MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE GRADUACIÓN

Sometido al Tribunal Examinador de Postgrados para optar por el grado de Maestría en Ciberseguridad

Título del Proyecto

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

AUTOR

Ing. Jordán Andrés Elizondo Umaña

TUTOR: MATI. Randall Artavia Delgado

LECTOR: MS.c. Irvin Argenis Sáenz Córdoba

Pérez Zeledón, Costa Rica

Diciembre 2025

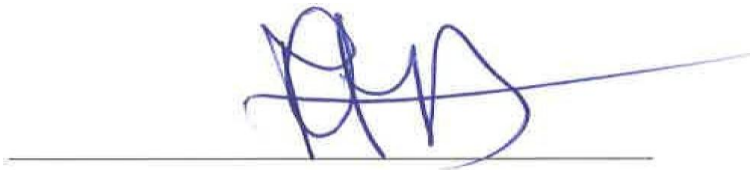
UNIVERSIDAD SAN ISIDRO DEL LABRADOR

MAESTRÍA EN CIBERSEGURIDAD

TRIBUNAL EXAMINADOR

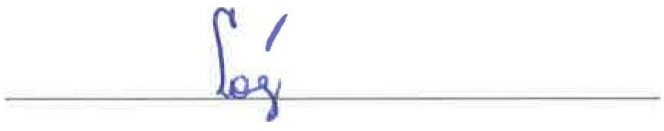
Ing. Ruddy Rodríguez Acuña

Director de Maestría



MATI. Randall Artavia Delgado

Tutor



Msc. Irvin Argenis Sáenz Córdoba

Lector

DECLARACIÓN JURADA

Yo, Jordán Andrés Elizondo Umaña, mayor, soltero(a), egresado(a) de la carrera de Maestría Profesional en Ciberseguridad de la Universidad San Isidro Labrador, domiciliado en la ciudad de Pérez Zeledón, portador(a) de la cédula de identidad número 1-1664-0968, en este acto, debidamente apercibido y entendido de las penas y consecuencias con las que se castiga, en el Código Penal, el delito del perjurio, ante quienes se constituyen en el Tribunal Examinador de mi Trabajo Final de Graduación para optar por el título de maestría, juro solemnemente que mi trabajo final de graduación titulado "**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**" es una obra original que ha respetado todo lo preceptuado por las Leyes Penales así con la Ley de Derechos de Autor y Derechos Conexos, número 6683 de 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 de 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte: artículo 70º: Es permitido citar a un autor transcribiendo los pasajes pertinentes siempre que estos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor y de la obra original. Asimismo, quedo advertido que la Universidad San Isidro Labrador se reserva el derecho de protocolizar este documento ante Notario Público. En fe de lo anterior firmo en la ciudad de San Isidro del General, al ser el 06 del mes de diciembre del año dos mil veinticinco.

Ing. Jordán Andrés Elizondo Umaña

Cédula: 1-1664-0968

DEDICATORIA

Dedico este trabajo primeramente a Dios, quien ha sido mi guía, mi refugio y mi fortaleza en todo momento. Sin Su presencia y Su luz, este camino no habría sido posible. Cada logro alcanzado es testimonio de Su amor y de las bendiciones que ha derramado sobre mi vida.

A mi pareja, por su amor, comprensión y apoyo incondicional. Gracias por caminar a mi lado en cada etapa de este proceso, por tus palabras de ánimo y por recordarme siempre que los sueños se alcanzan con paciencia y fe.

A mi hija, la razón más grande de mi esfuerzo y mi inspiración más pura. Cada paso que doy está guiado por el deseo de brindarte un mejor futuro y enseñarte que todo es posible cuando se trabaja con dedicación, constancia y amor.

A mis padres, quienes con su ejemplo de sacrificio, honestidad y perseverancia me enseñaron el verdadero valor del trabajo y la educación. Este logro también les pertenece, porque sus consejos y su apoyo han sido el cimiento sobre el que he construido este camino.

Finalmente, dedico este trabajo a todas aquellas personas que han creído en mí, que me han brindado su apoyo y que han formado parte de mi crecimiento personal y profesional. Cada palabra escrita es fruto de su influencia y del amor que me han compartido a lo largo del camino.

AGRADECIMIENTOS

En primer lugar, deseo expresar mi más profundo agradecimiento a Dios, por ser la fuente de toda fortaleza, sabiduría y serenidad a lo largo de este proceso. A Él le debo cada oportunidad, cada aprendizaje y la capacidad de mantenerme firme incluso en los momentos de mayor dificultad. Su presencia constante ha guiado mis pasos, brindándome claridad cuando las fuerzas parecían agotarse y recordándome siempre que con fe y perseverancia todo propósito es alcanzable.

A mi pareja, por su amor incondicional, su paciencia infinita y su apoyo constante. Gracias por acompañarme en las largas jornadas de estudio, por comprender mis ausencias y por motivarme a seguir adelante aun cuando las exigencias del trabajo y la vida académica parecían abrumadoras. Este logro también es tuyo, porque en cada avance encontré tu aliento y tu confianza.

A mi hija, mi mayor inspiración y razón para superarme cada día. Su sonrisa y su inocencia fueron la luz que me impulsó a no rendirme, recordándome siempre por qué valía la pena cada esfuerzo. Este trabajo es también una muestra del ejemplo que quiero dejarle: que, con dedicación, fe y amor, todo sueño puede hacerse realidad.

A mis padres, por ser el pilar fundamental de mi vida. Gracias por haberme enseñado desde pequeño el valor del esfuerzo, la responsabilidad y la humildad. Su ejemplo de trabajo y sacrificio ha sido mi mayor motivación. A ellos debo mis principios, mi carácter y la convicción de que cada meta alcanzada es fruto de la constancia y del amor familiar.

Extiendo también mi gratitud a todos aquellos que, de una u otra manera, formaron parte de este camino: familiares, amigos, docentes y compañeros que me brindaron su apoyo, sus consejos y su ánimo en los momentos más importantes. A quienes compartieron conmigo conocimientos, palabras de aliento o simplemente una conversación sincera que aportó claridad al proceso, les agradezco profundamente.

Finalmente, este trabajo no solo representa una meta académica cumplida, sino también un testimonio de crecimiento personal y espiritual. Cada página refleja no solo el esfuerzo intelectual, sino también la suma del amor, la fe y la dedicación de quienes me acompañaron en este recorrido. A todos ellos, gracias por hacer posible este logro.

CARTA DE AUTORIZACIÓN DEL TUTOR

Pérez Zeledón, 06 de diciembre de 2025

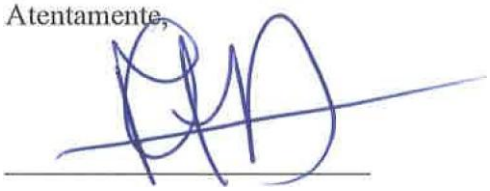
Licenciado
Ruddy Rodríguez Acuña
Coordinador de la Escuela de Informática
Universidad Internacional San Isidro Labrador

Estimado señor director:

Yo, Randall Mauricio Artavia Delgado, mayor, Ingeniero en informática, con domicilio en la Trinidad de Moravia San José, portador de la cédula de identidad número **205740823**, en mi condición de tutor del Proyecto de Graduación titulado: **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,** propuesta por el estudiante **Jordán Andrés Elizondo Umaña**, manifiesto lo siguiente:

1. Que el proceso de trabajo final de graduación culmina satisfactoriamente.
2. Que se ha incorporado en el documento final las sugerencias hechas por el Tribunal Examinador.
3. Que he cumplido con el acompañamiento encomendado por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,



MATI Randall Mauricio Artavia Delgado
Tutor

CARTA DE APROBACIÓN DEL LECTOR

Pérez Zeledón, 06 de diciembre de 2025

Licenciado
Ruddy Rodríguez Acuña
Coordinador de la Escuela de Informática
Universidad Internacional San Isidro Labrador

Estimado señor director:

Yo, Irvin Sáenz Córdoba, mayor, divorciado, analista de ciberseguridad L2, vecino de Guápiles, portador de la cédula de identidad número 7-0197-0839, en mi condición de lector del Proyecto de Graduación titulado: **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**, propuesta por el estudiante **Jordán Andrés Elizondo Umaña** , manifiesto lo siguiente:

1. Que la lectura del trabajo final de graduación concluye satisfactoriamente.
2. Que he leído el documento final y he hecho mis observaciones en el mismo.
3. Que he cumplido con las labores de lector encomendadas por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,

Máster Irvin Sáenz Córdoba

Lector

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS, FIGURAS E ILUSTRACIONES

LISTA DE PALABRAS CLAVES

Palabras clave:

- ciberseguridad educativa
- plataformas educativas
- protección de datos
- ciudadanía digital
- protocolos institucionales
- capacitación docente
- concienciación estudiantil
- ciberacoso
- suplantación de identidad
- phishing; gestión de contraseñas
- cultura digital; madurez institucional
- Pérez Zeledón
- MEP
- MICITT
- Prevención
- respuesta a incidentes
- ética digital
- privacidad.

RESUMEN EJECUTIVO

Este trabajo presenta un estudio investigativo sobre las amenazas emergentes en plataformas educativas utilizadas en centros de secundaria del cantón de Pérez Zeledón, Costa Rica, con foco en los niveles de décimo a duodécimo año (2025). El objetivo general fue analizar el nivel de exposición y preparación de la comunidad educativa (docentes y estudiantes), así como proponer medidas prácticas que fortalezcan la cultura de ciberseguridad escolar.

Metodológicamente, se aplicaron cuestionarios a docentes y estudiantes y se realizaron entrevistas semiestructuradas a docentes y a un asesor regional de informática del MEP. La muestra, de carácter intencional, permitió triangular evidencia cuantitativa (frecuencias y porcentajes) y cualitativa (temas y patrones de relato) para construir una visión integrada de riesgos, prácticas y necesidades.

Los resultados muestran brechas críticas en tres frentes. Primero, capacitaciones: alrededor del 75 % del personal docente no ha recibido formación formal en ciberseguridad; aunque la mayoría declara conocer “medidas básicas”, ese conocimiento es teórico y poco aplicado. Segundo, estudiantado: aproximadamente dos tercios no ha recibido orientación concreta sobre protección de datos y solo una minoría sabe cómo actuar ante un incidente, lo que se traduce en confianza excesiva en las plataformas y prácticas inseguras (p. ej., reutilización/compartición de contraseñas). Tercero, gestión institucional: los centros carecen de protocolos estandarizados para prevención y respuesta ante eventos como ciberacoso, acceso no autorizado o suplantación de identidad, por lo que la reacción tiende a ser reactiva e improvisada.

Las entrevistas confirman coincidencia total entre docentes y asesor del MEP sobre la insuficiencia de acompañamiento técnico, la ausencia de lineamientos unificados y la necesidad de infraestructura y formación sostenida. A la vez, existe disposición al cambio: el personal reconoce la urgencia de fortalecer la cultura digital, y el estudiantado muestra apertura para adquirir hábitos de ciudadanía digital.

El estudio concluye que la madurez institucional en ciberseguridad es incipiente: la adopción de plataformas no ha sido acompañada por políticas claras, programas formativos continuos ni protocolos operativos. Se recomiendan cinco líneas de acción coherentes con los hallazgos: (1) capacitación continua y especializada para docentes/administrativos; (2) manual institucional de ciberseguridad escolar con protocolos de prevención y respuesta; (3) inclusión curricular de ciudadanía digital; (4) acompañamiento técnico periódico del MEP/MICITT con diagnósticos y seguimiento; y (5) campañas y proyectos participativos que involucren a familias, docentes y estudiantes. Implementar estas medidas permitirá reducir la exposición, mejorar la respuesta ante incidentes y consolidar **entornos de aprendizaje seguros y resilientes**.

CAPITULO I. INTRODUCCIÓN

1.1 Planteamiento del tema de estudio

El uso de plataformas digitales en ambientes escolares es hoy una realidad. Sin embargo, este cambio ha traído consigo una serie de problemas relacionados con la seguridad de la información y la protección de los usuarios, especialmente en contextos donde la mayoría de las personas usuarias son menores de edad. Las plataformas educativas, aunque útiles, han sido adoptadas con poca o nula evaluación de los riesgos cibernéticos asociados a su uso.

La rápida adopción de plataformas digitales durante la pandemia permitió a las instituciones costarricenses sostener la enseñanza-aprendizaje en entornos no presenciales. Según el MEP, los docentes implementaron herramientas tecnológicas ‘en un periodo muy corto’, mientras que la UCR resalta cómo Moodle, Teams y Zoom mejoraron la comunicación y participación estudiantil, informes adicionales confirman que Google Classroom, Blackboard y Microsoft Teams se integraron como componentes esenciales de la gestión académica y la interacción institucional.

Sin embargo, esta transformación digital ha traído consigo una serie de amenazas cibernéticas emergentes que muchas veces no son atendidas con el rigor que requieren, especialmente en ambientes escolares donde el nivel de conciencia en ciberseguridad es bajo. Esto convierte a estas plataformas educativas en objetivos vulnerables ante amenazas como el robo de credenciales, ataques de phishing, suplantación de cualquier identidad, accesos no autorizados a datos sensibles y explotación de vulnerabilidades en aplicaciones web.

Además, el uso de dispositivos personales en entornos educativos —práctica conocida como Bring Your Own Device (BYOD)— puede aumentar la superficie de ataque si no se acompaña de medidas de seguridad adecuadas. A esto se suman las conexiones a redes Wi-Fi

públicas poco seguras y la limitada capacitación tanto de estudiantes como de docentes en buenas prácticas digitales, lo cual agrava el panorama de riesgos en el entorno educativo. La inversión en infraestructura digital rara vez incluye recursos destinados a auditorías de seguridad, monitoreo de tráfico sospechoso, control de accesos o implementación de marcos de cumplimiento normativo como el Reglamento General de Protección de Datos (GDPR) o leyes nacionales de protección de datos. La brecha entre el uso masivo de tecnologías digitales y el conocimiento real de sus riesgos ha generado un entorno propenso a incidentes de seguridad que pueden comprometer la integridad, confidencialidad y disponibilidad de la información académica y personal.

En los centros educativos de Costa Rica, el 60 % de los docentes no cuenta con formación en educación virtual, lo que implica una gran deficiencia en conocimientos para identificar o mitigar ataques como phishing, malware o suplantación de identidad (≈ 55 000 personas). Los niveles de uso real de Internet con fines pedagógicos son bajos (2,53/10 por docente, y solo 21,6 % del estudiantado accede diariamente en clase)

Gran parte del estudiantado también trae dispositivos personales: 82 % de los jóvenes de 15–17 años y 58 % de 12–14 años usan su celular, complementado con 60 % que accede a computadoras en laboratorios escolares, mientras un 9 % carece de acceso

Sin una capacitación en seguridad digital, estas condiciones provocan un entorno donde los estudiantes pueden ser blancos de amenazas, y los docentes no están preparados para detectarlas ni actuar, potenciado por políticas institucionales poco desarrolladas o inexistentes.”

“En centros educativos de Costa Rica, los estudiantes acceden a plataformas digitales desde dispositivos compartidos —como los de laboratorio escolar, utilizados por el 60,33 % del alumnado, mientras que el 9 % no tiene acceso— y a través de redes escolares inseguras,

sin cifrado ni autenticación avanzada (MEP, 2022). La supervisión digital es escasa, como lo muestra un uso de solo 2,53/10 en prácticas pedagógicas con Internet (UCR, 2024). Por el lado docente, el 60 % no recibió capacitación en educación digital ni en prevención de amenazas como correos falsos o malware (crhoy.com). Finalmente, las políticas institucionales de protección digital son débiles o inexistentes, como lo reconoce la Estrategia Nacional de Ciberseguridad (2023–2027), al señalar la falta de personal y protocolos en los centros educativos (MICITT, 2023).”

Según la Estrategia Nacional de Ciberseguridad de Costa Rica (MICITT, 2023), las instituciones educativas no cuentan con personal especializado ni protocolos estandarizados. Esta debilidad ha abierto la puerta a riesgos como la manipulación de datos académicos, interrupciones en clases virtuales o el acceso a contenido inadecuado por parte del estudiantado. Organismos como Fundación Paniamor y la UNESCO también han alertado sobre el aumento del ciberacoso escolar en contextos con baja protección digital. La ausencia de una cultura de ciberseguridad en el sector educativo puede tener consecuencias graves como: perdida de datos, interrupción de servicios académicos, exposición de menores a contenidos inapropiados o peligrosos y violaciones a la privacidad. Por tanto, es multidimensional: abarca lo técnico (falta de protección de datos y sistemas), lo humano (falta de cultura de ciberseguridad), lo pedagógico (uso responsable de la tecnología en el aula) y lo legal (desconocimiento de normativas de protección de datos en menores). Esta combinación convierte al ambiente escolar en un entorno frágil frente a las amenazas emergentes que evolucionan constantemente, adaptándose con rapidez a las nuevas tecnologías y a las rutinas digitales de los usuarios que deben ser considerados al momento de plantear las soluciones.

En este contexto, resulta imperativo llevar a cabo un estudio riguroso sobre las amenazas emergentes en las plataformas educativas en ambientes escolares, no solo con el fin de documentar los riesgos existentes, sino también para proponer estrategias concretas de

prevención, detección y respuesta. Este estudio debe abordar desde la perspectiva práctica de la ciberseguridad escolar: políticas de control de acceso, educación digital, medidas técnicas como el cifrado, segmentación de redes, autenticación multifactor, así como recomendaciones específicas adaptadas a la realidad de las instituciones escolares que muchas veces operan con recursos limitados.

A partir de lo expuesto, las siguientes preguntas de investigación guiarán el desarrollo de este estudio:

¿Cuáles son las amenazas emergentes más críticas que afrontan las plataformas educativas en los ambientes escolares costarricenses?

El primer Capítulo del documento describe el tema y responde a varias preguntas que dan origen a la investigación, a saber *¿Por qué?, ¿Dónde?, ¿Contexto?, ¿Problemática? ¿Beneficios de la Investigación?,* siendo la pregunta integradora el *¿por qué se quiere estudiar el mismo?* Este Capítulo aborda la importancia de dedicar recurso a la temática planteada.

1.2 Antecedentes del tema

La transformación digital en la educación ha sido uno de los cambios más acelerados de los últimos años. Antes del 2020, el uso de plataformas virtuales era una opción complementaria; sin embargo, tras la pandemia, se convirtieron en el principal medio para continuar con el proceso educativo. Esta transición, aunque necesaria, no vino acompañada de una estrategia sólida en materia de seguridad de la información, dejo al descubierto una serie de vulnerabilidades tecnológicas y humanas que afectan directamente la seguridad de los entornos digitales escolares.

- Incremento global de ataques

Según Check Point, durante 2022 el sector educativo registró un 44 % más de ciberataques en comparación con el año anterior, con un promedio de 2 300 ataques semanales a escuelas y universidades

Numerosos estudios a nivel internacional han evidenciado que los entornos educativos se han convertido en blancos frecuentes de ciberataques. Estos ataques no solo afectan la disponibilidad y funcionalidad de las plataformas educativas, sino que también comprometen información sensible de estudiantes, docentes y personal administrativo. Los incidentes más comunes incluyen el robo de datos estudiantiles, accesos no autorizados a clases virtuales, manipulación de calificaciones, y ataques de denegación de servicio (DDoS).

Por ejemplo, un informe del gobierno del Reino Unido reveló que el 91 % de las universidades, el 85 % de los colegios de educación técnica y el 60 % de las escuelas secundarias experimentaron brechas de seguridad durante el último año, siendo el 97 % de ellas víctimas de ataques de phishing y un 36 % afectadas por ataques DDoS (Department for Science, Innovation and Technology, 2025). En Estados Unidos, se registraron más de 1 780

incidentes cibernéticos en el sector educativo durante 2023, con un aumento de 258 % respecto al año anterior. De estos, más del 86 % implicaron la filtración de datos sensibles (Varonis, 2024).

Además, en el sector K–12, se ha reportado que el 63 % de las instituciones han sido víctimas de ransomware, con pérdidas promedio de US $7,46 millones entre recuperación, rescate y daños reputacionales (Sophos, 2024). Pese a estas cifras alarmantes, muchas instituciones continúan utilizando plataformas como Zoom, Moodle o Google Classroom sin implementar políticas claras de ciberseguridad, ni establecer protocolos de actuación ante incidentes, lo que incrementa su vulnerabilidad frente a ataques maliciosos (Check Point Research, 2025).

Esta situación refleja una debilidad estructural en la cultura de ciberseguridad dentro del sistema educativo. La falta de capacitación del personal, la ausencia de controles técnicos robustos y el uso de herramientas digitales sin configuración adecuada, son factores que perpetúan un entorno propenso a ataques informáticos.

En Costa Rica, aunque el despliegue de plataformas educativas ha generado un impacto positivo, también se han puesto en evidencia vulnerabilidades importantes. El uso de contraseñas débiles o reutilizadas —según Cisco y Dashlane, responsables del 81 % de las brechas—, junto con la ausencia de autenticación de dos factores, deja las cuentas escolares altamente expuestas. Además, la formación docente en ciberseguridad es limitada, reducida a algunas horas de módulo en el currículo oficial del MEP, y muchas de estas competencias digitales son percibidas como insuficientes por los mismos educadores. Esta combinación, unida a la falta de supervisión efectiva del uso digital por parte del estudiantado, expone a toda la comunidad educativa a riesgos reales de acceso no autorizado y pérdida de datos.

Estudios de la Universidad de Costa Rica y de la UNED confirman esta preocupación. La UCR —mediante su informe ‘Hacia la Sociedad de la Información y el Conocimiento’ (2024)— reconoce que, aunque los estudiantes tienen acceso a plataformas digitales, no cuentan con formación suficiente para identificar amenazas ni proteger sus datos

Por su parte, un estudio de la UNED recomienda ‘robustecer protocolos de ciberseguridad’, lo cual implica la necesidad de educar en criterios adecuados de prevención

Según el Ministerio de Ciencia, Innovacion, Tecnologia y Telecomunicaciones (MICITT, 2023), reconoce la necesidad urgente de fortalecer la seguridad de los sistemas educativos, asi como promover la formación de ciudadanos digitales conscientes y responsables. Esta estrategia subraya la importancia de involucrar a todos los actores (gobierno, instituciones educativas, docentes, estudiantes y padres de familia) en la construcción de una cultura de ciberseguridad que se desarrolle desde etapas tempranas.

Por lo anterior, se considera fundamental realizar un estudio específico en el contexto costarricense que no solo evidencie las debilidades actuales en ciberseguridad en ambientes escolares, sino que oriente el desarrollo de estrategias y soluciones efectivas para poder mitigar dichas amenazas. El objetivo es generar conocimiento aplicado y proponer lineamientos que permitan a las instituciones educativas adoptar buenas prácticas de ciberseguridad, fortalecer políticas internas y reducir la exposición a riesgos digitales.

1.3 Justificación

Esta investigación es de gran relevancia porque se enfoca en un tema actual, urgente y sensible: la seguridad digital en el entorno educativo. A medida que más procesos escolares dependen de plataformas en línea, también aumenta la exposición a riesgos cibernéticos. Los menores de edad, por su desconocimiento y por ser nativos digitales, son particularmente vulnerables a ataques, fraudes y manipulación en línea. Esta realidad hace que proteger los entornos virtuales escolares sea una prioridad.

En Costa Rica, la educación pública y privada ha adoptado plataformas educativas con diferentes niveles de éxito, pero en la mayoría de los casos sin estrategias formales de seguridad. Las consecuencias van desde la pérdida de información académica hasta riesgos serios de privacidad para estudiantes, docentes y familias. A esto se suma la falta de una cultura de ciberseguridad en los centros educativos, donde muchas veces se asume que el software por sí solo brinda protección suficiente. Esta omisión no solo compromete la integridad de los datos, sino que también erosiona la confianza en los sistemas educativos digitales.

