Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), enero-febrero 2026,
Volumen 10, Número 1.

https://doi.org/10.37811/cl_rcm.v10i1

CONCIENCIA Y PRÁCTICAS EN CIBERSEGURIDAD EN BACHILLERATO: ANÁLISIS TEMÁTICO PARA INTERVENCIONES EDUCATIVAS

CYBERSECURITY AWARENESS AND PRACTICES IN BACCALAUREATE: THEMATIC ANALYSIS FOR EDUCATIONAL INTERVENTIONS

Verónica Garcés Rodríguez
Instituto Universitario de las Américas y el Caribe

Soraya Concepción Elizondo Jimenez
Facultad de Ciencias Químicas, San Nicolás de los Garza

DOI: https://doi.org/10.37811/cl_rcm.v10i1.22706

Conciencia y Prácticas en Ciberseguridad en Bachillerato: Análisis Temático para Intervenciones Educativas

Verónica Garcés Rodríguez[1]
vgarces@unac.edu.mx
https://orcid.org/0009-0009-3617-3257
Instituto Universitario de las Américas y el Caribe, San Pablo, Colima

Soraya Concepción Elizondo Jimenez
soraya.elizondojm@uanl.edu.mx
https://orcid.org/0009-0009-9488-4575
Facultad de Ciencias Químicas, San Nicolás de los Garza, Nuevo León

RESUMEN

La ciberseguridad es un tema cada vez más relevante en el ámbito educativo, especialmente en el nivel medio superior, donde los estudiantes interactúan constantemente con entornos digitales. El objetivo de esta investigación fue analizar el nivel de conciencia y las prácticas de ciberseguridad de alumnos de bachillerato para identificar áreas clave de intervención. Se aplicó un cuestionario con escala Likert, estructurado en dominios temáticos, a fin de evaluar hábitos, conocimientos y actitudes relacionados con la seguridad digital. Los resultados evidencian un conocimiento básico sobre ciberseguridad, pero también una falta de prácticas sólidas y conscientes en el uso de plataformas digitales. Entre los hallazgos más relevantes, destaca la necesidad urgente de fortalecer la difusión y formación en temas como protección de datos personales y gestión de contraseñas. Se concluye que es fundamental implementar estrategias educativas específicas que fomenten una cultura de ciberseguridad entre los estudiantes y contribuyan a su bienestar digital.

Palabras clave: ciberseguridad, plataformas digitales, seguridad digital, conciencia digital

[1] Autor principal
Correspondencia: vgarces@unac.edu.mx

Cybersecurity Awareness and Practices in Baccalaureate: Thematic Analysis for Educational Interventions

ABSTRACT

Cybersecurity has become an increasingly relevant topic in education, especially at the high school level, where students frequently interact with digital environments. This study aimed to analyze the level of awareness and cybersecurity practices among high school students to identify key areas for intervention. A Likert-scale questionnaire, structured by thematic domains, was applied to assess students' habits, knowledge, and attitudes related to digital security. The results show a basic understanding of cybersecurity but a lack of strong and conscious practices in the use of digital platforms. One of the most significant findings is the urgent need to strengthen awareness and training on topics such as personal data protection and password management. The study concludes that it is essential to implement targeted educational strategies that promote a culture of cybersecurity among students and contribute to their digital well-being.

Keywords: cybersecurity, digital platforms, digital security, digital awareness

Artículo recibido 15 enero 2026

Aceptado para publicación: 19 febrero 2026

INTRODUCCIÓN

Hoy en día la ciberseguridad se ha convertido en una necesidad transversal en diversos sectores, especialmente en el educativo. El uso constante de plataformas digitales por parte de los estudiantes de bachillerato conlleva riesgos que, en muchas ocasiones, no son reconocidos ni gestionados adecuadamente.

Esta situación muestra la necesidad de formar ciudadanos digitales que sean capaces de proteger su información y actuar con responsabilidad en entornos virtuales, ya sea en el uso de las plataformas digitales de la institución educativa y/o las aplicaciones para elaboración de tareas donde comúnmente se utilizan cuentas personales de Google.

