Elaboración de un Estudio Investigativo sobre las Amenazas Emergentes en Plataformas Educativas en ambientes escolares basado en sanas prácticas de la industria de Ciberseguridad en el contexto académico para los estudiantes del grado decimo hasta duodécimo en el año 2025, Dirección Regional de Pérez Zeledón

Jordan Andrés Elizondo Umaña
elizondojordan96@gmail.com
Maestría en Ciberseguridad
Universidad San Isidro Labrador

***Resumen*— Este estudio analiza las amenazas emergentes en plataformas educativas utilizadas en instituciones de secundaria del cantón de Pérez Zeledón, Costa Rica. La investigación evaluó el nivel de exposición, preparación y vulnerabilidades de estudiantes y docentes mediante cuestionarios y entrevistas semiestructuradas. Los resultados evidencian brechas críticas en formación digital, ausencia de protocolos institucionales y escaso conocimiento sobre prácticas básicas de seguridad. A partir de estos hallazgos se plantea una propuesta basada en buenas prácticas de la industria de la ciberseguridad para fortalecer la protección de los entornos escolares y promover una cultura digital preventiva.**

Palabras claves— ciberseguridad educativa, plataformas educativas, amenazas digitales, protocolos escolares, MEP, MICITT, ciudadanía digital.

***Abstract*— This study analyzes emerging cybersecurity threats affecting digital educational platforms in secondary schools in Pérez Zeledón, Costa Rica. The research evaluated exposure levels, digital preparedness, and vulnerabilities among students and teachers through questionnaires and semi-structured interviews. Results indicate critical gaps in digital training, lack of institutional cybersecurity protocols, and limited awareness of basic security practices. Based on these findings, the study proposes a set of cybersecurity measures aligned with industry best practices to strengthen the protection of school digital environments and foster a preventive culture.**

Keywords— educational cybersecurity, learning platforms, digital threats, school protocols, digital citizenship.

I. INTRODUCCIÓN

La incorporación de la tecnología en los procesos educativos costarricenses representa uno de los cambios estructurales más significativos de las últimas décadas. En el contexto reciente, especialmente a partir de la pandemia por COVID-19, las instituciones educativas de secundaria adoptaron plataformas digitales como medios esenciales para la continuidad pedagógica. Herramientas como Google Classroom, Microsoft Teams, Edutec, Moodle, Zoom y otras soluciones en la nube se convirtieron en parte integral del quehacer académico diario. Sin embargo, esta adopción masiva ocurrió sin que existiera una planificación estratégica, una cultura institucional fortalecida o una formación adecuada en ciberseguridad para los actores involucrados.

El ecosistema escolar tiene particularidades que lo diferencian de otros sectores: la mayoría de usuarios son menores de edad, un grupo poblacional con vulnerabilidades cognitivas y emocionales asociadas a su etapa de desarrollo, sumado a una limitada comprensión de los riesgos digitales. Paralelamente, gran parte del personal docente carece de conocimientos sólidos sobre amenazas informáticas, protocolos de protección de datos, gestión segura de plataformas y aspectos legales relacionados con el tratamiento de información personal.

Este desfase entre el uso intensivo de tecnologías y el nivel de preparación de la comunidad educativa crea un entorno propicio para que amenazas emergentes—como phishing, ransomware, suplantación de identidad, filtración de datos académicos, ciberacoso, accesos no autorizados y manipulación de credenciales—afecten la integridad, disponibilidad y confidencialidad de los datos escolares. En muchos casos, estas amenazas se presentan sin ser detectadas o son manejadas de manera informal, lo cual incrementa el impacto real sobre estudiantes, docentes e instituciones.

La presente investigación analiza a profundidad esta situación en el contexto del cantón de Pérez Zeledón, aportando datos empíricos obtenidos mediante cuestionarios aplicados a estudiantes y docentes, así como entrevistas a docentes y a un asesor del Ministerio de Educación Pública (MEP). El objetivo central es ofrecer una visión clara del panorama actual y formular una propuesta de medidas prácticas, contextualizadas y fundamentadas en buenas prácticas de la industria de la ciberseguridad.

1.1. Antecedentes del tema

Diversos informes internacionales sustentan la preocupación creciente sobre los riesgos digitales en entornos educativos. Check Point Research reporta que durante 2022 y 2023 el sector educativo se posicionó entre los más atacados a nivel mundial, con un incremento del 44% en intentos de intrusión semanales. En países como Estados Unidos se contabilizaron más de 1.780 incidentes en instituciones del sector K-12 durante 2023, incrementando las filtraciones de datos personales y afectando procesos académicos completos.

En el Reino Unido, un informe del Department for Science, Technology and Innovation (2025) reveló que más del 91% de las universidades, el 85% de los centros técnicos y el 60% de las escuelas secundarias experimentaron incidentes de seguridad en el último año. Esta vulnerabilidad se asocia a contraseñas débiles, falta de autenticación multifactor, ausencia de auditorías, desconocimiento docente y configuraciones inseguras en plataformas digitales.

En América Latina, tanto el BID como la UNESCO han documentado la desigualdad en acceso, la falta de acompañamiento técnico y la escasa adopción de políticas de ciberseguridad. La región presenta un grado moderado de digitalización, pero con profundas brechas formativas, lo cual aumenta la exposición de estudiantes y docentes a riesgos digitales.

En Costa Rica, la Estrategia Nacional de Ciberseguridad (MICITT, 2023) reconoce que las instituciones educativas carecen de protocolos claros, personal técnico especializado y estrategias unificadas para la prevención y respuesta ante incidentes. La mayoría de los centros dependen de personal docente que, aunque comprometido, no ha recibido formación suficiente para gestionar amenazas digitales.

1.2. Importancia de abordar el tema

La relevancia de este estudio radica en que protege a la población más vulnerable del sistema educativo: los menores de edad. Los estudiantes participan en plataformas digitales sin conciencia de los riesgos inherentes al uso de Internet. Asimismo, comparten información personal, utilizan contraseñas débiles, acceden desde dispositivos poco seguros y se exponen a situaciones de acoso digital sin saber cómo actuar.