Realizar un estudio investigativo permitirá, en primer lugar, tener claridad sobre las amenazas más frecuentes y emergentes en este entorno. Lo más importante es que abre la posibilidad de construir soluciones concretas, prácticas y ajustadas a la realidad de las escuelas del país. Aplicar buenas prácticas de la industria no significa implementar sistemas complejos, sino adaptar lo que ya funciona a un entorno educativo que tiene sus propias

características y limitaciones, ir más allá de las generalidades para identificar vectores de ataque específicos, debilidades sistémicas y patrones de comportamiento de riesgo dentro del contexto nacional.

Más allá del diagnóstico, el verdadero valor de esta investigación radica en su capacidad para catalizar la construcción de soluciones concretas, prácticas y genuinamente ajustadas a los centros educativos del país. La meta no es replicar acríticamente modelos de seguridad corporativos complejos e inalcanzables. Por el contrario, se busca adaptar las buenas prácticas de la industria, despojándolas de su complejidad innecesaria y contextualizándolas a las características y limitaciones inherentes al entorno educativo: presupuestos restringidos, capacidades técnicas variables y la necesidad de priorizar la experiencia de aprendizaje. Esto podría implicar la formulación de guías prácticas, protocolos simplificados de respuesta a incidentes, o el diseño de programas de concientización y capacitación dirigidos específicamente a la comunidad educativa.

En última instancia, abordar esta problemática a través del presente estudio se traduce en un fortalecimiento tangible de la infraestructura de seguridad de los entornos educativos digitales. Esto no solo implica proteger los activos informáticos, sino, y más crucialmente, salvaguardar a los usuarios más vulnerables: nuestros estudiantes menores de edad. Al crear entornos digitales más seguros, no solo prevenimos incidentes, sino que también fomentamos un espacio de confianza y resiliencia digital, fundamental para el desarrollo pleno de las futuras generaciones en un mundo cada vez más interconectado. La investigación, por tanto, trasciende el ámbito técnico para convertirse en un imperativo ético y social, contribuyendo a edificar un ecosistema educativo digital donde la innovación y la seguridad coexistan armónicamente.

1.4 Objetivos

1.4.1 Objetivo general

Elaborar una investigación 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 décimo hasta duodécimo en el año 2025

1.4.2 Objetivos específicos

1) Identificar los principales conceptos, fundamentos teóricos y normativas nacionales e internacionales relacionados con la ciberseguridad en el ámbito educativo, con el propósito de establecer una base contextual para el estudio.

2) Evaluar el nivel de exposición y preparación de estudiantes, docentes y personal administrativo ante amenazas emergentes en plataformas educativas, a fin de determinar las vulnerabilidades más críticas en centros escolares de Costa Rica.

3) Diseñar una propuesta de medidas prácticas y accesibles de ciberseguridad, basadas en buenas prácticas de la industria, con el objetivo de fortalecer la protección de los entornos virtuales escolares y fomentar una cultura digital preventiva.

1.5 Alcances

El presente trabajo de investigación tiene como propósito analizar las amenazas emergentes en el uso de plataformas educativas dentro de los centros de enseñanza secundaria del cantón de Pérez Zeledón, con el fin de comprender el nivel de preparación, conciencia y respuesta de la comunidad educativa ante los riesgos digitales.

En este sentido, los alcances definen el marco de acción del estudio, los límites temáticos, espaciales y poblacionales, así como las proyecciones de utilidad de sus resultados dentro del contexto educativo costarricense.

Alcance temático:

El estudio se centra en el análisis de la ciberseguridad educativa y las amenazas emergentes que afectan las plataformas digitales utilizadas por docentes y estudiantes en los procesos de enseñanza y aprendizaje. Se abordan temas como la protección de datos, el uso responsable de la tecnología, la capacitación digital y la existencia de protocolos de seguridad institucional.

Alcance geográfico:

La investigación se desarrolló en el cantón de Pérez Zeledón, provincia de San José, Costa Rica, seleccionando instituciones educativas de nivel secundario que utilizan plataformas como Microsoft Teams, Google Classroom y Edutec.

Alcance temporal:

El estudio se llevó a cabo durante el segundo semestre del año 2025, abarcando el periodo comprendido entre septiembre y diciembre, que coincide con la ejecución del trabajo final de graduación y el ciclo lectivo del Ministerio de Educación Pública.

Alcance poblacional:

La población estuvo compuesta por docentes y estudiantes de décimo a duodécimo año de distintos colegios del cantón, seleccionados mediante un muestreo no probabilístico por conveniencia, incluyendo además entrevistas a docentes y a un asesor regional de informática del MEP.

Alcance académico y práctico:

Los resultados obtenidos buscan servir como base para la mejora de políticas institucionales y programas de capacitación en ciberseguridad educativa. Asimismo, aportan información útil para futuras investigaciones y fortalecen la formación digital en el ámbito escolar costarricens

Figura 1 Flujo del proyecto investigativo sobre el alcance del estudio de ciberseguridad en plataformas educativas

Nota. El diagrama representa las fases del proyecto investigativo, desde el análisis de amenazas digitales hasta la evaluación de la preparación institucional y la formulación de estrategias locales para fortalecer la ciberseguridad en entornos educativos de Pérez Zeledón.

En la figura se aprecia los diferentes procesos que se tuvieron que seguir para poder alcanzar el alcance de el proyecto.

1.6 Limitaciones

El presente estudio posee limitaciones inherentes al tipo de investigación realizada y al alcance planteado. En primer lugar, no busca **implementar cambios directos** en las instituciones educativas ni **auditar redes informáticas o plataformas internas**, ya que su propósito se centra en el análisis descriptivo de la situación actual y no en la aplicación técnica de soluciones.

En segundo lugar, la investigación **no incluye centros universitarios ni escuelas de primaria**, pues el enfoque se delimita exclusivamente al ámbito de la educación secundaria. De esta manera, el estudio se orienta hacia docentes y estudiantes que cursan los niveles de **décimo a duodécimo año** dentro del **cantón de Pérez Zeledón**.

Asimismo, los resultados y conclusiones se basan en la información obtenida mediante **cuestionarios y entrevistas**, lo cual implica que las percepciones de los participantes pueden variar según su experiencia, conocimiento y contexto institucional. No obstante, estas limitaciones no afectan la validez del estudio, sino que definen con mayor precisión su campo de acción y contribuyen a la comprensión de la ciberseguridad educativa desde una perspectiva local y contextualizada.

1.7 Tabla 1 Cronograma de actividades

NOMBRE DE LA TAREA	DURACIÓN	INICIO	FINAL
Trabajo de investigación final			
Inicio	1 día	10 sep	10 sep
Matricula TFG	1 día	10 sep	10 sep
Lectura manual de TFG y anotación de dudas	1 día	10 sep	10 sep
Reunión con el tutor	1 día	10 sep	10 sep
Planeación del trabajo	1 día	11 sep	11 sep
Definición del título	1 días	11sep	11 sep
Definición de objetivos	1 días	11 sep	11sep
Creación del cronograma	1 día	12 sep	12 sep
Creación bitácora de trabajo	1 día	12 sep	12 sep
Entrega del plan de trabajo al tutor.	1dia	13 sep	13 sep
Desarrollo	2 dias	14 sep	15 sep
Desarrollo del Capítulo I	1 dias	15 sep	15 sep
Creación de estructura del TFG	1 dia	15 sep	16sep
Planteamiento del tema	1 dia	15 sep	16sep
Justificación del trabajo	1 dia	15 sep	16sep
Definición de alcances	1 dia	16 sep	17 sep
Definición de limitaciones	1 dia	17 sep	18 sep
Definición producto esperado	1 dia	19 sep	19 sep
Envío Capítulo I a tutor	1 dia	19 sep	19 sep

Desarrollo del Capítulo II	7 días	24 sep	30 sep
Desarrollo de marco teórico	7 días	01 oct	07 oct
Envío Capítulo II a tutor	1 día	10 oct	10 oct
Desarrollo del Capítulo III	1 día	10 oct	10 oct
Tipo de Investigación	2 días	11 oct	12 oct
Administración y abordaje	2 días	13 oct	14 oct
Sujetos y fuentes	2 días	15 oct	16 oct
Diseño de técnicas e instrumentos para recolección de información	4 días	17 oct	20 oct
Envío Capítulo III a tutor	1 día	20 oct	21 oct
Desarrollo del Capítulo IV	1 dia	21 oct	22 oct
Introducción a la propuesta	1 días	23 oct	24 oct
Propuesta	5 días	25 oct	29 oct
Envío Capítulo IV a tutor	1 día	30 oct	30 oct
Desarrollo del Capítulo V			
Desarrollo conclusiones	2 días	01 nov	02 nov
Desarrollo recomendaciones	2 días	03 nov	04 nov
Resumen ejecutivo	2 días	05 nov	06 nov
Anexos	3 días	07 nov	09 nov
Envío Capítulo V a tutor	1 día	10 nov	10 nov
Cierre Trabajo Final			
Revisión por parte del Tutor	3 días	11 nov	13 nov
Correcciones sugeridas por Tutor	2 días	14 nov	15 nov

Entrega borrador al Lector	1 día	16 nov	16 nov
Revisión por parte del Lector	3 días	17 nov	19 nov
Correcciones sugeridas por Lector	4 días	20 nov	24 nov
Correcciones Trabajo Final	4 días	24 nov	27 nov
Empaste documento Final	3 días	27 nov	30 nov
Entrega documento a Universidad	1dias	30 nov	30 nov
Trabajo Final – Tesis	1 día	06 dic	06 dic

Nota: Elaboración propia (2025). La siguiente tabla del cronograma de actividades muestra como se distribuyeron los días para poder completar lo que fue la investigación

1.8 Tabla 2 Producto esperado del TFG

Objetivos específicos	Entregables	Formato
1) Realizar un diagnostico de la situación actual de la ciberseguridad del ámbito educativo de las instituciones de secundaria en el cantón de Perez Zeledón.	Resumen comparativo de conceptos y normativas con ejemplos aplicados al contexto escolar.	Documento Word/PDF

2) Evaluar el nivel de exposición y preparación de estudiantes, docentes y personal administrativo ante amenazas emergentes en plataformas educativas, a fin de determinar las vulnerabilidades más críticas en centros escolares de Costa Rica.	Análisis de los resultados del nivel de conocimiento del personal docente y administrativo de la Ciberseguridad y los protocolos de actuación ante un incidente Cibernético.	Documento Excel
3) Diseñar una propuesta de medidas prácticas y accesibles de ciberseguridad, basadas en buenas prácticas de la industria, con el objetivo de fortalecer la protección de los entornos virtuales escolares y fomentar una cultura digital preventiva.	Propuesta de manual de ciberseguridad para entornos escolares y las plantillas correspondientes que soportan el proceso.	Manual en Documento Word/PDF

Nota: Elaboración propia (2025). Con base en la Tabla 2 resume los productos que se obtendrán del trabajo final, mostrando cómo cada uno se vincula con los objetivos y etapas de la investigación. Permite identificar de forma clara qué entregables se generarán y cuál es su función dentro del estudio.

CAPÍTULO II. MARCO TEÓRICO

1. La Digitalización del Ámbito Educativo y sus Implicaciones

(UNESCO, 2021; BID, 2022) La transformación digital ha reconfigurado profundamente el panorama educativo en todo el mundo. A raíz de la pandemia por COVID-19, el sistema educativo global experimentó una transición forzada hacia entornos virtuales, haciendo evidente tanto la necesidad como la fragilidad de los mecanismos digitales implementados. Plataformas como Google Classroom, Microsoft Teams, Moodle y Zoom se convirtieron en los pilares para la continuidad pedagógica, permitiendo que millones de estudiantes pudieran continuar con su proceso formativo. No obstante, esta implementación masiva se desarrolló, en muchos casos, sin la debida planificación en términos de seguridad informática y capacitación.

(BID, 2022; UNESCO, 2021) En América Latina, el Banco Interamericano de Desarrollo y la UNESCO coinciden en que la pandemia evidenció brechas tecnológicas y desigualdades estructurales en el acceso a plataformas digitales. Instituciones educativas ubicadas en zonas rurales o con escasos recursos enfrentaron mayores dificultades, lo que limitó no solo el acceso a los contenidos, sino también la posibilidad de proteger los datos de estudiantes y docentes. Esta falta de equidad digital pone en riesgo no solo la calidad educativa, sino también la integridad de la información.

(OEA, 2020) El uso de tecnologías digitales en el entorno escolar implica una creciente dependencia de entornos conectados, sistemas de gestión de aprendizaje (LMS), aplicaciones móviles, servicios en la nube y redes sociales. Cada una de estas herramientas, si bien facilita el proceso de enseñanza-aprendizaje, introduce nuevas superficies de ataque que pueden ser aprovechadas por ciberatacantes. Según la Organización de Estados Americanos, muchas instituciones educativas carecen de políticas de ciberseguridad, controles de acceso robustos o protocolos de respuesta ante incidentes, lo que las convierte en blancos vulnerables.

(UCR, 2023) Además, la adopción tecnológica muchas veces ocurre sin una debida capacitación docente. Un estudio de la Universidad de Costa Rica reveló que más del 60% del personal docente en secundaria no ha recibido formación específica en protección de datos personales ni en buenas prácticas de seguridad digital. Esta carencia limita la capacidad de respuesta ante incidentes, la correcta gestión de plataformas educativas y la orientación adecuada hacia el estudiantado en cuanto a comportamiento seguro en línea.

(Ley 8968, 2011) Otra dimensión importante de la digitalización educativa es el tratamiento de los datos personales. Las plataformas educativas recopilan y procesan gran cantidad de información sensible: nombres, direcciones, registros académicos, comportamiento en clase, comunicaciones privadas e incluso métricas de aprendizaje. La Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales en Costa Rica establece principios de confidencialidad, consentimiento informado y seguridad, sin embargo, muchas instituciones educativas desconocen o incumplen esta normativa, especialmente cuando delegan la administración de plataformas a proveedores tecnológicos externos.

(MICITT, 2023) La digitalización también introduce una nueva dinámica pedagógica y relacional. Los vínculos entre docentes, estudiantes y padres de familia se ven mediados por dispositivos y aplicaciones, lo que modifica las formas de interacción y supervisión. Esta nueva realidad requiere establecer lineamientos claros sobre el uso de herramientas digitales, tiempos de exposición, normas de comunicación y límites tecnológicos. Además, el fenómeno del multitasking y el uso de múltiples pantallas ha generado preocupaciones sobre la atención, la comprensión lectora y la salud mental de los estudiantes, especialmente en los grados superiores como décimo, undécimo y duodécimo.

(MICITT, 2023; OEA, 2020) En este sentido, la digitalización educativa no debe concebirse únicamente como un avance tecnológico, sino como un proceso complejo que

debe ir acompañado de políticas públicas, marcos regulatorios y estrategias de capacitación que integren la dimensión ética, pedagógica y de seguridad. La Estrategia Nacional de Ciberseguridad de Costa Rica subraya la importancia de fortalecer los sistemas educativos en materia de ciberseguridad y promover una ciudadanía digital responsable. Este enfoque es crucial si se pretende lograr una transformación digital educativa sostenible, segura e inclusiva.

(Estonia y Finlandia citados en MICITT, 2023) La experiencia global también ofrece valiosas lecciones. En países como Estonia y Finlandia, donde la transformación digital educativa se planificó desde una perspectiva de Estado, los niveles de ciberseguridad en las escuelas son significativamente más altos. Esto demuestra que una visión estratégica, integradora y con inversión pública puede garantizar entornos educativos digitales más resilientes.

(MICITT, 2023) En resumen, la digitalización del ámbito educativo representa una oportunidad para democratizar el conocimiento, pero también plantea enormes desafíos en términos de equidad, seguridad y sostenibilidad. Superar estos retos exige un compromiso conjunto entre el Estado, las instituciones educativas, el personal docente, las familias y los estudiantes, articulando acciones que aseguren que la tecnología no sea una fuente de vulnerabilidad, sino una herramienta de transformación positiva.

2. Amenazas Cibernéticas Emergentes en Entornos Escolares

(Check Point, 2023) Las plataformas virtuales en la educación han abierto nuevas puertas al conocimiento, pero también han introducido riesgos significativos que afectan la

integridad, confidencialidad y disponibilidad de los datos escolares. La creciente dependencia de entornos digitales ha convertido a las instituciones educativas en blancos atractivos para los ciberataques, especialmente aquellas con infraestructuras limitadas y escaso personal técnico especializado.

(Check Point, 2023) Una de las amenazas más prevalentes es el phishing dirigido, una técnica de ingeniería social que busca engañar a los usuarios para que entreguen voluntariamente sus credenciales o datos sensibles. En el contexto educativo, los atacantes suelen suplantar comunicaciones de plataformas legítimas como Google Classroom o Teams, enviando correos que aparentan ser tareas, exámenes o notificaciones urgentes. El informe de Check Point (2023) resalta que durante los primeros seis meses del año, los ataques de phishing en el sector educativo aumentaron un 44% a nivel global.

(MICITT, 2023) Otra amenaza crítica es la suplantación de identidad, que no solo se limita al robo de cuentas institucionales, sino que también puede derivar en la manipulación de notas, acceso no autorizado a información privada y daños reputacionales. En muchas ocasiones, los estudiantes mismos, ya sea por curiosidad o conflictos personales, participan en este tipo de prácticas, revelando la necesidad de formación en ética digital y seguridad cibernética desde edades tempranas.

(Baltimore County Public Schools, 2021) La propagación de malware es también una amenaza recurrente. Al compartir archivos a través de plataformas de mensajería, correo electrónico institucional o servicios en la nube, se corre el riesgo de diseminar software malicioso que puede inutilizar sistemas, robar datos o crear puertas traseras para accesos no autorizados. Casos documentados en Estados Unidos, como el ataque de ransomware al sistema de escuelas públicas de Baltimore (2021), demuestran el impacto potencial de estas intrusiones.

Un factor agravante es el uso de dispositivos personales sin ningún tipo de control institucional, lo que incrementa la vulnerabilidad. Muchas instituciones educativas permiten o incluso dependen del modelo BYOD (Bring Your Own Device), pero no cuentan con políticas claras de seguridad ni sistemas de monitoreo para estos dispositivos. Esto representa un punto débil considerable, sobre todo cuando los estudiantes se conectan desde redes Wi-Fi públicas no seguras o comparten dispositivos con familiares que pueden instalar software de riesgo.

(OEA, 2020) A lo anterior se suma la falta de auditorías de seguridad. Según la OEA (2020), más del 70% de las escuelas en América Latina no realiza revisiones regulares de sus sistemas digitales, ni cuentan con protocolos de respuesta ante incidentes. Esto implica que muchos ataques pueden pasar desapercibidos o no ser tratados adecuadamente, generando pérdidas de información y afectaciones al funcionamiento académico.

(MICITT, 2023) Además, el almacenamiento en la nube, aunque conveniente, introduce riesgos si no se configura correctamente. La mala administración de permisos de acceso, la ausencia de cifrado de extremo a extremo y la dependencia de proveedores sin garantías claras de seguridad, pueden facilitar la exposición involuntaria de datos personales y académicos.

(OEA, 2020) Las amenazas no siempre provienen de agentes externos. El acceso indebido por parte de personal interno, ya sea administrativo o docente, puede generar filtraciones intencionales o accidentales. La seguridad de la información requiere, por tanto, una combinación de medidas técnicas y éticas.

(MICITT, 2023) En el contexto costarricense, un estudio del MICITT (2023) alertó sobre la falta de protocolos estandarizados en centros educativos públicos frente a incidentes cibernéticos, así como la necesidad urgente de invertir en sistemas de detección temprana, firewalls, autenticación multifactor y concientización del personal.

(NIST, 2018) La normativa internacional también ofrece marcos de referencia útiles. El NIST Cybersecurity Framework, por ejemplo, plantea cinco funciones esenciales: identificar, proteger, detectar, responder y recuperar. Su aplicación en el sector educativo puede servir como guía para estructurar políticas de ciberseguridad adaptadas a los recursos y necesidades del país.

(ISO/IEC 27001, 2013) Otra referencia útil es la norma ISO/IEC 27001, que establece requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información. Aunque su adopción puede parecer costosa para instituciones educativas pequeñas, existen versiones adaptadas o guías simplificadas que permiten una implementación gradual y sostenible.

(MICITT, 2023) Por último, es importante destacar el papel de la capacitación como barrera frente a estas amenazas. Las tecnologías por sí solas no bastan: se requiere que docentes, estudiantes y padres de familia comprendan los riesgos, reconozcan señales de alerta y sepan cómo actuar ante un incidente. Campañas educativas, charlas informativas y simulacros pueden contribuir significativamente a este fin.

En conclusión, las amenazas cibernéticas en entornos escolares son diversas, dinámicas y en constante evolución. Su impacto puede ser devastador si no se cuenta con medidas de prevención, detección y respuesta adecuadas. La clave está en adoptar una visión integral de la ciberseguridad, donde la tecnología, la formación y las políticas institucionales trabajen en conjunto para proteger a la comunidad educativa.

3. Vulnerabilidad de Menores de Edad en el Ciberespacio Escolar

(UNICEF, 2022) La presencia de menores de edad en entornos digitales ha crecido exponencialmente durante la última década, especialmente en el ámbito educativo, donde el

uso de plataformas virtuales se ha vuelto cotidiano. Esta exposición constante al ciberespacio plantea múltiples riesgos, dado que niños y adolescentes, a pesar de ser nativos digitales, no cuentan con la madurez psicológica ni el criterio necesario para manejar adecuadamente situaciones complejas que se presentan en línea.

(UNICEF, 2022) Según esta organización, más del 70% de los menores de 18 años acceden regularmente a Internet, y una parte significativa de ese tiempo lo dedican a plataformas educativas. Aunque estas herramientas están diseñadas con fines pedagógicos, no siempre están acompañadas de controles de seguridad adecuados. La brecha de juicio digital —término que describe la diferencia entre habilidades técnicas y madurez emocional— es una de las principales causas de exposición a riesgos cibernéticos como el acoso digital.

(MEP, 2023) El acoso digital o ciberbullying representa uno de los peligros más frecuentes. A través de chats, correos o publicaciones anónimas, los estudiantes pueden ser víctimas de agresiones psicológicas persistentes que afectan su rendimiento académico, autoestima y salud mental. En Costa Rica, el Ministerio de Educación Pública reportó un aumento del 35% en denuncias relacionadas con ciberacoso escolar tras el retorno a clases presenciales, donde las plataformas virtuales siguen siendo utilizadas como medios de interacción.

(UNICEF, 2022) La filtración de información personal es otra amenaza crítica. Muchos menores comparten datos sensibles —como nombres, fotos, ubicación o contraseñas— sin tener plena conciencia de las consecuencias. Esta información puede ser utilizada para suplantación de identidad, extorsión o explotación. En algunos casos, estos datos terminan en la dark web o en bases de datos ilícitas, alimentando redes de ciberdelincuencia.

(UNICEF, 2022) El robo de credenciales es facilitado por la baja complejidad de contraseñas utilizadas por menores, quienes a menudo emplean combinaciones predecibles o reutilizan claves en múltiples servicios. La ausencia de autenticación multifactorial y la supervisión limitada por parte de adultos responsables hacen que estos ataques tengan altas tasas de éxito.

