digital de docentes y estudiantes para identificar carencias formativas y diseñar programas de capacitación adaptados a las necesidades y condiciones de cada grupo, garantizando un uso efectivo de la tecnología.
- Establecer normas precisas para el manejo de datos personales en entornos educativos, asegurando que docentes, estudiantes y demás actores educativos estén informados y capacitados en prácticas de protección de datos.

- Impulsar la creación de normativas que obliguen a las plataformas educativas a cumplir con estándares de seguridad y privacidad de datos, garantizando la protección de la información de los usuarios.
- Fomentar la colaboración entre familias, docentes e instituciones para alinear esfuerzos en la formación ética digital. Esto puede lograrse mediante iniciativas conjuntas que establezcan acuerdos sobre el uso de dispositivos móviles, el respeto en entornos digitales y la concienciación sobre los riesgos y beneficios de la tecnología.
- Promover el uso de plataformas digitales como herramientas de aprendizaje, incentivando metodologías innovadoras que permitan desarrollar competencias digitales y fortalecer el pensamiento crítico en entornos educativos.

Referencias bibliográficas

Agnelli Faggioli , A. (2020). Las tecnologías de la información y la comunicación y su avance en el contexto educativo. *Revista Metropolitana de Ciencias Aplicadas, 3*(1), 94-101.

Alcívar-Cedeño, A., Bastidas Logroño, D., Toctaguano Cruz, S., & Mora Marcillo, A. (2023). Interacción Humano-Computador en el Metaverso Educativo. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 5*(2), 94–104.

Arras Vota, A., Bordas Beltrán, J., Porras Flores, D., & Gutiérrez Diez, M. (2021). Evolución en el uso de las tecnologías de la información y comunicación (TIC) y competencias de los docentes de la Universidad Autónoma de Chihuahua (México), durante la pandemia. *Formación universitaria, 14*(6), 183-192. doi:http://dx.doi.org/10.4067/S0718-50062021000600183.

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de protección de datos.* Quito: Lexis.sa.

Azuero Azuero, Á. (2019). Significatividad del marco metodológico en el desarrollo de proyectos de investigación. *Revista Arbitrada Interdisciplinaria Koinonía, 4*(8), 110. doi:10.35381/r.k.v4i8.274

Caballero, M., Lerma, L., & Serrano, D. (2022). *Ciberseguridad paso a paso.* ANAYA.

Cajamarca-Correa , M., Cangas-Cadena, A., Sánchez-Simbaña, S., & Pérez-Guillermo, A. (2024). Nuevas tendencias en el uso de recursos y herramientas de la Tecnología Educativa para la Educación Universitaria. *Journal of Economic and Social Science Research, 4*(3), 127–150. doi:https://doi.org/10.55813/gaea/jessr/v4/n3/124

Carissa, V. (2020). *La privacidad es poder.* XcUiDi. doi:10.46652/pacha.v3i7.91

Carmona Vásquez , J., & Monsalve Giraldo, E. (2024). *Plataforma de ciberseguridad para el aprendizaje y entrenamiento de hacking ético para estudiantes universitarios.* Antioquia: Ingeniería de Sistemas y Computación.

Castro Rodríguez, Y. (2020). El plagio académico desde la perspectiva de la ética de la publicación científica. *Revista Cubana de Información en Ciencias de la Salud 2020, 31*(4).

Copola, M. (16 de 1 de 2023). *Qué es una plataforma digital, qué tipos existen y ejemplos*. Recuperado el 21 de 7 de 2024, de https://blog.hubspot.es/website/que-es-plataforma-digital

Cortés-Nájera, M. d. (2022). La Integridad Académica, un desafío en tiempos de pandemia. *Con-Ciencia Boletín Científico De La Escuela Preparatoria, 9*(3), 96-99.

Díaz Arce, D. (2023). Plagio a la Inteligencia Artificial en estudiantes de bachillerato: un problema real. *Revista Innova Educación, 5*(2), 108-116. doi:https://doi.org/10.35622/j.rie.2023.02.007

Espinosa Cevallos, P. (2024). Efectos de las Tecnologías de la Información y Comunicación en la educación. *Revista Ingenio Global, 3*(1), 63-77. doi:https://doi.org/10.62943/rig.v3n1.2024.75

Espinosa Izquierdo, J. G., Jaime Andrés, E. F., & Espinosa Arreaga, G. (2021). E-learning una herramienta necesaria para el aprendizaje. *Polo del conocimiento, 6*(3), 659-669. doi:https://doi.org/10.23857/pc.v6i3.2394

Espinoza Freire, E. (2018). Gestión del conocimiento mediado por tic en la Universidad técnica de Machala. *Fides Et Ratio, 16*(16), 199-219.