Por otra parte, la ciberseguridad escolar no solo tiene implicaciones técnicas, sino también pedagógicas, éticas, legales y psicológicas. La pérdida de información académica, la exposición a contenido nocivo, la filtración de datos, la suplantación y la interrupción de actividades pueden causar daños significativos en el proceso formativo y en la salud emocional del estudiantado.

A esto se suma que las instituciones deben cumplir con normativas nacionales como la Ley 8968 sobre protección de datos y la Ley 8990 para la protección de menores. Sin embargo, estas leyes se aplican de manera desigual debido al desconocimiento institucional.

Este estudio no solo visibiliza los riesgos, sino que constituye una herramienta esencial para fortalecer la cultura de ciberseguridad en centros educativos, orientando a docentes, administradores y responsables institucionales.

1.3. Objetivo General del TFG

Elaborar una investigación sobre las amenazas emergentes en plataformas educativas en ambientes escolares, basada en buenas prácticas de la industria de ciberseguridad, en el contexto académico de estudiantes de décimo a duodécimo año del cantón de Pérez Zeledón.

1.4. Alcances

El estudio abarca:

• Instituciones educativas de secundaria del cantón de Pérez Zeledón.

• Estudiantes de 10.º a 12.º año, docentes y personal administrativo.

• Plataformas educativas como Microsoft Teams, Google Classroom, Edutec y herramientas de comunicación digital.

• Amenazas emergentes, nivel de exposición, prácticas digitales y cultura de ciberseguridad institucional.

• El segundo semestre del año 2025 como período de análisis.

• La propuesta de lineamientos prácticos para fortalecer la ciberseguridad escolar.

1.5. Limitaciones

El presente estudio, aunque aporta evidencia sólida sobre la realidad de la ciberseguridad educativa en instituciones de secundaria del cantón de Pérez Zeledón, presenta un conjunto de limitaciones inherentes al enfoque metodológico, al alcance definido y a las condiciones particulares del contexto investigado. Estas limitaciones no debilitan los resultados obtenidos, pero son necesarias de reconocer para comprender el marco bajo el cual fueron construidas las conclusiones y para orientar futuras investigaciones en esta área emergente.

En primer lugar, la investigación no tuvo como propósito realizar auditorías técnicas exhaustivas sobre redes institucionales, infraestructura tecnológica, servidores, configuraciones internas de plataformas educativas ni análisis de vulnerabilidades en tiempo real. Esto se debe tanto a razones éticas —pues intervenir o analizar sistemas informáticos sin autorización constituye un riesgo legal y operativo para las instituciones— como a razones prácticas relacionadas con el alcance de un Trabajo Final de Graduación. Por ello, el estudio se centra en percepciones, prácticas, hábitos digitales, nivel de conocimiento y experiencias reportadas por docentes, estudiantes y un asesor del MEP, más no en evaluaciones forenses ni análisis de arquitectura de red.

En segundo lugar, la población estudiada se limita exclusivamente a instituciones de educación secundaria, excluyendo escuelas de primaria y centros universitarios. Esta

delimitación responde al interés particular de analizar los niveles educativos de décimo a duodécimo año, donde se evidencia un uso más intensivo de plataformas educativas digitales, una mayor independencia tecnológica por parte del estudiantado y una exposición más amplia a riesgos relacionados con redes sociales, navegación web, mensajería instantánea y duplas de estudio virtual. No obstante, esta decisión implica que los resultados no pueden generalizarse directamente a poblaciones de otras edades o niveles académicos, cuyos patrones de uso digital y vulnerabilidades pueden diferir sustancialmente.

Asimismo, la muestra estuvo condicionada por un muestreo no probabilístico por conveniencia, determinado por la disponibilidad de las instituciones para participar, el acceso otorgado por la administración escolar y las posibilidades reales de aplicación de instrumentos durante el calendario académico. Esto significa que la cantidad de docentes, estudiantes y entrevistados depende de factores externos al investigador, tales como horarios de clase, permisos institucionales, carga laboral docente, disponibilidad del personal y actividades institucionales paralelas. Si bien este tipo de muestreo es común y aceptado en investigaciones educativas aplicadas, implica que los hallazgos describen tendencias representativas dentro del grupo participante, pero no necesariamente reflejan la totalidad de la realidad educativa del cantón o del país.

Otra limitación importante es que los datos obtenidos provienen de cuestionarios autoadministrados y entrevistas, instrumentos que dependen directamente del nivel de sinceridad, percepción y conocimiento previo de los participantes. En temas como ciberseguridad, donde existe un alto grado de desconocimiento, es posible que docentes o estudiantes hayan respondido basándose en su interpretación personal, y no necesariamente en criterios técnicos. Además, algunos participantes pueden haber minimizado o sobreestimado incidentes por temor, desconocimiento o deseabilidad social. Esto es especialmente relevante en reportes de ciberacoso, suplantación de identidad o errores cometidos en el uso de plataformas. Aun así, el diseño metodológico consideró estos riesgos mediante triangulación de datos entre cuestionarios y entrevistas, fortaleciendo la validez interpretativa.

Una limitación adicional se relaciona con la falta de registros institucionales formales sobre incidentes digitales. La mayoría de centros educativos no documenta sistemáticamente los casos de ciberacoso, accesos no autorizados, hackeo de cuentas estudiantiles o filtraciones de datos. Esta carencia de evidencia documental implica que la investigación depende casi por completo de testimonios y experiencias narradas, lo cual reduce la posibilidad de trazar patrones históricos o evaluar la evolución de la ciberseguridad institucional.

También debe considerarse que el estudio se desarrolló en un periodo temporal específico (segundo semestre de 2025), coincidiendo con actividades escolares particulares, proyectos institucionales y dinámicas propias del cierre lectivo. Esto significa que las prácticas, hábitos o incidentes reportados pueden variar si el estudio se replicara en otro momento del año académico. Factores como la disponibilidad de Internet, la carga de trabajos, la interacción en plataformas o las capacitaciones institucionales pueden fluctuar según el periodo.