Esta situación se acentúa con el creciente número de incidentes que están relacionados con el robo de identidad, ciberacoso, exposición de datos y el phishing, los cuales, afectan directamente a los jóvenes que aún no cuentan con una formación especializada. En 2024, el panorama de la ciberseguridad se ha visto influenciado por tendencias emergentes con el incremento de ataques mediante ransomware, el uso de Telegram por parte de ciberdelincuentes y la consolidación del malware as a service como modelo accesible par atacantes. (CIBERLATAM, 2025)

Los adolescentes, particularmente en el primer semestre de bachillerato, representan un grupo clave para la intervención educativa en ciberseguridad, dado que al transitar de la secundaria a la preparatoria intensifican el uso de tecnologías sin haber recibido una formación sólida en materia de protección de datos, privacidad y comportamiento seguro en línea. El fortalecimiento de la ciberseguridad no solo se logra mediante la adquisición de conocimiento teórico, sino a través del desarrollo de una conciencia práctica que permita a los usuarios navegar con precaución, esto incluye la capacidad de discernir información, mantener interacciones seguras y principalmente conocer los riesgos disfrazados de oportunidades en línea. (TUTASEC, 2023)

El presente estudio se sustenta en dos ejes teóricos principales que son el desarrollo de habilidades digitales y la cultura de la ciberseguridad. El desarrollo de habilidades digitales implica adquirir conocimientos, destrezas y actitudes que facilitan el uso responsable y eficiente de las tecnologías y la red. (Morduchowicz, 2021) Sin embargo, estas habilidades no solo incluyen aspectos técnicos, sino

también la capacidad de tomar decisiones informadas, protegiendo la identidad digital y comprender los riesgos del entorno en línea.

Asimismo, fomentar una cultura de ciberseguridad implica comprender que la protección digital no se limita únicamente al uso de las herramientas tecnológicas, sino que también requiere el conocimiento de políticas, la aplicación de buenas prácticas y una formación continua que permita adaptarse a las amenazas en constante evolución. El propósito principal de la ciberseguridad es resguardar los sistemas de información, dispositivos, aplicaciones, datos y a las personas frente a amenazas como el software malicioso, el phishing y el robo de información. (Lindemulder & Kosinski, 2024)

Aunque los adolescentes son un grupo especialmente vulnerable ante el fraude en línea, muy pocos deciden actuar ante la situación. Solo tres de cada diez jóvenes que han sido estafados informan lo sucedido a las autoridades, mientras que, casi la mitad de los adultos entre 35 y 45 años sí lo hacen. Esta diferencia evidencia una menor conciencia del riesgo o una falta de orientación entre los más jóvenes. De hecho, únicamente una cuarta parte de los adolescentes de 15 a 17 años afirma conocer los riesgos del fraude digital y haber tomado precauciones. En el caso de los adultos, esta proporción casi se duplica. (AMRO, 2024)

Los datos anteriormente mencionados, evidencian una realidad realmente preocupante ya que, aunque los adolescentes sean usuarios activos del entorno digital, no siempre están preparados para enfrentar los riesgos. La baja tasa de denuncia y la limitada percepción del peligro reflejan claramente una falta de formación y acompañamiento que los deja expuestos a engaños en línea.

En España, la Policía Nacional ha usado su cuenta de TikTok para alertar a los usuarios sobre un tipo de estafa que ocurre en repetidas ocasiones, el cual, indica que los delincuentes intentan hacerse pasar por el hijo (a) de la víctima para ganarse su confianza y así pedirle dinero. Aunque, este engaño no es nuevo, todavía está muy presente, por eso piden que la gente no caiga en la trampa. Este fraude no solo se realiza por medio de WhatsApp, sino también por corre electrónico o llamadas, los estafadores suelen hacerse pasar por empleados de bancos, técnicos de soporte, autoridades y normalmente usan lenguaje técnico, hablan alterados para simular que es algo urgente y así las personas puedan confiar y lograr su objetivo. (Malagón, 2025)

Dese un punto de vista formativo, esta investigación surge de la observación directa en el entorno escolar, donde se detecta que los estudiantes usan intensivamente diversas plataformas digitales sin contar con conocimientos sólidos sobre ciberseguridad. La falta de cultura de prevención en el uso de contraseñas, el manejo de datos y la navegación segura puede derivar en consecuencias perjudiciales tanto académicas como personales.

El objetivo de esta investigación es analizar el nivel de conciencia y las prácticas de ciberseguridad de estudiantes de bachillerato a través de un cuestionario con escala Likert, con el fin de identificar áreas prioritarias para el diseño de estrategias educativas que fortalezcan la seguridad digital de los estudiantes.

