Universidad Siglo 21


Trabajo Final de Grado. Trabajo de investigación en tecnologías informáticas

**Carrera:** Licenciatura en informática

# Evaluación de la Ciberseguridad y Privacidad en Instituciones Educativas de los Niveles Primario y Secundario en Trenque Lauquen, Provincia de Buenos Aires

**Autor**: Fabián Eduardo Medina

**Legajo**: VINF 10493

**Tutor**: Pablo Alejandro Virgolini

Trenque Lauquen, Buenos Aires. Junio de 2025

## Resúmen

El presente trabajo analiza el estado de la ciberseguridad en instituciones educativas de nivel primario y secundario del Partido de Trenque Lauquen, provincia de Buenos Aires. A partir de un enfoque cualitativo de diseño descriptivo, se indagaron las percepciones del personal docente, directivo y técnico, sus prácticas digitales habituales y el nivel de conciencia institucional frente a amenazas como el phishing, el ransomware y la fuga de datos. Para ello se emplearon entrevistas semiestructuradas, observación técnica pasiva, análisis documental y un cuestionario diagnóstico tipo quiz. Los resultados evidencian la existencia de prácticas riesgosas normalizadas, una baja percepción del riesgo cibernético y la ausencia de políticas institucionales sistemáticas. No obstante, se detectó una predisposición favorable a recibir formación y mejorar las condiciones actuales. La discusión articula estos hallazgos con conceptos como cultura institucional, resiliencia digital y alfabetización crítica, señalando la necesidad de intervenciones realistas que integren dimensión técnica y pedagógica. El estudio permite cumplir con los objetivos propuestos y ofrece una base diagnóstica para futuras acciones en el ámbito escolar.


Palabras clave: ciberseguridad, instituciones educativas, riesgos digitales, cultura institucional, phishing


## Abstract

This research analyzes the state of cybersecurity in primary and secondary educational institutions in the district of Trenque Lauquen, Buenos Aires Province, Argentina. Using a qualitative and descriptive design, the study explores the perceptions of teaching, administrative, and technical staff, their digital practices, and the institutional

awareness level regarding threats such as phishing, ransomware, and data breaches. The data collection included semi-structured interviews, passive technical observation, document analysis, and a diagnostic quiz. The findings reveal normalized risky practices, low risk perception, and a lack of institutional cybersecurity policies. However, a willingness to receive training and improve was also identified. The discussion links these findings with concepts such as institutional culture, digital resilience, and critical digital literacy, highlighting the need for realistic interventions that integrate both technical and pedagogical approaches. The study fulfills its stated objectives and provides a diagnostic foundation for future actions within the school environment.

Keywords: cybersecurity, educational institutions, digital risks, institutional culture, phishing.

# Índice

## Introducción

La digitalización ha reconfigurado profundamente diversos ámbitos sociales, y en las últimas décadas, las Tecnologías de la Información y la Comunicación (TIC) se han integrado cada vez más en la vida cotidiana a nivel global (Leiva, 2015). En el ámbito educativo, esta incorporación tecnológica se ha acelerado drásticamente, impulsada de manera notable por eventos recientes como la pandemia del COVID-19, que forzó una migración rápida y masiva a entornos virtuales y plataformas digitales para garantizar la continuidad pedagógica (Cheng & Wang, 2022; SOWNDHARYAA K.M., 2024; UNESCO, 2023; Mentasti, S. 2021). Este salto a la virtualidad, aunque necesario, transformó rápidamente los procesos de enseñanza, aprendizaje y gestión administrativa, incrementando significativamente la superficie de exposición de las instituciones educativas a riesgos emergentes y crecientes en el ámbito de la ciberseguridad (SOWNDHARYAA K.M., 2024; UNESCO, 2023). La digitalización en la educación, por ende, no solo ofrece oportunidades sino que también presenta nuevos desafíos, requiriendo enfoques y estrategias proactivas para gestionar los riesgos que conlleva (Kozak & Lion, 2005; Rodríguez, 2009). En este nuevo paradigma, como destacan Ravichandran et al. (2025), los docentes asumen una doble responsabilidad: no solo impartir conocimiento, sino también salvaguardar la información sensible y velar por la seguridad de sus estudiantes en estos entornos virtuales cada vez más complejos.

Análisis académicos y reportes internacionales subrayan de manera consistente la particular vulnerabilidad del sector educativo frente a la miríada de ciberataques existentes. A nivel global, este sector se ha posicionado reiteradamente como uno de los más afectados (SOWNDHARYAA K.M., 2024; UNESCO, 2023), llegando a concentrar

un porcentaje alarmante de los ataques de ransomware dirigidos a nivel sectorial (UNESCO, 2023; Guerrero Sumalave, 2023). Específicamente, un informe de Sophos (2023), citado por Torres Jara (2024), revela una cruda realidad: en el año 2023, el 80% de las organizaciones de educación primaria y el 79% de las de educación superior encuestadas a escala mundial informaron haber sido víctimas de ataques de ransomware, lo que evidencia no solo la magnitud sino también la amplitud del problema a través de los diferentes niveles educativos. Datos recientes confirman que esta tendencia global no solo se mantiene, sino que se intensifica, y que, a pesar de la creciente y necesaria digitalización, el sector educativo a menudo carece de la preparación adecuada para enfrentar esta escalada de amenazas (SOWNDHARYAA K.M., 2024; Guerrero Sumalave, 2023). Esta falta de preparación se agudiza por una percepción frecuentemente errónea de que las instituciones educativas no custodian información de gran valor. No obstante, la realidad es que estas entidades manejan un vasto y diverso volumen de datos altamente sensibles, que incluyen información personal detallada y registros académicos de estudiantes (tanto menores como adultos), datos profesionales y personales de docentes y personal administrativo, información de las familias, así como datos financieros institucionales e investigaciones académicas (Cheng & Wang, 2022; SOWNDHARYAA K.M., 2024). La potencial vulneración, exfiltración o secuestro de estos datos sensibles plantea, en consecuencia, serios y multifacéticos riesgos que comprometen la privacidad, la seguridad e incluso la integridad física y emocional de toda la comunidad educativa (Rivera-Vargas et al., 2024; SOWNDHARYAA K.M., 2024; Gamito Gomez et al., 2020).

Las instituciones educativas, incluyendo las de nivel primario y secundario, presentan características inherentes que las convierten en blancos atractivos y, a menudo,

menos resilientes que otros sectores. Los factores que contribuyen a esta vulnerabilidad son multifacéticos y abarcan aspectos técnicos, humanos y organizacionales (Leiva, 2015). Entre los factores técnicos se encuentran la frecuente coexistencia de sistemas informáticos legados junto con tecnologías modernas, una alta y creciente dependencia de servicios de terceros y plataformas en la nube (SOWNDHARYAA K.M., 2024), infraestructuras tecnológicas a menudo débiles, desactualizadas o insuficientes, y una notable falta de personal técnico con formación especializada en seguridad informática o, en muchos casos, la ausencia total de soporte técnico dedicado a tiempo completo (SOWNDHARYAA K.M., 2024; Artavia Madrigal et al., 2023; Guerrero Sumalave, 2023). Desde una perspectiva organizacional, la gestión de la ciberseguridad en los centros educativos, tal como lo analiza Torres Jara (2024) [Torres Jara, 2024] para el contexto costarricense, requiere una visión integral que abarque la evaluación de riesgos, el establecimiento de políticas claras, protocolos de actuación, y la capacitación continua, tareas que recaen significativamente en la figura directiva. La naturaleza inherentemente abierta de los entornos educativos, diseñada para fomentar la colaboración y el acceso, junto con el uso cada vez mayor de dispositivos personales (BYOD) por parte de estudiantes y personal, que se conectan a las redes institucionales, amplifican aún más la superficie de ataque y la complejidad de la gestión de la seguridad (Cheng & Wang, 2022; SOWNDHARYAA K.M., 2024).