Finalmente, es relevante señalar que la investigación se centró en la dimensión humana, pedagógica y administrativa de la ciberseguridad escolar, más no en las posibles soluciones técnicas avanzadas que instituciones con mayor presupuesto podrían implementar, como firewalls de nueva generación, sistemas de detección de intrusiones, auditorías de código, políticas de segmentación de red o herramientas especializadas de monitoreo. Estas tecnologías, aunque deseables, exceden el ámbito de un estudio basado en prácticas educativas en zonas rurales y semiurbanas de Pérez Zeledón.

A pesar de estas limitaciones, los resultados proporcionan una visión clara, contextualizada y pertinente del estado actual de la ciberseguridad escolar en el cantón, constituyendo una base sólida para futuras líneas de acción, estudios comparativos y propuestas de mejora institucional.

II. METODOLOGIA

2.1. Descripción de supuestos

El desarrollo de esta investigación se fundamenta en una serie de supuestos teóricos, metodológicos y contextuales derivados del uso real de plataformas educativas en instituciones de secundaria del cantón de Pérez Zeledón. En primer lugar, se parte del supuesto de que todas las instituciones involucradas utilizan plataformas digitales de forma habitual, ya sea para distribución de contenido, envío de tareas, comunicación o evaluaciones. Este supuesto es coherente con la realidad nacional: tras la pandemia, el MEP institucionalizó de manera tácita el uso de herramientas como Teams y Classroom, generando dependencia en la dinámica escolar.

Otro supuesto clave radica en que los docentes y estudiantes poseen conocimientos previos, aunque desiguales, sobre el uso de herramientas tecnológicas. Esto no implica un dominio técnico, sino el reconocimiento de que al menos algún nivel de interacción con entornos virtuales existe, lo cual permite aplicar instrumentos que evalúan prácticas, percepciones y experiencias.

También se presupone que los incidentes de seguridad no siempre son identificados como tales por los usuarios. Por ejemplo, los estudiantes pueden experimentar suplantación de cuentas, ciberacoso o pérdida de datos sin categorizarlos formalmente como “incidentes digitales”. Por ello, las preguntas del cuestionario están diseñadas en términos accesibles para garantizar respuestas honestas y basadas en experiencias vividas.

Finalmente, se asume que la sinceridad de los participantes permitirá obtener información válida, aunque condicionada por limitaciones cognitivas, emocionales o contextuales propias de cada actor.

2.2. Restricciones de la investigación

Las restricciones metodológicas se relacionan directamente con la dinámica escolar. La principal restricción fue el tiempo disponible para la aplicación de instrumentos, pues las instituciones mantienen horarios estrictos, periodos de exámenes y actividades extracurriculares que limitan las intervenciones de investigación. Esta condición determinó el número final de participantes y los periodos de recolección.

Otra restricción corresponde a la infraestructura tecnológica heterogénea. Mientras algunas instituciones cuentan con conectividad adecuada, otras presentan limitaciones de ancho de banda que dificultaron el acceso simultáneo a cuestionarios en línea, obligando en ciertos casos a realizar la aplicación en formato físico.

El acceso institucional también representó una restricción, pues cada centro educativo posee lineamientos internos sobre visitas, encuestas y gestión de datos. Esto condicionó el tipo de instrumentos aplicables, la cantidad de grupos visitados y la disponibilidad de docentes.

Asimismo, las instituciones no permiten el análisis interno de redes, equipos o servidores por razones legales y éticas. Esta investigación se concentró en el componente humano y pedagógico, renunciando deliberadamente a mecanismos de auditoría técnica profunda que requerirían permisos especiales.

Por último, la falta de registros institucionales sobre incidentes de ciberseguridad dificulta la comparación histórica, lo cual restringe el análisis longitudinal y obliga a basar las conclusiones principalmente en datos auto-reportados**.**

2.3. Riesgos de la investigación

El principal riesgo metodológico identificado es el subregistro de incidentes. Muchos estudiantes o docentes no cuentan sus experiencias por temor a represalias, vergüenza o desconocimiento. Además, en instituciones donde el clima organizacional es rígido, algunos participantes pueden minimizar eventos reales.

Otro riesgo se relaciona con la deseabilidad social, es decir, la tendencia de los participantes a responder “lo que creen correcto” en lugar de brindar información real sobre sus prácticas digitales. Este sesgo es común en estudios sobre hábitos tecnológicos, donde los participantes desean parecer más precavidos de lo que realmente son.

El riesgo técnico más importante es la variabilidad en el acceso a dispositivos, que afecta la consistencia del levantamiento de datos. Algunos estudiantes respondieron desde celulares, otros desde computadoras institucionales o personales, lo que puede influir en su comprensión de ciertas preguntas.

También existe el riesgo de que algunos participantes confundan conceptos técnicos, como phishing, malware, ataques por fuerza bruta o robo de credenciales. Para minimizar este riesgo, el cuestionario fue redactado en lenguaje accesible, sin tecnicismos que pudieran dificultar la interpretación.

2.4. Sujetos de información

Los sujetos de información se seleccionaron estratégicamente según su rol en el ecosistema educativo digital:

• **Docentes de secundaria**

Son actores fundamentales porque utilizan plataformas educativas para administrar clases, proporcionar materiales, evaluar y comunicarse con estudiantes. La investigación reveló que, aunque la mayoría emplea estas herramientas a diario, muchos lo hacen sin formación formal en ciberseguridad, lo que los convierte en un punto crítico.

• **Estudiantes de décimo a duodécimo año**

Estos estudiantes presentan alto nivel de exposición digital dentro y fuera del aula. Sus hábitos tecnológicos —como el uso de múltiples redes sociales, mensajería instantánea, gaming online y plataformas educativas— aumentan la superficie de ataque. Son un grupo vulnerable porque suelen subestimar los riesgos y carecen de una guía institucional sólida.

• **Asesor Regional del MEP**

Este informante clave aporta una visión macro sobre las prácticas institucionales, la ausencia de políticas claras, la heterogeneidad de capacidades entre centros y las necesidades urgentes que enfrenta el sistema educativo.

2.5. Fuentes de información

El estudio utilizó fuentes:

Primarias:

• Cuestionarios a docentes y estudiantes.

• Entrevistas semiestructuradas.

• Observación indirecta del uso de plataformas.

Secundarias:

• Documentos del MEP.