METODOLOGÍA

El presente estudio adopta un enfoque cuantitativo, con un diseño no experimental, transversal y descriptivo, debido a que se centró en observar y analizar el nivel de conciencia de los estudiantes, así como las prácticas de ciberseguridad, sin usar variables. El propósito fue identificar áreas fundamentales que orienten futuras estrategias educativas en materia de seguridad digital.

Para la recolección de datos se diseñó un cuestionario estructurado por 18 reactivos de los cuales diez fueron de opción cerrada con escala Likert con cinco niveles de respuesta, de 1 que representa Totalmente en desacuerdo a 5 que indica Totalmente de acuerdo, lo anterior para medir conocimientos, actitudes y prácticas relacionadas con contraseñas, plataformas digitales, navegación segura y protección de datos. El resto, fueron preguntas abiertas las cuales permitieron identificar percepciones, experiencias y sugerencias de los estudiantes sobre el uso responsable de la tecnología y los riesgos a los que se enfrentan en línea. Este diseño mixto permitió tanto la cuantificación de tendencias generales, así como la exploración cualitativa de respuestas espontáneas, enriqueciendo el análisis.

La población objetivo fueron estudiantes de bachillerato de una institución pública ubicada en el área metropolitana de Monterrey, Nuevo León, para lo cual, se utilizó un muestreo no probabilístico por conveniencia, obteniendo una muestra de 85 estudiantes de segundo semestre. Este tamaño de muestra es adecuado para estudios descriptivos, ya que nos permite identificar los patrones generales y necesidades formativas en ciberseguridad.

El instrumento fue aplicado de manera digital mediante una aplicación en línea llamada Microsoft Forms, la cual se aplicó a dos grupos en la última semana de clases, la participación de los estudiantes fue voluntaria y se garantizó el anonimato y la confidencialidad de las respuestas.

Los datos de las preguntas cerradas fueron exportados y analizados mediante hoja de cálculo de Microsoft Excel, aplicando estadística descriptiva como frecuencias, promedios y medidas de dispersión. Las respuestas abiertas fueron revisadas mediante un análisis temático inicial, con la finalidad de identificar percepciones que sean comunes y áreas de interés educativo en torno a la ciberseguridad.

RESULTADOS

El cuestionario aplicado a 86 estudiantes de segundo semestre permitió conocer su nivel de conciencia, actitudes y prácticas respecto a la ciberseguridad. A continuación, se presentan los resultados divididos en dos apartados: reactivos cerrados con escala Likert y análisis de las preguntas abiertas.

Resultados cuantitativos

En la *Tabla 1* se presentan los porcentajes de las respuestas de los 10 reactivos de tipo Likert, organizados según los cinco niveles de respuesta.