Los ciberataques dirigidos al sector educativo adoptan diversas formas y explotan estas vulnerabilidades de manera sistemática (SOWNDHARYAA K.M., 2024; Artavia Madrigal et al., 2023, citado en tu borrador). El phishing, definido como un intento de adquirir información sensible (como nombres de usuario, contraseñas y detalles de tarjetas de crédito) haciéndose pasar por una entidad confiable en una comunicación

electrónica (Ravichandran et al., 2025), sigue siendo un vector de ataque prevalente y altamente efectivo. Este tipo de ataque, a menudo vehiculizado a través de correos electrónicos maliciosos, se apoya en sofisticadas técnicas de ingeniería social que explotan la confianza, la curiosidad o el temor de los usuarios, convirtiendo la vulnerabilidad humana en su principal aliado (Artavia Madrigal et al., 2023, citado en tu borrador; Zianni & Nessier, 2014; Rochina Rochina, 2021; Queiruga et al., 2023). El ransomware, un tipo de software malicioso que restringe el acceso a determinados archivos o partes del sistema operativo y exige un rescate a cambio de quitar esta restricción (Ravichandran et al., 2025; Torres Jara, 2024), se ha convertido en una de las amenazas más lucrativas y disruptivas para las escuelas y universidades a nivel global, con la capacidad de paralizar por completo las actividades institucionales. La fuga de información o el robo de datos sensibles, ya sea por acción de malware, accesos no autorizados o incluso por descuidos internos, representa otra amenaza constante, exacerbada por la falta de políticas de protección de datos adecuadas y procedimientos seguros para el manejo de la extensa información personal y académica que custodian las instituciones (SOWNDHARYAA K.M., 2024; Artavia Madrigal et al., 2023, citado en tu borrador). A estas se suman otros riesgos como la distribución de malware diverso y los ataques de denegación de servicio (DoS) que, aunque menos comprendidos por algunos docentes (Ravichandran et al., 2025), pueden tener consecuencias igualmente graves.

Más allá de las amenazas técnicas directas a la infraestructura y los datos institucionales, es crucial reconocer que los jóvenes en edad escolar también se enfrentan a un espectro amplio de riesgos digitales derivados de su interacción en la vida cotidiana online. Entre estos se incluyen el cyberbullying, el sexting (intercambio de mensajes o imágenes de contenido sexual), el grooming (acoso y abuso sexual online por parte de

adultos que se hacen pasar por menores), la exposición a contenido inapropiado o violento, y el contacto con desconocidos con intenciones dudosas (Gamito Gomez et al., 2020; Rivera-Vargas et al., 2024). El informe de Garmendia et al. (2024) [Garmendia et al., 2024] para España, basado en percepciones docentes, indica que, si bien algunos riesgos como las estafas económicas o el robo de cuentas son reportados con baja frecuencia, situaciones como la difusión de peleas online, mensajes hirientes (incluyendo aquellos basados en identidad de género u orientación sexual) y el acoso online son más recurrentes, especialmente en la educación secundaria. Estos riesgos, si bien no siempre constituyen ataques directos a los sistemas informáticos de la escuela, representan amenazas severas para la seguridad, el bienestar emocional y el desarrollo psicosocial del alumnado, y a menudo se interconectan con vulneraciones de la privacidad y el uso inseguro de plataformas digitales y redes sociales (Gamito Gomez et al., 2020; Rivera-Vargas et al., 2024). Estudios sobre el uso de internet en niños y preadolescentes han documentado consistentemente que muchos, a pesar de poseer habilidades técnicas para operar dispositivos y aplicaciones, no cuentan con las competencias digitales críticas suficientes para un uso seguro y reflexivo de la tecnología (Gamito Gomez et al., 2020). Con frecuencia, estos jóvenes experimentan situaciones conflictivas en línea, manifestando una preocupante desconexión entre el conocimiento teórico que puedan tener sobre los riesgos y sus prácticas online reales, que a menudo resultan inseguras (Gamito Gomez et al., 2020). Esta brecha muestra con claridad que hace falta más formación práctica y acompañamiento real desde lo pedagógico para trabajar contenidos y desarrollar habilidades relacionadas con la seguridad digital y la convivencia positiva en el entorno online, directamente desde el ámbito escolar (Gamito Gomez et al., 2020; Zianni & Nessier, 2014). En este sentido, diversas iniciativas académicas y propuestas de

políticas públicas buscan activamente acercar la ciberseguridad y la alfabetización digital crítica a las escuelas secundarias, reconociendo el rol fundamental de la educación formal en esta área (Queiruga et al., 2023; Rodríguez, 2009).

Un factor crítico, y consistentemente señalado como recurrente en la literatura especializada, que contribuye de manera decisiva a la vulnerabilidad de las instituciones educativas es el denominado **riesgo humano**. Este se encuentra intrínsecamente asociado a la insuficiente capacitación y al bajo nivel de concienciación tanto del personal (docente, administrativo y directivo) como de los estudiantes respecto a las prácticas seguras en línea y la identificación de amenazas (SOWNDHARYAA K.M., 2024; World Economic Forum citado en Cheng & Wang, 2022; Zianni & Nessier, 2014). Diversos estudios, tanto a nivel global como regional, coinciden en señalar que los usuarios, por acción u omisión, son a menudo el eslabón más débil en la cadena de la ciberseguridad, y que esta falta de conocimiento y preparación es una vulnerabilidad activamente explotada por los ciberdelincuentes mediante técnicas de ingeniería social (Zianni & Nessier, 2014; Artavia Madrigal et al., 2023, citado en tu borrador; Guerrero Sumalave, 2023). La investigación de Ravichandran et al. (2025) en el contexto de docentes escolares en India, por ejemplo, reveló que una mayoría significativa (70%) no había recibido capacitación formal en ciberseguridad, y aunque un 40% de los encuestados consideraba tener un nivel "moderado" de conciencia, un preocupante 25% admitió tener un conocimiento "bajo" o "muy bajo" sobre el tema. De manera similar, el estudio de Garmendia et al. (2024) [Garmendia et al., 2024] en España, aunque muestra que los docentes buscan formarse (principalmente de manera autónoma online), también evidencia que una proporción considerable considera que la formación institucional recibida es escasa o poco útil, y un 10% optó directamente por la autoformación, lo que

sugiere deficiencias en la oferta formativa estructurada. Es más, este mismo estudio español reportó que, si bien nueve de cada diez docentes afirmaban saber comunicarse online o bloquear mensajes no deseados, menos de siete de cada diez se sentían capaces de denunciar contenidos negativos (68.6%) o identificar cuándo alguien era acosado online (64.2%), evidenciando brechas en competencias digitales críticas para la ciberseguridad y la convivencia digital. La pandemia de COVID-19, con el consiguiente y abrupto aumento de la digitalización en todos los niveles educativos, no hizo más que exacerbar y poner en evidencia estas carencias preexistentes en el uso seguro de las tecnologías (Mentasti S., 2021).

Investigaciones recientes han documentado que una parte considerable de alumnos de primaria y secundaria no ha recibido formación previa sobre seguridad en Internet y que, a pesar de declarar conocer algunos riesgos, sus prácticas online no siempre se corresponden con dicho conocimiento, manifestando comportamientos inseguros y reclamando, ellos mismos, más formación en el ámbito escolar (Gamito Gomez et al., 2020). La problemática no se limita a los estudiantes; un estudio en una universidad latinoamericana (Guerrero Sumalave, 2023) encontró que el personal administrativo encuestado mostraba una falta significativa de conocimiento sobre incidentes de ciberseguridad, así como un profundo desconocimiento de los procedimientos institucionales, las políticas de seguridad existentes, el personal responsable y el presupuesto asignado a esta área crítica. Este panorama evidencia una brecha importante en la preparación de los adultos que conforman las instituciones educativas en la región. En este sentido, el trabajo de Herrero-Martín et al. (2022) [Herrero-Martín et al., 2022] con futuros docentes en España, resalta la importancia de abordar la ciberseguridad desde la formación inicial, ya que si bien una intervención

formativa específica logró aumentar la sensibilidad y percepción del riesgo entre los estudiantes de magisterio, este cambio actitudinal no siempre se traduce directamente en una modificación de las prácticas de seguridad personal. Esto sugiere la necesidad de estrategias formativas que vayan más allá de la mera sensibilización y se enfoquen en el desarrollo de competencias prácticas y hábitos seguros. En definitiva, estos hallazgos concatenados sugieren que, a pesar de que el personal educativo y técnico utiliza cada vez más herramientas digitales en su quehacer diario, su nivel de conciencia y preparación específica ante los riesgos y amenazas de la ciberseguridad sigue siendo una cuestión pendiente y un área de urgente intervención (Zianni & Nessier, 2014; UNESCO, 2023; Ravichandran et al., 2025).