• Estrategia Nacional de Ciberseguridad (MICITT).

• Informes de UNESCO, BID, OEA, Check Point, Sophos, Cisco.

• Normativas nacionales vigentes.

• Estudios académicos previos recopilados en el TFG.

2.6. Población y muestreo

La población total abarca a todos los estudiantes y docentes de instituciones de secundaria del cantón. Sin embargo, por las restricciones de acceso y tiempo, se aplicó un:

Muestreo no probabilístico por conveniencia

Este método permite seleccionar participantes accesibles, disponibles y dispuestos a colaborar, lo cual es común en investigaciones educativas aplicadas. En este caso, las instituciones facilitaron horarios específicos y grupos particulares según sus posibilidades.

Justificación del muestreo

El muestreo por conveniencia es pertinente cuando:

• El acceso está mediado por permisos institucionales;

• Se requiere compatibilidad con horarios escolares;

• El objetivo es describir tendencias locales;

• La investigación tiene naturaleza exploratoria-aplicada.

Si bien este tipo de muestreo no permite extrapolar resultados a toda la población nacional, sí es válido para describir patrones reales dentro del contexto investigado**.**

El muestreo por conveniencia permite trabajar con personas que tienen conocimiento directo del tema y que están dispuestas a compartir sus experiencias sobre las amenazas digitales, el manejo de información sensible y las prácticas de seguridad dentro de las aulas virtuales. Este enfoque facilita la recolección de datos de manera más cercana y real, priorizando la calidad y profundidad de la información por encima del número de participantes.

Con este método, se espera obtener una visión representativa del contexto educativo de Pérez Zeledón, reflejando los principales comportamientos, desafíos y necesidades en materia de ciberseguridad escolar.

2.7. Tipo de muestreo

Los tipos de muestreo son: el probabilístico y el no probabilístico. En el muestreo probabilístico, todos los miembros de la población tienen la misma posibilidad de ser seleccionados, lo que permite hacer generalizaciones estadísticas. En cambio, en el muestreo no probabilístico la elección de los participantes depende de las características del estudio, del criterio del investigador y de la disponibilidad de los sujetos.

Dado el enfoque cualitativo de esta investigación, se optó por un muestreo no probabilístico por conveniencia. Este tipo de muestreo resulta el más adecuado cuando se busca obtener información a partir de personas que estén directamente relacionadas con el fenómeno y que puedan ofrecer datos útiles, más que representar a toda una población.

En este caso, se seleccionarán docentes y funcionarios de instituciones de educación secundaria del cantón de Pérez Zeledón que utilizan plataformas digitales como **Google Classroom, Microsoft Teams** y **Moodle**. La elección se basa en su experiencia y en su disposición para participar en la investigación.

El muestreo por conveniencia permite trabajar con personas que tienen conocimiento directo del tema y que están dispuestas a compartir sus experiencias sobre las amenazas digitales, el manejo de información sensible y las prácticas de seguridad dentro de las aulas virtuales. Este enfoque facilita la recolección de datos de manera más cercana y real, priorizando la calidad y profundidad de la información por encima del número de participantes.

Con este método, se espera obtener una visión representativa del contexto educativo de Pérez Zeledón, reflejando los principales comportamientos, desafíos y necesidades en materia de ciberseguridad escolar.

2.8. Diseño de técnicas e instrumentos para recolectar información

Las técnicas e instrumentos de recolección de información son los medios que permiten obtener los datos necesarios para cumplir con los objetivos de la investigación. Las técnicas hacen referencia a los procedimientos o estrategias que el investigador utiliza para acercarse a la realidad estudiada, mientras que los instrumentos son los recursos o herramientas concretas que facilitan ese proceso.

En esta investigación, el diseño de técnicas e instrumentos se pensó cuidadosamente para obtener información clara, confiable y contextualizada sobre la ciberseguridad en los entornos educativos del cantón de Pérez Zeledón. Dado que el estudio tiene una naturaleza cualitativa, se prioriza la profundidad en la comprensión de las experiencias y percepciones de los docentes, más que la cantidad de respuestas.

Para cumplir con los objetivos propuestos, se utilizarán principalmente dos técnicas de recolección de datos: la entrevista semiestructurada y la encuesta estructurada, aplicadas a los docentes de instituciones de educación secundaria que emplean plataformas digitales como Google Classroom, Microsoft Teams y Moodle.

La entrevista semiestructurada se empleará como técnica cualitativa, ya que permite establecer un diálogo abierto con los participantes. Esta herramienta busca conocer de forma más cercana las experiencias personales, percepciones y prácticas que los docentes desarrollan frente a las amenazas digitales. El instrumento correspondiente será una guía de entrevista, elaborada con preguntas abiertas organizadas por ejes temáticos, tales como:

- Uso de plataformas digitales en el aula.
- Experiencias frente a incidentes o riesgos cibernéticos.
- Nivel de conocimiento sobre buenas prácticas de seguridad digital.
- Existencia o ausencia de protocolos institucionales.
- Opinión sobre la cultura digital y la responsabilidad compartida en materia de ciberseguridad.

Por otra parte, la encuesta estructurada se utilizará como técnica complementaria para obtener una visión más general del fenómeno. Este instrumento será un cuestionario digital, elaborado mediante Google Forms, con preguntas cerradas y escalas tipo Likert que permitan identificar tendencias, niveles

de conocimiento y frecuencia de determinadas prácticas de seguridad digital.

Ambos instrumentos fueron diseñados tomando en cuenta la claridad del lenguaje, la pertinencia de las preguntas y la adecuación al contexto educativo costarricense.

La combinación de entrevistas y encuestas permitirá triangular los resultados, es decir, contrastar la información obtenida por distintos medios, fortaleciendo así la validez del estudio. De esta forma, se espera obtener una comprensión completa y equilibrada del estado de la ciberseguridad educativa en Pérez Zeledón, a partir de datos que reflejen tanto las experiencias personales como las percepciones generales del profesorado.

2.8.1 Instrumentos aplicados en la investigación

Para la recolección de información se emplearon tres instrumentos principales:

1. Cuestionario dirigido a docentes, con el propósito de conocer su percepción, conocimientos y prácticas en torno a la ciberseguridad escolar, así como las dificultades que enfrentan para aplicar medidas preventivas en las aulas.