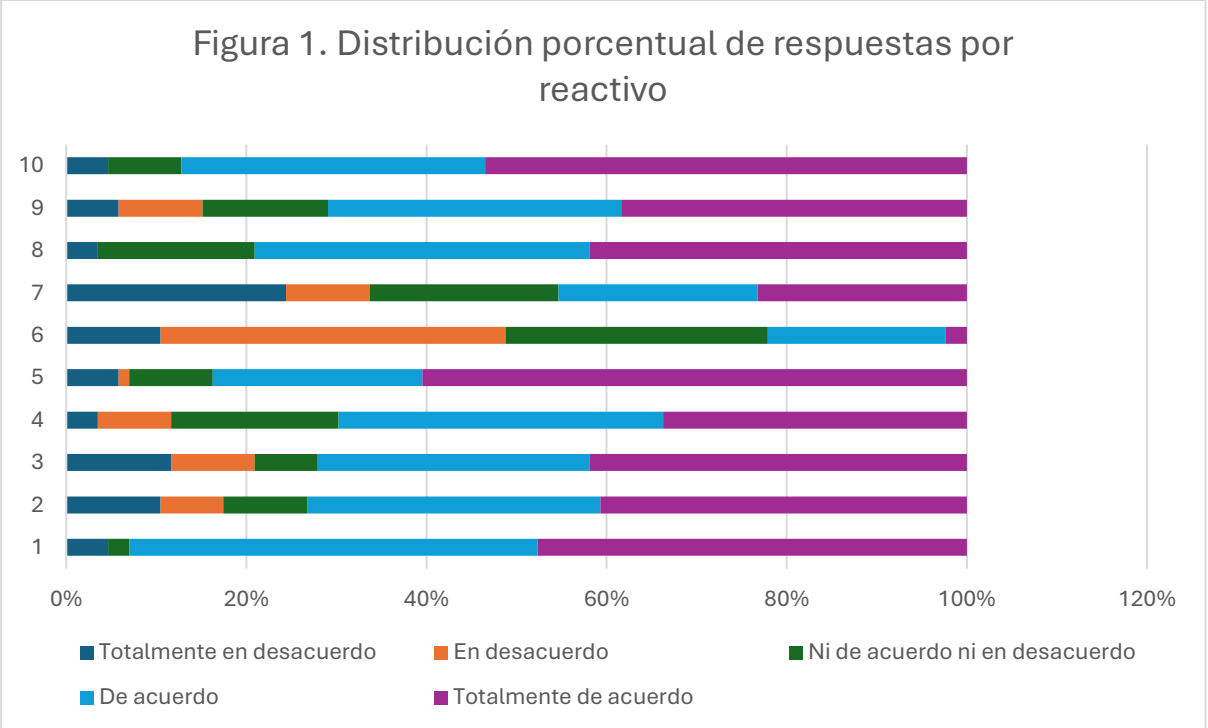
Tabla 1 Porcentaje De Respuestas Por Reactivo (Escala Likert)

Reactivos	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
Sé qué es la ciberseguridad y por qué es importante.	5%	0%	2%	45%	48%
Uso contraseñas seguras y diferentes para cada una de mis cuentas.	10%	7%	9%	33%	41%
Tengo activada la verificación en dos pasos en al menos una de mis cuentas.	12%	9%	7%	30%	42%
Puedo identificar un correo sospechoso o intento de phishing.	3%	8%	19%	36%	34%

Nunca comparto mis contraseñas con otras personas.	6%	1%	9%	23%	60%
Siempre cierro sesión cuando uso computadoras compartidas o públicas.	10%	38%	29%	20%	2%
He recibido información o capacitación sobre ciberseguridad en mi escuela.	24%	9%	21%	22%	23%
Me siento preparado(a) para proteger mis cuentas personales y escolares en línea.	3%	0%	17%	37%	42%
Utilizo herramientas o aplicaciones para gestionar mis contraseñas de forma segura.	6%	9%	14%	33%	38%
Considero que el tema de la ciberseguridad debería ser parte de nuestras clases escolares.	5%	0%	8%	34%	53%

Nota: Elaboración propia con base en el cuestionario aplicado a los estudiantes.

Figura 1. Distribución porcentual de respuestas por reactivo



Nota: Elaboración propia con base en el cuestionario aplicado a los estudiantes.

De forma general, se observa que los estudiantes tienen conciencia sobre la ciberseguridad, especialmente en los reactivos 1, 5 y 10, con porcentajes superiores al 80% en las opciones “de acuerdo” y “totalmente de acuerdo”. Por el contrario, los reactivos 6 y 7 muestran áreas de oportunidad claras.

A continuación, se describen los hallazgos más relevantes por reactivo:

Reactivo 1. El 93% reconoció saber qué es la ciberseguridad (45% de acuerdo y 48% totalmente de acuerdo), lo que indica una comprensión generalizada del concepto.

Reactivo 2. El 74% dijo usar contraseñas seguras y distintas, aunque un 16% expresó desacuerdo. Esto sugiere que todavía es necesario reforzar buenas prácticas en cuanto a la gestión de contraseñas.

Reactivo 3. El 72% afirmó tener activada la verificación en dos pasos. Sin embargo, un 21% indicó no contar con esta medida, posiblemente por desconocimiento o falta de orientación sobre cómo configurarla.

Reactivo 4. El 70% indicó poder identificar correos sospechosos o intentos de phishing, pero un 19% se mantuvo en una posición neutral y un 11% expresó no estar capacitado para ello. Esto refleja una vulnerabilidad importante ante intentos de fraude digital.

Reactivo 5. El 83% aseguró que nunca comparte sus contraseñas. Esta práctica adecuada muestra un nivel de cuidado y confidencialidad favorable entre los estudiantes.