Las consecuencias de los ciberataques perpetrados contra el ámbito escolar trascienden ampliamente las meras pérdidas económicas o el compromiso puntual de datos (SOWNDHARYAA K.M., 2024). Un incidente de seguridad puede desencadenar una cascada de efectos negativos, resultando en la interrupción prolongada de las actividades académicas y administrativas esenciales, la erosión de la confianza de la comunidad educativa (padres, alumnos, personal) en la capacidad de la institución para protegerlos, la generación de costos significativos asociados a la recuperación de sistemas, la respuesta al incidente y la posible implementación de nuevas medidas de seguridad (Sophos, 2023, citado en tu borrador; Rivera-Vargas et al., 2024). Además, las instituciones pueden enfrentarse a serias derivaciones legales por incumplimiento de normativas de protección de datos personales, como la Ley 25.326 en Argentina (Rivera-Vargas et al., 2024; Borghello & Temperini, 2013). Torres Jara (2024) [Torres Jara, 2024] sistematiza los riesgos derivados de una ciberseguridad deficiente en centros educativos, entre los que destacan: la pérdida y exposición de datos confidenciales de estudiantes y

personal; la amenaza constante de malware y virus que pueden dañar sistemas y robar información; la falta de integridad de la información académica (ej. manipulación de calificaciones); la facilitación del acoso cibernético y el ciberbullying; el robo de propiedad intelectual desarrollada por la institución; y la exposición de los menores a contenido inapropiado o peligroso. La exposición de datos sensibles de menores, en particular, plantea serios y duraderos riesgos para su privacidad y seguridad futura (SOWNDHARYAA, K. M. 2024; Rivera-Vargas et al., 2024). Estos riesgos, como advierte la UNESCO (2023), se ven a menudo agravados en el entorno educativo por la falta de un marco de protección legal específico y suficientemente robusto para los datos de la niñez en el ámbito digital, así como por la frecuente adquisición e implementación de tecnologías educativas sin la debida diligencia en términos de seguridad y privacidad. Finalmente, la ausencia de protocolos formales y ensayados de respuesta ante incidentes agrava significativamente las consecuencias de un ataque, pudiendo llevar a la pérdida de evidencia crucial, a una respuesta tardía o inadecuada que permita la propagación del ataque, o a una gestión comunicacional deficiente que incremente la desconfianza (Guerrero Sumalave, 2023; Ravichandran et al., 2025).

A pesar de la creciente digitalización y la documentada exposición a una amplia gama de riesgos cibernéticos, y ante la evidente brecha entre la amenaza real y el nivel de preparación y los recursos disponibles en las instituciones educativas, persiste en muchos casos una percepción generalizada de que las escuelas "no tienen nada importante que proteger" y, consecuentemente, una preocupante falta de conciencia sobre la gravedad y la multiplicidad de las implicaciones de los problemas de ciberseguridad (Rivera-Vargas et al., 2024). Esta subestimación del riesgo se traduce en que muchas instituciones educativas carezcan de planes formales y actualizados de respuesta ante incidentes, no

dispongan de protocolos claros y difundidos de seguridad digital, y no implementen programas de capacitación y concienciación continua y obligatoria para todo el personal (Guerrero Sumalave, 2023; Ravichandran et al., 2025). El estudio de Ravichandran (Ravichandran et al., 2025) encontró que un alarmante 60% de los docentes desconocía los mecanismos de denuncia disponibles para incidentes de ciberseguridad y que el 70% no había participado en programas de sensibilización. Por su parte, el trabajo de Torres Jara (2024) en Costa Rica subraya que la gestión de la ciberseguridad es una responsabilidad directiva que debe incluir la identificación de vulnerabilidades, el diseño de lineamientos y la promoción de una cultura de seguridad, aspectos que a menudo se descuidan por falta de conocimiento, recursos o priorización. En España, aunque Garmendia et al. (2024) [Garmendia et al., 2024] reportan que la práctica totalidad del profesorado asegura que su centro escolar tiene protocolos de convivencia digital y ciberseguridad y que se informa a familias y estudiantes, también señalan que uno de cada diez docentes admite desconocer el contenido específico de dichos protocolos, especialmente en primaria.

Si bien existen en Argentina iniciativas y un marco legal general que roza la problemática, como la Ley de Protección de Datos Personales (Ley 25.326), la Ley de Delitos Informáticos (Ley 26.388) y la Ley Argentina Digital (Ley 27.078), la normativa específica y las políticas públicas integrales y operativas de ciberseguridad diseñadas para el ámbito educativo –particularmente para los niveles primario y secundario– aún requieren un desarrollo sustancial y, fundamentalmente, una implementación efectiva y sostenida. Dicha implementación debe necesariamente contemplar la realidad heterogénea de las escuelas argentinas, los recursos humanos y financieros disponibles, y las particularidades de cada contexto (Leiva, 2015; Artavia Madrigal et al., 2023, citado

en tu borrador; Estrategia Ciberseguridad PBA 2021-2024, citada en tu borrador). La protección de datos personales y la promoción de una seguridad digital robusta en el entorno escolar no deben ser consideradas un lujo o un añadido opcional, sino un derecho fundamental de niños, niñas y adolescentes en la era digital, así como una condición necesaria para garantizar un entorno de aprendizaje seguro y de calidad (Rivera-Vargas et al., 2024; UNESCO, 2023).

En este complejo escenario de creciente digitalización, persistente vulnerabilidad del sector educativo y una aparente brecha entre los riesgos existentes y el nivel de preparación institucional y personal, emerge con claridad la necesidad impostergable de comprender en profundidad la situación específica de la ciberseguridad en ámbitos locales y contextos particulares. Si bien análisis a nivel nacional (Leiva, 2015; Estrategia Ciberseguridad PBA 2021-2024, citada en tu borrador; Borghello & Temperini, 2013; Queiruga et al., 2023) e investigaciones en otros países y regiones (Garmendia et al., 2024; Ravichandran et al., 2025; Torres Jara, 2024); Guerrero Sumalave, 2023) evidencian la magnitud global del problema y la existencia de diversas iniciativas y desafíos comunes, resulta crucial y metodológicamente pertinente analizar cómo se manifiesta esta realidad en contextos educativos concretos. El estudio localizado, como el que se propone en la presente investigación para las escuelas de nivel primario y secundario en ciudades del interior de la provincia de Buenos Aires, permite identificar con mayor precisión los desafíos particulares, las vulnerabilidades situacionales específicas y, consecuentemente, las áreas de mejora y las estrategias de intervención más adecuadas y contextualizadas (Benítez Larghi et al., 2010).

El Partido de Trenque Lauquen, una localidad con características representativas del interior de la Provincia de Buenos Aires, con una matrícula escolar significativa en

los niveles primario y secundario y una progresiva, aunque quizás desigual, incorporación de tecnologías en sus instituciones educativas, representa un ámbito de estudio pertinente y relevante para este análisis. Actualmente, existe un vacío de conocimiento específico y detallado sobre las percepciones que el personal docente, directivo y técnico de esta localidad posee respecto a la ciberseguridad; sobre las prácticas de seguridad digital que efectivamente se implementan en sus escuelas; acerca del nivel de conciencia real ante amenazas específicas como el phishing, el ransomware y la fuga de datos; y sobre las estrategias y recursos (formales e informales) con los que cuentan o que desarrollan para hacer frente a estos desafíos en dicho contexto geográfico y socio-educativo. La presente investigación, por lo tanto, busca explícitamente contribuir a llenar este vacío de conocimiento, aportando evidencia empírica que pueda servir de base para futuras intervenciones y políticas.

Para abordar este problema y contribuir a llenar el vacío de conocimiento identificado, la presente investigación se guía por la siguiente pregunta general: ¿Cuál es el estado de la ciberseguridad en las escuelas de nivel primario y secundario del Partido de Trenque Lauquen, ¿cuáles son sus vulnerabilidades y prácticas de seguridad asociadas, y qué estrategias de mejora son pertinentes para este contexto?

A fin de responder a este interrogante principal y explorar las diversas facetas de la problemática, el estudio plantea las siguientes preguntas específicas:

- ¿Cuáles son las percepciones del personal docente, directivo y técnico de las escuelas de nivel primario y secundario del Partido de Trenque Lauquen respecto a la ciberseguridad escolar y los riesgos digitales?

- ¿Qué prácticas de seguridad digital y manejo de la tecnología son habituales entre el personal de las escuelas de nivel primario y secundario de Trenque Lauquen, e implican algún nivel de riesgo?
- ¿Cuál es el nivel de conciencia institucional en las escuelas de nivel primario y secundario del Partido de Trenque Lauquen ante amenazas de ciberseguridad como el phishing, el ransomware y la fuga de datos?

La realización de esta investigación se justifica por múltiples y convergentes razones de **relevancia académica, social y práctica**, fundamentadas en la creciente y compleja problemática de la ciberseguridad en el ámbito educativo, tal como se ha delineado previamente.

- **Desde la perspectiva académica:** Este estudio busca generar conocimiento empírico original y profundamente contextualizado sobre las dinámicas de la ciberseguridad en un nivel educativo (primario y secundario) y un ámbito geográfico (ciudades del interior de la Provincia de Buenos Aires, específicamente Trenque Lauquen) que, si bien comparte desafíos globales, presenta particularidades aún poco exploradas en la literatura científica argentina. Al contrastar la situación local con el panorama más amplio delineado por estudios nacionales (Leiva, 2015; Queiruga et al., 2023) e internacionales (Garmendia et al., 2024; Ravichandran et al., 2025; Torres Jara, 2024), la investigación aportará matices importantes. Se considera fundamental investigar con mayor profundidad las brechas en la conciencia y preparación del personal adulto en las instituciones educativas (Guerrero Sumalave, 2023; Ravichandran et al., 2025) y la urgente necesidad de una formación docente en seguridad digital que sea continua, efectiva y adaptada a los riesgos emergentes (Zianni & Nessier, 2014; Herrero-Martín et al., 2022 [Herrero-Martín et al., 2022]; Garmendia et al., 2024 [Garmendia et al., 2024]).