2. Cuestionario aplicado a estudiantes, diseñado para identificar sus hábitos digitales, el nivel de conciencia sobre seguridad en plataformas educativas y las principales vulnerabilidades percibidas en el entorno escolar.

3. Entrevistas semiestructuradas a docentes y personal técnico del MEP, cuyo análisis permitió obtener información cualitativa complementaria sobre las amenazas cibernéticas más frecuentes, el grado de capacitación institucional y las medidas que se han adoptado en los centros educativos de Pérez Zeledón.

Los tres instrumentos fueron diseñados y aplicados de forma digital mediante Google Forms y posteriormente procesados en Microsoft Excel para su análisis y tabulación.

2.9. Detalle de técnica e instrumentos de aplicación

Para lograr una comprensión integral del fenómeno investigado, se seleccionaron y diseñaron cuidadosamente las técnicas e instrumentos de recolección de información más apropiados para el contexto educativo costarricense. Cada uno cumple una función específica dentro del proceso de obtención y análisis de los datos. De acuerdo con **Hernández Sampieri, Fernández y Baptista (2014)**, la elección de las técnicas debe responder a los objetivos del estudio y al tipo de información que se requiere, garantizando la validez, confiabilidad y pertinencia de los resultados.

En este estudio se emplearán dos técnicas principales: entrevistas semiestructuradas y encuestas estructuradas, aplicadas a docentes de instituciones de educación secundaria del cantón de Pérez Zeledón que utilizan plataformas digitales como Google Classroom, Microsoft Teams o Moodle.

La entrevista semiestructurada será el instrumento central para recopilar información cualitativa, ya que permite una interacción directa entre el investigador y el participante. Esta herramienta genera un espacio de diálogo abierto, en el que las respuestas no están limitadas a opciones predefinidas, sino que pueden desarrollarse libremente. El instrumento para esta técnica será una guía de entrevista, compuesta por preguntas abiertas organizadas en ejes temáticos relacionados con los objetivos específicos del trabajo.

Los principales ejes de la guía de entrevista serán:

- Experiencias personales en el uso de plataformas digitales (Google Classroom, Microsoft Teams, Moodle).
- Percepción de amenazas y vulnerabilidades frecuentes.
- Conocimientos básicos sobre buenas prácticas de ciberseguridad.
- Existencia o ausencia de protocolos institucionales de protección digital.
- Capacitación recibida por parte del MEP u otras entidades.
- Opinión sobre la responsabilidad compartida en la seguridad digital escolar.
- Recomendaciones o propuestas personales para mejorar la protección en el entorno educativo.

Por otro lado, se aplicará una encuesta estructurada con enfoque cuantitativo, orientada a identificar patrones, tendencias y niveles de conocimiento entre el personal docente. Este instrumento permitirá obtener información sistematizada y comparable, útil para describir la magnitud de las amenazas y las prácticas preventivas más comunes.

El **cuestionario** se elaborará en formato digital mediante Google Forms, lo que facilitará su distribución y recolección remota. Estará compuesto por cuatro secciones:

1) **Datos generales del participante**: edad, años de experiencia, tipo de institución, nivel educativo en el que imparte clases.
2) **Uso de plataformas educativas:** frecuencia de conexión y tipos de herramientas utilizadas.

3) **Percepción de amenazas:** nivel de exposición y tipo de incidentes conocidos.

4) **Medidas de prevención:** capacitación, cultura digital y acciones de protección aplicadas.

2.10. Diseño de técnicas e instrumentos para recolectar información

Según **Hernández Sampieri, Fernández y Baptista (2014)**, las variables son las características, atributos o propiedades que pueden ser medidas, observadas o analizadas dentro de una investigación. Estas permiten identificar los elementos que forman parte del fenómeno estudiado y sirven de guía para el diseño de los instrumentos y la interpretación de los resultados.

Se busca comprender la realidad de la ciberseguridad educativa en los centros de secundaria del cantón de Pérez Zeledón. Aunque el enfoque cualitativo no trabaja con variables numéricas en el sentido estricto, sí considera categorías de análisis que orientan la observación, la formulación de preguntas y la interpretación de los datos obtenidos.

De esta manera, las variables y categorías se organizan en torno a los principales aspectos del problema de estudio:

- Uso de plataformas digitales: comprende la frecuencia, tipo de herramientas utilizadas y nivel de dominio tecnológico del personal docente.
- Percepción de amenazas cibernéticas: aborda cómo los docentes identifican, interpretan y enfrentan los riesgos digitales que surgen en el uso de plataformas educativas.
- Nivel de conocimiento sobre ciberseguridad: analiza la preparación del personal educativo en temas de protección digital, contraseñas seguras, privacidad y prevención de ataques.
- Existencia de políticas o protocolos institucionales: evalúa si los centros educativos cuentan con lineamientos, medidas o reglamentos sobre seguridad digital.
- Cultura digital y responsabilidad compartida: estudia la actitud de los docentes frente al uso seguro de la tecnología y su disposición para aplicar buenas prácticas dentro del aula.
- Capacitación y apoyo institucional: indaga sobre las oportunidades de formación recibidas en materia de ciberseguridad, tanto desde el Ministerio de Educación Pública (MEP) como de otras entidades.

Estas variables y categorías permiten estructurar el análisis de la información recolectada y facilitan la interpretación de los resultados de manera ordenada y coherente con los objetivos del estudio. Tal como señalan Hernández Sampieri et al. (2014), la determinación de variables "constituye el eje que une el planteamiento del problema con la obtención y el análisis de los datos", garantizando así la coherencia metodológica de todo el proceso investigativo.

2.10.1. Clasificación

Las variables se clasifican según su función dentro del estudio en independientes, dependientes y de control. Esta clasificación permite organizar la información de forma más clara y entender cómo interactúan los distintos factores que componen el fenómeno investigado.

En esta investigación, la clasificación de variables se establece de la siguiente manera:

Variable independiente:

- Corresponde al fenómeno que se considera el punto de partida del estudio. En este caso, la variable independiente es las amenazas cibernéticas emergentes en el uso de plataformas educativas digitales, ya que estas son el eje central que influye sobre las demás variables analizadas.