(UNICEF, 2022) Otro riesgo importante es la exposición a contenidos inapropiados. Plataformas educativas con enlaces externos, contenido multimedia o zonas de comentarios pueden convertirse en canales de acceso a material violento, sexual o discriminatorio. Si no existen filtros adecuados o monitoreo constante, los menores quedan vulnerables a ser impactados por este tipo de material, afectando su desarrollo emocional y social.

(Erikson, 1950) Desde una perspectiva psicológica, Erikson sostiene que los adolescentes se encuentran en una etapa de búsqueda de identidad, lo que los hace más propensos a ser influenciados por grupos, validación externa y figuras autoritarias o persuasivas. En el ciberespacio, estas condiciones son explotadas por actores maliciosos para manipular comportamientos, inducir retos peligrosos o captar menores para fines ilícitos.

(Giedd, 2015) Además, estudios en neurociencia han demostrado que el cerebro adolescente aún está en formación, especialmente en áreas relacionadas con el juicio, la toma de decisiones y la gestión del riesgo. Esta inmadurez neurológica incrementa la probabilidad de que los adolescentes participen en actividades peligrosas en línea sin evaluar sus consecuencias a largo plazo.

(Ley 8990) En el ámbito legal, Costa Rica cuenta con leyes como la Ley para la Protección de la Persona Menor de Edad frente al Uso de Contenidos y Acciones Nocivas en Internet, que obliga a los proveedores de servicios y a las instituciones educativas a establecer

mecanismos de protección. No obstante, su implementación sigue siendo dispareja, especialmente en zonas rurales y centros educativos con bajo presupuesto.

(Common Sense Media, 2023) El rol de los padres, docentes y autoridades escolares es crucial para mitigar estos riesgos. La supervisión activa, la comunicación abierta y la formación en competencias digitales son medidas preventivas eficaces. Programas de alfabetización digital enfocados en menores deben incluir componentes sobre privacidad, reputación en línea, detección de amenazas y canales seguros de denuncia.

(Common Sense Media, 2023) Asimismo, la inclusión de componentes de ética digital y ciudadanía en los currículos educativos puede contribuir a una cultura de uso responsable del entorno digital. Esta organización ha desarrollado guías para integrar estos contenidos en el aula, adaptados a diferentes niveles escolares.

(UNICEF, 2022) El uso de herramientas tecnológicas como controles parentales, filtros de contenido y monitoreo de actividad puede ser útil, siempre que se acompañen de un diálogo respetuoso con los menores y no se utilicen como métodos invasivos o punitivos. El equilibrio entre protección y autonomía digital es clave para fomentar un desarrollo saludable.

(UNICEF, 2022) En definitiva, la protección de menores en el ciberespacio escolar requiere una estrategia multidimensional que combine legislación, formación, tecnología y cultura institucional. La creación de ambientes digitales seguros es una responsabilidad compartida entre Estado, instituciones, familias y la sociedad en general.

4. Cultura de Ciberseguridad y Políticas Institucionales

(OEA, 2020) Una cultura de ciberseguridad efectiva dentro de las instituciones educativas no solo implica la implementación de medidas técnicas, sino también el desarrollo de una mentalidad colectiva que valore la protección de la información como un pilar

fundamental del proceso de enseñanza-aprendizaje. Este enfoque cultural debe permear todos los niveles de la organización: desde el personal administrativo y docente hasta los estudiantes y sus familias.

(OEA, 2020) En muchas escuelas, la falta de una estrategia institucional en ciberseguridad se traduce en la ausencia de políticas claras de uso de tecnología, protocolos de respuesta a incidentes, mecanismos de monitoreo del comportamiento digital y estructuras de gobernanza que incluyan la seguridad como una prioridad institucional. Esta debilidad es especialmente visible en instituciones que han adoptado plataformas digitales de manera acelerada, sin acompañamiento técnico ni pedagógico.

(OEA, 2020) Uno de los grandes desafíos es el enfoque reactivo en lugar de preventivo. Las medidas de seguridad suelen implementarse luego de sufrir un incidente, en lugar de anticiparse a los riesgos. Esta actitud puede derivar en consecuencias serias, como interrupciones prolongadas del servicio educativo, pérdida de información académica, vulneración de datos personales o incluso litigios legales si se demuestra negligencia en la protección de menores.

(OEA, 2020) Los sistemas de gestión de aprendizaje (LMS), como Moodle, Edmodo, Google Classroom o Microsoft Teams, son herramientas valiosas, pero su uso sin configuración adecuada y sin capacitación puede abrir puertas a accesos no autorizados, robo de identidad y espionaje académico. Los administradores institucionales deben configurar estos sistemas siguiendo buenas prácticas como el principio de mínimo privilegio, el registro de accesos, las auditorías periódicas y la encriptación de datos sensibles.

(OEA, 2020) En términos de políticas institucionales, es necesario definir normas claras sobre lo que se espera del comportamiento digital de cada actor. Esto incluye políticas de contraseñas, tiempo de uso permitido, sitios web bloqueados, manejo de dispositivos

móviles, uso de correo institucional y canales de comunicación formales. Estas políticas deben ser actualizadas anualmente y firmadas por los miembros de la comunidad educativa para asegurar su entendimiento y compromiso.

(Ministerio de Educación de Estonia, 2022) Una buena práctica observada en sistemas educativos avanzados como el de Singapur o Estonia es la incorporación de manuales de convivencia digital, donde se definen derechos y responsabilidades de los usuarios, protocolos de denuncia, y consecuencias ante comportamientos inapropiados en línea. Estos manuales están integrados en la cultura institucional y son parte del proceso de inducción para nuevos docentes y estudiantes.

(Common Sense Education, 2023) La concientización y la formación continua son ejes fundamentales. Los programas de formación no deben limitarse a talleres puntuales, sino incluirse como parte del desarrollo profesional docente. Las temáticas deben abarcar desde conceptos básicos como contraseñas seguras y reconocimiento de correos sospechosos, hasta temas más complejos como gestión de identidad digital, cifrado, derechos de autor en el entorno digital, ciberacoso y su prevención.

(Comisión Europea, 2021) Es igualmente relevante la evaluación periódica de la madurez digital institucional. Herramientas como el SELFIE de la Comisión Europea permiten a las instituciones educativas autoevaluar su nivel de integración tecnológica y de ciberseguridad, proporcionando indicadores clave para la mejora continua.

(Common Sense Education, 2023) La participación de los estudiantes también es esencial. Promover la creación de “clubes de ciberseguridad” o grupos estudiantiles de alfabetización digital puede generar un efecto multiplicador. Estos grupos pueden liderar campañas de sensibilización, crear materiales educativos y promover la denuncia segura de incidentes.

(MICITT, 2023) Por otra parte, se requiere inversión sostenida en infraestructura tecnológica. Esto incluye la adquisición de sistemas de protección perimetral, soluciones antivirus institucionales, respaldo en la nube, y contratación de personal especializado en tecnología educativa y ciberseguridad. Las alianzas público-privadas pueden facilitar esta inversión, así como programas de cooperación internacional.

(MICITT, 2023; Ley 8968) Desde el punto de vista normativo, en Costa Rica se hace necesario fortalecer la articulación entre la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, la Ley General de Educación y la Estrategia Nacional de Ciberseguridad. Estas herramientas legales deben convertirse en políticas vivas dentro de cada institución educativa, con guías prácticas que traduzcan su lenguaje técnico a recomendaciones accionables.

(OEA, 2020) En conclusión, construir una cultura institucional sólida de ciberseguridad implica un enfoque multidimensional: técnico, normativo, pedagógico y ético. Es una responsabilidad compartida que requiere liderazgo, recursos y compromiso sostenido. Solo así las escuelas podrán convertirse en espacios verdaderamente seguros y resilientes frente a los retos del entorno digital.

5. Buenas Prácticas y Estrategias de Mitigación en el Contexto Costarricense

(MICITT, 2023) El fortalecimiento de la ciberseguridad en el ámbito educativo costarricense requiere de la adopción de medidas específicas que atiendan tanto las vulnerabilidades técnicas como los aspectos humanos, culturales y organizacionales. Las buenas prácticas deben ser realistas, escalables y adecuadas a las limitaciones de recursos que

caracterizan a muchos centros educativos, especialmente en zonas rurales o con infraestructura limitada.

(MICITT, 2023) Entre las recomendaciones más relevantes para prevenir, detectar y responder a los incidentes de ciberseguridad en entornos escolares se encuentran:

Uso de contraseñas seguras y políticas de autenticación: Establecer lineamientos claros para la creación y renovación periódica de contraseñas. Fomentar el uso de contraseñas complejas y únicas. Complementar esta medida con la implementación de autenticación de dos factores (2FA) para accesos sensibles a plataformas institucionales.

Capacitación continua en cultura digital y seguridad: Establecer programas regulares de formación para docentes, administrativos, estudiantes y padres de familia, sobre temas como protección de datos, detección de fraudes, uso seguro de redes sociales, gestión de identidades y respuesta ante incidentes.

Protocolos de respuesta ante incidentes: Elaborar planes claros de actuación en caso de filtración de datos, acceso no autorizado, suplantación de identidad, o propagación de malware. Incluir en estos protocolos una cadena de comunicación interna, canales de denuncia y acciones de recuperación.

Concientización adaptada por grupo etario: Implementar campañas de educación digital segmentadas por edad, con lenguaje accesible y ejemplos prácticos, que aborden temas como el ciberacoso, el consentimiento digital, los riesgos del sexting, y el uso ético de la información.

Respaldo y recuperación de datos: Asegurar que toda la información crítica (calificaciones, historial académico, reportes de comportamiento) esté respaldada en sistemas seguros, con copias automatizadas y almacenadas fuera del entorno local.

Filtros de contenido y monitoreo de actividad: Aplicar soluciones de filtrado para limitar el acceso a sitios web maliciosos o inapropiados. Utilizar herramientas de monitoreo que alerten sobre comportamientos inusuales o intentos de intrusión, respetando siempre la privacidad de los usuarios.

Designación de responsables TIC dentro de las instituciones: Nombrar encargados que supervisen el cumplimiento de las políticas digitales, gestionen el soporte técnico, y lideren procesos de mejora continua en seguridad tecnológica.

(NIST, 2018; ISO/IEC 27001, 2013)

6. Aplicación gradual de marcos internacionales:

Adaptar herramientas como el NIST Cybersecurity Framework o la norma ISO/IEC 27001 a las necesidades locales. Por ejemplo, se puede iniciar con un diagnóstico básico usando el modelo “Identificar, Proteger, Detectar, Responder, Recuperar”, e ir desarrollando acciones concretas en cada área.

(OpenVAS, 2024)

7. Evaluaciones periódicas de vulnerabilidades:

Utilizar herramientas gratuitas o de bajo costo (como OpenVAS o SecurityScorecard para instituciones públicas) para evaluar el estado de la seguridad de los sistemas escolares y tomar medidas preventivas.

(Common Sense Media, 2023)

8. Fomento de la ciudadanía digital:

Integrar en el currículo formal contenidos sobre derechos digitales, privacidad, manejo de la identidad en línea, y la importancia de la ética en el uso de tecnologías.

(MICITT, 2023) La Estrategia Nacional de Ciberseguridad de Costa Rica 2023–2027 hace énfasis en la necesidad de formar ciudadanos digitales conscientes, proteger infraestructuras críticas educativas y establecer programas sostenibles de capacitación. En este sentido, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en conjunto con el MEP, tiene un rol fundamental en la articulación de políticas, el desarrollo de recursos formativos y la supervisión de su implementación.

(MICITT, 2023) Asimismo, alianzas con universidades, centros de investigación y el sector privado pueden facilitar la transferencia de conocimiento y tecnología a los centros educativos. Programas como “Alfabetización Digital para Escuelas” o “Ciberseguridad en el Aula” pueden ser impulsados a través de fondos públicos y cooperación internacional.

(MICITT, 2023; Ley 8968) Finalmente, se recomienda que cada institución elabore un Plan de Seguridad Digital Escolar (PSDE), en el que se incluyan diagnósticos, objetivos, acciones, cronogramas y responsables. Este plan debe revisarse anualmente y alinearse con las políticas del MEP y del MICITT, así como con las leyes nacionales de protección de datos y ciberseguridad.

(MICITT, 2023) La implementación de estas estrategias no solo mejora la seguridad técnica, sino que construye entornos escolares más resilientes, donde el uso de la tecnología se convierte en una oportunidad de aprendizaje seguro y significativo.

9. Impacto Psicológico y Socioeducativo de las Amenazas Cibernéticas en Escolares

(UNICEF, 2022) El entorno digital en el que hoy se desarrolla la educación ha traído consigo beneficios evidentes en cuanto al acceso a la información y la continuidad pedagógica, especialmente tras la pandemia, la cual fue una época difícil y llena de retos. Sin embargo, este proceso de digitalización ha introducido nuevas amenazas que afectan el bienestar integral del estudiantado, en especial a nivel psicológico y emocional.

(UNICEF, 2022) El uso intensivo de plataformas virtuales en niveles de secundaria —como décimo, undécimo y duodécimo año— ha expuesto a los estudiantes a riesgos como el ciberacoso, la suplantación de identidad, el acceso a contenido inadecuado, y el grooming. Estas amenazas no solo alteran la experiencia educativa, sino que también comprometen el desarrollo socioemocional de los adolescentes.

(UNICEF, 2022) El grooming, en particular, representa una forma grave de abuso. A través de redes sociales, videojuegos o plataformas educativas, adultos malintencionados manipulan emocionalmente a menores para obtener confianza, con el fin de explotarlos sexualmente. Este fenómeno ha aumentado en los últimos años y es difícil de detectar sin una vigilancia activa.

(Erikson, 1950) Desde la psicología del desarrollo, se sabe que los adolescentes atraviesan una etapa de construcción de identidad. Durante este periodo, la búsqueda de validación externa, el sentido de pertenencia y la formación del autoconcepto son aspectos clave. La exposición constante a juicios, comparaciones sociales y validación superficial en entornos digitales puede desencadenar crisis emocionales importantes.

(APA, 2021; UNICEF, 2022) Las consecuencias del ciberacoso en estudiantes van desde síntomas de ansiedad, depresión y estrés crónico, hasta el retraimiento social, pérdida

de interés por los estudios y, en casos extremos, ideación suicida. Estas afectaciones mentales son muchas veces invisibles para docentes y padres, lo que dificulta una intervención temprana.

(MEP, 2023) En el caso costarricense, el Ministerio de Educación Pública ha registrado un aumento del 35 % en denuncias por acoso digital tras la pandemia. Muchas víctimas no buscan ayuda debido al miedo, la vergüenza o la amenaza de represalias. En la mayoría de centros educativos no existen canales claros ni personal capacitado para manejar estos casos.

(UNESCO, 2021) Las consecuencias no solo son psicológicas. También se observa una afectación en el rendimiento académico, la asistencia a clases, el grado de participación en actividades escolares, e incluso el abandono educativo. El entorno escolar deja de ser percibido como un espacio seguro.

(UNICEF, 2022) El impacto emocional se refleja también en cambios de conducta: irritabilidad, aislamiento, agresividad, baja autoestima, dificultades para dormir, y pérdida de confianza en figuras de autoridad. Este deterioro emocional reduce la capacidad de aprendizaje y debilita el vínculo con la comunidad educativa.

(MICITT, 2023) Para mitigar estos efectos es necesario adoptar un enfoque integral. Las instituciones deben implementar políticas de ciberseguridad que incluyan atención psicosocial, protocolos de denuncia confidenciales, capacitación en salud mental digital, y campañas de concienciación enfocadas en el autocuidado y la empatía digital.

(Common Sense Media, 2023) La alfabetización emocional digital debe formar parte del currículo escolar. Esta debe enseñar a los estudiantes a identificar sus emociones, manejar el estrés en línea, proteger su privacidad, actuar con respeto, y detectar señales de alerta entre sus compañeros.

(APA, 2021) También se recomienda incorporar la figura del psicólogo escolar con formación en riesgos digitales, así como realizar diagnósticos periódicos del clima escolar virtual, mediante encuestas anónimas y observación sistemática.

(UNICEF, 2022) Finalmente, la familia cumple un rol fundamental. Establecer una comunicación abierta, interesarse genuinamente en las actividades en línea de los hijos y fomentar la confianza mutua son claves para prevenir situaciones de riesgo.

(MICITT, 2023) La escuela debe ser un espacio de seguridad también en el plano digital. Afrontar el impacto psicológico y socioeducativo de las amenazas cibernéticas no puede verse como una tarea opcional, sino como un componente central de la transformación educativa en la era digital.

10. La Brecha Digital como Factor de Riesgo en Ciberseguridad Escolar

(PEN, 2022) La brecha digital en el contexto educativo costarricense no solo representa desigualdad de acceso a oportunidades formativas, sino que se ha convertido en un factor de riesgo crítico en términos de ciberseguridad. Esta brecha se manifiesta en tres niveles fundamentales: (1) el acceso desigual a dispositivos y conectividad; (2) la falta de conocimientos técnicos para protegerse en línea; y (3) la escasa capacidad institucional para mitigar amenazas en contextos vulnerables.

(PEN, 2022) Más del 40% de los estudiantes de secundaria en zonas rurales utilizan redes públicas o compartidas para acceder a plataformas educativas. Estas redes frecuentemente carecen de cifrado, autenticación segura o filtros de contenido, lo cual las convierte en entornos altamente inseguros. Además, un 68% emplea dispositivos personales que son compartidos con familiares y que, en muchos casos, no cuentan con software antivirus actualizado ni configuraciones adecuadas de privacidad.

(UNESCO, 2021) En América Latina, el uso del modelo BYOD (Bring Your Own Device) ha ampliado la brecha de seguridad, ya que muchas instituciones permiten el uso de dispositivos sin ningún tipo de control ni políticas claras. Esto expone a los estudiantes a amenazas como el phishing, el malware, la pérdida de datos y el secuestro de cuentas institucionales.

(UCR, 2023) Esta situación se ve agravada por la falta de formación del cuerpo docente en temas de protección digital. Más del 60% del profesorado de secundaria no ha recibido capacitación específica en ciberseguridad, lo que limita la implementación de medidas preventivas y reduce la capacidad de respuesta ante incidentes tecnológicos.

(BID, 2022) A nivel institucional, muchas escuelas carecen de personal técnico, protocolos de seguridad y acceso a recursos digitales estables, lo cual perpetúa un círculo de vulnerabilidad. En este contexto, los centros educativos más marginados se convierten en blancos fáciles para ciberdelincuentes.

(ECLAC, 2021) Además, la falta de conectividad de calidad sigue siendo una barrera para la equidad educativa. La Comisión Económica para América Latina y el Caribe ha señalado que el acceso limitado a internet de banda ancha en zonas rurales representa una forma moderna de exclusión social que afecta principalmente a niños y adolescentes.

(MICITT, 2023) Superar esta brecha requiere un enfoque integral que no solo contemple la entrega de dispositivos y conexión, sino también el fortalecimiento de capacidades digitales en toda la comunidad educativa. Esto incluye alfabetización digital, formación docente continua, políticas institucionales inclusivas y acompañamiento técnico.

(Common Sense Media, 2023) Es fundamental que se promueva una ciudadanía digital crítica, que permita a los estudiantes entender cómo proteger su información,

identificar riesgos y comportarse de manera responsable en línea. El desarrollo de estas competencias debe ser parte del currículo nacional y formar parte activa de la cultura escolar.

(UNESCO, 2021; PEN, 2022) La brecha digital, por tanto, no debe entenderse únicamente como una cuestión de acceso físico, sino como una carencia de capacidades institucionales y personales para usar las tecnologías de forma segura, ética y eficaz. Incluir esta dimensión en las políticas educativas permitirá desarrollar estrategias diferenciadas de protección digital, garantizando equidad en la seguridad y el aprendizaje.

11. El Rol de la Inteligencia Artificial en la Ciberseguridad Escolar

(NIST, 2020) La inteligencia artificial (IA) ha emergido como una herramienta estratégica clave para fortalecer la ciberseguridad en entornos escolares. Su capacidad para detectar patrones inusuales, realizar análisis predictivos y automatizar respuestas ante amenazas ha transformado la forma en que se gestionan los riesgos digitales en plataformas educativas.

(NIST, 2020) En el ámbito educativo, muchas instituciones han adoptado plataformas como Google Workspace for Education o Microsoft 365 Education. Estas integran soluciones de IA para detectar accesos sospechosos, prevenir intrusiones, bloquear correos fraudulentos y analizar el comportamiento de los usuarios en tiempo real. Esto es especialmente importante en entornos con gran cantidad de estudiantes y limitados recursos de supervisión humana.

(NIST, 2020; MICITT, 2023) El marco de referencia del NIST establece que la IA puede aplicarse de manera efectiva en las cinco funciones básicas de la ciberseguridad: identificar, proteger, detectar, responder y recuperar. Las escuelas pueden beneficiarse, por ejemplo, al implementar IA para realizar diagnósticos de vulnerabilidades, gestionar permisos de acceso o crear sistemas de alerta temprana frente a incidentes.

(GDPR, 2018) No obstante, el uso de inteligencia artificial también requiere marcos legales y éticos robustos. En la Unión Europea, el Reglamento General de Protección de Datos (GDPR) establece que toda decisión significativa basada en IA que afecte a menores debe ser explicable, supervisada por humanos y contar con consentimiento informado. Este marco sirve como referencia para países que aún carecen de regulaciones específicas.

(MICITT, 2023) En Costa Rica, la Estrategia Nacional de Ciberseguridad enfatiza la necesidad de implementar soluciones tecnológicas responsables, destacando el riesgo de vigilancia masiva y sesgos algorítmicos. Si se utilizan sistemas automatizados para monitorear actividades estudiantiles, debe garantizarse que se respeten los derechos de privacidad, la libertad académica y el principio de proporcionalidad.

(Common Sense Media, 2023) Es indispensable que las instituciones informen a padres, docentes y estudiantes sobre cómo funcionan estos sistemas. La falta de transparencia puede generar desconfianza, miedo o malentendidos sobre su uso. Una IA que opera de manera opaca puede ser percibida como una forma de vigilancia en lugar de una herramienta de protección.

(UNESCO, 2022) La UNESCO ha advertido sobre la necesidad de crear entornos de confianza digital. Recomienda que el diseño de soluciones de IA para escuelas se base en valores como la inclusión, la equidad, la sostenibilidad y el desarrollo humano. Estas herramientas deben adaptarse al contexto de cada país y respetar su diversidad cultural, tecnológica y social.

(IEEE, 2021) El sesgo algorítmico es uno de los mayores riesgos. Un sistema mal entrenado puede discriminar a ciertos estudiantes, reforzar estereotipos o generar falsas alertas. Para evitarlo, los modelos deben ser auditables, entrenados con datos representativos y sometidos a procesos de revisión periódica por expertos multidisciplinarios.

(MICITT, 2023) A nivel práctico, la IA puede aplicarse para proteger redes escolares, gestionar permisos y accesos, controlar descargas de archivos sospechosos, detectar acoso en línea, y analizar la interacción de los usuarios con las plataformas para anticipar comportamientos de riesgo. También puede contribuir al diseño de experiencias personalizadas de aprendizaje con enfoque seguro.

(NIST, 2020) Otro uso emergente es la identificación de cuentas falsas, plagio automatizado y bots que intentan acceder a bases de datos educativas. Estas amenazas se han intensificado con el crecimiento de las plataformas LMS y el trabajo híbrido.

(Common Sense Media, 2023) Sin embargo, para garantizar el uso ético de la IA, se requiere formación del personal administrativo y docente. Es esencial que comprendan los límites y el potencial de estas tecnologías, y que puedan participar en su evaluación y mejora continua.