- **Socialmente:** La investigación es de alta relevancia porque se enfoca en identificar y comprender los riesgos que afectan directamente la seguridad, privacidad y bienestar de toda la comunidad educativa –estudiantes (particularmente niños, niñas y adolescentes), docentes y familias– en un entorno que es clave para el desarrollo individual y el progreso social. Al poner en evidencia las vulnerabilidades y los desafíos específicos del contexto, se espera contribuir a una mayor concienciación sobre la importancia crítica de la seguridad digital, no como un tema meramente técnico, sino como un componente esencial de la convivencia, la protección de derechos (especialmente de los menores [Rivera-Vargas et al., 2024; Gamito Gomez et al., 2020; UNESCO, 2023]) y la formación ciudadana en el siglo XXI.

- **Desde una perspectiva práctica:** Al diagnosticar las vulnerabilidades específicas, comprender las prácticas de seguridad (o la ausencia de ellas) y evaluar el nivel de conciencia existente en el contexto local de Trenque Lauquen, este estudio sentará bases sólidas para el diseño y la proposición de recomendaciones de mejora y estrategias de intervención que sean realistas, factibles, pertinentes y adaptadas a las capacidades y limitaciones de las escuelas en contextos similares. El fin último es contribuir tangiblemente al fortalecimiento de la resiliencia de estas instituciones ante la constante evolución de las amenazas cibernéticas (Rochina Rochina, 2021; Guerrero Sumalave, 2023; Torres Jara, 2024).

El objetivo de este trabajo, por tanto, no se limita a una mera descripción del problema, sino que busca ponerlo en evidencia con datos concretos, ilustrarlo con las realidades del contexto estudiado y, fundamentalmente, proponer caminos de acción y mejora que sean significativos y aplicables.

El objetivo general de este trabajo es analizar el estado de la ciberseguridad en escuelas de nivel primario y secundario del Partido de Trenque Lauquen, provincia de Buenos Aires, identificando sus vulnerabilidades, prácticas habituales y nivel de preparación institucional, con el propósito de proponer estrategias de mejora contextualizadas.

Los objetivos específicos que guían esta investigación son:

1. Identificar las percepciones del personal docente, directivo y técnico respecto a la ciberseguridad escolar y los riesgos digitales, a fin de determinar el nivel de conocimiento y valoración institucional sobre el tema.

2. Describir las prácticas tecnológicas frecuentes en el ámbito educativo que puedan implicar riesgos para la seguridad digital, con el fin de relevar posibles vulnerabilidades asociadas al uso cotidiano de dispositivos y sistemas.

3. Explorar el nivel de conciencia institucional frente a amenazas como el phishing, el ransomware y la fuga de datos, con el objetivo de evaluar la capacidad de prevención y respuesta ante incidentes de ciberseguridad.

## Marco Teórico

El avance sostenido de las tecnologías digitales en el ámbito educativo trajo múltiples beneficios, pero también nuevos desafíos. Uno de los más urgentes es la necesidad de proteger la información sensible y garantizar prácticas seguras en el uso de dispositivos y redes dentro de las instituciones escolares. La ciberseguridad, en este contexto, ya no puede ser pensada como un tema técnico exclusivo de especialistas, sino como una dimensión transversal que afecta el funcionamiento cotidiano de las escuelas.

Estudios recientes (Guerrero Sumalave, 2023; Torres Jara, 2024) advierten sobre la falta de políticas claras, protocolos de actuación ante incidentes y capacitación específica del personal en materia de seguridad digital. Esto genera un panorama en el que la mayoría de las instituciones educativas se encuentra expuesta a riesgos que, aunque poco visibles, pueden tener consecuencias significativas.

Desde un enfoque de cultura institucional, la ciberseguridad escolar puede entenderse como parte de un entramado de prácticas, percepciones y normas —explícitas o implícitas— que definen cómo una escuela gestiona la tecnología y protege la información. Esta perspectiva resulta coherente con lo planteado en la introducción, en tanto permite comprender que las vulnerabilidades en el ámbito educativo no dependen exclusivamente de la infraestructura tecnológica, sino también de los hábitos, la formación y las prioridades institucionales frente al uso seguro de herramientas digitales.

Este trabajo también se apoya en el enfoque de alfabetización digital crítica, que no se limita a saber usar herramientas digitales, sino que implica comprender los riesgos asociados a su uso y actuar con responsabilidad en entornos conectados (Zianni & Nessier, 2014; UNESCO, 2023). Esta perspectiva resulta clave para entender por qué muchos docentes o directivos, a pesar de utilizar tecnología en su trabajo diario, no reconocen amenazas como el phishing o el ransomware como parte de su realidad institucional.

Por último, el concepto de resiliencia digital institucional resulta relevante para interpretar los hallazgos del estudio. Rochina Rochina (2021) propone que las escuelas deben desarrollar capacidades no solo para prevenir incidentes, sino también para detectar, responder y recuperarse de ellos, aun cuando no cuenten con grandes recursos tecnológicos.

En este marco conceptual se apoya la investigación, que busca comprender cómo se perciben, enfrentan y gestionan los riesgos de ciberseguridad en instituciones educativas reales, en contextos concretos y con los recursos disponibles.

## Métodos

### *Diseño*

Para el análisis de los datos recolectados se utilizó un enfoque cualitativo con elementos de análisis mixto. Las entrevistas y observaciones fueron procesadas mediante una codificación temática manual, agrupando las respuestas según categorías emergentes como: nivel de conocimiento en ciberseguridad, uso de herramientas digitales, percepción de riesgo, y prácticas institucionales. Esta codificación permitió identificar patrones recurrentes y diferencias entre los distintos roles entrevistados (directivos, docentes y personal técnico).

En el caso del cuestionario tipo quiz sobre detección de correos fraudulentos (phishing), se aplicó un análisis cuantitativo descriptivo, calculando el porcentaje de respuestas correctas por participante y promediando los resultados por grupo. Estos datos fueron luego triangulados con las entrevistas y observaciones, con el fin de detectar coherencias o contradicciones entre lo que los sujetos declaraban saber y lo que efectivamente demostraban en el ejercicio práctico.

Finalmente, se realizó una comparación entre las distintas instituciones participantes, teniendo en cuenta variables como nivel educativo (primario o secundario) y presencia o ausencia de personal técnico especializado, a fin de enriquecer la interpretación de los resultados.

### *Participantes*

La población objetivo de este estudio estuvo compuesta por personal directivo, docente y técnico del área de Medios de Apoyo Técnico Pedagógico (EMATP) de escuelas de nivel primario y secundario ubicadas en el Partido de Trenque Lauquen, Provincia de Buenos Aires. Se eligieron estos perfiles por su contacto directo con el uso de tecnologías en el ámbito educativo y su conocimiento sobre las prácticas institucionales vinculadas a la seguridad informática.

La muestra fue seleccionada de forma intencional y por conveniencia, criterios propios de una investigación cualitativa. Se priorizó la inclusión de personas que pudieran aportar experiencias, percepciones y conocimientos relevantes sobre la ciberseguridad en sus instituciones. Entre los criterios de inclusión, se consideró pertenecer al plantel docente, directivo o técnico de escuelas públicas de Trenque Lauquen, estar en ejercicio al momento del estudio, y manifestar voluntad de participar. Como criterios de exclusión, se descartaron participantes que no pertenecieran a los niveles educativos analizados o que no tuvieran vínculo directo con la tecnología escolar.

Se estimó inicialmente contar con aproximadamente 20 participantes, distribuidos entre al menos cinco instituciones. El objetivo fue mantener una representatividad mínima entre los distintos roles, buscando incluir al menos tres directivos, quince docentes y dos referentes técnicos (EMATP), aunque la conformación final dependió de la disponibilidad real de los entrevistados.

Previo a la recolección de datos, se obtuvo consentimiento informado por escrito de todas las personas participantes, explicándoles los objetivos del estudio, las condiciones de anonimato y confidencialidad, y el uso posterior de la información. El modelo de consentimiento se presenta en el Anexo 1.