Variables dependientes:

Representan los efectos o manifestaciones del fenómeno principal dentro del contexto educativo. En este trabajo, las variables dependientes son:

- Nivel de preparación del personal docente frente a la ciberseguridad.
- Percepción de vulnerabilidades y riesgos digitales.
- Existencia de protocolos o políticas institucionales de seguridad.
- Frecuencia de incidentes o ataques reportados en el entorno escolar.

Variables de control:

Estas variables no son objeto directo de estudio, pero se consideran para evitar sesgos en el análisis y comprender mejor el contexto. Incluyen:

- Características sociodemográficas de los docentes, como edad, género y años de experiencia profesional.
- Tipo de institución educativa, diferenciando entre centros públicos y privados.
- Plataforma utilizada, ya sea Google Classroom, Microsoft Teams o Moodle.

Esta clasificación facilita organizar la información durante la recolección y el análisis de los datos, permitiendo observar cómo las amenazas cibernéticas afectan distintos aspectos del entorno educativo.

2.10.2. Definición

Definir las variables permite establecer con claridad los conceptos que serán analizados dentro de la investigación, delimitando su alcance y las dimensiones que las componen. Una definición precisa facilita la construcción de los

instrumentos de recolección y la interpretación de los resultados.

En el presente estudio, las variables se definen de la siguiente manera:

- Amenazas cibernéticas emergentes:

Se refiere a los incidentes digitales que afectan el entorno educativo, tales como phishing, robo de credenciales, suplantación de identidad, acceso no autorizado o infección por malware. Estas amenazas pueden comprometer la información de estudiantes, docentes o instituciones, alterando la integridad y la seguridad de los sistemas digitales utilizados en el proceso de enseñanza-aprendizaje.

- Nivel de preparación docente:

Hace referencia al grado de conocimiento, capacitación y aplicación de medidas de ciberseguridad por parte del personal docente. Incluye la capacidad de identificar riesgos, adoptar prácticas seguras en el uso de plataformas educativas y promover una cultura de prevención digital en el aula.

- Protocolos institucionales de seguridad:

Comprende la existencia y aplicación de normativas, procedimientos o guías de actuación que regulan la respuesta ante incidentes de seguridad digital dentro de las instituciones educativas. Esta variable evalúa si las instituciones cuentan con políticas claras y si el personal docente conoce y sigue dichas directrices.

- Percepción de vulnerabilidades:

Corresponde a la valoración subjetiva que los docentes tienen sobre los riesgos de seguridad asociados al uso de plataformas digitales. Incluye la manera en que interpretan la posibilidad de sufrir ataques o pérdidas de información y la confianza que sienten en las medidas de protección disponibles.

Estas definiciones permiten orientar la recolección y el análisis de los datos de forma estructurada, asegurando la coherencia entre los conceptos teóricos y la realidad observada en los centros educativos de Pérez Zeledón.

III. ANALISIS DE RESULTADOS

El presente estudio investigativo nace de la necesidad de comprender y atender las amenazas cibernéticas emergentes que enfrentan los entornos educativos actuales, especialmente en los niveles de decimo a duodécimo año. En los últimos años, el uso de plataformas digitales en el ámbito académico se ha convertido en una herramienta indispensable para la enseñanza y el aprendizaje; sin embargo, este avance también ha traído consigo una seria de riesgos y vulnerabilidades que pueden afectar tanto la seguridad de la información como el bienestar de los propios estudiantes y docentes.

3.1 Resultados del cuestionario aplicado a docentes

Pregunta	Respuesta	Frecuencia (n)	Porcentaje (%)	N total
¿Ha recibido formación formal en ciberseguridad o uso seguro de tecnologías por parte de su institución o el MEP?	No	4	50%	8
	Si	2	25%	8
	Muy Poco	1	12,5%	8
	Otro	1	12,5%	8
¿Conoce qué medidas básicas de seguridad digital debe aplicar en el uso de plataformas educativas?	Si	8	100%	8
¿Se promueve entre estudiantes y docentes una cultura de seguridad digital (uso de contraseñas seguras, protección de datos, etc.)?	Si	5	62,5%	8
	No	1	12,5%	8
	Otro	2	25%	8
¿Se han implementado protocolos de acción en caso de incidentes digitales, como ciberacoso o acceso no autorizado?	No	6	75%	8
	Si	1	12,5%	8
	Otro	1	12,5%	8

¿Qué tipo de herramientas o capacitación cree usted que serían más útiles para mejorar la seguridad en el uso de plataformas educativas?	Capacitación institucional continua	3	37,5%	8
	Manual de buenas prácticas	2	25%	8
	Cursos o talleres prácticos	2	25%	8
	Otras sugerencias (campañas, asesoría técnica, charlas)	1	12,5%	8

Tabla 1. Resultados del cuestionario aplicado a docentes sobre prácticas y conocimiento en ciberseguridad educativa.

Esta propuesta lo que busca es analizar de una manera integral como se manifiestan esas amenazas dentro de las plataformas educativas, y de qué manera la aplicación de sanas prácticas de la industria de la ciberseguridad puede servir como una guía para fortalecer la protección de los usuarios en contextos escolares.

Esta propuesta de investigación también plantea el desarrollo de un estudio practico que permita identificar, analizar y abordar las amenazas cibernéticas emergentes presentes en el uso de plataformas educativas dentro de los centros escolareas costarricenses, especialmente en los niveles de decimo a duodécimo año.

El trabajo se enfocará en recopilar información real mediante la aplicación mediante la aplicación de instrumentos dirigidos a estudiantes y docentes, con el fin de conocer el nivel de preparación, las percepciones del riesgo y las medidas de seguridad que actualmente se aplican en los entornos académicos digitales. A partir de esa información, se elaborará un diagnóstico que refleje las principales debilidades y oportunidades de mejora en materia de ciberseguridad educativa.

El desarrollo del trabajo seguirá un enfoque mixto, combinando elementos descriptivos y analíticos que faciliten la comprensión de la situación actual y la formulación de soluciones aplicables. Además, se emplearán herramientas digitales y métodos de análisis que permitan presentar los resultados de manera clara y accesible para la comunidad educativa.