Reactivo 6. Solo el 24% afirmó cerrar sesión en computadoras compartidas o públicas, mientras que el 48% reconoció no hacerlo y el 29% no lo tiene claro. Este resultado revela una debilidad crítica en el manejo básico de la seguridad digital.

Reactivo 7. Apenas el 45% indicó haber recibido información o capacitación sobre ciberseguridad en su escuela, lo que señala una carencia importante de formación institucional formal en este tema.

Reactivo 8. El 79% expresó sentirse preparado para proteger sus cuentas, aunque esta percepción contrasta con algunas prácticas deficientes observadas en otros reactivos. Esto sugiere una sobreestimación de sus propias habilidades en algunos casos.

Reactivo 9. El 71% reportó usar herramientas para gestionar sus contraseñas de forma segura, aunque un 15% expresó desacuerdo y un 14% se mantuvo neutral. Esto sugiere que el uso de gestores aún no es una práctica generalizada.

Reactivo 10. El 87% consideró que la ciberseguridad debería incluirse como parte de las clases escolares, mostrando un amplio respaldo estudiantil hacia la inclusión de este tema en el currículo educativo.

Las preguntas abiertas permitieron explorar con mayor profundidad las experiencias, preocupaciones y conocimientos del alumnado en relación con su seguridad digital. A partir del análisis de contenido, se identificaron cinco categorías principales:

Medidas que aplican. La mayoría mencionó el uso de contraseñas seguras, la no compartición de credenciales y, en algunos casos, la activación de la verificación en dos pasos (2FA), uso de VPN o navegación en modo incógnito. No obstante, también hubo estudiantes que admitieron no tomar ninguna medida o usar la misma contraseña en todos sus accesos.

Experiencias con correos sospechosos. Alrededor de la mitad de los estudiantes indicó haber recibido correos extraños o fraudulentos. Las respuestas ante estos casos fueron diversas: algunos los eliminaron, otros los ignoraron y unos cuantos reaccionaron con miedo o confusión. Incluso hubo quienes buscaron apoyo en familiares o investigaron el origen del mensaje. Este hallazgo revela que, aunque hay cierta intuición para detectar posibles amenazas, también hay falta de conocimiento para actuar adecuadamente ante ellas.

Percepción de riesgos. Los principales riesgos identificados por los estudiantes incluyen robo de identidad, extorsiones, hackeos, ciberacoso y fraudes financieros. También expresaron preocupación por ser grabados o vigilados sin consentimiento, o por la pérdida de información personal a través de plataformas maliciosas. Esto muestra que los estudiantes tienen conciencia de que navegar sin precauciones puede traer consecuencias reales y graves.

Temas que desean aprender. Muchos estudiantes expresaron interés por aprender a crear contraseñas más seguras, identificar correos falsos o peligrosos, proteger su información personal y actuar ante un intento de hackeo. También mencionaron que desean conocer más sobre el uso de herramientas como gestores de contraseñas, aplicaciones de seguridad, antivirus, y cómo usar de forma correcta recursos como el 2FA o las VPN. El hecho de que varios estudiantes respondieran “todo” o “no sé” también evidencia que, aunque hay interés, aún falta claridad sobre qué implica realmente la ciberseguridad.

Sugerencias a sus compañeros. Las recomendaciones más comunes fueron: no compartir contraseñas, tener precaución con los enlaces o páginas web desconocidas, no confiar en personas que no conocen en línea, y proteger su información en redes sociales. Estas respuestas reflejan una actitud preventiva emergente y el deseo de promover una cultura de cuidado digital entre pares.

DISCUSIÓN

Los resultados obtenidos en este estudio permiten observar con mayor claridad cómo piensan y actúan los estudiantes de bachillerato con relación a la ciberseguridad. Aunque en general muestran una buena disposición y cierta conciencia sobre el tema, también se detectan áreas que necesitan más atención, sobre todo en lo que se refiere a la práctica cotidiana y a la formación recibida por parte de la escuela.