*Instrumentos*

Para abordar los objetivos del estudio, se utilizaron distintas estrategias metodológicas que permitieron explorar tanto las percepciones del personal como las prácticas institucionales en torno a la ciberseguridad:

a) **Entrevistas semiestructuradas**: Se llevaron a cabo entrevistas individuales con directivos, docentes y personal técnico de las instituciones participantes. El guion abordó temas vinculados a la percepción de riesgos, usos cotidianos de la tecnología y prácticas de seguridad digital. Las entrevistas, de unos 20 minutos de duración, se grabaron con autorización previa y se complementaron con notas de campo.

b) **Análisis documental**: Se revisaron documentos institucionales disponibles como reglamentos internos, políticas de uso de TIC y manuales (cuando existían). El objetivo fue detectar la existencia y el alcance de normativas formales relacionadas con la seguridad digital. En caso de haberse registrado incidentes, también se indagó cómo fueron abordados por la institución.

c) **Observación técnica pasiva:** Durante las visitas a las escuelas, se realizaron observaciones *in situ* no intrusivas para relevar condiciones y prácticas vinculadas a la seguridad física y lógica. Se prestó especial atención a aspectos como: equipos sin protección, acceso no restringido a PCs administrativas, visibilidad de contraseñas, estado del software de seguridad, y actualizaciones del sistema.

d) **Evaluación de la capacidad de detección de phishing mediante herramienta interactiva:** Se utilizó el *Phishing Quiz* desarrollado por Jigsaw (Google) como técnica de evaluación diagnóstica. La herramienta plantea correos electrónicos simulados y pide al usuario que determine si son legítimos o fraudulentos. Cada participante resolvió el quiz en un dispositivo, y se registraron sus aciertos, errores y

reacciones espontáneas durante la actividad. Esto sirvió para complementar y triangular los datos obtenidos en entrevistas y observación.

*Análisis de Datos*

El análisis de los datos recolectados se desarrolló bajo un enfoque cualitativo con elementos de análisis mixto, en coherencia con el diseño exploratorio-descriptivo de la investigación. Se optó por este enfoque por tratarse de un fenómeno poco explorado en el contexto educativo del interior bonaerense, donde era necesario comprender tanto las percepciones como las prácticas cotidianas relacionadas con la ciberseguridad. El estudio se llevó a cabo en un corte transversal, ya que se recolectaron datos en un único momento temporal, sin seguimiento longitudinal.

Las entrevistas semiestructuradas, las notas de observación y los documentos institucionales fueron organizados y analizados mediante codificación temática manual. Esta técnica consistió en la lectura intensiva del material, la identificación de unidades de significado, y su agrupamiento en categorías emergentes vinculadas a los objetivos de investigación. Para garantizar la coherencia del análisis, se aplicaron procedimientos de triangulación entre las distintas fuentes de información: entrevistas, observaciones y resultados del cuestionario interactivo. Aunque no se utilizó software especializado, se priorizó la fidelidad en la transcripción, la sistematización y la codificación, lo que permitió detectar patrones comunes y divergencias en las respuestas según el rol del participante y la institución de pertenencia.

Respecto a los datos obtenidos a través de la herramienta interactiva de Google (Phishing Quiz), se realizó un análisis cuantitativo descriptivo básico. Se calcularon medidas como el promedio de respuestas correctas por grupo, la frecuencia de errores y las puntuaciones individuales, que fueron luego comparadas con los discursos recogidos

en entrevistas. Esta triangulación permitió detectar coherencias (por ejemplo, personas que decían no saber del tema y fallaban en el quiz) y contradicciones (quienes creían estar formados pero cometían errores frecuentes), aportando solidez a la interpretación de los hallazgos.

Finalmente, los resultados fueron organizados en función de los objetivos específicos del trabajo, permitiendo construir una mirada integral sobre el nivel de conciencia, las prácticas y las vulnerabilidades institucionales en torno a la ciberseguridad escolar en el contexto local de Trenque Lauquen.

## Resultados

A continuación se presentan los hallazgos obtenidos a partir del trabajo de campo, organizados según los objetivos específicos de la investigación. Para efectos de este análisis, se entiende por *percepciones* a las creencias y valoraciones expresadas por los participantes en relación con la ciberseguridad; por *prácticas riesgosas*, a aquellas acciones habituales que implican vulnerabilidades en el uso de la tecnología; y por *conciencia institucional*, al nivel de conocimiento, reacción y capacidad preventiva frente a amenazas digitales como el phishing, el ransomware y la fuga de datos.

### *Percepciones sobre la ciberseguridad escolar*

Este apartado presenta los resultados correspondientes al primer objetivo específico, orientado a indagar las percepciones del personal escolar respecto a la ciberseguridad y los riesgos digitales.

Las entrevistas revelaron una baja percepción general sobre la importancia y presencia de la ciberseguridad en el quehacer cotidiano de las instituciones. Un directivo expresó: *"En la escuela no se suele hablar de ciberseguridad, no se lo considera como un tema clave."* Esta idea se repitió varias veces, generalmente asociada a que nunca

habían vivido incidentes graves, como indicó un docente: *"No se la considera importante porque no han ocurrido eventos que tengan que ver con eso, no hemos tenido situaciones graves más que algún virus, y eso se ha solucionado con algún técnico."*

En general, se tiende a subestimar lo expuestas que están las escuelas y cuán sensible es la información que manejan a diario. Varios participantes manifestaron que las instituciones educativas no serían un objetivo de interés para ciberdelincuentes: *"¿Quién se va a interesar en una escuela?, no tenemos información que a ellos les sirva."* Esta idea se complementó con la noción de que los problemas de ciberseguridad son más propios de otros ámbitos: *"Esos problemas de ciberseguridad es ámbito de grandes empresas, no de pequeñas escuelas."* Consecuentemente, el conocimiento sobre incidentes de ciberseguridad específicos que hayan afectado a otras instituciones educativas resultó ser prácticamente nulo: *"No, nunca escuchamos nada sobre eso."*

Respecto a la información manejada (datos de alumnos, personal, gestión administrativa), aunque se le reconoce utilidad interna, no se percibe un valor que pudiera atraer un interés externo malicioso, según coincidieron docentes y directivos: *"No creo que sea de interés para personas fuera del ámbito escolar, es información que utiliza solamente la escuela y no ven cómo a alguien externo les puede interesar."*

En cuanto a los riesgos digitales concretos que se vienen a la mente del personal, estos se asociaron principalmente con problemas técnicos como algún virus, el mal funcionamiento de equipos o la exposición de los alumnos a contenido inapropiado en internet. También se mencionó el cyberbullying entre alumnos mediante la creación de stickers de whatsaap con fotos, reconociendo que eso genera problemas en la realidad. Sin embargo, términos como alumnos exponiéndose no fueron comprendidos de manera

unificada, y la percepción general fue que el resto de riesgos digitales nunca le iban a suceder dado que nunca había sucedido en el ámbito escolar.

*Prácticas digitales y riesgos tecnológicos*

Este apartado detalla los hallazgos vinculados al segundo objetivo específico, referente a la detección de prácticas tecnológicas habituales y posibles riesgos asociados.

*Análisis Documental*

Durante el relevamiento en las instituciones, se solicitó acceso a documentos que pudieran referir a políticas de uso de TIC, protocolos de seguridad o manuales de buenas prácticas. En ninguna de las escuelas visitadas se pudo obtener documentación formal y específica sobre ciberseguridad o protocolos de respuesta a incidentes.

*Observación Técnica Pasiva*

Las observaciones *in situ* permitieron identificar diversas condiciones y prácticas con implicaciones para la seguridad:

- En todas las escuelas se constató la existencia de routers ubicados en pasillos de circulación general o aulas de libre acceso, sin resguardo físico.
- Se observaron conexiones de red por cable Ethernet dispuestas de forma improvisada, sin canalizaciones ni fijación estructural, facilitando el acceso físico a puntos de red.
- Varias computadoras, especialmente en áreas administrativas, quedaban encendidas fuera del horario escolar con sesiones activas y, en algunos casos, con almacenamiento automático de contraseñas institucionales en navegadores web.
- Se identificó el uso de cuentas de usuario genéricas o compartidas en algunos equipos de uso compartido, sin autenticación diferenciada.

- No se observaron normativas visibles ni cartelería orientativa sobre el uso seguro de tecnologías.
- No se observaron rutinas claras de respaldo ni señales de que haya políticas activas para mantener actualizados los equipos o el software.