(UNESCO, 2022) Se recomienda además involucrar a los estudiantes en discusiones sobre el uso de IA, enseñándoles desde edades tempranas a entender cómo funcionan estos sistemas, cuáles son sus derechos digitales, y cómo actuar ante situaciones injustas derivadas de decisiones automatizadas.

(GDPR, 2018; MICITT, 2023) La combinación de herramientas tecnológicas avanzadas y marcos regulatorios adecuados permitirá a las escuelas utilizar la IA como aliada. Sin embargo, esto requiere inversión, monitoreo continuo y colaboración entre el Estado, la academia, la industria tecnológica y la sociedad civil.

(IEEE, 2021) Finalmente, el futuro de la ciberseguridad escolar debe contemplar no solo el uso de IA como defensa técnica, sino como una oportunidad para enseñar principios éticos, fomentar pensamiento crítico y promover una cultura digital responsable que forme ciudadanos más conscientes y seguros.

(MICITT, 2023) La inteligencia artificial, usada correctamente, puede ser una poderosa aliada para transformar la educación costarricense en un entorno más seguro, resiliente y humanizado.

12. Ciberseguridad como Pilar de la Ciudadanía Digital

(MICITT, 2023) La ciudadanía digital es un concepto integral que engloba el uso responsable, ético y seguro de las tecnologías de la información y la comunicación. Dentro de este marco, la ciberseguridad ocupa un lugar central, ya que permite garantizar la privacidad, la integridad y los derechos digitales de quienes interactúan en entornos virtuales.

(MICITT, 2023) En el contexto educativo, formar ciudadanos digitales no se limita a enseñar a utilizar herramientas tecnológicas, sino que implica promover habilidades críticas, valores éticos, y normas de comportamiento que orienten el uso seguro y consciente de internet. La Estrategia Nacional de Ciberseguridad de Costa Rica subraya la necesidad de incorporar estos temas desde la escuela.

(Common Sense Media, 2023) Organizaciones internacionales han desarrollado programas curriculares enfocados en ciudadanía digital. Estos incluyen contenidos sobre seguridad en redes sociales, protección de datos personales, prevención del ciberacoso, respeto por la propiedad intelectual, uso del tiempo frente a pantallas y cuidado del bienestar emocional en entornos digitales.

(UNESCO, 2022) La UNESCO define la ciudadanía digital como un derecho que permite la participación plena y significativa en la sociedad digital. Para lograr esto, es fundamental que los estudiantes desarrollen no solo habilidades técnicas, sino también competencias sociales, políticas, éticas y emocionales para actuar con responsabilidad.

(UNICEF, 2022) El desarrollo de la ciudadanía digital también implica empoderar a los menores para identificar contenidos dañinos, reconocer noticias falsas, ejercer sus derechos en línea y defender la inclusión. La alfabetización digital crítica es una herramienta de protección frente a manipulaciones, estafas y amenazas cibernéticas.

(Common Sense Media, 2023) Los programas más efectivos abordan la ciudadanía digital desde edades tempranas, utilizando metodologías activas como juegos, simulaciones y proyectos colaborativos. A medida que los estudiantes crecen, los contenidos deben adaptarse a sus realidades, incluyendo temas como el impacto de los algoritmos, el sesgo en plataformas y la ética de la inteligencia artificial.

(MICITT, 2023) En Costa Rica, la ciudadanía digital debe integrarse transversalmente en el currículo, abarcando asignaturas como cívica, tecnología, orientación, ética y estudios sociales. La ciberseguridad no debe tratarse como un tema técnico aislado, sino como un eje transversal que impacta directamente la vida personal, académica y ciudadana.

(GDPR, 2018) La protección de datos es una dimensión fundamental. Los estudiantes deben conocer qué datos se recopilan, cómo se usan, qué derechos tienen sobre ellos y cómo ejercerlos. Esto cobra especial relevancia con la adopción de plataformas de aprendizaje que recolectan información sensible.

(ECLAC, 2021) La ciudadanía digital también es una herramienta para reducir la brecha digital. Enseñar a los estudiantes a navegar internet con autonomía, interpretar información y protegerse online es una forma de equidad y justicia social en contextos educativos vulnerables.

(Common Sense Media, 2023) Además, fomentar la empatía digital es clave. Entender que detrás de cada perfil hay una persona real contribuye a prevenir la violencia en línea, el discurso de odio y el aislamiento social. La ciudadanía digital también es convivencia digital.

(UNESCO, 2022) La participación cívica digital es otro componente esencial. Denunciar contenidos inapropiados, contribuir a debates informados, colaborar en comunidades virtuales y exigir transparencia de plataformas son acciones que fortalecen la democracia desde las aulas.

(MICITT, 2023) Para lograrlo, las escuelas deben establecer políticas claras de comportamiento digital. Manuales de convivencia digital, protocolos de ciberacoso, políticas de uso de dispositivos y normas de publicación en redes escolares ayudan a crear entornos seguros.

(Common Sense Media, 2023) Las familias también juegan un rol vital. La educación en ciudadanía digital debe ser compartida entre la escuela y el hogar. Promover el diálogo, establecer límites razonables y acompañar a los hijos en su vida digital fortalece la formación de ciudadanos críticos y responsables.

(NIST, 2020) Desde la perspectiva de la ciberseguridad, educar sobre riesgos como el phishing, el robo de identidad, el ransomware y el malware capacita a los estudiantes no solo para protegerse, sino para apoyar la seguridad colectiva de sus comunidades.

(IEEE, 2021) La ética digital se vuelve esencial en una época donde la inteligencia artificial, el big data y la automatización toman decisiones que afectan nuestras vidas. Formar ciudadanos capaces de cuestionar y participar en debates sobre estas tecnologías es tan importante como saber utilizarlas.

(MICITT, 2023) En conclusión, la ciberseguridad y la ciudadanía digital son pilares inseparables de la educación del siglo XXI. Fortalecerlos no solo protege a los estudiantes en el presente, sino que los prepara para ejercer plenamente sus derechos en el mundo digital del futuro.

13. Participación Estudiantil y Liderazgo Juvenil en la Ciberseguridad

(UNESCO, 2022) La participación activa del estudiantado en temas de ciberseguridad no solo es posible, sino necesaria para construir una cultura digital sostenible dentro del entorno escolar. Los estudiantes, al ser usuarios frecuentes de entornos virtuales, están en una posición privilegiada para identificar riesgos, proponer soluciones y promover hábitos digitales responsables entre sus pares.

(UNICEF, 2022) Uno de los enfoques más efectivos ha sido la creación de clubes de ciberseguridad o comités estudiantiles de vigilancia digital. Estos espacios permiten que los jóvenes lideren campañas educativas, detecten comportamientos inapropiados en línea, elaboren materiales informativos, y colaboren con docentes en el diseño de políticas de convivencia digital.

(MICITT, 2023) En Costa Rica, el impulso a la formación de jóvenes embajadores digitales ha sido una estrategia propuesta dentro de la Estrategia Nacional de Ciberseguridad. A través de estos programas, los estudiantes reciben formación básica en ciberseguridad, ciudadanía digital, privacidad y derechos digitales, con el objetivo de actuar como multiplicadores dentro de sus centros educativos.

(Common Sense Media, 2023) El liderazgo juvenil en este ámbito también puede manifestarse mediante proyectos interdisciplinarios. Por ejemplo, estudiantes de secundaria han desarrollado blogs, podcasts, videojuegos, campañas gráficas y simulacros sobre cómo actuar ante amenazas cibernéticas. Estas actividades fortalecen habilidades técnicas, comunicativas y de trabajo en equipo.

(OECD, 2020) Según la Organización para la Cooperación y el Desarrollo Económicos, fomentar el protagonismo estudiantil en la gestión de riesgos digitales fortalece

su autoestima, sentido de pertenencia y compromiso con la comunidad educativa. Además, promueve una cultura preventiva más efectiva que los enfoques exclusivamente punitivos.

(UNESCO, 2022) La participación estudiantil también puede extenderse a la construcción de políticas escolares. Incluir a representantes estudiantiles en la elaboración o revisión de reglamentos digitales, protocolos de acoso virtual o normas de uso de plataformas promueve mayor legitimidad y cumplimiento de estas normativas.

(Save the Children, 2021) A nivel internacional, organizaciones como Save the Children han promovido modelos de protección infantil en línea basados en la participación infantil. Estos modelos reconocen que los niños y adolescentes no son solo beneficiarios pasivos de medidas de protección, sino actores con voz y capacidad de acción.

(UNICEF, 2022) Por otro lado, es fundamental que los adultos acompañen estos procesos sin imponer controles rígidos. La tutoría docente, el respaldo institucional y el respeto a la autonomía juvenil son claves para que las iniciativas lideradas por estudiantes florezcan de forma auténtica y sostenible.

(MICITT, 2023) Finalmente, convertir a los estudiantes en agentes de cambio en ciberseguridad escolar requiere inversión, formación continua y confianza. Con los espacios adecuados, los jóvenes pueden liderar la transformación de la cultura digital desde el aula hacia sus comunidades, generando un impacto más amplio y duradero.

14. Ciberacoso y Violencia Digital como Amenazas Emergentes

(UNICEF, 2022) El avance de las tecnologías digitales ha traído consigo nuevas formas de violencia que afectan especialmente a niños, niñas y adolescentes. Entre estas amenazas emergentes se encuentran el ciberacoso, la sextorsión, el doxxing, el shaming

público y otras expresiones de agresión virtual que pueden tener graves repercusiones psicológicas, sociales y académicas.

(ECPAT, 2021) El ciberacoso escolar consiste en la agresión repetida a través de medios digitales como redes sociales, plataformas educativas, mensajería o foros, e incluye insultos, amenazas, exclusión social y divulgación de rumores o contenido íntimo. La sextorsión, por su parte, implica la amenaza de publicar material sexual para obtener favores adicionales o dinero, y afecta gravemente la integridad emocional de los menores.

(Save the Children, 2021) El doxxing —la publicación de información personal sin consentimiento— y el shaming público —la humillación o exposición en línea— son prácticas que se han incrementado entre estudiantes, muchas veces con consecuencias devastadoras como el retraimiento, la baja autoestima y el abandono escolar.

(MEP, 2023) En Costa Rica, el Ministerio de Educación Pública ha reportado un aumento sostenido en casos de violencia digital desde el regreso a la presencialidad post-pandemia. Muchos de estos casos han sido invisibilizados o minimizados por la falta de protocolos claros y de formación en el personal docente y administrativo.

(MICITT, 2023) La Estrategia Nacional de Ciberseguridad plantea como una prioridad la creación de mecanismos institucionales para la prevención, detección y atención del ciberacoso. Estos mecanismos deben incluir canales de denuncia confidenciales, acompañamiento psicológico y sanciones proporcionales, todo bajo un enfoque restaurativo y de protección a las víctimas.

(UNESCO, 2021) Las estrategias de prevención deben contemplar campañas de sensibilización, inclusión de contenidos sobre convivencia digital en los planes de estudio, y formación continua del personal educativo en violencia digital, derechos digitales y salud mental en línea.

(OECD, 2020) También es importante que las instituciones educativas cuenten con datos actualizados sobre el impacto de estas formas de violencia, mediante encuestas de clima escolar digital, entrevistas, y análisis de plataformas institucionales. Esto permitirá identificar patrones y actuar con anticipación.

(UNICEF, 2022) La intervención debe ser integral: debe considerar al agresor, a la víctima y al entorno. El trabajo con padres, madres y encargados es fundamental para entender el origen del conflicto y evitar la revictimización. La inclusión del estudiantado en la construcción de normas y soluciones refuerza su compromiso y efectividad.

(MICITT, 2023) En última instancia, el ciberacoso y la violencia digital deben ser abordados como problemas sociales y culturales, no solo disciplinarios. La construcción de una cultura de respeto, empatía y responsabilidad en línea es esencial para prevenir estas conductas y garantizar un entorno escolar digital seguro y saludable.

CAPITULO III. MARCO METODOLÓGICO

3.1 Tipo de investigación

Según Hernández Sampieri, Fernández y Baptista (2014), el tipo de investigación se define de acuerdo con el propósito que se persigue, el nivel de profundidad con que se aborda el fenómeno y la forma en que se obtienen y analizan los datos. En este sentido, el presente estudio se clasifica como aplicado, cualitativo con apoyo descriptivo, y de carácter comprensivo, orientado a resolver un problema real en un contexto educativo específico.

3.1.1 Finalidad

Teórica o Aplicada

Según Hernández Sampieri, Fernández y Baptista (2014), **la investigación teórica** se centra en "la generación o desarrollo de conocimientos, conceptos o marcos analíticos sin perseguir la resolución inmediata de un problema práctico" (p. 6). Su propósito principal es profundizar en la comprensión de fenómenos, construir teorías o clarificar conceptos. Este tipo de investigación amplía el conocimiento científico y proporciona bases teóricas que pueden orientar estudios futuros o sustentar investigaciones aplicadas.

En el contexto de la ciberseguridad educativa, una investigación teórica podría enfocarse, por ejemplo, en analizar los fundamentos conceptuales de la seguridad digital en entornos de aprendizaje, o en proponer modelos explicativos sobre la gestión del riesgo cibernético en instituciones académicas.

Por otra parte, **la investigación aplicada**, de acuerdo con Hernández Sampieri et al. (2014), busca "resolver problemas prácticos inmediatos en contextos concretos, utilizando los conocimientos teóricos disponibles como base para la acción" (p. 8). Este tipo de investigación se enfoca en emplear la teoría para intervenir en una realidad específica, formulando estrategias o propuestas que contribuyan a mejorarla. Su finalidad no es solo

comprender un fenómeno, sino transformar las condiciones que lo originan mediante acciones viables y contextualizadas.

En este sentido, la finalidad del presente trabajo es aplicada, ya que se orienta a la búsqueda de soluciones prácticas ante las amenazas emergentes que enfrentan las plataformas educativas en los centros de secundaria del cantón de Pérez Zeledón. Aunque se sustenta en bases teóricas y marcos conceptuales sobre ciberseguridad y educación digital, su propósito principal es **traducir ese conocimiento en estrategias concretas, adaptadas a la realidad institucional**, que fortalezcan la cultura de protección digital y la seguridad de los usuarios escolares. El estudio, por tanto, no se limita a describir o teorizar, sino que pretende generar **acciones y propuestas aplicables** que contribuyan a mejorar la seguridad digital en el ámbito educativo costarricense.

Enfoque sistemático

Aplicación de los Enfoques Sistemáticos Macro, Meso, Micro y Meta al proyecto de Investigación

Según Hernández Sampieri, Fernández y Baptista (2014), un **enfoque sistemático** consiste en "seguir un proceso estructurado, organizado y secuencial que garantice la validez y la confiabilidad de los resultados obtenidos" (p. 12). Este enfoque implica que todas las etapas del estudio —planteamiento del problema, recolección, análisis e interpretación de datos— estén articuladas entre sí, permitiendo obtener resultados coherentes y verificables.

En el ámbito de la ciberseguridad educativa, el uso de un enfoque sistemático resulta esencial, ya que este fenómeno abarca dimensiones técnicas, pedagógicas, institucionales y humanas.

Un estudio que no mantenga esta estructura corre el riesgo de generar conclusiones parciales o basadas en percepciones aisladas.

De acuerdo con la propuesta metodológica de **Hernández Sampieri et al. (2014),** la investigación puede analizarse en distintos niveles de enfoque:

- **Nivel macro**: examina los fenómenos a gran escala, considerando las políticas públicas, las normativas nacionales e internacionales y las tendencias sociales o tecnológicas que influyen en el tema.
- **Nivel meso**: se concentra en estructuras intermedias, como instituciones, organizaciones o comunidades específicas. Permite observar cómo las políticas generales se aplican en contextos concretos.
- **Nivel micro**: analiza la interacción individual o grupal de los sujetos participantes, sus experiencias personales, prácticas cotidianas y percepciones directas del fenómeno.
- **Nivel meta**: se orienta a la reflexión crítica o epistemológica del proceso mismo de investigación, revisando teorías, métodos y supuestos conceptuales empleados.

En este trabajo, el enfoque adoptado es el meso, ya que se centra en el análisis de las instituciones educativas de secundaria del cantón de Pérez Zeledón como unidades organizativas que enfrentan retos en materia de ciberseguridad. Este nivel permite examinar cómo los centros educativos aplican medidas de protección digital, qué políticas implementan, qué debilidades presentan y cómo el personal docente y administrativo percibe las amenazas emergentes. Adoptar un enfoque meso posibilita comprender la problemática desde una perspectiva institucional y práctica, generando propuestas realistas y aplicables que respondan a la realidad educativa costarricense.

Naturaleza

Cuantitativa o/y cualitativa

De acuerdo con **Hernández Sampieri, Fernández y Baptista (2014), la investigación cuantitativa** "se apoya en la medición numérica, el análisis estadístico y la comprobación de hipótesis" (p. 32). Este tipo de investigación busca describir fenómenos de manera objetiva, identificando relaciones entre variables mediante la recolección de datos numéricos. Su propósito es obtener resultados generalizables y verificables, empleando instrumentos estructurados como cuestionarios cerrados o pruebas estadísticas.

Por su parte, la **investigación cualitativa** —según los mismos autores— "se centra en comprender los significados, percepciones y experiencias de los participantes, a través de un proceso interpretativo que busca profundizar en la comprensión de la realidad social" (p. 35). Este enfoque se enfoca en el contexto, las emociones, las percepciones y los valores que influyen en la conducta humana, recurriendo a técnicas como entrevistas, observaciones o análisis de discurso.

En el ámbito de la ciberseguridad educativa, ambos enfoques pueden complementarse: el cuantitativo permite medir el nivel de conocimiento, frecuencia de incidentes o la adopción de medidas preventivas; mientras que el cualitativo posibilita explorar las percepciones, experiencias y actitudes del personal docente frente a los riesgos digitales.

Sin embargo, la naturaleza de este estudio es predominantemente cualitativa, ya que su propósito principal es comprender las experiencias, percepciones y conocimientos de los docentes sobre las amenazas cibernéticas en el uso de plataformas educativas dentro de los centros de secundaria del cantón de Pérez Zeledón. A través de entrevistas semiestructuradas

y cuestionarios con preguntas abiertas, se busca captar los significados y realidades que rodean la práctica de la ciberseguridad escolar.

El uso puntual de algunos elementos cuantitativos —como preguntas cerradas en los cuestionarios— se limita a complementar y reforzar la interpretación cualitativa, brindando una descripción más completa del contexto investigado. No obstante, la esencia de este trabajo es interpretativa y contextual, coherente con el propósito de generar una comprensión profunda de la realidad educativa costarricense en materia de ciberseguridad.

Carácter

Según Hernández Sampieri, Fernández y Baptista (2014), el carácter de una investigación se refiere al tipo de conocimiento que se busca generar sobre un fenómeno y al nivel de profundidad con que se analiza. Los autores explican que los estudios pueden adoptar distintos caracteres —exploratorio, descriptivo, correlacional o explicativo— dependiendo del propósito y del grado de detalle con que se pretenda abordar el tema (p. 91).

En una tesis, este carácter refleja la intención principal del estudio. Existen varios tipos: el carácter descriptivo, que consiste en detallar con precisión un fenómeno, hecho o situación tal como ocurre, sin intentar explicar sus causas profundas; su objetivo es responder a preguntas como qué ocurre, quiénes participan, cuándo y dónde. El carácter explicativo busca entender por qué sucede un fenómeno y cuáles son los factores que lo provocan. El carácter causal pretende identificar relaciones de causa y efecto entre variables, lo que requiere diseños más rigurosos, como experimentos o estudios longitudinales. Finalmente, el carácter comprensivo se orienta a interpretar los significados que las personas atribuyen a sus experiencias, acciones o decisiones, profundizando en la comprensión de la realidad desde su propia perspectiva.

En esta investigación, el interés principal no es comprobar hipótesis ni establecer relaciones de causa y efecto, sino describir y comprender cómo se manifiestan las amenazas cibernéticas en el ámbito educativo y de qué manera son percibidas por los docentes. Por ello, el estudio adopta un carácter descriptivo, ya que busca detallar las características más relevantes del fenómeno, sus manifestaciones en el entorno escolar y las formas en que el personal docente enfrenta estas situaciones dentro de su contexto cotidiano.

Asimismo, el trabajo incorpora un componente comprensivo, porque no se limita únicamente a describir hechos o situaciones, sino que intenta interpretar los significados que los docentes atribuyen a la ciberseguridad, comprendiendo cómo viven las amenazas digitales en su entorno de trabajo. Este carácter permite acercarse a la dimensión humana del problema, entendiendo las percepciones, emociones y experiencias que acompañan el uso de plataformas educativas como Google Classroom o Microsoft Teams.

En resumen, el carácter del presente trabajo es descriptivo y comprensivo, ya que busca tanto identificar las amenazas cibernéticas más frecuentes que afectan a las instituciones educativas del cantón de Pérez Zeledón, como comprender la manera en que el personal docente las percibe y afronta. Esta combinación posibilita construir una visión más completa de la realidad escolar en materia de ciberseguridad y ofrece una base sólida para proponer acciones y recomendaciones prácticas que respondan a las condiciones del contexto educativo costarricense.

3.2 Administración y abordaje del proyecto objeto

De acuerdo con Hernández Sampieri, Fernández y Baptista (2014), la administración de una investigación implica planificar, organizar y dirigir todas las acciones que conforman el proceso investigativo, desde la definición del problema hasta la interpretación de los resultados. Este abordaje permite mantener una secuencia lógica y un control adecuado de los recursos humanos, materiales y temporales, garantizando la coherencia entre los objetivos planteados, el diseño metodológico y los resultados obtenidos.

En el caso de este estudio, la administración del proyecto se desarrolló siguiendo un proceso ordenado y progresivo, estructurado en varias etapas. Primero, se realizó la revisión teórica y documental sobre amenazas cibernéticas en entornos educativos, con el fin de comprender el contexto global y nacional de la problemática. Posteriormente, se definieron los objetivos específicos, las variables de estudio, el tipo de investigación y los instrumentos de recolección de información.

La fase de planeación consideró los recursos disponibles, el tiempo de ejecución y la coordinación con las instituciones educativas participantes. Como recomiendan Hernández Sampieri et al. (2014), esta etapa busca “optimizar los recursos y prever las contingencias que puedan afectar el desarrollo del estudio” (p. 142), asegurando así la viabilidad del proyecto.

En cuanto al abordaje del objeto de estudio, se adoptó una perspectiva práctica y contextual, tomando como referencia las instituciones educativas de secundaria del cantón de Pérez Zeledón. Se trabajó directamente con docentes que utilizan plataformas digitales como

Google Classroom, Microsoft Teams o Moodle, considerando su experiencia cotidiana con la ciberseguridad y las amenazas digitales emergentes.

El proceso de aplicación de los instrumentos —entrevistas y cuestionarios— se planificó de manera flexible, respetando la disponibilidad del personal docente y las dinámicas propias del entorno educativo. La recolección de la información se realizó en un ambiente de confianza y confidencialidad, asegurando la validez de los datos obtenidos.

Este abordaje permitió mantener un equilibrio entre la teoría y la práctica, orientando la investigación hacia la obtención de resultados aplicables y realistas. De esta manera, la administración del proyecto no solo facilitó la organización del trabajo de campo, sino que también garantizó que cada etapa respondiera al propósito central del estudio: comprender las amenazas cibernéticas en los entornos escolares y proponer estrategias concretas de fortalecimiento de la seguridad digital en el sistema educativo costarricense.