Por ejemplo, la mayoría de los estudiantes dijo saber qué es la ciberseguridad y por qué es importante. También afirmaron, en gran medida, que usan contraseñas seguras, no las comparten y consideran que este tema debería enseñarse en clase. Esto refleja que hay una base de conocimiento y una actitud favorable hacia la protección de su información. Sin embargo, al revisar otros reactivos, aparecen contradicciones importantes. A pesar de que el 79% se siente preparado para proteger sus cuentas, solo el 24% aseguró cerrar sesión al usar computadoras compartidas, y apenas el 72% tiene activada la verificación en dos pasos. Esto indica que hay una diferencia entre lo que los estudiantes creen saber y lo que realmente aplican en su vida digital.

Este tipo de resultados coinciden con lo observado en estudios recientes. Por ejemplo, la Encuesta Global de Seguridad Online 2023 de Microsoft reveló que el 74 % de los adolescentes encuestados experimentó al menos un peligro en internet, como desinformación, ciberacoso o fraude; sin embargo, muchos jóvenes confiesan no saber cómo actuar ante estas amenazas o tienden a normalizarlas como algo “parte de internet”. (Prensa, 2023)

Además, Infobae (2025) indica que un estudio de Save the Children alerta que el 97 % de los jóvenes han sufrido algún tipo de violencia sexual en internet, tales como, como grooming, sextorsión y destaca que esta exposición aumenta cuando no hay formación o acompañamiento por parte de los adultos. (García Arenales, 2025)

Un dato que llama mucho la atención es que solo el 45% del alumnado dijo haber recibido información o capacitación sobre ciberseguridad por parte de la escuela. Esto es preocupante si tomamos en cuenta

que hoy en día la mayoría de las actividades escolares, administrativas e incluso personales se hacen en línea. En este sentido, hay una clara necesidad de que las instituciones educativas asuman un rol más activo, no solo informando a los estudiantes, sino enseñando con ejemplos, simulaciones y casos reales qué hacer ante situaciones como correos sospechosos, enlaces falsos, robo de identidad o ciberacoso.

Las respuestas a las preguntas abiertas también aportan información muy valiosa. Varios estudiantes dijeron que usan contraseñas difíciles, que activan alertas de inicio de sesión o que no comparten sus datos con nadie. Incluso hubo quienes mencionaron el uso de VPN, navegación en modo incógnito y autenticación biométrica. Esto muestra que algunos ya han incorporado medidas más avanzadas en su rutina digital, lo cual es positivo. Sin embargo, también hubo respuestas que revelan desinformación o falta de acciones concretas. Algunos estudiantes dijeron que usan la misma contraseña para todo, que no toman ninguna medida o que no saben qué podrían hacer en caso de recibir un intento de fraude.

En cuanto a los riesgos que perciben, las respuestas fueron bastante consistentes. La mayoría mencionó el robo de información, extorsiones, hackeos, fraudes, acoso y manipulación por parte de personas desconocidas. Este nivel de conciencia es un buen punto de partida, ya que demuestra que los estudiantes están expuestos a estos temas y que los reconocen como amenazas reales. El problema es que, aunque identifican los riesgos, no siempre saben cómo prevenirlos o cómo actuar si llegaran a enfrentar alguno.

Otro aspecto interesante fue lo que respondieron cuando se les preguntó qué les gustaría aprender o reforzar. Muchos mencionaron temas muy concretos: cómo crear contraseñas más seguras, cómo proteger sus cuentas, cómo identificar correos maliciosos y qué hacer si los hackean. Esto indica que hay interés y apertura para aprender, pero también que no se les ha proporcionado información suficiente o accesible. En algunos casos, los estudiantes simplemente respondieron “todo” o “no sé”, lo cual refuerza la idea de que falta una guía clara sobre qué significa estar seguro en línea.

Por último, las recomendaciones que los propios estudiantes dieron a sus compañeros reflejan una cultura emergente de autocuidado digital. Les sugieren no compartir contraseñas, no abrir correos o enlaces de desconocidos, tener cuidado con lo que publican y no confiar en cualquiera en internet. Estas respuestas muestran que sí hay una conciencia colectiva que puede aprovecharse como punto de partida para proyectos educativos donde los mismos jóvenes compartan buenas prácticas entre sí.

En conjunto, todos estos resultados indican que estamos frente a una generación que reconoce los riesgos digitales, pero que necesita más apoyo para convertir esa conciencia en acciones efectivas. Las escuelas pueden jugar un papel clave si integran la ciberseguridad como parte de la formación básica, no como un tema técnico, sino como parte de la vida diaria de los estudiantes. Esto puede hacerse a través de talleres, campañas, simulaciones o actividades en clase donde se analicen casos reales.