*Prácticas Reportadas en Entrevistas*

Las entrevistas con directivos y docentes revelaron las siguientes prácticas tecnológicas habituales:

- Uso de Dispositivos: Es común el uso de dispositivos personales (teléfonos celulares y, en algunos casos, computadoras propias de los docentes) para tareas laborales, complementando las netbooks provistas por programas gubernamentales para alumnos. Un docente señaló: *"Solemos utilizar nuestros propios teléfonos celulares y algunos docentes sus computadoras, es normal que los docentes utilicen los propios."*
- Gestión de Cuentas y Contraseñas: Si bien todo el personal docente cuenta con correo laboral de la plataforma ABC para comunicaciones oficiales y acceso a plataformas, las prácticas de gestión de contraseñas son deficientes. Sobre las computadoras de uso compartido por alumnos, se indicó: *"Las computadoras se suelen prestar, por lo tanto no cuentan con contraseñas. No hay registros oficiales del préstamo..."*. Para los equipos de uso administrativo, aunque se utiliza el correo ABC, *"algunas veces su contraseña queda guardada."*
- Conexión de Dispositivos Externos: El personal conecta dispositivos personales como pendrives a los equipos de la escuela de manera rutinaria: *"Si, todo el tiempo. No toman ninguna medida, confían en el antivirus."*

- Descarga e Instalación de Software: No existen normas o restricciones sobre la instalación de software. Se han reportado problemas en las computadoras de alumnos debido a la frecuente instalación de videojuegos.
- Uso de Redes Wi-Fi: La red Wi-Fi escolar cuenta con clave, pero existen varias redes y se desconoce su nivel de seguridad. El personal suele conectarse a cualquier red disponible si la de la escuela no funciona.

*Conciencia institucional ante amenazas digitales*

Este apartado presenta los resultados vinculados al tercer objetivo específico, centrado en evaluar el grado de conciencia institucional ante amenazas concretas.

Las entrevistas evidenciaron un conocimiento limitado sobre amenazas específicas. El término phishing no fue reconocido espontáneamente: *"No, nunca lo escucharon [el término phishing]"*. Sin embargo, al describir situaciones de engaño, algunos participantes mencionaron haber recibido mensajes de texto sospechosos en sus celulares personales solicitando dinero, a menudo suplantando la identidad de conocidos: *"He recibido alguna vez mensajes de texto a mi celular personal por personas que escribían desde el whatsaap de un pariente, pidiendo plata o un adelanto..."*. Se observó que quienes fueron víctimas transfirieron dinero incluso con datos de CBU a nombre de desconocidos, mientras que otros evitaron la estafa por avisos previos. No obstante, no se reportó la recepción de correos electrónicos sospechosos o fraudulentos en las cuentas institucionales.

Respecto al "ransomware", el desconocimiento fue total: *"No, nunca [lo escucharon]. Cuando se les explicó de qué se trataban afirmaron estar seguros que un ataque de ese estilo nunca había sucedido en una escuela que conocieran y no tenían*

*preocupación de que les vaya a suceder. Porque esos ataques suceden en empresas que puedan pagar grandes sumas de dinero, la escuela no cuenta con dinero."*

En cuanto a noticias sobre ciberataques a otras instituciones, mencionaron haber escuchado algo pero le restaron importancia, reiterando la creencia de que *"esas cosas suceden en grandes empresas."*

La protección depende casi exclusivamente del antivirus que ya venía instalado en las máquinas, en el que confían sin mayores controles: *"Todas las computadoras tienen antivirus que viene desde que las entregaron, confiamos que eso es suficiente, nunca hemos tenido problemas grandes o graves con respecto a eso."*

Para situaciones de cyberbullying u otros delitos informáticos que involucran a alumnos, se indicó la existencia de equipos de orientación (psicopedagogos, asistentes sociales) y la realización de charlas a familias y alumnos, aunque se percibe que *"Los alumnos no son conscientes de la gravedad o las consecuencias que tienen actos que involucren esos delitos."*

*Evaluación Diagnóstica: Phishing Quiz*

Para complementar la evaluación de la conciencia sobre phishing, se administró una versión abreviada (seis ejercicios) del Phishing Quiz, desarrollado por Jigsaw en Google, a los entrevistados. Los resultados se resumen en la Tabla 1 y se describen a continuación:

| Ejercicio | Descripción Breve del Estímulo | % Acierto | Observación Principal / Criterio de Juicio Erróneo (si aplica) |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | Correo con errores sutiles y URL falsa (Phishing) | 0% | Considerado legítimo por todos los participantes. |
| 2 | Correo con URL claramente maliciosa (Phishing) | 100% | Identificado correctamente tras explicación sobre verificación de URLs. |
| 3 | Factura de luz con montos en dólares (Phishing) | 100% | Identificado como phishing, pero por criterio erróneo ("no puede venir en dólares"). |
| 4 | Mensaje legítimo de Dropbox sobre falta de espacio | 60% | Mayoría lo consideró phishing por "no usar ese servicio". |
| 5 | SMS con código de verificación no solicitado (Phishing/Smishing) | 100% | Identificado correctamente tras explicación sobre acción no propia. |
| 6 | Aviso de acceso sospechoso vía email (Phishing) | 15% | Mayoría lo consideró legítimo, sin verificar URL/remitente. |

**Tabla 1** *Resultados del Phishing Quiz por Ejercicio Aplicado al Personal Escolar (N=20)*

En el primer ejercicio, que presentaba un correo con errores sutiles de formato y una URL engañosa, la totalidad de los entrevistados lo consideró legítimo, evidenciando un desconocimiento inicial sobre indicadores clave de phishing. Tras una breve explicación sobre la importancia de verificar las URLs, en el segundo ejercicio (un intento de phishing claro con URL maliciosa), todos los participantes lo identificaron correctamente. El tercer ejemplo, una supuesta factura de luz con montos en dólares, fue también identificado como phishing por todos, aunque el criterio principal aducido fue la moneda ("no puede venir en dólares") y no necesariamente el análisis técnico del mensaje. En el cuarto caso, un mensaje legítimo de Dropbox alertando sobre falta de espacio, una parte de los participantes lo marcó incorrectamente como phishing, argumentando que "nunca usan ese servicio", una parte de los participantes lo marcó incorrectamente como phishing, argumentando que 'nunca usan ese servicio', lo que muestra un posible vínculo entre la familiaridad personal y la interpretación del mensaje. El quinto ejercicio, un SMS con un código de verificación no solicitado, fue reconocido correctamente como un intento de suplantación por todos los participantes, luego de una explicación sobre cómo interpretar dichos mensajes si no se ha iniciado ninguna acción propia. Finalmente, en el sexto ejercicio, un aviso por correo electrónico sobre un supuesto acceso sospechoso a una cuenta, la mayoría lo consideró legítimo, posiblemente influenciados por la similitud superficial con alertas reales, pero omitiendo la verificación de detalles cruciales como la URL del remitente o los enlaces, siendo en realidad según el diseño del ejercicio, un correo considerado como intento de phishing. En síntesis, los resultados del quiz reflejan dificultades en el reconocimiento de correos de phishing sin intervención formativa, con una alta dependencia de indicadores superficiales o explicaciones puntuales. Sin embargo, se observó que breves instancias de clarificación durante el ejercicio

permitieron mejorar la detección en casos específicos, lo que indica una receptividad a la formación.

**Conocimiento de Políticas, Recursos y Capacitación**

Si bien no fue planteado como un objetivo específico inicial, se identificó un patrón transversal vinculado al conocimiento institucional sobre ciberseguridad y recursos disponibles, lo cual se presenta a continuación. Las entrevistas reflejaron que los principales desafíos en ciberseguridad percibidos por el personal se centran en aspectos operativos básicos: *"el uso que se le da a las computadoras por parte de los alumnos es puramente del aula... Con respecto a lo administrativo no hay grandes inconvenientes que veamos a futuro."* No se identificaron grandes desafíos o preocupaciones específicas sobre la seguridad de la información.

Respecto a los recursos, los directivos y docentes consideraron en general que cuentan con lo necesario para la realidad de las escuelas, mencionando los equipos existentes, el antivirus preinstalado y el referente tecnológico distrital, como manifestó un directivo: *"Considero que si, que con lo que tienen en cuanto a computadoras, antivirus y el referente tecnológico... creo que contamos con lo necesario para la realidad de las escuelas."* Nadie relacionó directamente tener más equipos o mejor infraestructura con una mejora concreta en la ciberseguridad: *"si bien siempre hace falta más equipos... no vemos la relación entre más equipos, infraestructura, o políticas con un mejor nivel de ciberseguridad."*

Todo el soporte técnico recae en un solo referente que depende de la jefatura distrital y tiene que cubrir más de 25 escuelas, lo que vuelve la asistencia muy esporádica (más de 25), lo que resulta en una atención esporádica: *"la atención se da muy pocas*

*veces por mes o a veces cuatro por año."* No existe personal específico encargado de la ciberseguridad en las escuelas visitadas.

En cuanto a políticas formales o protocolos escritos sobre uso seguro de la tecnología o respuesta a incidentes, los entrevistados manifestaron desconocimiento: *"No, nunca. Nunca se ha escrito nada al respecto, o que haya dispuesto el ministerio de educación."* De manera similar, no se reportó haber recibido capacitación específica sobre ciberseguridad: *"No hemos hecho ninguna capacitación al respecto."*

## Discusión

El objetivo general de esta investigación fue analizar el estado de la ciberseguridad en escuelas de nivel primario y secundario del Partido de Trenque Lauquen, identificando sus vulnerabilidades, prácticas habituales y nivel de preparación institucional, con el propósito de proponer estrategias de mejora contextualizadas.