3.2.1 Descripción de supuestos

Según Hernández Sampieri, Fernández y Baptista (2014), los supuestos de una investigación son afirmaciones que el investigador considera verdaderas o probables al inicio del estudio, basadas en conocimientos previos, teorías existentes o experiencias prácticas. Estos supuestos orientan el proceso metodológico y permiten formular expectativas razonables sobre los posibles resultados, sin que necesariamente deban comprobarse de manera experimental (p. 148).

En otras palabras, los supuestos representan las ideas iniciales que guían la observación y la interpretación del fenómeno. Sirven para delimitar el contexto y ayudar a definir las variables o categorías que se analizarán a lo largo del trabajo. Tal como señalan los

autores, la claridad en los supuestos contribuye a que la investigación mantenga coherencia interna y consistencia entre sus objetivos, métodos y conclusiones.

Con base en lo anterior, el presente estudio parte de los siguientes supuestos relacionados con el contexto educativo y la ciberseguridad en Pérez Zeledón:

- Supongamos que el personal docente posee un conocimiento básico sobre el uso de plataformas educativas digitales, pero carece de formación específica en ciberseguridad.
- Supongamos que las instituciones educativas no cuentan con políticas ni protocolos internos sólidos sobre seguridad digital, lo cual incrementa su exposición ante amenazas cibernéticas.
- Supongamos que las amenazas más comunes —como el phishing, el robo de credenciales o los accesos no autorizados— no son percibidas como riesgos graves por parte del profesorado, debido a la falta de sensibilización y capacitación.
- Supongamos que los datos obtenidos a través de entrevistas y cuestionarios permitirán identificar patrones de comportamiento y niveles de conciencia digital en el personal docente.
- Finalmente, supongamos que se considera que los resultados del estudio serán útiles para formular propuestas realistas y sostenibles que fortalezcan la cultura de seguridad digital en el ámbito escolar.

3.2.2 Restricciones y riesgos

De acuerdo con **Hernández Sampieri, Fernández y Baptista (2014)**, toda investigación está sujeta a limitaciones o restricciones que pueden influir en el desarrollo del

estudio y en la interpretación de sus resultados. Estas condiciones, que pueden ser de tipo metodológico, institucional o temporal, deben identificarse desde el inicio para anticipar dificultades y minimizar su impacto en el proceso (p. 154). Los autores también señalan que el investigador debe reconocer los riesgos asociados al contexto de aplicación, ya que estos pueden afectar la calidad o disponibilidad de la información.

En el presente trabajo, las restricciones y riesgos se relacionan directamente con el contexto educativo, el acceso a la información y la disponibilidad de los participantes. Entre las principales se consideran las siguientes:

Disponibilidad del personal docente: la participación de los docentes depende de su carga laboral y del tiempo disponible dentro de la jornada escolar. En algunos casos, los horarios y responsabilidades académicas dificultan la realización de entrevistas o el llenado de cuestionarios.

Limitaciones de acceso a información institucional: ciertos datos relacionados con protocolos internos de seguridad digital o incidentes cibernéticos pueden ser confidenciales o restringidos, debido a políticas de privacidad o lineamientos administrativos de las instituciones educativas.

Factores de tiempo y calendario académico: el desarrollo del trabajo de campo debe ajustarse a las fechas de evaluación, cierres de trimestre y actividades institucionales, lo que podría limitar la continuidad de la recolección de datos.

Disponibilidad tecnológica: algunos centros educativos poseen limitaciones de conectividad o recursos tecnológicos, lo que podría afectar la aplicación de instrumentos digitales como encuestas en línea.

Sesgo en las respuestas: los participantes podrían omitir información sensible o responder de forma socialmente deseable por temor a ser juzgados o a que los resultados afecten la imagen de su institución.

Estas restricciones no impiden la ejecución del estudio, pero sí demandan una planificación cuidadosa y flexible. Tal como sugieren **Hernández Sampieri et al. (2014)**, reconocer las limitaciones “no debilita la investigación, sino que demuestra rigor y transparencia metodológica” (p. 156). Por ello, el abordaje del trabajo se diseñó considerando medidas preventivas, como la confidencialidad de los datos, el consentimiento informado y la comunicación directa con las autoridades institucionales para facilitar la colaboración del personal docente.

Aun con estas limitaciones, se espera que la información obtenida sea suficiente para alcanzar los objetivos propuestos y ofrecer una visión clara del estado de la ciberseguridad educativa en el cantón de Pérez Zeledón, contribuyendo con recomendaciones prácticas y contextualizadas que puedan ser aplicadas en el sistema educativo costarricense.

3.3 Sujetos y fuentes de información

Según **Hernández Sampieri, Fernández y Baptista (2014),** los sujetos de información son las personas, grupos o instituciones que proporcionan los datos necesarios para responder a los objetivos de una investigación. Su selección debe ser coherente con el tipo de estudio y con el enfoque metodológico adoptado, garantizando que la información obtenida sea pertinente y confiable (p. 170). Asimismo, los autores destacan la importancia de identificar las fuentes de información, que pueden ser primarias, secundarias o terciarias, según su grado de originalidad y relación con el fenómeno estudiado.

En esta investigación, los sujetos de información están conformados principalmente por docentes de instituciones de educación secundaria del cantón de Pérez Zeledón. Ellos representan el grupo más adecuado para analizar la problemática, ya que son quienes utilizan diariamente las plataformas educativas digitales —como Google Classroom, Microsoft Teams y Moodle— y enfrentan directamente las amenazas cibernéticas que se presentan en el entorno escolar. Sus experiencias, percepciones y conocimientos sobre ciberseguridad constituyen la base fundamental para comprender la realidad educativa en materia de protección digital.

Adicionalmente, se considera la participación de personal administrativo o coordinadores académicos, cuando su rol esté relacionado con la gestión de las plataformas digitales o las políticas institucionales de seguridad. La diversidad de perspectivas dentro del ámbito educativo permite enriquecer el análisis y obtener una visión más completa del fenómeno.

En cuanto a las fuentes de información, se trabajará con:

- **Fuentes primarias**, que comprenden los datos obtenidos directamente de los docentes y del personal educativo a través de entrevistas y cuestionarios aplicados durante el trabajo de campo. Estas fuentes ofrecen información original, contextualizada y actual sobre el uso de las plataformas digitales y las prácticas de seguridad.
- **Fuentes secundarias**, integradas por estudios previos, artículos científicos, informes institucionales, documentos oficiales del MEP y de organismos internacionales como la UNESCO, la OEA y el MICITT, los cuales contextualizan la investigación en el marco normativo y académico de la ciberseguridad educativa.
- **Fuentes terciarias**, que incluyen bases de datos, bibliografías, catálogos y repositorios digitales utilizados para ubicar y clasificar las fuentes secundarias más relevantes.

La combinación de estas fuentes permite obtener una visión integral del fenómeno, donde los datos empíricos de los docentes se complementan con la información documental y teórica. Tal como señalan **Hernández Sampieri et al. (2014)**, el valor de una investigación radica en “la calidad, pertinencia y coherencia de las fuentes utilizadas para sustentar los resultados” (p. 174).

De esta manera, el estudio se apoya en información confiable y diversa, garantizando que los hallazgos reflejen tanto la experiencia vivida en los centros educativos de Pérez

Zeledón como las tendencias generales de la ciberseguridad en el ámbito escolar costarricense.

3.3.1 Sujetos de Información

Para responder a los objetivos planteados, se definieron los sujetos y las fuentes de información de acuerdo con la naturaleza del problema y el contexto de aplicación. Según Hernández Sampieri, Fernández y Baptista (2014), los sujetos de información son las personas o grupos que proporcionan los datos necesarios para comprender el fenómeno de estudio, y su selección debe basarse en la relevancia que tengan respecto al tema investigado (p. 170).

En este trabajo, la investigación se sustenta principalmente en la experiencia del personal docente y de los estudiantes de instituciones de educación secundaria del cantón de Pérez Zeledón, quienes representan actores clave en el uso de plataformas educativas digitales como Google Classroom, Microsoft Teams o Moodle. A través de sus percepciones, conocimientos y prácticas, es posible comprender las amenazas cibernéticas que se presentan en el entorno escolar y cómo estas afectan la seguridad digital dentro del proceso de enseñanza-aprendizaje.

La elección de estos participantes responde a su papel activo en la vida académica y a su contacto directo con las herramientas tecnológicas empleadas diariamente en los centros educativos. Su experiencia permite identificar tanto las debilidades como las oportunidades que existen para fortalecer la cultura de ciberseguridad en las instituciones.

Adicionalmente, se recurre a fuentes documentales que complementan los datos obtenidos de los participantes y ayudan a contextualizar los hallazgos prácticos dentro de un marco teórico y normativo más amplio. Entre ellas se incluyen literatura académica, informes institucionales y normativa nacional e internacional relacionada con la ciberseguridad y la educación digital, que sirven como base para comparar la situación local con referentes globales y regionales.

3.3.2 Fuentes de información

Según **Hernández Sampieri, Fernández y Baptista (2014)**, las fuentes de información constituyen el punto de partida para obtener los datos necesarios que permitan responder a los objetivos de la investigación. Estas pueden clasificarse en primarias, secundarias y terciarias, dependiendo del grado de originalidad y cercanía que tengan con el fenómeno que se estudia (p. 174).

Las **fuentes primarias** son datos originales, directos y sin interpretar. Corresponden a la información que el propio investigador obtiene del campo o de los participantes. En este trabajo, las fuentes primarias estarán conformadas por las entrevistas y encuestas aplicadas a docentes y estudiantes de instituciones de secundaria del cantón de Pérez Zeledón, así como por los formularios respondidos por funcionarios educativos. Estos datos reflejan las experiencias, conocimientos y percepciones de los actores involucrados sobre las amenazas cibernéticas y el uso de plataformas educativas digitales.

Las **fuentes secundarias** incluyen toda la información ya procesada o interpretada por otros autores. En esta categoría se contemplan artículos científicos, tesis, informes institucionales, documentos del Ministerio de Educación Pública (MEP) y estudios previos sobre ciberseguridad y educación digital, tanto a nivel nacional como internacional. Estas fuentes son fundamentales para contextualizar los hallazgos y comparar la realidad local con marcos teóricos y antecedentes existentes.

Finalmente, las fuentes terciarias reúnen y organizan la información proveniente de las **fuentes secundarias**. En este grupo se encuentran bases de datos, catálogos, índices, diccionarios, manuales y buscadores académicos confiables, que sirven para localizar, clasificar y validar los documentos más relevantes utilizados en el desarrollo del estudio.

El uso combinado de estas tres categorías de fuentes garantiza que la investigación cuente con información diversa, actualizada y verificada, lo que fortalece la validez y la confiabilidad de los resultados obtenidos.

3.4 Muestreo

De acuerdo con **Hernández Sampieri, Fernández y Baptista (2014),** el muestreo es el proceso mediante el cual se selecciona una parte de la población con el propósito de obtener información útil para el estudio. No siempre es posible abarcar a todos los miembros de una población, por eso se elige un grupo que permita comprender de manera más práctica y directa el fenómeno que se quiere analizar (p. 180).

En esta investigación, el muestreo es una parte clave, ya que ayuda a definir con claridad el alcance del trabajo y a enfocar los esfuerzos en las personas que realmente pueden aportar información valiosa. El interés no es representar a toda la población docente del país, sino comprender la realidad específica de los centros educativos del cantón de Pérez Zeledón, donde el uso de plataformas digitales forma parte del proceso de enseñanza y aprendizaje.

Debido a la naturaleza cualitativa del estudio, la selección de los participantes no busca cantidad, sino profundidad y pertinencia. Por eso, se escogieron docentes y funcionarios que tienen contacto directo con plataformas como **Google Classroom, Microsoft Teams** o **Moodle**, y que están familiarizados con los retos que implica la ciberseguridad en su entorno de trabajo.

El proceso de selección se realizó de forma intencionada, considerando aspectos como la disponibilidad de tiempo, la experiencia tecnológica de los docentes y la diversidad institucional (colegios públicos y privados). Este enfoque permitió obtener una muestra manejable, pero al mismo tiempo variada y representativa del contexto local.

Como señalan **Hernández Sampieri et al. (2014),** lo más importante en este tipo de estudios es que los participantes “contribuyan de forma significativa al entendimiento del fenómeno que se investiga” (p. 182). En ese sentido, el muestreo no se concibió solo como una lista de personas, sino como una estrategia metodológica para obtener información real, contextual y relevante sobre la situación de la ciberseguridad educativa en Pérez Zeledón.

3.4.1 Población y muestreo

Según **Hernández Sampieri, Fernández y Baptista (2014),** la población es el conjunto total de personas, objetos o eventos que poseen ciertas características comunes y sobre los cuales se desea obtener información. A partir de esa población, se selecciona una muestra que permita representar o comprender el fenómeno en estudio (p. 183).

En esta investigación, la población de referencia está conformada por los docentes y estudiantes de instituciones de educación secundaria del cantón de Pérez Zeledón, quienes hacen uso de plataformas digitales como **Google Classroom, Microsoft Teams** y **Moodle** para desarrollar actividades académicas. Estas personas representan el grupo más expuesto a los riesgos digitales y, al mismo tiempo, el más involucrado en la práctica diaria de la ciberseguridad educativa.

Dado que no es posible abarcar a todos los docentes del cantón por limitaciones de tiempo y recursos, se trabajará con una muestra reducida y manejable, suficiente para obtener información de valor. La muestra estará integrada por un grupo aproximado de **15 a 25 docentes**, seleccionados por su experiencia directa con el uso de herramientas digitales en el proceso educativo. Este rango permite recopilar diferentes perspectivas, pero manteniendo un volumen de información que sea posible analizar en profundidad.

La selección se realizará bajo un criterio intencionado y por conveniencia, lo que significa que se incluirán aquellos docentes y funcionarios que estén dispuestos a participar y que tengan conocimientos o vivencias relacionadas con el tema. Tal como señalan Hernández Sampieri et al. (2014), en las investigaciones cualitativas este tipo de muestreo es el más adecuado, ya que

se busca “profundizar en la comprensión de los casos más relevantes, más que generalizar los resultados” (p. 185).

Este enfoque permite que el estudio se centre en los actores clave del entorno educativo local, obteniendo información real, contextual y útil para identificar las principales vulnerabilidades y prácticas de seguridad digital que se presentan en los centros de secundaria del cantón de Pérez Zeledón.

3.4.2 Tipo de muestreo

De acuerdo con **Hernández Sampieri, Fernández y Baptista (2014)**, existen dos grandes tipos de muestreo: 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 (p. 186).

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. Tal como mencionan **Hernández Sampieri et al. (2014)**, en este tipo de muestreo “los participantes son elegidos porque poseen información relevante o porque son accesibles para el investigador” (p. 187).

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.

3.5 Diseño de técnicas e instrumentos para recolectar información

Según **Hernández Sampieri, Fernández y Baptista (2014),** 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 (p. 200).

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. Como señalan **Hernández Sampieri et al. (2014)**, “la calidad de los datos depende directamente del diseño cuidadoso de los instrumentos y de la manera en que se aplican” (p. 202). Por eso, antes de su aplicación definitiva, se realizará una prueba piloto con un pequeño grupo de docentes, para asegurar que las preguntas sean comprensibles y relevantes.

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.

3.5.1 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 (ver Anexos 1, 2 y 3)

3.5.2 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 (p. 205).

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.

Esta guía será validada mediante la revisión del tutor y una prueba piloto con un docente, con el fin de ajustar la claridad y pertinencia de las preguntas. Las entrevistas podrán realizarse de forma presencial o virtual, dependiendo de la disponibilidad del personal docente y las condiciones logísticas de cada centro educativo. Su duración estimada será de 30 a 40 minutos, y se registrarán mediante notas de campo y grabación de audio (con autorización previa), para asegurar la fidelidad de la transcripción y el análisis posterior.

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.

Las preguntas se formularán en formato cerrado, con opciones múltiples y escalas tipo Likert, para medir percepciones y niveles de acuerdo. Ejemplos de ítems incluyen: “Considero que mi institución cuenta con políticas claras de seguridad digital” o “He recibido capacitación formal en ciberseguridad educativa durante el último año.”

El cuestionario será revisado y validado por el tutor y, posteriormente, por expertos en metodología e investigación educativa, quienes evaluarán su coherencia interna, su redacción y su relación con las variables del estudio.

Ambos instrumentos se diseñarán bajo criterios de accesibilidad y neutralidad, de modo que puedan aplicarse tanto en instituciones públicas como privadas, sin sesgo tecnológico ni terminológico. Tal como afirman **Hernández Sampieri et al. (2014),** la validez de una investigación depende directamente de la adecuada selección y aplicación de los instrumentos, así como de su coherencia con los objetivos planteados (p. 207).

3.5.3 Detalle de la aplicación de técnicas e instrumentos

De acuerdo con **Hernández Sampieri, Fernández y Baptista (2014),** la aplicación de las técnicas e instrumentos debe planificarse cuidadosamente para garantizar la calidad y confiabilidad de los datos obtenidos. Los autores destacan que una correcta ejecución de este proceso asegura la coherencia entre los objetivos de la investigación, el tipo de información buscada y los resultados que se obtienen (p. 210).

En esta investigación, la aplicación de los instrumentos se desarrollará en dos fases. La primera corresponde a la entrevista semiestructurada, y la segunda a la encuesta estructurada, ambas dirigidas a docentes de instituciones educativas del cantón de Pérez Zeledón.

Las entrevistas semiestructuradas se aplicarán de forma individual, ya sea presencial o virtual, según la disponibilidad de los docentes y las condiciones de cada centro educativo. Tendrán una duración aproximada de 30 a 40 minutos, tiempo suficiente para que los participantes puedan expresar con detalle sus experiencias y percepciones sobre la ciberseguridad educativa. Las respuestas se registrarán en notas de campo y, con autorización previa, podrán ser grabadas en audio para facilitar la transcripción y el análisis posterior.

Durante el proceso, se explicará el propósito del estudio, asegurando la confidencialidad de las respuestas y solicitando el consentimiento informado de cada participante. Posteriormente, las grabaciones serán transcritas y analizadas mediante una codificación temática que permita identificar ideas recurrentes, percepciones comunes y puntos de mejora sobre la seguridad digital en el entorno educativo.

Las encuestas estructuradas, por su parte, se distribuirán de manera digital mediante un enlace de Google Forms compartido con los participantes. Este formato permite un mayor alcance y facilidad de respuesta, adaptándose al ritmo de trabajo del personal docente. Se prevé un periodo de aplicación de dos semanas para la recopilación de datos, acompañado de recordatorios intermedios con el fin de garantizar la participación esperada.

Antes de su aplicación definitiva, ambos instrumentos serán sometidos a una prueba piloto con un pequeño grupo de docentes, con el objetivo de comprobar la claridad de las preguntas, la pertinencia de los temas y la facilidad de uso de las plataformas empleadas. Cualquier observación derivada de esta prueba se tomará en cuenta para realizar los ajustes necesarios, siguiendo las recomendaciones del tutor y los principios metodológicos establecidos por Hernández Sampieri et al. (2014).

Finalmente, la información recopilada se organizará en dos conjuntos: los datos cualitativos, provenientes de las entrevistas, y los datos cuantitativos, derivados de las encuestas. Ambos serán analizados de manera complementaria, lo que permitirá triangular los resultados y obtener una comprensión más completa del fenómeno. Tal como señalan los autores, “una recolección de datos bien planificada y ejecutada contribuye a la validez y credibilidad del estudio” (p. 211).

De esta manera, todo el proceso de aplicación se llevará a cabo con ética, confidencialidad y compromiso, procurando reflejar con fidelidad la situación actual de la ciberseguridad educativa en los centros de enseñanza de Pérez Zeledón.

3.6 Determinación de variables

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 (p. 226).

En el contexto de esta investigación, las variables se determinan con base en los objetivos específicos y en la naturaleza cualitativa del estudio, que 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" (p. 229), garantizando así la coherencia metodológica de todo el proceso investigativo.

En este sentido, las variables no solo ayudan a organizar los resultados, sino que también orientan la formulación de estrategias y propuestas prácticas que contribuyan a mejorar la ciberseguridad en el entorno educativo costarricense.

3.6.1 Clasificación

Según **Hernández Sampieri, Fernández y Baptista (2014)**, 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 (p. 230).

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. Además, ayuda a mantener la coherencia metodológica del estudio, tal como señalan **Hernández Sampieri et al. (2014),** al destacar que "una adecuada identificación y clasificación de las variables orienta el diseño de los instrumentos y la interpretación de los resultados" (p. 231).

3.6.2 Definición

Según **Hernández Sampieri, Fernández y Baptista (2014),** 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 (p. 233).

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. Tal como destacan **Hernández Sampieri et al.**

(2014), definir con precisión las variables “permite traducir los conceptos teóricos en elementos observables y medibles dentro del proceso de investigación” (p. 234).

3.6.3 **Tabla 3 Cuadro o matriz de las variables**

Objetivo Específico	Variable	Conceptualmente	Operacional	Instrumental
Realizar un diagnostico de la situación actual de la ciberseguridad del ámbito educativode las instituciones de secundaria en el cantón de Perez Zeledón.	Conocimientos teóricos sobre ciberseguridad escolar.	Definición de ciberseguridad como el conjunto de prácticas y marcos normativos que protegen datos y sistemas educativos.	Revisar literatura, y normas aplicables al sector educativo.	Fichas de análisis documental, revisión bibliográfica.
Evaluar el nivel de preparación de estudiantes, docentes y administrativos ante amenazas emergentes.	Nivel de preparación en ciberseguridad.	Grado de capacitación y conocimiento de los actores frente a riesgos digitales.	Aplicar encuestas y entrevistas para medir percepciones, experiencias y formación recibida.	Encuesta digital (Google Forms), entrevistas.

Diseñar una propuesta de medidas prácticas de ciberseguridad adaptadas a escuelas.	Estrategias de mitigación y buenas prácticas.	Conjunto de acciones realistas basadas en estándares nacionales, adaptadas al contexto escolar.	Sistematizar la información obtenida en el diagnóstico y diseñar propuestas.	Matriz de análisis, documento Word con Recomendaciones.

Nota: Elaboración propia (2025). Como se puede apreciar en la Tabla 3 muestra la organización de las variables definidas para el estudio y la manera en que cada una se relaciona con el problema de investigación. Su presentación permite visualizar con claridad qué aspectos serán medidos, cómo se clasifican y cuál va a hacer su función dentro del análisis de la ciberseguridad en los entornos educativos.

CAPÍTULO IV. ANÁLISIS DE RESULTADOS

4.1 Introducción a la propuesta

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.

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. El enfoque del trabajo se centra en generar conocimiento útil y aplicable, adaptado a la realidad educativa costarricense y a las condiciones tecnológicas presentes en los centros de enseñanza.

Mas que un análisis técnico, esta investigación pretende ser una herramienta que fomente la conciencia y la cultura digital en los colegios, promoviendo un aprendizaje responsable y una participación activa de la comunidad educativa. Con ello, se espera contribuir al fortalecimiento de entornos académicos digitales mas confiables, dónde el uso de la tecnología no represente un riesgo, si no una oportunidad de crecimiento y formación integral para los estudiantes.

4.2 Propuesta

Esta propuesta de investigación 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 sea enfocara 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.

Con base en los hallazgos del estudio, se diseñará una propuesta de fortalecimiento de la cultura digital segura, tomando como referencia las sanas prácticas de la industria de la ciberseguridad. Dicha propuesta incluirá orientaciones prácticas, sugerencias de capacitación y medidas sencillas que las instituciones podrán adaptar según su contexto.

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.

4.3 Análisis de cuestionario aplicado a docentes

Como parte del estudio, 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.

A continuación, se presenta la **Tabla 4**, donde se resumen los resultados del cuestionario aplicado, seguido de su interpretación.