También es importante reconocer que este estudio tiene algunas limitaciones. Por ejemplo, se aplicó en una sola institución y con una muestra no probabilística, por lo que los resultados no pueden generalizarse a todos los estudiantes de bachillerato. Sin embargo, los hallazgos son útiles para identificar patrones y diseñar intervenciones que respondan a las necesidades reales de los jóvenes.

En futuras investigaciones sería valioso incluir entrevistas o grupos focales para profundizar en las experiencias personales, así como ampliar la muestra a diferentes contextos escolares. También sería útil medir el impacto de algún programa formativo o intervención educativa para evaluar si hay cambios reales en las prácticas digitales de los estudiantes.

En resumen, los resultados de este estudio muestran que, aunque los estudiantes tienen disposición y cierta conciencia sobre la ciberseguridad, todavía hay muchas áreas en las que requieren orientación, formación y acompañamiento. Las instituciones educativas tienen la oportunidad y la responsabilidad de ayudarles a construir hábitos digitales seguros que los protejan en su vida escolar y personal.

CONCLUSIONES

Este estudio permitió conocer, de forma clara y directa, cómo perciben y cómo viven los estudiantes de bachillerato el tema de la ciberseguridad. A partir de los datos obtenidos, se puede decir que los jóvenes tienen una noción general del tema y reconocen que es importante, pero en muchos casos no aplican de manera consistente las medidas básicas para proteger su información.

Un dato que resalta es la diferencia entre lo que los estudiantes dicen que saben y lo que realmente hacen. Por ejemplo, aunque la mayoría aseguró sentirse preparada para proteger sus cuentas, varios no utilizan la verificación en dos pasos o no cierran sesión al usar computadoras públicas. Esto nos muestra que hay seguridad en lo que creen saber, pero no siempre se refleja en su comportamiento. Esta brecha entre conocimiento y acción es clave, porque muchas veces se piensa que basta con “saber lo básico”

para estar protegido, cuando en realidad, los riesgos actuales requieren una participación más activa y consciente.

Por otro lado, el hecho de que solo una parte del alumnado haya recibido capacitación formal en ciberseguridad por parte de la escuela refuerza la idea de que este tema todavía no se aborda como debería en el entorno educativo. La mayoría de los estudiantes considera que la ciberseguridad debería incluirse como parte del currículo, y este es uno de los aportes más importantes de esta investigación: el tema no es ajeno para ellos, lo reconocen, lo valoran y, sobre todo, están dispuestos a aprender más al respecto.

Además, muchas de las respuestas abiertas muestran que algunos estudiantes ya han desarrollado prácticas positivas, como usar contraseñas seguras, activar alertas de inicio de sesión, no compartir datos personales o incluso utilizar herramientas como VPN o navegación en modo incógnito. Esto indica que hay una base sobre la cual se puede trabajar, especialmente si se les brindan más herramientas, ejemplos prácticos y espacios donde puedan hablar abiertamente sobre sus experiencias digitales.

También fue muy valioso identificar qué riesgos perciben como más importantes. Los más mencionados fueron el robo de identidad, el acceso no autorizado a cuentas, el ciberacoso y las extorsiones. El hecho de que los estudiantes estén conscientes de estas situaciones ya representa un primer paso para construir una cultura de cuidado digital. Sin embargo, esa conciencia no basta si no va acompañada de conocimientos concretos sobre cómo prevenir estos riesgos y qué hacer si ocurren.

Otro punto que se resalta en este estudio es que muchos estudiantes no saben con exactitud qué deberían aprender o reforzar sobre ciberseguridad. Algunos dijeron “todo”, otros “no sé”, y unos más mencionaron temas muy amplios. Esto indica que no solo falta información, sino también orientación. No se trata únicamente de darles datos técnicos, sino de guiarlos paso a paso, con ejemplos aplicables a su realidad: redes sociales, correos escolares, plataformas educativas, juegos en línea, entre otros.

En cuanto al cumplimiento del objetivo de este trabajo —identificar el nivel de conciencia y las prácticas de ciberseguridad en estudiantes de bachillerato—, se logró con claridad. Se obtuvo una visión amplia de lo que los estudiantes piensan, lo que hacen y lo que están dispuestos a mejorar. Además, se visibilizó una necesidad urgente: llevar la ciberseguridad al aula de manera estructurada, cercana y continua.