Fernández Bedoya, V. (2020). Tipos de justificación en la investigación científica. *Espíritu Emprendedor TES, 4*(3), 65–76. doi:https://doi.org/10.33970/eetes.v4.n3.2020.207

Fortine. (01 de 05 de 2024). *Fortine*. Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

Fuenmayor Tobar, J., Torres Lozano, D., Monsalve Pérez, L., & Becerra Moreno, A. (2024). La inteligencia artificial y Blockchain, dos elementos decisivos en el futuro de la ciberseguridad. *AGUNKUYAA, 14*(1). doi:https://doi.org/10.33132/27114260.2431

Garcia, P., & Pesantez, D. (2023). Análisis de ciberseguridad en plataformas e-learning: revisión sistemática de la literatura. *Revista Perspectivas, 5*(1), 19-23. doi:https://doi.org/10.47187/perspectivas.5.1.179

Gascón Marcén, A. (2021). El reglamento general de protección de datos como modelo de las recientes propuestas de legislación digital europea. *Cuadernos de Derecho Transnacional, 13*(2), 210-219. doi:https://doi.org/10.20318/cdt.2021.6256

Gaviria Lopera, J., Villamizar Jaimes, A., Soto Durán, D., & Reyes Gamboa , A. (2023). Buenas prácticas en la gestión en seguridad. *Revista Ibérica de Sistemas e Tecnologias de Información, 6*(3), 50-61.

Guevara Alban, G., Verdesoto Arguello, A., & Castro Molina, N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-

acción). *RECIMUNDO, 4*(3), 163–173. doi:https://doi.org/10.26820/recimundo/4.(3).julio.2020.163-173

Mariscal San Martin, L., Ponce Mariscal, A., Cintra Lugones, Á., & Céspedes Acuña, J. (2022). La era digital: nuevos desafíos éticos para el docente. *Maestro Y Sociedad, 7*(1), 1009–1017.

Mariscal-San Martin, L., & Ponce Mariscal, A. (s.f.).

Martín Fernández, A., Jódar Reyes, M., & Valenzuela López, I. (2022). Tecnologías de la información y comunicación (TIC) en formación y docencia. *Formación Médica Continuada en Atención Primaria, 29*(3), 28-38. doi:https://doi.org/10.1016/j.fmc.2022.03.004

Morales Paredes, P., & Chicaiza, P. (2021). Ciberseguridad en plataformas educativas. *Dialnet, 10*(2), 54-59. doi:10.17993/3ctic.2021.102.49-75

Navarro , G. (2022). *Introducion a las vulneabilidades.* Catalunya: Universidad de Catalunya.

Novas, N. (2022). Implementación de las Tics en la enseñanza/aprendizaje de la historia: retos y desafíos. *Revista Digital de Comunicación,, 11*(1), 159-170.

Ordóñez Pineda, L., & Calva Jiménez, S. (2020). Amenazas a la privacidad de los menores de edad a partir del Sharenting. *Revista chilena de derecho y tecnología, 9*(2), 105-130. doi:http://dx.doi.org/10.5354/0719-2584.2020.55333

Ordoñez Valencia, M., Ordoñez Zúñiga, N., Mantilla-Ordóñez, J., Garcés Wila, M., Vera Arroyo, D., & Coronel Méndez, W. (2022). Análisis de herramientas de metaverso y su impacto en contextos educativos. *Revista Internacional de Estudios Interdisciplinarios, 3*(2), 610–630. doi:https://doi.org/10.51798/sijis.v3i2.366

Orozco, H., & lamberto, J. (2022). La ética en la investigación científica: consideraciones desde el área educativa. *Perspectivas, 10*(19), 11-21.

Paz Saavedra, L., & Gisbert Cervera, M. (2020). Desafíos para las universidades colombianas frente a políticas nacionales e internacionales de integración de TIC en la educación. *Revista Electrónica De Tecnología Educativa*(73), 51-65. doi:https://doi.org/10.21556/edutec.2020.73.1617

Quintero Ayala, L. (2020). Educación inclusiva: tendencias y perspectivas. *Educación y Ciencia*(24), 11-23. doi:https://doi.org/10.19053/0120-7105.eyc.2020.24.e11423

Rodríguez Samudio, R. (2019). La privacidad en las ciudades inteligentes. *CES Derecho, 19*(2),

675-695. doi:10.21615/cesder.10.2.7

Rodríguez, P. (2021). Aplicaciones educativas digitales y la falta de seguridad de los datos personales de sus usuarios. *Revista Iberoamericana para la Investigación y el Desarrollo Educativo, 12*(23), 34-36. doi:https://doi.org/10.23913/ride.v12i23.980

Salgado Reyes, N. (2023). Evolución de la Educación y las aplicaciones tecnologías. *Polo del conocimiento, 8*(4), 1319-1328. doi:https://doi.org/10.23857/pc.v8i4.5502