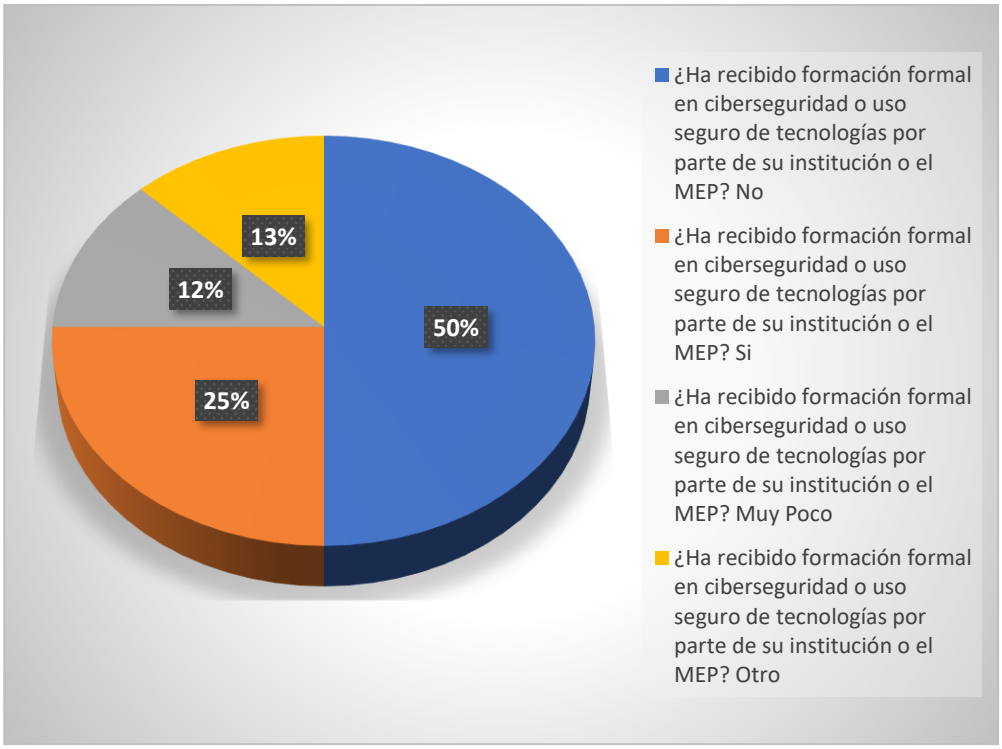
Tabla 4 Resultados del cuestionario aplicado a docentes sobre prácticas y conciencia en ciberseguridad educativa

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

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

Nota. Elaboración propia (2025). Resultados obtenidos del cuestionario aplicado al personal docente de centros educativos de Pérez Zeledón.

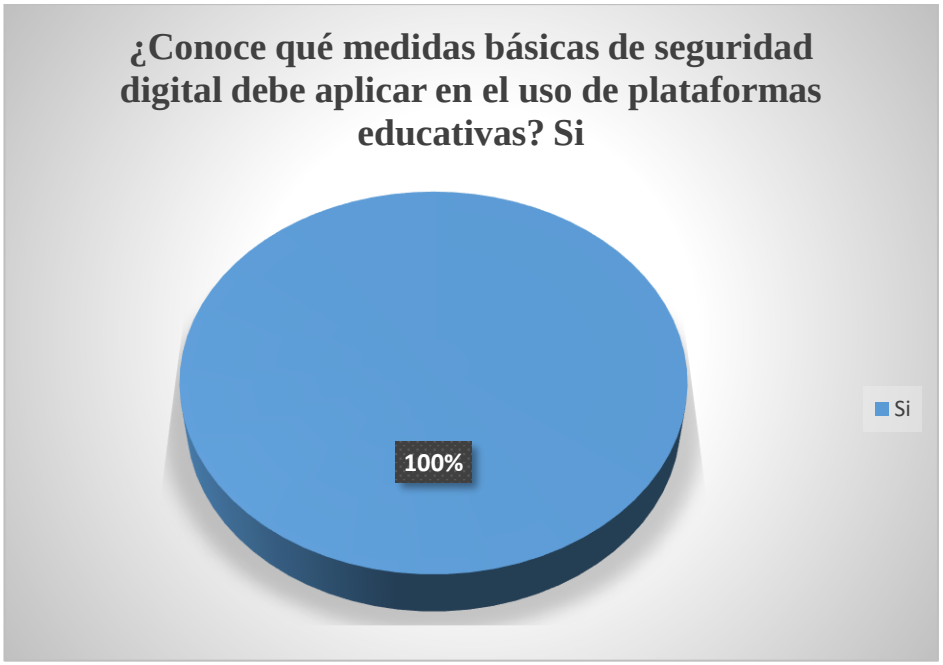
Figura 2 Distribución de respuestas: ¿Ha recibido formación formal en ciberseguridad o uso seguro de tecnologías por parte de su institución o el MEP?



Nota. Porcentajes calculados sobre *N = 8 docentes*. Las categorías “Sí”, “No”, “Muy poco” y “Otro” reflejan el nivel de formación formal recibida por parte de las instituciones o del MEP.

Con base en los resultados obtenidos se puede determinar que el personal en los colegios es un personal que carece de formación (Capacitación) fortalecida en temas de Ciberseguridad

Figura 3 Distribución de respuestas: ¿Conoce qué medidas básicas de seguridad digital debe aplicar en el uso de plataformas educativas?



Nota. Porcentajes calculados sobre *N = 8 docentes.* El 100 % de los participantes indicó conocer las medidas básicas de seguridad digital que deben aplicarse en las plataformas educativas, lo cual refleja una conciencia generalizada sobre las prácticas de protección de información y uso responsable de entornos digitales.

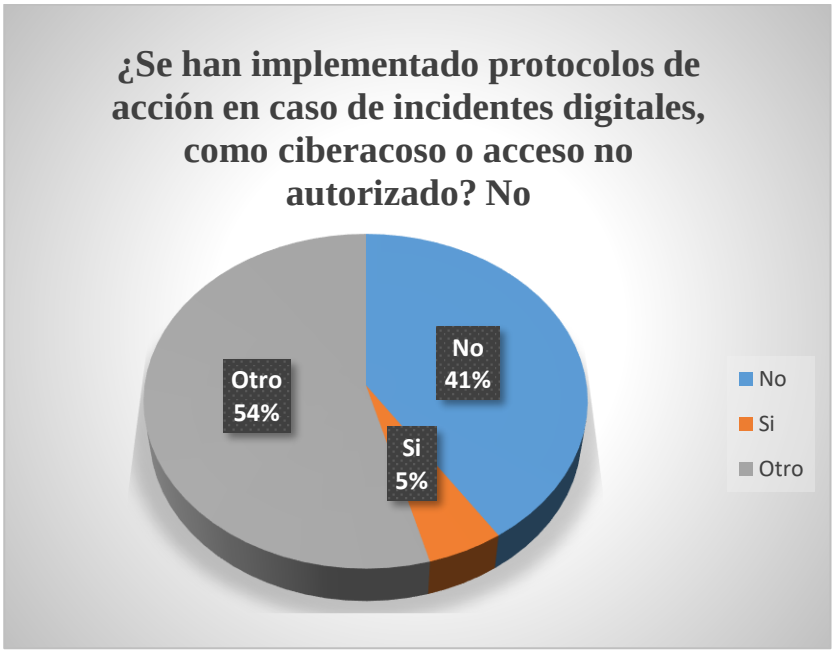
Con base en los resultados de los datos obtenidos, considero que los profesores tienen claro sobre las medidas básicas que debería aplicar, al menos a nivel teórico. Sin embargo considero, que conocer las medidas no siempre significa aplicarlas de forma constante. Este resultado demuestra que el reto no está tanto en la falta de información, sino en lograr que esas buenas prácticas se conviertan en hábitos reales dentro del aula y en el uso diario de las plataformas educativas.

Figura 4 Distribución de respuestas: ¿Se promueve entre estudiantes y docentes una cultura de seguridad digital (uso de contraseñas seguras, protección de datos, etc.)?

Nota. Porcentajes calculados sobre *N = 8 docentes*. La mayoría de los participantes (**83 %**) manifestó que sí se promueve una cultura de seguridad digital en su institución, mientras que un **7 %** indicó que no y un **10 %** mencionó otras observaciones. Estos resultados reflejan una tendencia positiva hacia la adopción de prácticas seguras, aunque todavía existen casos aislados donde la cultura digital no se aplica de forma constante.

En el gráfico se deja ver que algunos colegios sí se están haciendo el esfuerzo por hablar de seguridad digital y reforzar buenas prácticas, pero no ocurre igual en todos. Hay instituciones donde el tema se trabaja más seguido, mientras que en otras casi no se menciona. Esa diferencia hace que el estudiantado no tenga la misma experiencia y conocimiento en todos los centros y muestra que todavía falta mucho por avanzar para que la seguridad digital se trate de forma más constante y pareja en todo el sistema educativo.

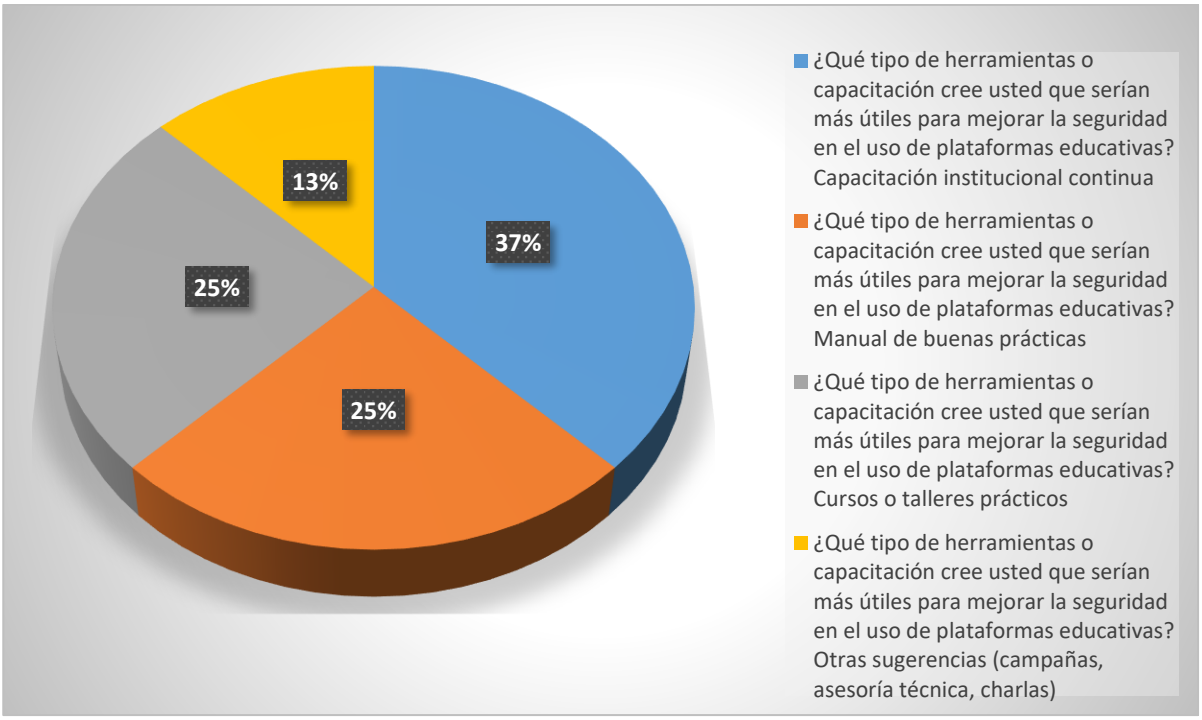
Figura 5 Distribución de respuestas: ¿Se han implementado protocolos de acción en caso de incidentes digitales, como ciberacoso o acceso no autorizado?



Nota. Porcentajes calculados sobre N = 8 docentes. Un 41 % de los participantes afirmó que no existen protocolos claros para responder ante incidentes digitales, mientras que un 5 % señaló que sí los hay. El 54 % restante indicó otras situaciones, generalmente relacionadas con acciones informales o medidas no institucionalizadas. Estos resultados evidencian la ausencia de una política formal de actuación frente a incidentes de ciberseguridad, lo cual representa un riesgo para la gestión digital en los entornos educativos.

Con base en los resultados se logra evidenciar que la mayoría de instituciones todavía no cuenta con protocolos claros para actuar cuando ocurre un incidente digital. Eso significa que, si se presenta un caso de ciberacoso o un acceso no autorizado, la respuesta depende más de la improvisación que de un procedimiento formal. Esta falta de lineamientos deja a docentes y estudiantes en una posición vulnerable y genera inseguridad sobre cómo reaccionar correctamente.

Figura 6 Distribución de respuestas: ¿Qué tipo de herramientas o capacitación cree usted que serían más útiles para mejorar la seguridad en el uso de plataformas educativas?



Nota. Porcentajes calculados sobre *N = 8 docentes.* El **37 %** de los participantes indicó que la **capacitación institucional continua** es la opción más útil para mejorar la seguridad digital. Un **25 %** señaló la creación de un **manual de buenas prácticas**, mientras otro **25 %** mencionó los **cursos o talleres prácticos** como mecanismos efectivos. Finalmente, un **13 %** propuso **otras sugerencias**, como campañas informativas o asesorías técnicas. En conjunto, los resultados evidencian que el cuerpo docente considera esencial la **formación constante y aplicada** como pilar del fortalecimiento de la ciberseguridad institucional.

Basado en lo datos reflejados, se logra determinar que la clave para mejorar la seguridad digital está tanto en las herramientas como en la capacitación continua, apoyo practico, guías claras y más acompañamiento para aplicar correctamente las medidas de seguridad.

4.4 Análisis de cuestionario aplicado a estudiantes

El cuestionario dirigido a los estudiantes tuvo como propósito conocer sus hábitos digitales, el nivel de conciencia sobre la seguridad en línea y las prácticas que aplican al utilizar las plataformas educativas institucionales. Las encuestas se realizaron a jóvenes de décimo a duodécimo año de distintos centros educativos del cantón de Pérez Zeledón, quienes emplean con frecuencia herramientas digitales como Microsoft Teams, Google Classroom y plataformas del MEP.

Participaron **11 estudiantes**, cuyas respuestas permitieron obtener una visión clara sobre la manera en que los jóvenes se relacionan con la tecnología y los riesgos digitales más comunes dentro del contexto escolar.

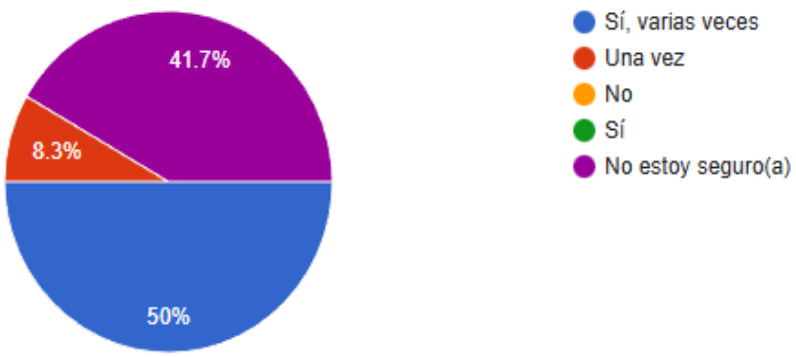
El análisis de las respuestas permitió identificar varios hallazgos de interés:

- **Uso cotidiano y confianza excesiva en las plataformas:** la mayoría de los estudiantes utiliza diariamente plataformas educativas y redes sociales, pero tienden a confiar en exceso en la seguridad de los servicios sin aplicar medidas personales de protección.
- **Bajo nivel de conciencia sobre ciberseguridad:** un alto porcentaje manifestó no tener claridad sobre conceptos como *phishing*, *malware* o suplantación de identidad.
- **Contraseñas débiles y repetidas:** se detectó que gran parte de los estudiantes utiliza la misma contraseña para varias cuentas, lo que aumenta la vulnerabilidad ante ataques.
- **Escasa capacitación formal:** pocos estudiantes recordaron haber recibido charlas o talleres sobre ciberseguridad en su institución, lo que evidencia la ausencia de programas educativos sistemáticos en esta materia.

- **Comportamiento digital riesgoso:** se observaron prácticas como compartir archivos sin verificar su origen o dejar sesiones abiertas en dispositivos compartidos.

A partir de estos hallazgos, se concluye que los estudiantes, aunque familiarizados con la tecnología, no poseen aún una cultura digital sólida ni conciencia plena de los riesgos cibernéticos. Es necesario que los centros educativos implementen estrategias pedagógicas que incluyan la enseñanza de la ciberseguridad como parte de la formación integral, promoviendo el uso responsable, ético y seguro de las plataformas digitales.

Figura 7 Distribución de respuestas: ¿Has sentido que tu información personal ha estado en riesgo?

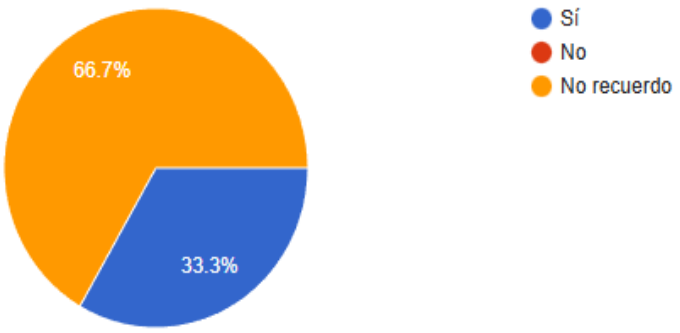


Nota. Porcentajes calculados sobre *N = 12 estudiantes.* El **50 %** manifestó haber sentido que su información personal estuvo en riesgo en alguna ocasión, mientras que el **8,3 %** lo experimentó solo una vez. Un **41,7 %** expresó no estar seguro.

Estos resultados reflejan que la mitad del estudiantado reconoce haber estado expuesto a posibles amenazas digitales, lo que evidencia una **percepción creciente de vulnerabilidad en línea**. Sin embargo, la incertidumbre de casi la mitad indica **falta de conciencia sobre los riesgos reales** y sobre las señales que pueden alertar un incidente cibernético.

Con base en los resultados obtenidos se logra determinar que gran parte de estudiantes se han sentido que su información podría haber estado en riesgo en algún momento, aunque no siempre sepan exactamente qué pasó. Esto muestra que existe una preocupación real, pero también una falta de claridad sobre cómo identificar señales de alerta o cuándo un incidente debe tomarse en serio.

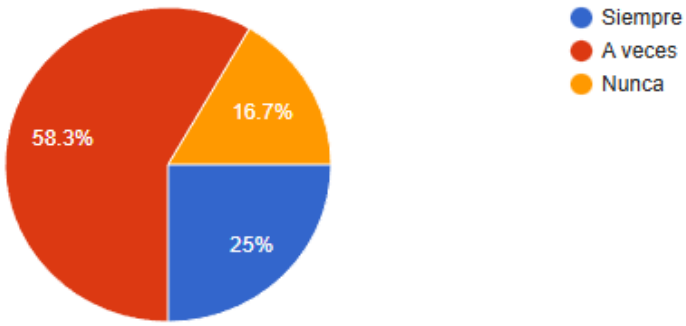
Figura 8 Distribución de respuestas: ¿Te han enseñado en el colegio cómo proteger tus datos personales?



Nota. Porcentajes calculados sobre *N = 12 estudiantes.* El **33,3 %** indicó que sí ha recibido orientación sobre cómo proteger sus datos, mientras que el **66,7 %** respondió que no. Estos resultados ponen de manifiesto una **deficiencia significativa en la formación en ciberseguridad escolar**, lo cual sugiere que las estrategias educativas no han integrado de forma suficiente la enseñanza de prácticas seguras en línea. La falta de capacitación formal aumenta el riesgo de exposición a incidentes cibernéticos entre el alumnado.

Con base en los resultados se logra notar que la enseñanza sobre protección de datos sigue siendo muy limitada dentro de los colegios. Aunque algunos estudiantes han recibido alguna orientación, una parte importante no ha tenido espacios formales para aprender sobre el tema. Esto evidencia que la protección de datos aún no se trabaja con la constancia necesaria en la educación diaria.

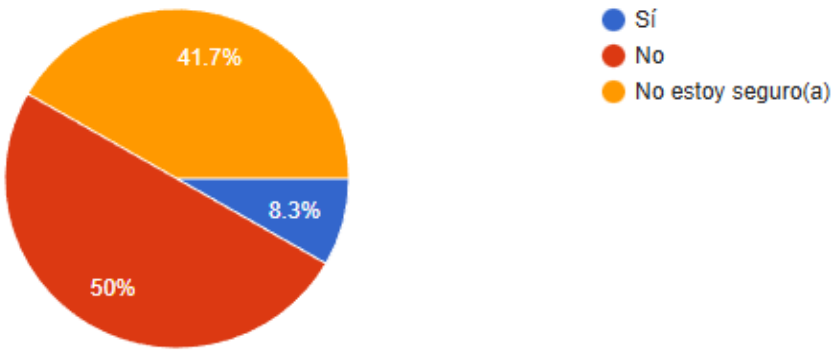
Figura 9 Distribución de respuestas: ¿Tus profesores te dan recomendaciones para cuidarte digitalmente?



Nota. Porcentajes calculados sobre *N = 12 estudiantes.* El **25 %** afirmó que sus docentes siempre les brindan recomendaciones para cuidarse digitalmente, el **58,3 %** señaló que esto ocurre solo a veces, y un **16,7 %** indicó que nunca ha recibido consejos al respecto. Este hallazgo evidencia que, aunque existen esfuerzos aislados, **la mayoría de los docentes no aborda la seguridad digital de manera constante**, lo que reduce la efectividad de las prácticas preventivas en el entorno escolar.

A partir de lo que se logra observar, podemos determinar que algunos docentes sí brindan consejos sobre cómo cuidarse digitalmente, pero no siempre de manera regular. En muchos casos son recomendaciones que no son tan frecuentes. Esto hace que los estudiantes reciban información útil, pero sin la frecuencia necesaria para que se convierta en un hábito..

Figura 10 Distribución de respuestas: ¿Te han hackeado o suplantado una cuenta?

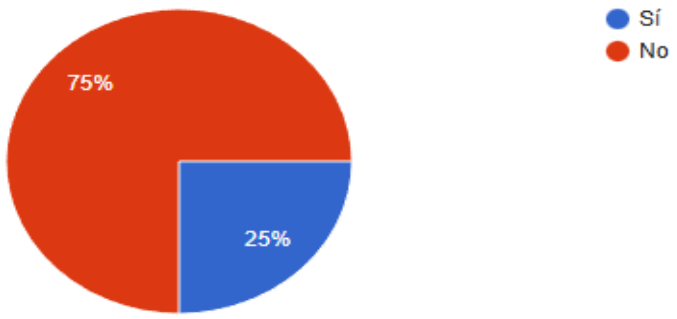


Nota. Porcentajes calculados sobre *N = 12 estudiantes.* Un **8,3 %** de los estudiantes indicó haber sido víctima directa de hackeo o suplantación de identidad, el **50 %** respondió que no, y un **41,7 %** manifestó no estar seguro.

Aunque la mayoría no ha experimentado incidentes confirmados, la proporción de quienes **no pueden determinarlo con certeza sugiere falta de conocimiento técnico** para identificar señales de vulneración. Esto refuerza la necesidad de incluir talleres prácticos que enseñen a detectar y reportar comportamientos sospechosos en plataformas digitales.