En relación con el primer objetivo específico, orientado a identificar las percepciones del personal docente, directivo y técnico respecto a la ciberseguridad escolar y los riesgos digitales, se evidenció una subestimación generalizada del problema. Esta visión, expresada en frases como “la escuela no es objetivo de interés”, refleja lo señalado por Guerrero Sumalave (2023) y Herrero-Martín et al. (2022), quienes destacan que la falta de conciencia institucional sobre amenazas digitales limita la adopción de políticas preventivas. La cultura institucional aparece fragmentada, con una delegación de responsabilidades que obstaculiza el abordaje colectivo de la seguridad digital.

En cuanto al segundo objetivo, vinculado a la descripción de prácticas tecnológicas que implican riesgos de seguridad, se detectaron situaciones reiteradas como el uso de cuentas compartidas, contraseñas almacenadas en los navegadores y redes

abiertas sin autenticación robusta. Estas acciones coinciden con lo advertido por Torres Jara (2024) y Zianni & Nessier (2014), quienes subrayan que la exposición a amenazas se incrementa cuando no existen criterios institucionales claros sobre el uso seguro de tecnologías. El problema no reside únicamente en lo que se hace, sino en el desconocimiento de las consecuencias que conllevan ciertas prácticas normalizadas.

Respecto al tercer objetivo, orientado a explorar el nivel de conciencia institucional frente a amenazas específicas como el phishing, el ransomware y la fuga de datos, los resultados del diagnóstico aplicado muestran una comprensión parcial y basada en intuiciones más que en conocimientos técnicos. Como indica la UNESCO (2023), la alfabetización digital crítica exige más que familiaridad: requiere la capacidad de reconocer patrones de riesgo. El hecho de que los participantes identificaran ciertos correos de phishing por razones erróneas —como desconfiar de montos en dólares— muestra que los criterios empleados no siempre responden a fundamentos sólidos. Esta debilidad compromete la capacidad institucional de prevenir incidentes.

En este marco, resulta pertinente recuperar el concepto de resiliencia digital institucional (Rochina Rochina, 2021), entendida como la capacidad de prevenir, detectar, responder y recuperarse de incidentes. Si bien las escuelas evaluadas no cuentan con protocolos ni personal específico en ciberseguridad, se identificaron elementos positivos, como la disposición a formarse y el interés por mejorar. Esto sugiere que, si se diseñan estrategias adecuadas y contextualizadas, el personal educativo podría fortalecerse como agente activo en la construcción de una cultura de seguridad digital.

En cuanto a las **limitaciones del estudio**, es importante señalar que el trabajo se centró en un único distrito geográfico, lo que restringe la generalización de los resultados.

Además, se basó exclusivamente en el testimonio del personal adulto —sin incluir a estudiantes ni familias— y en una herramienta diagnóstica breve, sin validación formal como instrumento académico. También deben considerarse los sesgos propios de las entrevistas autodeclarativas, así como las limitaciones metodológicas propias de una investigación de grado, tanto en tiempo como en recursos.

A pesar de ello, los hallazgos permiten afirmar que se cumplieron los objetivos propuestos y que la investigación ofrece una base sólida para comprender el estado actual de la ciberseguridad en el ámbito escolar del Partido de Trenque Lauquen, aportando elementos concretos para futuras intervenciones y desarrollos institucionales más robustos.

*Limitaciones del estudio*

Este trabajo, si bien aporta una mirada detallada sobre la ciberseguridad en instituciones educativas del Partido de Trenque Lauquen, presenta algunas limitaciones que es importante señalar para contextualizar adecuadamente los resultados.

En primer lugar, el estudio se desarrolló en una zona geográfica acotada, lo que restringe la posibilidad de generalizar los hallazgos a otras regiones del país. Las dinámicas institucionales, los recursos disponibles y la cultura organizacional pueden variar significativamente entre distritos, por lo que los resultados deben interpretarse en función del contexto local.

En segundo lugar, la recolección de datos se basó fundamentalmente en entrevistas con personal docente, directivo y técnico, sin incluir de manera directa la perspectiva de estudiantes o familias, quienes también forman parte del ecosistema

educativo y podrían aportar miradas complementarias sobre las prácticas digitales y los riesgos percibidos.

Asimismo, la herramienta diagnóstica utilizada para evaluar el reconocimiento de intentos de phishing —si bien útil como recurso ilustrativo— no puede considerarse una prueba exhaustiva ni definitiva del nivel de conciencia en seguridad digital del personal. Se trató de un ejercicio acotado, con limitaciones propias de su diseño y sin validación formal como instrumento académico.

Otra limitación relevante tiene que ver con el carácter autodeclarativo de la información recabada mediante entrevistas. Es posible que algunos participantes hayan omitido prácticas inseguras o hayan respondido de manera socialmente deseable, lo cual podría influir en la representación de ciertas conductas.

Por último, deben considerarse también las restricciones de tiempo y recursos propios de una investigación de grado, que condicionaron tanto el número de escuelas incluidas como la profundidad de ciertas técnicas complementarias de recolección de datos (como encuestas masivas o análisis técnico forense de equipos).

A pesar de estas limitaciones, se considera que el trabajo ofrece una base sólida para comprender la problemática de la ciberseguridad en el ámbito escolar y orientar futuras investigaciones o intervenciones más amplias y sistemáticas.

## Referencias

Artavia Madrigal, C., Guevara García, M., Mora Zumbado, I., Murillo Murillo, T., Ramírez González, M., & Solano Ruiz, V. (2023). Análisis del sistema educativo costarricense: Desafío crítico para la ciberseguridad del país. *Revista Nuevo Humanismo, 11*(1), 136-163. https://revistas.ulacit.ac.cr/index.php/rhombus/article/view/89

Benítez Larghi, S., Lemus, M., & Welschinger Lascano, N. (2010). Massive inclusion of digital technologies in schools: Argentinian young adolescents' appropriation of computers and the Internet in popular and middle classes. *Revista Argentina de Sociología, 8*(15), 291-319.

Borghello, C., & Temperini, M. (2013). *Ciberseguridad Nacional Argentina: Cracking de servidores de la Administración Pública*. Ponencia presentada en el Simposio Argentino de Informática y Derecho, Argentina. https://sedici.unlp.edu.ar/handle/10915/94081

Cheng, E. C. K., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information, 13*(4), 192. https://doi.org/10.3390/info13040192

Gamito Gomez, R., Aristizabal Llorente, P., Vizcarra Morales, M. T., & León Hernández, I. (2020). Seguridad y protección digital de la infancia: Retos de la escuela del siglo XXI. *Educar, 56*(1), 219-237. https://doi.org/10.5565/rev/educar.1113

Garmendia, M., Martínez, G., Larrañaga, N., Jiménez, E., & Olveira, R. (2024). *Competencia digital docente, ciberseguridad y convivencia digital del alumnado en Educación Primaria y Secundaria*. SIC-Spain 3.0; Universidad del País Vasco. Recuperado de https://www.ehu.eus/es/web/eukidsonline/informes-libros

Google. (n.d.). *Phishing quiz*. https://phishingquiz.withgoogle.com/?hl=es

Guerrero Sumalave, D. F. (2023). *Modelo de gestión de ciberseguridad para resolver incidentes en instituciones de educación superior* (Tesis de maestría). Universidad Francisco de Paula Santander Ocaña, Colombia. Recuperado de https://repositorioinstitucional.ufpso.edu.co/handle/20.500.14167/1685

Herrero-Martín, J., Rodríguez-Merino, C., Valdivielso Alba, R., & Amo-Filva, D. (2022). Ciberseguridad y educación: Variables de sensibilidad y cambio en la formación del profesorado. En *Actas del VIII Congreso de Innovación Educativa y Docencia en Red (IN-RED 2022)* Universitat Politècnica de València. https://doi.org/10.4995/INRED2022.2022.15855

Keefer, P., Roseth, B., & Santamaria, J. (2024). *General skills training for public employees: Experimental evidence on cybersecurity training in Argentina* (IDB Working Paper No. IDB-WP-1643). Inter-American Development Bank. https://www.econstor.eu/handle/10419/309120

Kozak, D., & Lion, C. (2005). *Redes y escuela: ¿Dentro o fuera? Falsos dilemas sobre las TICs y su influencia en niños/as y jóvenes*. Ponencia presentada en el V Congreso Internacional Virtual de Educación. Recuperado de http://sedici.unlp.edu.ar/handle/10915/24389

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers, 14*(2), 49. https://doi.org/10.3390/computers14020049

Leiva, E. A. (2015). Estrategias nacionales de ciberseguridad: Estudio comparativo basado en enfoque top-down desde una visión global a una visión local. *Revista Latinoamericana de Ingeniería de Software, 3*(4), 161-176.