Solano-Gutiérrez, G. (2024). La Tecnología en la Educación a Distancia: Revisión de Progresos y Obstáculos a Superar. *Revista Científica Zambos, 3*(2), 48-73. doi: https://doi.org/10.69484/rcz/v3/n2/17

Soto Rodríguez, A. (2021). El plagio y su impacto a nivel académico y profesional. *E-Ciencias De La Información, 2*(1), 1-13. doi:https://doi.org/10.15517/eci.v2i1.1213

Suárez Álvarez, R., Vázquez Barrio, T., & Torrecillas Lacave, T. (2020). Metodología y formación docente cuestiones claves para la integración de las TIC en la educación. *Ámbitos. Revista Internacional De Comunicación*(49), 197-215. doi:https://doi.org/10.12795/Ambitos.2020.i49.12

Suárez-Guerrero, C., & Lloret-Catalá, C. (2022). La Digitalización de la Educación en Pandemia. Mirada del. *Revista Iberoamericana sobre Calidad, Eficacia y Cambio en Educación, 20*(4), 127-146. doi:https://doi.org/10.15366/reice2022.20.4.007

Victor Hugo, F. (65–76). Tipos de justificación en la investigación científica. *Espíritu Emprendedor TES*, 2020.

Vital Carrillo, M. (2021). Plataformas Educativasy herramientas digitalespara el aprendizaje. *Vida Científica, 9*(18), 9-12.

Apéndice A. Encuesta

Desafíos Éticos en Privacidad, Seguridad y Ética en las TICs

Objetivo:

Esta encuesta tiene como objetivo
comprender la percepción y los desafíos que los estudiantes enfrentan en torno a los temas de privacidad, seguridad y ética en el uso de las Tecnologías de la Información y la Comunicación (TICs).

* Indica que la pregunta es obligatoria

Instrucciones: Por favor, selecciona la opción que mejor refleje tu opinión para cada pregunta. Tus respuestas son anónimas y confidenciales.

1. **1.** ¿Con qué frecuencia lees las políticas de privacidad antes de usar un servicio en línea o aplicación? *

   Marca solo un óvalo.

   - ◯ Siempre
   - ◯ A veces
   - ◯ Rara Vez

2. **2.** ¿Cuán preocupado/a estás por la privacidad de tus datos personales cuando navegas en línea? *

   Marca solo un óvalo.

   - ◯ Muy preocupado/a
   - ◯ Moderadamente preocupado/a
   - ◯ Poco preocupado/a
   - ◯ No me preocupa

3. 3.¿Alguna vez has experimentado una vulneración de privacidad en línea (por ejemplo, robo de información personal)? *

Marca solo un óvalo.

- Si
- No
- No estoy seguro/a

4. 4.¿Crees que las empresas tecnológicas respetan adecuadamente la privacidad de sus usuarios? *

Marca solo un óvalo.

- Si
- No
- No estoy seguro/a

5. 5.¿Con qué frecuencia usas contraseñas seguras (combinación de letras, números y símbolos) para tus cuentas en línea? *

Marca solo un óvalo.

- Siempre
- A veces
- Rara vez
- Nunca

6. *

6.¿Alguna vez has recibido mensajes sospechosos o enlaces desconocidos que te hayan hecho sentir inseguro en línea?

Marca solo un óvalo.

- Sí
- No
- No estoy seguro/a

7. 7.¿Te sientes seguro/a usando redes públicas de Wi-Fi para acceder a cuentas personales (correo, redes sociales, banca en línea)? *

Marca solo un óvalo.

- Sí
- No
- A veces

8. 8. ¿Qué tan importante consideras que es la seguridad en línea para tu vida diaria? *

Marca solo un óvalo.

- Muy importante
- Moderadamente importante
- Poco importante
- No importante

9. 9.¿Crees que es ético compartir información o imágenes de otras personas en redes sociales sin su consentimiento? *

Marca solo un óvalo.

- Sí
- No
- Depende de la situación

10. 10.¿Alguna vez has sido testigo de ciberacoso o comportamiento no ético en línea (como la difusión de noticias falsas o comentarios ofensivos)? *

Marca solo un óvalo.

- Sí
- No
- Prefiero no responder

11. 11. ¿Consideras que los desarrolladores de tecnologías deben ser responsables de las implicaciones éticas de sus productos? *

Marca solo un óvalo.