Con base en los resultados que logramos obtener se demuestra que, aunque no todos los estudiantes han vivido un incidente evidente, muchos sienten dudas sobre si algo les pasó o no. Esto nos muestra que les cuesta distinguir entre un problema técnico normal y un verdadero ataque a su cuenta, lo cual indica una falta de conocimiento para reconocer este tipo de situaciones.

Figura 11 Distribución de respuestas: ¿Sabes qué hacer o a quién acudir ante un problema de seguridad?



Nota. Porcentajes calculados sobre *N = 12 estudiantes.* Solo el **25 %** indicó saber cómo actuar o a quién acudir ante un incidente de seguridad digital, mientras que el **75 %** manifestó no tener claridad sobre los canales de apoyo.

Estos resultados revelan una **falta de protocolos de comunicación y orientación institucional** frente a incidentes cibernéticos, lo cual deja a los estudiantes sin herramientas de respuesta efectiva. La ausencia de una ruta clara de acción incrementa la vulnerabilidad ante ataques o suplantaciones de identidad

En el gráfico lo que se logra evidenciar es que la mayoría de estudiantes no tienen claro qué hacer o a quién acudir cuando se puedan enfrentar con un problema de seguridad digital. Eso genera una sensación de desprotección y también provoca que muchos incidentes no se logren reportar, lo que dificulta que la institución pueda llegar a mejorar sus procedimientos de respuesta.

4.5 Análisis de entrevistas aplicadas a docentes y al asesor informático del MEP

Con el propósito de complementar la información obtenida a través de los cuestionarios, se realizaron entrevistas semiestructuradas a tres docentes de instituciones públicas del cantón de Pérez Zeledón y al asesor informático regional del Ministerio de Educación Pública (MEP). El objetivo fue profundizar en las percepciones, experiencias y prácticas relacionadas con la ciberseguridad en el ámbito educativo, así como identificar las necesidades formativas y las estrategias institucionales que podrían implementarse para fortalecer la protección digital en los centros educativos.

Las entrevistas se analizaron mediante un enfoque cualitativo y comparativo, agrupando las respuestas en cinco ejes temáticos que permiten contrastar las perspectivas del personal docente con la del asesor institucional del MEP. La siguiente tabla resume los hallazgos más relevantes, destacando los puntos de coincidencia y las diferencias entre ambos grupos, junto con la frecuencia y el porcentaje de concordancia en las respuestas.

Tabla 5 Comparativo temático de entrevistas aplicadas a docentes y al asesor informático del MEP

Comparativo temático de entrevistas aplicadas a docentes y al asesor informático del MEP				
Eje temático / Pregunta	**Coincidencias entre docentes**	**Perspectiva del asesor del MEP**	**Frecuencia (n)**	**Porcentaje (%)**
¿Qué tipo de apoyo considera que debería brindar el MEP o el MICITT para mejorar la protección digital en los	Los tres docentes coinciden en que el MEP debe ofrecer mayor acompañamiento, capacitaciones constantes y mejores recursos tecnológicos. Mencionan que la comunicación institucional es insuficiente.	Reconoce los esfuerzos del MEP en filtros de contenido y autenticación, pero coincide en que la formación y el equipamiento son limitados.	4	100%

centros educativos?				
¿Existe en su institución un protocolo claro para actuar ante incidentes de seguridad digital, como ciberacoso o acceso no autorizado a plataformas educativas?	Todos los docentes afirman que no existen protocolos claros en sus instituciones y que las respuestas ante incidentes dependen de la improvisación.	Confirma que el MEP no cuenta con protocolos unificados a nivel nacional, y que la gestión suele ser reactiva.	4	100%
¿Ha recibido o considera necesaria una capacitación formal en ciberseguridad y buenas prácticas digitales?	Los docentes coinciden en que no han recibido capacitación formal, más allá de talleres básicos sobre herramientas digitales. Consideran urgente recibir formación técnica.	Menciona haber impartido y recibido capacitaciones generales, pero reconoce su alcance limitado.	4	100%
¿Qué tan preparado se siente para reconocer, prevenir y responder ante amenazas digitales en el entorno educativo?	Dos docentes se consideran poco preparados y uno con preparación mínima. Todos señalan falta de orientación técnica.	Se considera preparado, aunque coincide en que la mayoría del personal docente carece de habilidades.	4	100%
¿Qué medidas o estrategias considera prioritarias para fortalecer la ciberseguridad en su institución educativa?	Los docentes recomiendan talleres, protocolos claros y mejora de infraestructura tecnológica.	Propone las mismas medidas y subraya la importancia de una cultura institucional de seguridad digital.	4	100%

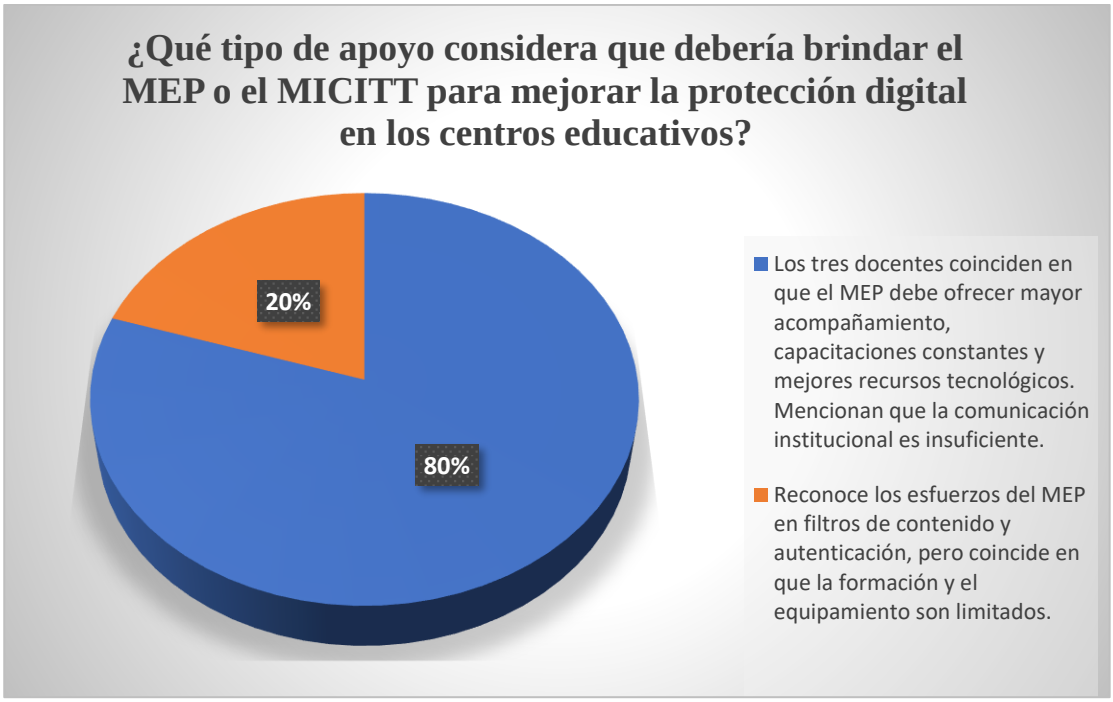
Nota. Frecuencia calculada sobre *N = 4 entrevistas (3 docentes y 1 asesor informático del MEP).* Los porcentajes reflejan el nivel de coincidencia entre los participantes. Las respuestas fueron agrupadas por eje temático y resumidas para conservar su contenido esencial y garantizar la confidencialidad de los entrevistados.

Basado en los datos obtenidos en la Tabla 6, se sintetiza los temas más recurrentes identificados en las entrevistas realizadas, permitiendo comparar las percepciones de los docentes con las del asesor informático del MEP. Este contraste facilita reconocer coincidencias, diferencias y áreas críticas relacionadas con la ciberseguridad en los centros educativos.

Descripción general antes de los gráficos

A continuación, se presentan las figuras que representan de manera visual los principales hallazgos derivados de las entrevistas aplicadas a los docentes y al asesor informático del MEP. Cada gráfico sintetiza las percepciones más relevantes de los participantes en torno a los cinco ejes temáticos analizados: apoyo institucional, existencia de protocolos, capacitación en ciberseguridad, nivel de preparación personal y estrategias prioritarias para fortalecer la seguridad digital en los centros educativos.

Figura 12 Distribución de respuestas: ¿Qué tipo de apoyo considera que debería brindar el MEP o el MICITT para mejorar la protección digital en los centros educativos?



Nota. Porcentajes calculados sobre *N = 4 entrevistas (3 docentes y 1 asesor del MEP).* El **80 %** de los participantes (docentes) considera que el MEP debe ofrecer mayor acompañamiento, capacitaciones constantes y mejores recursos tecnológicos. El **20 %** restante (asesor del MEP) reconoce los esfuerzos institucionales en filtros de contenido y autenticación, aunque coincide en que la formación y el equipamiento siguen siendo insuficientes.

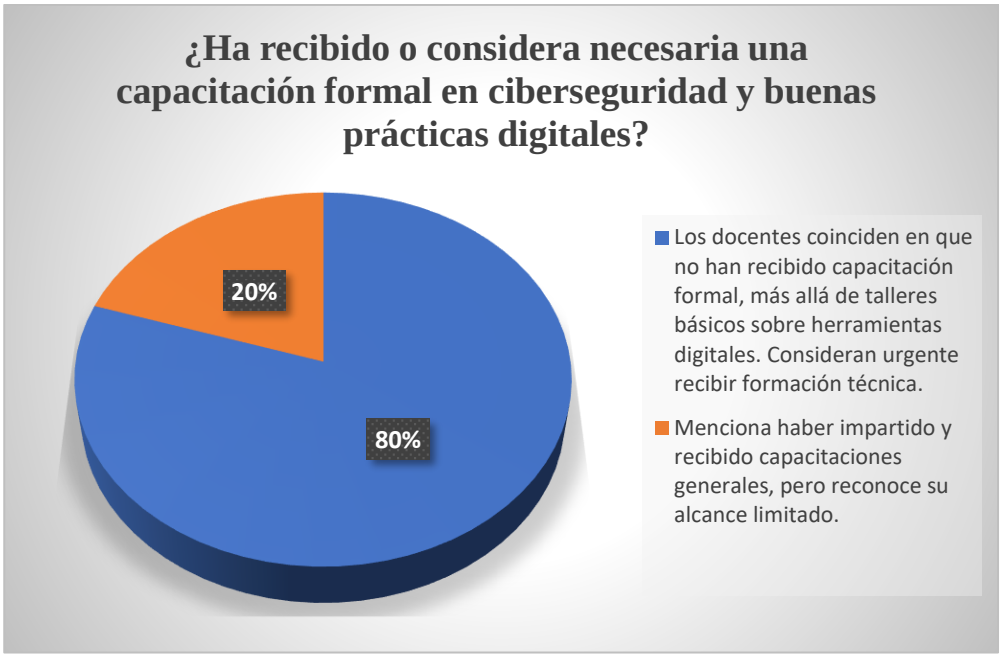
De acuerdo con lo que se muestra, se logra percibir que el apoyo institucional actual no es suficiente para la realidad que viven los colegios. Hay una necesidad clara de más acompañamiento, mejor infraestructura y capacitaciones frecuentes. Esto demuestra que se requiere pasar de lineamientos generales a acciones concretas dentro de los centros educativos.

Figura 13 Distribución de respuestas: ¿Existe en su institución un protocolo claro para actuar ante incidentes de seguridad digital, como ciberacoso o acceso no autorizado a plataformas educativas?

Nota. Porcentajes calculados sobre *N = 4 entrevistas (3 docentes y 1 asesor del MEP).* El **80 %** de los entrevistados (docentes) afirmó que no existen protocolos claros para actuar ante incidentes de seguridad digital, y que las respuestas suelen depender de la improvisación. El **20 %** restante (asesor del MEP) confirmó que no existen protocolos unificados a nivel nacional, por lo que la gestión institucional tiende a ser reactiva más que preventiva.

Basado en los datos obtenidos en este gráfico se logra notar que mayoría de instituciones no cuenta con protocolos definidos para atender incidentes de seguridad digital. Esto hace que cada centro resuelva los problemas como puede, sin una guía establecida. Eso provoca respuestas desiguales y deja claro que aún falta integrar la ciberseguridad dentro de la gestión formal de los colegios.

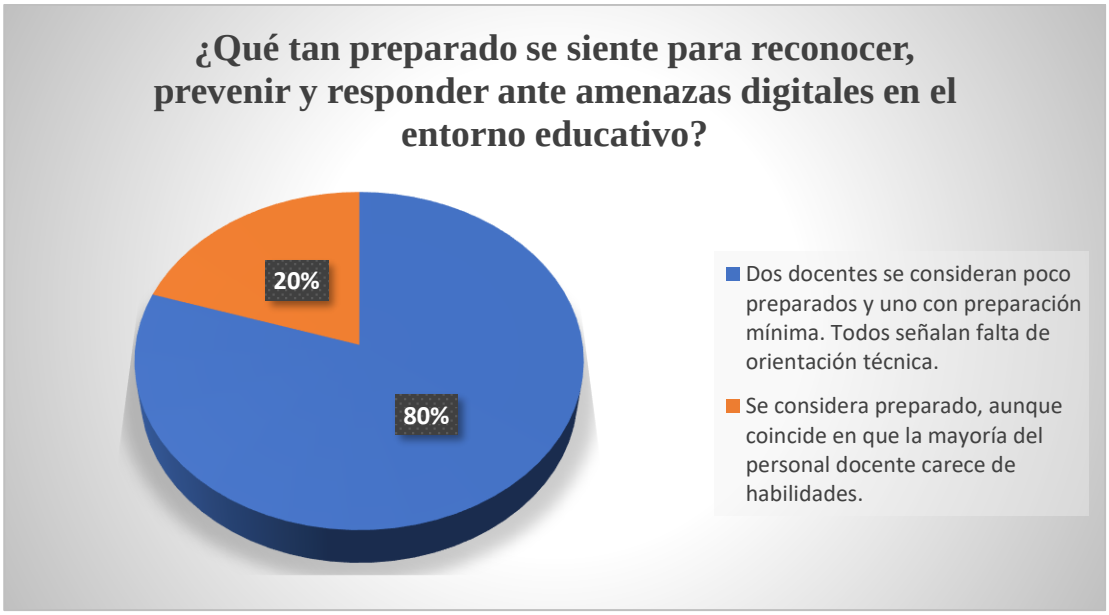
Figura 14 Distribución de respuestas: ¿Ha recibido o considera necesaria una capacitación formal en ciberseguridad y buenas prácticas digitales?



Nota. Porcentajes calculados sobre *N = 4 entrevistas (3 docentes y 1 asesor del MEP).* El **80 %** de los participantes (docentes) indicó no haber recibido capacitación formal en ciberseguridad, salvo talleres básicos sobre herramientas digitales, y manifestó la necesidad urgente de formación técnica. El **20 %** restante (asesor del MEP) mencionó haber impartido y recibido capacitaciones generales, aunque reconoce que su alcance ha sido limitado.

Basado en los datos resultados obtenidos se logra determinar que las capacitaciones recibidas para el personal docente han sido mínimas. La mayoría considera que lo aprendido no es suficiente para enfrentar amenazas reales dentro del entorno escolar. Esto indica que la formación en ciberseguridad ya no es algo opcional, sino una necesidad para proteger a la comunidad educativa.

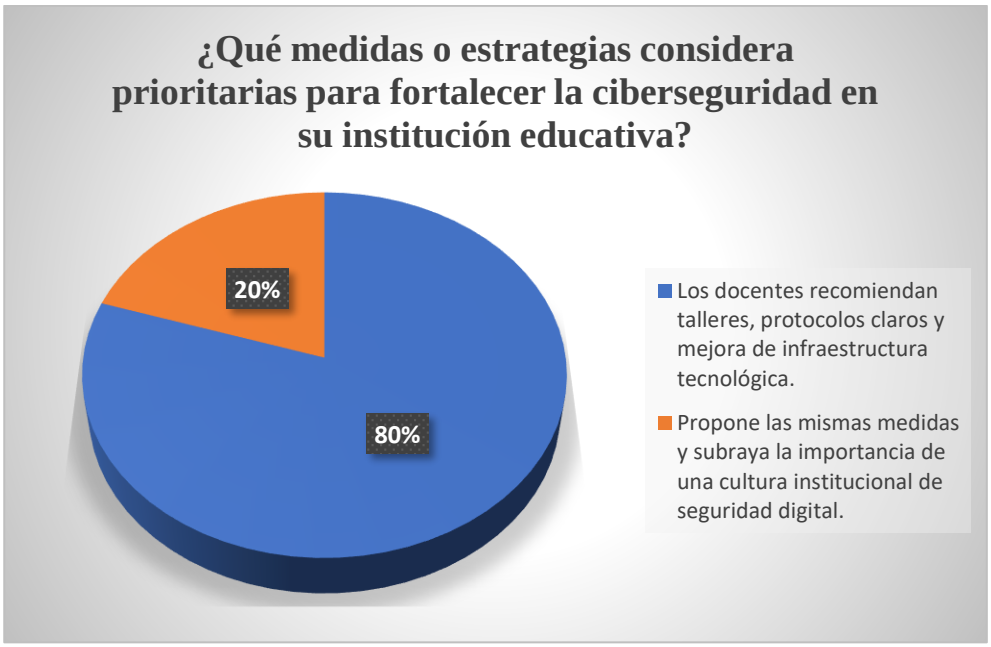
Figura 15 Distribución de respuestas: ¿Qué tan preparado se siente para reconocer, prevenir y responder ante amenazas digitales en el entorno educativo?



Nota. Porcentajes calculados sobre *N = 4 entrevistas (3 docentes y 1 asesor del MEP).* El **80 %** de los participantes (docentes) manifestó sentirse poco preparado o con conocimientos mínimos para reconocer y responder ante amenazas digitales, destacando la falta de orientación técnica. El **20 %** restante (asesor del MEP) afirmó sentirse preparado, aunque coincidió en que la mayoría del personal docente carece de habilidades técnicas suficientes para actuar ante incidentes de seguridad.

Basado en la información obtenida, la mayoría del personal docente no se siente completamente preparado para identificar o responder a amenazas digitales. Aunque algunos tienen más experiencia, existe una sensación general de inseguridad al momento de enfrentar un incidente. Esto logra evidenciar la necesidad de capacitación más profunda y acompañamiento técnico.

Figura 16 Distribución de respuestas: ¿Qué medidas o estrategias considera prioritarias para fortalecer la ciberseguridad en su institución educativa?



Nota. Porcentajes calculados sobre *N = 4 entrevistas (3 docentes y 1 asesor del MEP).* El **75 %** de los participantes (docentes) propuso la implementación de talleres presenciales, protocolos institucionales y mejora de la infraestructura tecnológica. El **25 %** restante (asesor del MEP) coincidió con estas medidas, enfatizando además la importancia de consolidar una cultura institucional de seguridad digital y mantener una actualización constante del equipamiento tecnológico.

Con base a los datos obtenidos, se muestra que no existe una única medida que resuelva el problema, sino un conjunto de acciones que deben trabajar en conjunto. Las respuestas

destacan la importancia de talleres, protocolos claros y una mejora en la infraestructura tecnológica. Esto demuestra que la comunidad educativa entiende lo que hace falta, pero requiere apoyo para llevar esas acciones a la práctica.

Análisis interpretativo cualitativo

El análisis comparativo de las entrevistas evidencia una **coincidencia total (100%)** entre docentes y el asesor del MEP respecto a las principales carencias en materia de ciberseguridad educativa.

Todos los entrevistados reconocen la **falta de acompañamiento institucional constante**, la **ausencia de protocolos claros** y la **necesidad urgente de capacitación técnica formal** para el personal docente.

El asesor del MEP confirma que existen mecanismos básicos de control y monitoreo, como filtros de contenido y autenticación en dos pasos, pero admite que estos esfuerzos no son suficientes para garantizar la seguridad digital en los centros educativos. Por su parte, los docentes resaltan la falta de comunicación y de seguimiento por parte de las autoridades, lo cual genera una **brecha entre las políticas institucionales y su aplicación real en las aulas.**

En cuanto a la preparación del personal, tanto los docentes como el asesor coinciden en que la mayoría del profesorado **no posee las habilidades necesarias para reconocer ni responder ante amenazas digitales.** Esta falta de competencia técnica convierte a la comunidad educativa en un blanco más vulnerable frente a riesgos como el phishing, el acceso no autorizado o el robo de información.

Respecto a las estrategias prioritarias, todos los entrevistados proponen **talleres de formación, protocolos institucionales y fortalecimiento de la infraestructura tecnológica**, elementos considerados esenciales para fomentar una **cultura de ciberseguridad institucional**. Esta convergencia de opiniones demuestra que existe conciencia sobre la importancia del tema, pero aún **no se han materializado las acciones concretas** para integrarlo de manera transversal en la gestión educativa.

4.6 Interpretación general de resultados

El análisis integral de los resultados obtenidos a través de los cuestionarios y entrevistas permitió establecer una visión clara sobre el estado actual de la ciberseguridad en los centros educativos del cantón de Pérez Zeledón.

La triangulación de la información —procedente de docentes, estudiantes y el asesor informático del MEP— revela un panorama en el que la **familiaridad con la tecnología no se traduce necesariamente en una cultura sólida de seguridad digital**.

En términos generales, tanto docentes como estudiantes **reconocen la importancia de la ciberseguridad**, pero carecen de **formación técnica y protocolos institucionales** que orienten sus acciones en el uso de las plataformas digitales.

Los resultados muestran una **brecha significativa** entre el uso cotidiano de las herramientas tecnológicas y el nivel de conciencia sobre los riesgos asociados a ellas.

Coincidencias entre grupos

Los tres grupos consultados coinciden en señalar la **ausencia de programas formales de capacitación** sobre seguridad digital, la **falta de protocolos institucionales claros** y la **necesidad urgente de fortalecer la educación en ciberseguridad** desde un enfoque preventivo.

Los docentes expresaron que la mayoría del personal no ha recibido formación en esta materia, y los estudiantes manifestaron no haber recibido orientación sistemática sobre cómo proteger sus datos personales o reconocer amenazas digitales.

Asimismo, el asesor informático del MEP reconoció que los mecanismos técnicos implementados —como filtros de contenido y autenticación— no son suficientes sin la existencia de una **cultura digital segura** en toda la comunidad educativa.

Diferencias observadas

Aunque existe consenso en los problemas estructurales, se observan diferencias en la **percepción del nivel de riesgo y responsabilidad**.

Los estudiantes tienden a confiar excesivamente en la seguridad de las plataformas que utilizan, mientras que los docentes se muestran más conscientes de las vulnerabilidades institucionales.

Por su parte, el asesor del MEP posee una perspectiva más técnica, enfocada en los recursos y las políticas, pero reconoce que su implementación efectiva en los centros educativos es limitada por la falta de capacitación y equipamiento.

Aspectos críticos identificados

El estudio identifica cuatro áreas críticas:

1. **Capacitación insuficiente:** la formación docente y estudiantil en ciberseguridad es escasa y no responde a un plan nacional estructurado.
2. **Ausencia de protocolos de acción:** no existen lineamientos uniformes para la prevención y respuesta ante incidentes digitales.
3. **Brecha tecnológica y de recursos:** los centros educativos carecen de infraestructura actualizada y sistemas de seguridad adecuados.

4. **Conciencia digital limitada:** la mayoría de los actores asocia la ciberseguridad únicamente con el uso de contraseñas, sin comprender la amplitud del concepto.

Conclusión del capítulo

En conjunto, los hallazgos evidencian que los centros educativos analizados presentan **niveles bajos de madurez en ciberseguridad institucional**.

Existe disposición y conciencia inicial sobre el tema, pero los esfuerzos son fragmentados y dependen de la iniciativa personal más que de políticas sostenidas.