Esta propuesta lo que busca es generar un aporte concreto al ámbito académico, orientado no solo a reconocer los riesgos del entorno digital, sino también a impulsar acciones que promuevan la prevención, la concientización y el uso responsable de las plataformas educativas en el uso escolar costarricense.

Se aplicó un cuestionario a docentes de diferentes instituciones educativas de la región de Pérez Zeledón, con el propósito de conocer su nivel de conocimiento sobre ciberseguridad, las prácticas que aplican en el uso de plataformas educativas y la percepción que tienen sobre los riesgos digitales dentro del entorno escolar.

En total participaron ocho docentes, quienes imparten lecciones en los niveles de décimo a duodécimo año y utilizan plataformas como Microsoft Teams, Classroom y Edutec para sus clases virtuales y actividades académicas.

3.2 – Resultados del cuestionario aplicado a estudiantes

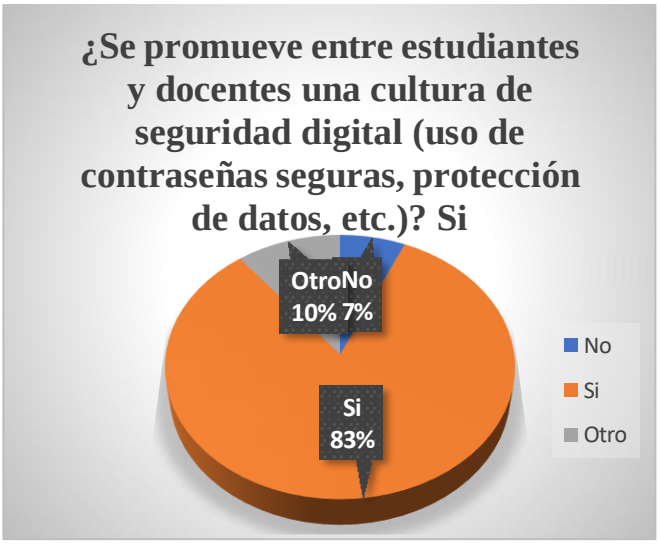

Figura 1. Prácticas de seguridad digital reportadas por estudiantes de secundaria.

3.3 Incidentes de ciberseguridad reportados



Figura 3. Incidentes de ciberseguridad experimentados por los estudiantes encuestados.

IV. Conclusiones y Recomendaciones

El análisis demuestra que la digitalización avanza más rápido que la capacidad institucional para manejarla. El sistema educativo se encuentra en una fase de madurez digital temprana: usa plataformas avanzadas, pero carece de cultura, políticas y formación en ciberseguridad. Las amenazas emergentes actúan sobre un terreno fértil: estudiantes vulnerables, docentes desinformados y estructuras administrativas insuficientes.

4.1. Conclusiones

La investigación desarrollada sobre las amenazas emergentes en plataformas educativas dentro de instituciones de secundaria del cantón de Pérez Zeledón permite concluir que la realidad encontrada evidencia una brecha sustancial entre el nivel de uso de herramientas tecnológicas y la madurez institucional requerida para garantizar entornos digitales seguros y confiables. Aunque las plataformas educativas se han convertido en recursos indispensables para el proceso de enseñanza aprendizaje, su integración se ha dado sin una estructura sólida de acompañamiento formativo, normativo y técnico, lo que incrementa la vulnerabilidad de estudiantes, docentes y centros educativos.

En primer lugar, se determinó que el personal docente es uno de los principales actores en riesgo, debido a su limitada formación en ciberseguridad. El 75% no ha recibido capacitación formal y la mayoría desconoce conceptos esenciales como configuraciones seguras, medidas de privacidad, políticas de contraseñas o procedimientos de respuesta ante incidentes. Esta falta de conocimiento no solo repercute en la gestión de sus propias cuentas y dispositivos, sino también en su capacidad para orientar al estudiantado, lo que convierte la formación digital en un tema relegado dentro de la vida institucional.

Por su parte, el estudiantado presenta prácticas tecnológicas que incrementan su nivel de exposición, como el uso repetido de contraseñas, la confianza excesiva en enlaces o mensajes desconocidos, la carencia de hábitos de verificación y la sobreexposición en redes sociales. Además, los datos recolectados evidencian que muchos jóvenes no identifican incidentes de ciberseguridad o los normalizan debido a la cultura digital imperante. A esto se suma que el 70% no recibe orientación docente, lo cual deja a los estudiantes desprovistos de herramientas básicas para protegerse.

Los centros educativos, en general, presentan ausencia de políticas, protocolos y lineamientos institucionales para gestionar incidentes de forma oportuna. La investigación reveló que no existe una estandarización nacional clara, lo que provoca que cada institución gestione los riesgos según su propio criterio o no los gestione en absoluto. Los casos de ciberacoso, suplantación, acceso indebido o pérdida de información se abordan de manera improvisada o se minimizan por desconocimiento, lo cual afecta la salud emocional y académica de los involucrados

Otro punto relevante es que la cultura digital institucional es predominantemente reactiva, enfocada en resolver problemas cuando ya han ocurrido, pero sin estrategias preventivas, capacitaciones periódicas o prácticas de fortalecimiento continuo. Esto evidencia que los centros educativos, aunque tecnológicamente dependientes, no han alcanzado un nivel de madurez que les permita anticipar amenazas o actuar con consistencia.

En conjunto, estos hallazgos permiten concluir que las amenazas emergentes no solo están presentes, sino que se ven potenciadas por la falta de formación en ciberseguridad, las prácticas inseguras del estudiantado, la debilidad institucional y la ausencia de políticas claras a nivel cantonal y nacional. Por ello, es urgente fortalecer la cultura digital escolar desde una perspectiva integral, articulando esfuerzos entre el MEP, MICITT, instituciones educativas, docentes, familias y estudiantes para configurar un ecosistema seguro, confiable y sostenible.

4.2. Recomendaciones

A partir de las conclusiones obtenidas, se plantea un conjunto de recomendaciones orientadas a mejorar la ciberseguridad en entornos escolares y promover una cultura digital preventiva y sostenible. Estas recomendaciones se presentan desde una perspectiva institucional, pedagógica, técnica y normativa, con el fin de que puedan aplicarse de forma progresiva según las capacidades de cada institución.

1. Implementar un Manual Institucional de Ciberseguridad Escolar

Se recomienda que cada institución cuente con un documento oficial que establezca políticas, normas y procedimientos claros sobre buenas prácticas digitales, uso responsable de plataformas, manejo de incidentes, protección de datos y roles de respuesta. Este manual debe adaptarse al contexto de secundaria e incluir secciones para estudiantes, docentes, administrativos y encargados de laboratorio o informática.

2. Fortalecer la capacitación docente mediante programas periódicos

Es fundamental crear un plan de formación continua dirigido a docentes y personal administrativo, abordando temas como contraseñas seguras, autenticación multifactor, reconocimiento de phishing, protección de datos, ética digital, manejo de incidentes y acompañamiento emocional ante casos de ciberacoso. Esta capacitación debe ser práctica, accesible y contextualizada. Idealmente, debería realizarse de manera semestral.

3. Incorporar la ciudadanía digital en el currículo escolar

La formación en competencias digitales debe convertirse en un eje transversal del currículo. Se recomienda incluir módulos sobre privacidad, identidad digital, ética, bienestar emocional

en línea, alfabetización mediática y prevención de riesgos. Esta formación debe adaptarse a las necesidades de estudiantes de secundaria y desarrollarse en paralelo con contenidos académicos tradicionales.

4. Establecer protocolos institucionales para la gestión de incidentes

Cada institución debe contar con un procedimiento formal para reportar, analizar y dar seguimiento a casos de acoso digital, suplantación, filtración de datos o accesos indebidos. Estos protocolos deben incluir tiempos de respuesta, responsables, documentación, preservación de evidencia y medidas de acompañamiento emocional para los afectados.

5. Promover campañas de sensibilización dirigidas a toda la comunidad educativa

Para fomentar una cultura preventiva, se recomienda organizar charlas, talleres, afiches, videos y actividades periódicas centradas en el uso seguro de plataformas, hábitos digitales saludables y prevención de riesgos. Las campañas deben dirigirse tanto a estudiantes como a docentes y padres de familia, buscando generar conciencia colectiva.

6. Fortalecer la infraestructura tecnológica y las configuraciones de seguridad

Aunque el estudio no evaluó infraestructura técnica, se recomienda mejorar aspectos como el uso de redes internas segmentadas, habilitación de autenticación multifactor institucional, actualizaciones constantes, filtros de contenido y gestión segura de dispositivos. Los centros educativos deben trabajar articuladamente con el MEP para obtener acompañamiento técnico.

7. Establecer alianzas con instituciones nacionales especializadas

Se sugiere articular esfuerzos con el MICITT, CSIRT-CR, universidades y organizaciones centradas en ciberseguridad para recibir asesoría, recursos educativos, auditorías básicas, materiales de apoyo y acompañamiento en casos complejos.

8. Implementar espacios estudiantiles de formación y liderazgo digital

Se recomienda crear clubes de ciberseguridad, laboratorios digitales, competencias internas o proyectos integradores que fomenten la participación activa del estudiantado en la construcción de su propia seguridad digital. Esto empodera a los jóvenes y fortalece la resiliencia institucional.

9. Integrar a las familias en el proceso de formación

Los encargados deben recibir orientación sobre riesgos digitales, control parental, acompañamiento emocional y diálogo responsable en casa. Su involucramiento mejora la coherencia entre la educación digital dentro y fuera del centro educativo.

10. Evaluar periódicamente el nivel de madurez digital institucional

Las instituciones deben realizar diagnósticos anuales para identificar debilidades, registrar avances y actualizar estrategias. Esta evaluación continua permitirá institucionalizar la cultura de ciberseguridad como un proceso permanente.

REFERENCIAS

[1] **Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO).** (2021). *Educación en un mundo digital: Informe de seguimiento global sobre la tecnología en la educación.* París: UNESCO. Recuperado de https://unesdoc.unesco.org/ark:/48223/pf0000379822

[2] **Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO).** (2022). *Recomendaciones sobre la ética de la inteligencia artificial.* París: UNESCO. Recuperado de https://unesdoc.unesco.org/ark:/48223/pf0000380455

[3] **Programa Estado de la Nación (PEN).** (2022). *Informe del Estado de la Educación 2022.* San José: Consejo Nacional de Rectores (CONARE). Recuperado de https://estadonacion.or.cr/educacion2022/

[4] **Universidad de Costa Rica (UCR).** (2024). *Hacia la Sociedad de la Información y el Conocimiento.* San José, Costa Rica. Recuperado de https://vinv.ucr.ac.cr/sites/default/files/files/informe_2024_completo_interactivo.pdf

[5] **Universidad de Costa Rica (UCR).** (2024). *En las aulas escolares de Costa Rica el internet y las tecnologías se usan muy poco.* San José, Costa Rica. Recuperado de https://www.ucr.ac.cr/noticias/2024/2/09/en-las-aulas-escolares-de-costa-rica-el-internet-y-las-tecnologias-se-usan-muy-poco.html

FUENTES PRIMARIAS (entrevistas)

[6] **Elizondo Umaña, Jordán Andrés.** Entrevista personal a **Efrén Flores Quesada**, docente del Liceo Sinaí. Transcripción. Pérez Zeledón, 29 de octubre de 2025.

[7] **Elizondo Umaña, Jordán Andrés.** Entrevista personal a **Jeison Corrales**, asesor de informática del Ministerio de Educación Pública (MEP). Transcripción. Pérez Zeledón, 30 de octubre de 2025.

[8] **Elizondo Umaña, Jordán Andrés.** Entrevista personal a **Erick Vargas Salazar**, docente del Colegio Técnico Profesional de Pejibaye. Transcripción. Pérez Zeledón, 30 de octubre de 2025.

[9] **Elizondo Umaña, Jordán Andrés.** Entrevista personal a **Michael Corrales Oviedo**, docente del Colegio La Asunción. Transcripción. Pérez Zeledón, 30 de octubre de 2025.