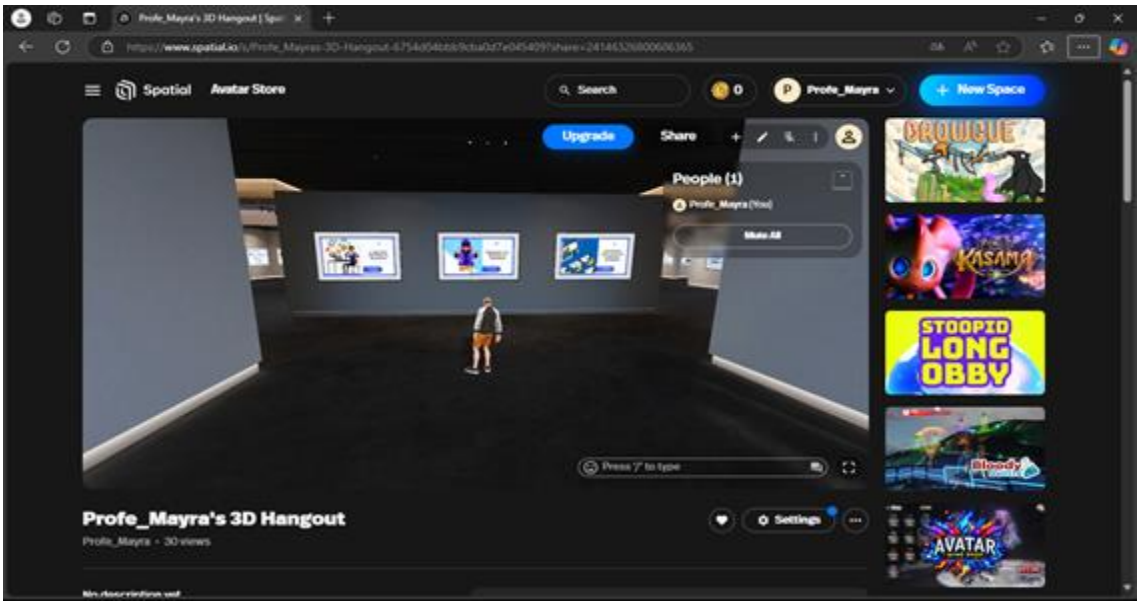
- Sí
- No
- No estoy seguro/a

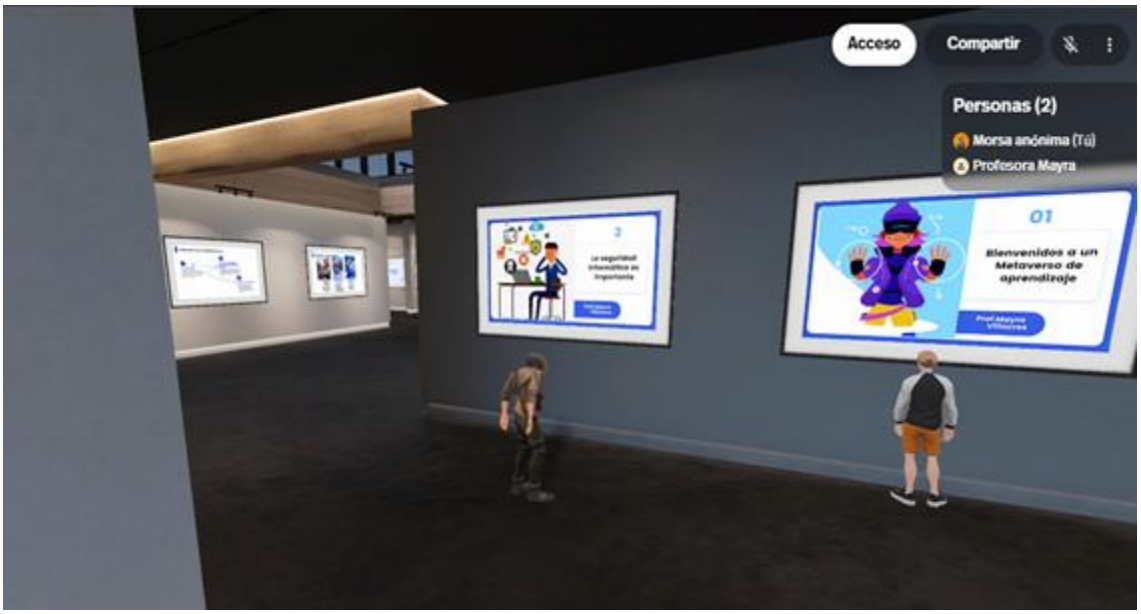
12. 12. ¿Qué tan informado/a te sientes sobre las implicaciones éticas del uso de la inteligencia artificial (IA) y otras tecnologías emergentes? *

Marca solo un óvalo.

- Muy informado/a
- Algo informado/a
- Poco informado/a
- Nada informado/a

Apéndice B. Diseño del Metaverso Informativo




Acceso
Compartir
Personas (2)
Morsa anónima (Tú)
Profesora Mayra
01
Bienvenidos a un Metaverso de aprendizaje