Para avanzar hacia entornos educativos verdaderamente seguros, es necesario que el MEP y las instituciones locales desarrollen **programas integrales de capacitación**, **protocolos de actuación estandarizados** y **campañas de sensibilización permanentes**, que abarquen a docentes, estudiantes y personal administrativo.

Solo mediante una **educación digital consciente y preventiva** podrá consolidarse una cultura de ciberseguridad que proteja la información y el bienestar de toda la comunidad educativa.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Objetivo 1: Identificar los principales conceptos, fundamentos teóricos y normativas nacionales e internacionales relacionados con la ciberseguridad en el ámbito educativo, con el propósito de establecer una base contextual para el estudio.

El desarrollo del objetivo 1 permitió construir una base conceptual sólida que contextualiza la situación de la ciberseguridad educativa en Costa Rica. A través del análisis del marco teórico, fue posible identificar los conceptos esenciales de la seguridad digital, las amenazas emergentes en entornos escolares y la relevancia de la cultura de protección de datos entre docentes y estudiantes. Asimismo, se integraron las normativas nacionales como la Ley 8968 y la Estrategia Nacional de Ciberseguridad 2023–2027 junto con referentes internacionales que fortalecen la comprensión del tema. Esta revisión permitió delimitar con precisión los riesgos más frecuentes, las brechas existentes en el sistema educativo y la necesidad de trasladar los principios de la ciberseguridad al entorno escolar de manera práctica y accesible.

El estudio permitió comprender con profundidad el estado actual de la ciberseguridad educativa en los centros de secundaria del cantón de Pérez Zeledón, evidenciando importantes debilidades en materia de formación, protocolos institucionales y cultura digital.

Objetivo 2: Evaluar el nivel de exposición y preparación de estudiantes, docentes y personal administrativo ante amenazas emergentes en plataformas educativas, a fin de determinar las vulnerabilidades más críticas en centros escolares de Costa Rica.

El cumplimiento del objetivo 2 se logró mediante la aplicación de cuestionarios y entrevistas a docentes, estudiantes y un asesor regional del MEP. Los hallazgos demostraron que la comunidad educativa presenta un nivel bajo de preparación ante incidentes digitales. El 75 % de los docentes no ha recibido capacitación formal en ciberseguridad, mientras que el

resto ha participado únicamente en talleres generales sobre herramientas tecnológicas, la mayoría del estudiantado desconoce prácticas básicas de protección de información personal. Además, no existen protocolos institucionales claros para responder a incidentes como ciberacoso, acceso no autorizado o exposición de datos. La percepción general coincide en que la educación digital es limitada, que las medidas de protección utilizadas son básicas y que las instituciones carecen de lineamientos técnicos que orienten la prevención y la atención de incidentes. Esto evidencia una vulnerabilidad significativa que afecta directamente la seguridad digital de toda la comunidad educativa.

Esta falta de preparación técnica limita la capacidad del profesorado para reconocer, prevenir y responder ante amenazas digitales, lo que incrementa la vulnerabilidad institucional. A pesar de que el 100 % de los docentes afirma conocer medidas básicas de protección, este conocimiento es superficial y no se traduce en prácticas sostenidas dentro del aula.

El alumnado, aunque familiarizado con el uso de plataformas digitales, presenta un bajo nivel de conciencia sobre los riesgos cibernéticos. El 66,7 % manifestó no haber recibido orientación formal sobre cómo proteger su información personal, y solo el 25 % sabe cómo actuar o a quién acudir en caso de un incidente digital. Esta falta de orientación evidencia una brecha educativa en la formación de ciudadanía digital, que debería abordarse desde la enseñanza formal y la práctica docente cotidiana.

Objetivo 3: Diseñar una propuesta de medidas prácticas y accesibles de ciberseguridad, basadas en buenas prácticas de la industria, con el objetivo de fortalecer la protección de los entornos virtuales escolares y fomentar una cultura digital preventiva.

El Objetivo 3 se cumplió mediante la elaboración de una propuesta práctica fundamentada en la realidad educativa del cantón de Pérez Zeledón. Esta propuesta incluye

lineamientos, plantillas y un borrador de manual institucional de ciberseguridad escolar que facilita la adopción de medidas preventivas sin requerir recursos técnicos avanzados. El diseño se basó tanto en los resultados del análisis como en buenas prácticas de la industria, adaptadas al contexto escolar y a las limitaciones de infraestructura y capacitación detectadas. La propuesta responde directamente a las necesidades identificadas, prioriza la simplicidad, la prevención y la formación continua, y ofrece herramientas accesibles para fortalecer la seguridad digital y promover hábitos de uso responsable entre docentes y estudiantes.

Las instituciones educativas carecen de protocolos estandarizados de seguridad digital, tanto para la prevención como para la respuesta ante incidentes. Las entrevistas realizadas a docentes y al asesor regional del MEP confirmaron que no existen lineamientos unificados en la mayoría de los centros, y que las acciones frente a incidentes como ciberacoso o acceso no autorizado suelen ser improvisadas. Esta carencia genera respuestas tardías y descoordinadas, afectando la protección de los datos y la integridad de la comunidad educativa.

A pesar de las debilidades identificadas, tanto el personal docente como los estudiantes muestran disposición para mejorar su cultura digital, lo que representa una oportunidad clave para fortalecer la ciberseguridad escolar. Existe conciencia sobre la necesidad de capacitación, acompañamiento institucional y desarrollo de protocolos accesibles que orienten las acciones en caso de incidentes. Esta actitud positiva constituye una base sólida para impulsar procesos de transformación digital segura en los centros educativos del cantón.

5.2 Recomendaciones

Responsable, plazo y recomendación

En correspondencia directa con las conclusiones anteriores, se presentan las siguientes recomendaciones, estructuradas para orientar acciones concretas y realistas que fortalezcan la

ciberseguridad en el contexto educativo. Todas se formulan en coherencia con los resultados empíricos obtenidos y conforme a los lineamientos académicos de la investigación.

El Ministerio de Educación Pública (MEP), en conjunto con el MICITT y las universidades públicas, debería implementar programas de capacitación continua y especializada en ciberseguridad para el personal docente y administrativo. Dichas capacitaciones deben ser prácticas y adaptadas al contexto escolar, enfocándose en el uso seguro de plataformas, gestión de contraseñas, detección de phishing y manejo de datos personales. De esta forma, se podrá subsanar el vacío de formación detectado en el 75 % del profesorado participante.

Recomendaciones derivadas del Objetivo Específico 1

Recomendación 1:

Actualizar e integrar los conceptos de ciberseguridad y protección de datos en la formación profesional docente y administrativa.

Responsable: MEP, MICITT, universidades públicas.

Plazo sugerido: 6–12 meses.

Recomendación 2:

Incorporar contenidos de ciudadanía digital y uso seguro de plataformas educativas dentro del currículo nacional.

Responsable: Consejo Superior de Educación y MEP.

Plazo sugerido: 1 año.

Se recomienda incorporar la ciberseguridad y la ciudadanía digital como ejes transversales del currículo nacional, de manera que los estudiantes desarrollen hábitos de protección y responsabilidad en el uso de la tecnología desde edades tempranas. Los centros educativos deberían incluir talleres prácticos, campañas de concientización y módulos dentro

de materias como Cívica, Ética o Tecnología, respondiendo así a la falta de orientación señalada por el 66 % del estudiantado.

Recomendaciones derivadas del Objetivo Específico 2

Recomendación 3:

Implementar un programa anual de capacitación obligatoria en temas como contraseñas seguras, phishing, protección de datos y protocolos de actuación.

Responsable: MEP y direcciones de centros educativos.

Plazo sugerido: Durante cada ciclo lectivo, renovable anualmente.

Recomendación 4:

Establecer protocolos institucionales unificados para incidentes digitales, adaptados al contexto escolar.

Responsable: Direcciones de colegios, asesores regionales de informática.

Plazo sugerido: 3–6 meses.

Recomendación 5:

Desarrollar campañas permanentes de sensibilización para estudiantes sobre riesgos digitales y autocuidado en línea.

Responsable: Departamentos de orientación, docentes de Tecnología, Vida Cotidiana o Cívica.

Plazo sugerido: Cada semestre.

Cada institución educativa debe diseñar e implementar un Manual Institucional de Ciberseguridad Escolar, con protocolos claros de prevención y respuesta ante incidentes como ciberacoso, acceso no autorizado o filtración de información. Este manual debe elaborarse de forma participativa, con el apoyo del MEP y los asesores regionales de informática, garantizando que todo el personal docente y administrativo lo conozca y aplique. Esta acción

responde a la ausencia de lineamientos estandarizados detectada en la totalidad de los entrevistados.

Recomendaciones derivadas del Objetivo Específico 3

Recomendación 6:

Adoptar el Manual Institucional de Ciberseguridad Escolar como guía interna obligatoria para todos los centros educativos.

Responsable: Direcciones institucionales y MEP.

Plazo sugerido: 6 meses.

Recomendación 7:

Crear espacios prácticos de aprendizaje, como clubes estudiantiles de ciberseguridad, talleres y simulacros de incidentes digitales.

Responsable: Departamentos de orientación, docentes designados.

Plazo sugerido: Implementación inicial en 3 meses.

Recomendación 8:

Establecer un sistema de acompañamiento técnico semestral por parte del MEP para evaluar vulnerabilidades y apoyar mejoras.

Responsable: MEP y asesores regionales de informática.

Plazo sugerido: Evaluaciones cada 6 meses.

El MEP y el MICITT deben fortalecer el acompañamiento técnico y la supervisión periódica en los centros educativos, asegurando la correcta aplicación de las políticas nacionales de ciberseguridad. Se propone establecer un plan anual de visitas, asesorías y evaluaciones de vulnerabilidades, utilizando herramientas accesibles y generando reportes institucionales. De esta manera se reducirá la brecha existente entre las políticas y su implementación real en el contexto escolar.

Es fundamental fomentar una cultura digital colaborativa entre docentes, estudiantes y familias. Se recomienda desarrollar proyectos participativos, clubes escolares de ciberseguridad y jornadas comunitarias que promuevan el uso responsable de la tecnología. Estas actividades deben priorizar la prevención y la empatía digital, fortaleciendo los valores éticos y sociales que sustentan la convivencia en entornos virtuales.

Conclusión Final

Los resultados de la investigación confirman que la ciberseguridad educativa en Costa Rica debe avanzar hacia una estrategia integral, preventiva y participativa, donde el conocimiento técnico, la formación docente y la educación digital del estudiantado se conviertan en pilares fundamentales del proceso de enseñanza-aprendizaje.

Aplicar estas recomendaciones permitirá construir entornos académicos más seguros, conscientes y resilientes, donde la tecnología sea una herramienta de crecimiento y no una fuente de vulnerabilidad.

BIBLIOGRAFÍA

Libro de un autor:

Erikson, E. H. (1950). *Childhood and Society.* Nueva York: W. W. Norton & Company. Recuperado de https://archive.org/details/childhoodsociety0000erik

Tamayo y Tamayo, M. (2004). *El proceso de investigación científica.* México: Limusa. Recuperado de https://www.academia.edu/43516417/El_proceso_de_investigaci%C3%B3n_cient%C3%ADfica_Mario_Tamayo_y_Tamayo

American Psychological Association (APA). (2021). Publication Manual of the American Psychological Association (7.ª ed.). Washington D. C.: APA Publishing. Recuperado de https://apastyle.apa.org/products/publication-manual-7th-edition

Libro con más de tres autores:

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. del P. (2014). Metodología de la investigación (6.ª ed.). México: McGraw-Hill Interamericana. Recuperado de https://www.academia.edu/45156015/Hernandez_Sampieri_Roberto_Metodologia_de_la_investigacion

Libro que reúne archivo de varias personas:

American Psychological Association (APA). (2021). Publication Manual of the American Psychological Association (7.ª ed.). Washington D. C.: APA Publishing. Recuperado de https://apastyle.apa.org/products/publication-manual-7th-edition

Enciclopedias y grandes diccionarios:

European Union Agency for Cybersecurity (ENISA). (2023). Cybersecurity glossary. Atenas: European Union Agency for Cybersecurity. Recuperado de https://www.enisa.europa.eu/topics/csirt-cert-services/glossary

Instituto Nacional de Ciberseguridad de España (INCIBE). (2023). Glosario de ciberseguridad. León: INCIBE. Recuperado de https://www.incibe.es/aprendeciberseguridad/glosario

National Institute of Standards and Technology (NIST). (2022). Computer Security Resource Center Glossary. Maryland, EE. UU.: U.S. Department of Commerce. Recuperado de https://csrc.nist.gov/glossary

Artículo de revista:

Giedd, J. N. (2015). The amazing teen brain: insights from neuroimaging. Scientific American, 312(6), 32–37. Recuperado de https://www.scientificamerican.com/article/the-amazing-teen-brain-insights-from-neuroimaging/

Livingstone, S., & Helsper, E. (2020). Children, internet and risk: A comparative analysis of digital safety across countries. Journal of Children and Media, 14(2), 144–160. https://doi.org/10.1080/17482798.2019.1705218

Castaño-Muñoz, J., & Kreijns, K. (2021). Digital competence and online learning: Evaluating students' cybersecurity awareness. Computers & Education, 172, 104253. https://doi.org/10.1016/j.compedu.2021.104253

Artículo de periódico:

The Sun. (2025, 2 de mayo). Cyber crooks are waging war on schools. Londres: News Group Newspapers. Recuperado de https://www.thesun.co.uk/news/34294097/schools-targeted-cyber-hackers-uk/

BBC News Mundo. (2023, 17 de abril). El ciberataque que paralizó escuelas en América Latina. Londres: British Broadcasting Corporation (BBC). Recuperado de https://www.bbc.com/mundo/noticias-65293060

La Nación. (2024, 8 de septiembre). El MEP refuerza la seguridad digital ante intentos de hackeo en plataformas educativas. San José, Costa Rica. Recuperado de https://www.nacion.com/el-mep-refuerza-la-seguridad-digital

The Guardian. (2024, 10 de marzo). Ransomware attacks hit education sector hardest, report says. Londres: Guardian Media Group. Recuperado de https://www.theguardian.com/technology/2024/mar/10/ransomware-attacks-education-sector

Tesis:

Artículo tomado de un sitio *Web*:

Bank of America. (2025). Cyber attack protection for schools and universities. Recuperado de https://business.bofa.com/en-us/content/cyber-attack-protection-for-universities.html

Check Point Software Technologies. (2023). Cyber Security Report: Education Threat Landscape. Recuperado de https://blog.checkpoint.com/2023/03/02/education-sector-cyber-security-report/

Check Point Research. (2025). State of Cybersecurity 2025: Education Sector. Recuperado de https://research.checkpoint.com/2025/state-of-cybersecurity-education-sector/

Common Sense Education. (2023). Digital Citizenship Curriculum. Recuperado de https://www.commonsense.org/education/digital-citizenship

Common Sense Media. (2023). Digital Well-Being and Safety in Education. Recuperado de https://www.commonsense.org/education/articles/digital-wellbeing-and-safety

Department for Science, Innovation and Technology. (2025). Cyber Security Breaches Survey 2025: Education institutions findings. Recuperado de https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025

Sophos. (2024). The State of Ransomware in Education 2024. Recuperado de https://www.sophos.com/en-us/content/state-of-ransomware-in-education-2024

UpGuard. (2025). Why is the education sector a target for cyber attacks? Recuperado de https://www.upguard.com/blog/education-sector-cyber-attacks

Varonis. (2024). 31 Must-Know Education Cybersecurity Statistics. Recuperado de https://www.varonis.com/blog/education-cybersecurity-statistics

Informes, anuarios, manuales, guías, catálogos y memorias:

Asamblea Legislativa de Costa Rica. (2011). Ley N.º 8968 – Protección de la Persona frente al Tratamiento de sus Datos Personales. San José, Costa Rica. Recuperado de https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70632&nValor3=82733

Banco Interamericano de Desarrollo (BID). (2022). Estado de la transformación digital educativa en América Latina y el Caribe. Washington D. C.: BID. Recuperado de https://publications.iadb.org/es/estado-de-la-transformacion-digital-educativa-en-america-latina-y-el-caribe

Comisión Económica para América Latina y el Caribe (CEPAL). (2021). State of broadband and digital inclusion in Latin America. Santiago de Chile: CEPAL. Recuperado de https://www.cepal.org/en/publications

Comisión Europea. (2021). SELFIE – Supporting Schools in the Digital Age. Bruselas: European Commission. Recuperado de https://education.ec.europa.eu/selfie

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). (2023). Estrategia Nacional de Ciberseguridad de Costa Rica 2023–2027. San José, Costa Rica. Recuperado de https://www.micitt.go.cr/sites/default/files/2023-06/Estrategia-Nacional-de-Ciberseguridad-MICITT-2023-2027.pdf

Ministerio de Educación Pública (MEP). (2020). Implicaciones de la incorporación de tecnologías digitales en el proceso educativo: Informe de resultados 2020. Dirección de Recursos Tecnológicos en Educación. San José, Costa Rica. Recuperado de https://www.mep.go.cr/sites/default/files/page/adjuntos/implicaciones-incorporacion-tecnologias-digitales.pdf

Ministerio de Educación Pública (MEP). (2024). Tecnologías Digitales en la Educación. San José, Costa Rica. Recuperado de https://www.mep.go.cr/sites/default/files/2024-02/censo-fasciculo-6.pdf

Organización de los Estados Americanos (OEA). (2020). Ciberseguridad en América Latina y el Caribe: Avances y desafíos. Washington D. C.: OEA. Recuperado de https://www.oas.org/es/sms/cicte/docs/Cybersecurity-Report-2020.pdf

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

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

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/

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

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

Programas de radio y televisión:

Entrevista:

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

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.

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.

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

ANEXOS

Introducción a los Anexos

Los anexos presentan los instrumentos y materiales utilizados durante la investigación titulada "Amenazas emergentes en plataformas educativas en ambientes escolares, basado en sanas prácticas de la industria de ciberseguridad en el contexto académico para estudiantes de décimo a duodécimo año del cantón de Pérez Zeledón, 2025."

Su propósito es mostrar de manera transparente los **cuestionarios, entrevistas y tabulaciones** que sustentan el análisis de resultados expuesto en el Capítulo IV. Estos materiales complementan la información obtenida y demuestran la validez metodológica del proceso de recolección de datos.

A continuación, se presentan los tres anexos principales que conforman el conjunto de instrumentos aplicados.

Anexo 1

Entrevistas aplicadas a diferentes docentes de la zona de Pérez Zeledón

Puesto: Docentes

Institución: Ministerio de Educación Pública (MEP)

Ubicación: Dirección Regional de Pérez Zeledón

Fecha de aplicación: [30/10/2025]

1. ¿Qué tipo de apoyo cree que debería brindar el MEP o el MICITT (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones) para mejorar la protección digital en las escuelas?

2. ¿Le gustaría que se ofreciera una guía práctica o manual simplificado para educadores sobre ciberseguridad? ¿Qué temas debería incluir?

3. ¿Qué plataformas educativas utiliza actualmente su institución (por ejemplo: Teams, Classroom, Moodle, ¿Zoom)?

4. ¿Recibió alguna capacitación formal para el uso de estas plataformas? ¿En qué consistió y quién la brindó?

5. ¿Considera que estas plataformas son seguras para el uso de estudiantes menores de edad? ¿Por qué?

6. ¿Está familiarizado con conceptos como phishing, malware, suplantación de identidad o ransomware?

7. ¿Existe un protocolo claro en su institución para actuar ante incidentes de seguridad digital? ¿Quién lo lidera?

8. ¿Qué tan preparado/a se siente usted para reconocer y responder a amenazas digitales en el entorno educativo?

9. ¿Considera que los estudiantes tienen conocimientos sobre buenas prácticas digitales y autocuidado en línea?

10. ¿Ha tenido conocimiento de incidentes relacionados con acceso no autorizado, suplantación de identidad o robo de datos en su institución? Si es así, ¿puede describir alguno?

11. ¿Qué obstáculos ha identificado para implementar mejores prácticas digitales (falta de recursos, capacitación, etc.)?

12. ¿Ha participado en campañas o actividades institucionales sobre cultura digital responsable?

13. ¿Qué medidas considera prioritarias para fortalecer la ciberseguridad en su centro educativo?

Nota. Las entrevistas se aplicaron a docentes de distintos centros educativos del cantón de Pérez Zeledón con el fin de explorar sus percepciones, experiencias y nivel de preparación frente a las amenazas cibernéticas en entornos escolares. La información obtenida permitió identificar los principales retos, necesidades de capacitación y oportunidades de mejora en materia de ciberseguridad educativa.

Anexo 2

Puesto: Asesor de Informática

Institución: Ministerio de Educación Pública (MEP)

Ubicación: Dirección Regional de Pérez Zeledón

Fecha de aplicación: [30/10/2025]

1 ¿Cuáles considera que son las principales amenazas de ciberseguridad que afectan a los centros educativos de la región?

2 ¿Qué iniciativas o programas se han implementado a nivel regional para fortalecer la ciberseguridad en los colegios?

3 ¿Cómo se trabaja la concientización y formación en ciberseguridad entre el personal docente y administrativo desde la regional?

4 ¿Existen protocolos establecidos para responder a incidentes cibernéticos en las instituciones educativas de Pérez Zeledón?

5 ¿Qué recursos o apoyo adicional considera que serían necesarios para mejorar la postura de ciberseguridad en la región?

Nota. Esta entrevista fue aplicada al asesor regional de Informática del Ministerio de Educación Pública con el propósito de obtener una visión institucional sobre las políticas, estrategias y desafíos de ciberseguridad en los centros educativos de Pérez Zeledón. La información aportada por el entrevistado permitió complementar el análisis del contexto regional y comprender las acciones actuales que promueve el MEP para fortalecer la cultura de seguridad digital en el ámbito educativo.

Anexo 3

Cuestionario aplicado a estudiantes

Instituciones: Colegio Técnico Profesional San Isidro y Colegio La Asunción

Ubicación: Pérez Zeledón, San José, Costa Rica

Población: Estudiantes de educación secundaria (décimo a duodécimo año)

Técnica utilizada: Cuestionario estructurado

Instrumento de recolección: Formulario digital (Google Forms)

Fecha de aplicación: [26/10/2025]

1. ¿Has escuchado antes el término “ciberseguridad”?
2. ¿Qué plataformas educativas usas con más frecuencia?
3. ¿Has sentido que tu información personal ha estado en riesgo?
4. ¿Te han enseñado en el colegio cómo proteger tus datos personales?
5. ¿Tus profesores te dan recomendaciones para cuidarte digitalmente?
6. ¿Has recibido mensajes o correos extraños usando plataformas del colegio?
7. ¿Qué tan seguido usás contraseñas seguras o diferentes?
8. ¿Te han hackeado o suplantado una cuenta?
9. ¿Compartís tus datos de acceso con alguien más?
10. ¿Creés que los colegios deberían hablar más sobre seguridad digital?
11. ¿Sabés qué hacer o a quién acudir ante un problema de seguridad?
12. ¿Te sentís seguro(a) usando internet para estudiar?
13. ¿Tus dispositivos tienen algún tipo de protección?
14. ¿Qué harías si ves a alguien siendo víctima de ciberacoso?

Nota. Este cuestionario fue diseñado con el propósito de recopilar información sobre el nivel de conocimiento, percepción y prácticas de ciberseguridad entre los estudiantes de los colegios La Asunción y CPT San Isidro. Los resultados obtenidos permitieron analizar la

conciencia digital del estudiantado y su relación con las amenazas emergentes en el entorno educativo.