El aporte principal de este estudio está en que no se queda solo en los datos, sino que da voz a los estudiantes y muestra desde su perspectiva cómo viven los riesgos digitales. Esta visión permite que futuras acciones, campañas o contenidos formativos no se diseñen desde la suposición, sino desde lo que realmente necesitan y piden los propios jóvenes.

También es importante señalar que este estudio abre la puerta a nuevas preguntas. Por ejemplo: ¿cómo cambia la percepción de la ciberseguridad si se ofrece una capacitación escolar estructurada?, ¿qué estrategias podrían motivar a los jóvenes a tomar más en serio su seguridad digital?, ¿cómo influye el entorno familiar o el acceso a tecnología en sus prácticas? Estas son líneas que pueden explorarse en futuras investigaciones.

Finalmente, los resultados aquí presentados invitan a las instituciones educativas a tomar un papel más activo. La ciberseguridad ya no es un tema exclusivo de quienes estudian informática o de quienes trabajan en tecnología. Es una necesidad básica para todos los usuarios de internet, especialmente para los jóvenes que pasan gran parte de su día conectados. La escuela no puede quedarse atrás. Lo ideal es que la formación en ciberseguridad no se limite a una charla aislada, sino que se integre en el día a día escolar, como parte de la educación para la vida.

En conclusión, este trabajo deja claro que los estudiantes están abiertos a aprender, que ya tienen ciertas bases y que ven la ciberseguridad como un tema necesario. Lo que falta es guiarlos, acompañarlos y generar espacios donde se hable del tema con claridad, sin complicaciones técnicas y desde la realidad que ellos viven. Solo así se podrá avanzar hacia una cultura digital más segura, más informada y más consciente.

REFERENCIAS BIBLIOGRÁFICAS

AMRO, A. (7 de Noviembre de 2024). Most teens don’t report online fraud. Obtenido de ABN AMRO : https://www.abnamro.com/en/news/most-teens-dont-report-online-fraud

CIBERLATAM. (11 de marzo de 2025). Tres tendencias que afectarán a la ciberseguridad en 2025. Obtenido de CIBERLATAM: https://www.segurilatam.com/ciberilatam/tres-tendencias-que-afectaran-a-la-ciberseguridad-de-2025_20250311.html

García Arenales, M. (8 de Julio de 2025). infobae. Obtenido de El 97% de los jóvenes ha sufrido violencia sexual en internet: los métodos para captar víctimas son cada vez más sofisticados:

https://www.infobae.com/espana/2025/07/08/el-97-de-los-jovenes-ha-sufrido-violencia-sexual-en-internet-los-metodos-para-captar-victimas-son-cada-vez-mas-sofisticados/

Lindemulder, G., & Kosinski, M. (12 de agosto de 2024). ¿Qué es la ciberseguridad? Obtenido de IBM: https://www.ibm.com/mx-es/topics/cybersecurity

Malagón, D. (24 de Mayo de 2025). Infobae. Obtenido de La Policía Nacional alerta de una estafa en auge: "Intentan suplantar la identidad de tu hijo": https://www.infobae.com/espana/2025/05/24/la-policia-nacional-alerta-de-una-estafa-en-auge-intentan-suplantar-la-identidad-de-tu-hijo

Morduchowicz, R. (2021). Competencias y habilidades digitales. Uruguay. Obtenido de https://unesdoc.unesco.org/ark:/48223/pf0000380113

Prensa, M. (7 de febrero de 2023). Microsoft. Obtenido de El 74% de los adolescentes encuestados en el Informe de Seguridad Online de Microsoft afirma haber experimentado algún riesgo en Internet: https://news.microsoft.com/es-es/2023/02/07/el-74-de-los-adolescentes-encuestados-en-el-informe-de-seguridad-online-de-microsoft-afirma-haber-experimentado-algun-riesgo-en-internet

TUTASEC. (25 de Julio de 2023). Ciberseguridad para niños y adolescentes: Un enfoque proactivo para proteger a la próxima generación. Obtenido de TUTASEC: https://tutasec.com/ciberseguridad-para-ninos-y-adolescentes-un-enfoque-proactivo-para-proteger-a-la-proxima-generacion/