Lewis, J. A. (Ed.). (2016). *Experiencias avanzadas en políticas y prácticas de ciberseguridad: Panorama general de Estonia, Israel, República de Corea y Estados Unidos*. Banco Interamericano de Desarrollo

https://publications.iadb.org/publications/spanish/document/Experiencias-avanzadas-en-pol%C3%ADticas-y-pr%C3%A1cticas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Rep%C3%BAblica-de-Corea-y-Estados-Unidos.pdf?download=true

Lugani, C. F., & Rizzo, A. C. (2014). Youth at risk by the use of Internet. En XX Congreso Argentino de Ciencias de la Computación (Buenos Aires, 2014). Red de Universidades con Carreras de Informática. https://sedici.unlp.edu.ar/handle/10915/42159

Mentasti, S. (2021). Enseñar en tiempos de pandemia: Reflexiones para repensar la escuela en la era digital. *Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología, (28)*, 303-309. https://doi.org/10.24215/18509959.28.e37

Pampín Pérez, A. (2023). *La ciberseguridad en Educación Secundaria: Análisis contextual y propuesta de recurso digital* (Trabajo Fin de Máster). Universidad de Santiago de Compostela, España. Recuperado de https://minerva.usc.es/entities/publication/23fae59f-8f0d-4b70-bce3-98fa60fa31b6

Pencheva, D., Hallett, J., & Rashid, A. (2019, October). Bringing cyber to school: Integrating cyber security into secondary school education. *IEEE Security & Privacy, 17*(5), 78-83. https://doi.org/10.1109/MSEC.2019.2915932

Queiruga, C., Banchoff Tzancoff, C., Martin, S., & Kimura, I. (2023). *Propuestas de acercamiento a la Informática para la escuela secundaria: Contenidos, estrategias*

*didácticas y materiales*. Ponencia presentada en el Simposio Argentino de Educación en Informática, Argentina. https://sedici.unlp.edu.ar/handle/10915/177060

Ravichandran, R., Singh, S., & Sasikala, P. (2025). Exploring school teachers' cyber security awareness, experiences, and practices in the digital age. *Journal of Cybersecurity Education, Research and Practice, 2025*(1). https://doi.org/10.62915/2472-2707.1214

Rivera-Vargas, P., Raffaghelli, J., & Miño-Puigcercós, R. (2024). Plataformas digitales comerciales en la educación pública: Desafíos emergentes sobre privacidad y protección de datos. *Edutec. Revista Electrónica de Tecnología Educativa, (87)*, 28-42. https://doi.org/10.21556/edutec.2024.87.3063

Rochina Rochina, C. G. (2021). *Diseño y evaluación de una metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un gateway* (Tesis de maestría). Escuela Superior Politécnica de Chimborazo, Ecuador. Recuperado de http://dspace.espoch.edu.ec/handle/123456789/14677

Rodríguez, N. E. (2009). *Seguridad informática para alumnos de la Escuela Secundaria: Software educativo, un aporte a la educación* (Tesis de grado). Universidad Nacional de La Plata, Argentina. Recuperado de http://sedici.unlp.edu.ar/handle/10915/4206

Sophos. (2023). *The state of ransomware 2023: Findings from an independent, vendor-agnostic survey*. Sophos. Recuperado de https://www.sophos.com/en-us/content/state-of-ransomware

Sowndharyaa, K. M. (2024). Education sector under siege: Cyber attack challenges. *Indian Journal of Legal Review, 4*(3), 63–68. Recuperado de https://ijlr.iledu.in/

Suárez, G., Bolino, P., Venosa, P., & Queiruga, C. (2023). Acercando la ciberseguridad a la escuela secundaria desde una perspectiva lúdica. En *Actas del Simposio Argentino de Educación en Informática (SAEI)*. Recuperado de https://revistas.unlp.edu.ar/JAIIO/article/view/18067

Torres Jara, M. V. (2024). *La gestión de la ciberseguridad en los centros educativos del contexto costarricense: La gestión de un director* (Artículo Especializado para Maestría). Universidad Internacional San Isidro Labrador, Costa Rica. Recuperado de https://uisil.net/repositorio/files/43/La%20gestion%20de%20la%20ciberseguridad%20en%20los%20centros%20educativos%20del%20contexto%20costarricense,%20%20la%20gestion%20de%20un%20director.pdf

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2), 39. https://doi.org/10.3390/fi13020039

UNESCO. (2023). *Informe GEM 2023: Tecnología en la educación ¿Una herramienta en los términos de quién?* UNESCO. Recuperado de https://unesdoc.unesco.org/ark:/48223/pf0000386165_spa

Zianni, E. E., & Nessier, A. F. (2014). Formación docente en seguridad TIC: Cuestiones pendientes. *Revista Iberoamericana de Educación, 65*, 127-134. Recuperado de https://rieoei.org/historico/documentos/rie65a07.pdf

# Anexos

## ANEXO 1

Modelo de Consentimiento informado

Título de la Investigación: Evaluación de la ciberseguridad y privacidad en instituciones educativas de los niveles primario y secundario en Trenque Lauquen, provincia de Buenos Aires.

Investigador: Fabian Eduardo Medina - Alumno de la Licenciatura en Informática, Universidad Siglo 21.

Propósito de la Investigación: El objetivo de esta investigación es comprender el estado actual de la ciberseguridad y la gestión de riesgos asociados en escuelas de nivel primario y secundario de Trenque Lauquen. Buscamos conocer las percepciones del personal docente, directivo y técnico, identificar prácticas habituales relacionadas con la tecnología y evaluar el nivel de conciencia sobre las amenazas digitales comunes. La información recolectada será utilizada para identificar vulnerabilidades, comprender los desafíos locales y proponer posibles estrategias de mejora adaptadas al contexto de las escuelas de la región.

Descripción de la Participación: Su participación en este estudio implicará lo siguiente:

Participar en una entrevista semiestructurada de aproximadamente veinte minutos, donde se le realizarán preguntas sobre sus percepciones y experiencias relacionadas con la ciberseguridad y el uso de la tecnología en el ámbito escolar.

Se le presentarán dos ejemplos breves de correos electrónicos simulados para evaluar su capacidad para identificar posibles amenazas como el phishing. Sus respuestas

serán registradas. Al igual que se desarrollará la práctica de un ejercicio del tipo quiz interactivo de simulación de correspondencia phishing.

Permitir la observación no intrusiva de las prácticas tecnológicas en su entorno laboral habitual durante una visita al establecimiento educativo.

Autorizar la revisión de documentos institucionales relevantes relacionados con políticas de uso de TIC o seguridad digital que puedan estar disponibles.

Su participación es completamente voluntaria.

Confidencialidad y Anonimato: La información que usted proporcione será tratada con estricta confidencialidad. Su identidad no será revelada en ningún momento. Los datos recolectados serán utilizados únicamente con fines de investigación y serán presentados de forma agregada o anonimizada en el trabajo final de grado (tesis) que se presentará en la Universidad Siglo 21. En el manuscrito final, no se incluirán datos que permitan su identificación directa o indirecta.

Riesgos y Beneficios: Su participación en esta investigación no implica riesgos físicos, psicológicos o legales de ningún tipo. La participación no implica un beneficio directo o recompensa para usted. Sin embargo, la información que brinde será de gran valor para comprender y visibilizar los desafíos de ciberseguridad en el ámbito educativo local, lo cual podría contribuir al desarrollo de futuras iniciativas de mejora y concientización que beneficien a la comunidad educativa en general.

Derecho a Retirarse: Su decisión de participar es completamente voluntaria. Usted tiene el derecho de negarse a participar o de retirar su consentimiento y abandonar la investigación en cualquier momento, sin necesidad de dar explicaciones y sin que ello implique ningún tipo de perjuicio para usted.

Declaración de Consentimiento: He leído la información proporcionada en este formulario. He tenido la oportunidad de hacer preguntas y mis preguntas han sido respondidas satisfactoriamente. Entiendo el propósito de esta investigación, los procedimientos en los que participaré, los riesgos y beneficios (si los hubiera) y la forma en que se manejará mi información. Entiendo que mi participación es voluntaria y que puedo retirarme en cualquier momento. Doy mi consentimiento para participar en esta investigación.

Asimismo, autorizo que la entrevista sea registrada mediante grabación y/o anotaciones manuscritas.

Nombre completo del Participante:

---

Función del Participante:

---

Firma del Participante:

---

Fecha: _____ Lugar: _____

Nombre completo del Investigador:

---

Firma del Investigador: