https://repository.uaeh.edu.mx/revistas/index.php/serendipia/issue/archive

Serendipia

Publicación semestral, Vol. 1, No. 2 (2026) 5-13

Serendipia

Ciberseguridad para estudiantes de Educación Media Superior

Cybersecurity for High School Students

Olivia Vázquez Bautista [a]

Abstract:

This article examines cybersecurity among Upper Secondary Education students as a multidimensional challenge that goes beyond technical infrastructure protection. Facing a disruptive digital scenario, exacerbated by the emergence of Artificial Intelligence (AI) and post-pandemic hyperconnectivity, the objective is to diagnose the technical, psychosocial, and legal vulnerabilities students face and to propose an educational intervention model. The research follows a qualitative and documentary approach, reviewing scientific literature, global agency reports (2020–2025), and current Mexican regulations such as "Ley Olimpia." The findings reveal a critical paradox: while students possess high operational skills, they lack security competencies, exhibiting vulnerability to sophisticated threats such as AI-assisted phishing, sexual content deepfakes, and social engineering. Furthermore, the study identifies that neurobiological factors specific to adolescence and a lack of awareness regarding the legal consequences of digital violence exacerbate these risks. The study concludes that current institutional policies must evolve into a "digital immunity" strategy that integrates cybersecurity as a transversal curricular component, incorporates gamification, and strengthens school governance to foster resilient and legally responsible digital citizenship.

Keywords:

Cybersecurity, Upper Secondary Education, Artificial Intelligence, Ley Olimpia, Adolescent Neuroscience, Cyber Hygiene, Deepfakes, Digital Citizenship, Phishing.

Resumen:

El presente artículo analiza la ciberseguridad en estudiantes de Educación Media Superior (EMS) como un desafío multidimensional que trasciende la protección técnica de infraestructura. Ante un escenario digital disruptivo, exacerbado por la irrupción de la Inteligencia Artificial (IA) y la hiperconectividad post-pandemia, el objetivo es diagnosticar las vulnerabilidades técnicas, psicosociales y legales que enfrenta el alumnado, así como proponer un modelo de intervención educativa. La investigación adopta un enfoque cualitativo y documental, revisando literatura científica, informes de organismos globales (2020-2025) y normativas mexicanas vigentes como la "Ley Olimpia". Los hallazgos revelan una paradoja crítica: aunque los estudiantes poseen altas destrezas operativas, carecen de competencias de seguridad, exhibiendo vulnerabilidad ante amenazas sofisticadas como el phishing asistido por IA, los deepfakes de contenido sexual y la ingeniería social. Se identifica, además, que factores neurobiológicos propios de la adolescencia y el desconocimiento de las consecuencias legales de la violencia digital agravan el riesgo. El estudio concluye que las políticas institucionales actuales deben evolucionar hacia una estrategia de "inmunidad digital" que integre la ciberseguridad como eje transversal curricular, incorpore la gamificación y fortalezca la gobernanza escolar para formar una ciudadanía digital resiliente y legalmente responsable.

***Palabras Clave**:*

Ciberseguridad, Educación Media Superior, Inteligencia Artificial, Ley Olimpia, Neurociencia adolescente, Ciberhigiene, Deepfakes, Ciudadanía Digital, Phishing.

[a] Autor de Correspondencia, Universidad Autónoma del Estado de Hidalgo | Escuela Preparatoria Número 3 | Pachuca de Soto-Hidalgo | México
https://orcid.org/0000-0002-5978-7608, Email: olivia.vazquez.uaeh@gmail.com

Fecha de recepción: 11/08/2025, Fecha de aceptación: 06/11/2025, Fecha de publicación: 05/01/2026

DOI: https://doi.org/10.29057/serendipia.v1i2.16793

Introducción

El uso de las Tecnologías de la Información y Comunicación (TIC) ha reconfigurado la identidad del estudiante de Educación Media Superior (EMS), desdibujando las fronteras entre el entorno académico y la vida privada. Si bien esta hiperconectividad ofrece oportunidades educativas sin precedentes, también sumerge a los jóvenes en un ecosistema digital hostil para el cual, paradójicamente, no están preparados. La narrativa de los "nativos digitales" ha ocultado una realidad preocupante: la destreza operativa para manejar dispositivos no equivale a la competencia para gestionar riesgos de seguridad.

El planteamiento del problema de esta investigación surge de la asimetría observada entre la alta exposición digital del alumnado y su baja percepción del riesgo. En el contexto actual, post-pandemia y con la irrupción de la Inteligencia Artificial, las amenazas han mutado. Ya no se trata solo de virus informáticos (malware); los estudiantes enfrentan peligros sofisticados como el phishing asistido por IA, la violencia digital automatizada (deepfakes) y fenómenos psicosociales devastadores como la sextorsión y el reclutamiento ilícito. Esta brecha de seguridad pone en riesgo no solo la infraestructura institucional, sino la integridad psicológica y legal de los menores.

El objetivo general del presente artículo es doble: primero, diagnosticar y clasificar las amenazas de ciberseguridad —tanto técnicas como conductuales— prevalentes en el entorno de la EMS, con énfasis en el contexto mexicano y la normativa institucional de la Universidad Autónoma del Estado de Hidalgo (UAEH). Segundo, diseñar una estrategia de intervención integral que trascienda el bloqueo tecnológico, fomentando una cultura de autoprotección y ciberhigiene.

El fundamento teórico se sustenta en el concepto de Ciudadanía Digital, entendida como la capacidad de participar en la sociedad en línea de manera crítica, ética y segura. Metodológicamente, el estudio adopta un enfoque cualitativo y documental, integrando la revisión de literatura reciente (2020-2025), marcos legales vigentes como la "Ley Olimpia", y reportes de organismos internacionales.

El manuscrito se estructura de la siguiente manera: inicialmente se define el marco conceptual de la ciberseguridad y se analizan las amenazas emergentes impulsadas por la IA y la neurobiología adolescente. Posteriormente, se examina el marco jurídico y las políticas institucionales existentes. Finalmente, se presentan los resultados del análisis de vulnerabilidades y se propone un modelo de fortalecimiento escolar basado en la transversalidad curricular y la gobernanza institucional.

Metodología

Para el desarrollo de la presente investigación, se empleó un enfoque cualitativo de alcance descriptivo y documental. El proceso de recolección de información se estructuró en tres fases secuenciales: revisión sistemática de literatura, análisis de marcos normativos y diagnóstico contextual.

La búsqueda bibliográfica se realizó en bases de datos indexadas (Scopus, Redalyc, Scielo y Google Académico) y repositorios de organismos internacionales (UNICEF, UNESCO, ITU), utilizando cadenas de búsqueda booleanas como: "Ciberseguridad AND Educación Media Superior", "Digital Literacy AND Adolescents", y "Riesgos psicosociales en internet". Se seleccionaron documentos publicados preferentemente en el periodo 2020-2025 para garantizar la vigencia de los datos ante la rápida obsolescencia tecnológica.

Los criterios de inclusión consideraron: a) artículos revisados por pares que aborden competencias digitales en jóvenes de 15 a 18 años; b) informes técnicos de agencias de ciberseguridad gubernamentales (como INCIBE y CISA); y c) normativas vigentes en el contexto mexicano. Posteriormente, se realizó un análisis de contenido para categorizar las amenazas en dimensiones técnicas y conductuales, contrastando la teoría con las políticas institucionales vigentes en la Universidad Autónoma del Estado de Hidalgo (UAEH).

Concepto de Ciberseguridad

La ciberseguridad se define como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, guías de gestión de riesgos, acciones, capacitación, mejores prácticas, garantías y tecnologías que se utilizan para proteger los activos de la organización y de los usuarios en el ciberentorno (Gobierno de México).

En el contexto educativo, la ciberseguridad se enfoca en resguardar la confidencialidad, integridad y disponibilidad de la información personal y académica de los estudiantes y el ecosistema digital escolar.

En sí, la ciberseguridad se puede entender como la protección de sistemas, redes y datos frente a accesos no autorizados; y ha adquirido relevancia mundial ante el incremento de delitos informáticos. Diversos organismos, como la UNESCO y la Unión Internacional de Telecomunicaciones, han destacado la urgencia de fortalecer la educación digital desde niveles tempranos.

Amenazas Digitales en la Educación Media Superior

Los estudiantes de EMS son blancos frecuentes de ataques debido a su alta participación en plataformas sociales, su posible falta de discernimiento en la privacidad

y el uso de dispositivos personales poco protegidos. Las amenazas más comunes se clasifican en técnicas y psicosociales:

Técnicas:

Estas amenazas afectan tanto la vida personal como el

rendimiento académico.

- **Malware:** Software malicioso que incluye virus, troyanos y ransomware, diseñado para dañar sistemas o robar datos (Gobierno de México, 2024).
- **Phishing y Vishing:** Técnicas de ingeniería social que buscan obtener información confidencial (contraseñas, datos bancarios) a través de comunicaciones engañosas que simulan ser entidades legítimas.
- **Vulnerabilidades en Dispositivos y Redes:** Conexión a redes Wi-Fi públicas no seguras y falta de actualización de software (UNICEF, 2022).

Psicosociales:

Los estudiantes tienden a subestimar los riesgos por una percepción de invulnerabilidad. La presión social, el deseo de aprobación y la exposición constante en plataformas digitales contribuyen a decisiones poco seguras.

- **Ciberacoso (Cyberbullying):** Uso de medios digitales para acosar, intimidar, avergonzar o humillar a otra persona, siendo una de las amenazas más comunes entre jóvenes (ESET, 2018).
- **Grooming:** Conducta de un adulto que intenta ganarse la confianza de un menor en línea con el objetivo de obtener material sexual o un encuentro.
- **Sexting y Sextorsión:** El intercambio de material íntimo y el subsiguiente chantaje para evitar su difusión no consentida (ESET, 2018).
- **Reclutamiento Ilícito Digital:** El uso de plataformas y videojuegos para captar a jóvenes para actividades criminales, aprovechando su vulnerabilidad socioeconómica (Infobae, 2025).

Retos Emergentes: La Inteligencia Artificial y Factor Neuropsicológico

El panorama de amenazas ha evolucionado drásticamente con la popularización de herramientas de Inteligencia Artificial Generativa (IAG). Si bien estas tecnologías ofrecen ventajas educativas, en manos de adolescentes sin supervisión ética representan un vector de riesgo emergente que las instituciones educativas apenas comienzan a comprender.

- **Deepfakes y Violencia Sexual Digital.** La amenaza más alarmante para el estudiantado de EMS es la proliferación de deepfakes de contenido sexual no consentido. Aplicaciones accesibles permiten a los estudiantes crear imágenes o videos falsos hiperrealistas utilizando el rostro de compañeros o docentes. Según informes de Human Cloud (2024), el 90% de los deepfakes en línea son pornografía no consentida, y las escuelas son el nuevo epicentro de esta modalidad de acoso. Esto trasciende el ciberbullying tradicional, causando daños reputacionales y psicológicos irreversibles en las víctimas, y complicaciones legales graves para los agresores menores de edad (Sensity AI,2024).
- **Sofisticación del Phishing con IA.** Anteriormente, los correos de phishing eran detectables por errores ortográficos o gramaticales. Hoy, herramientas de IAG permiten a los ciberdelincuentes redactar mensajes persuasivos, libres de errores y adaptados al contexto escolar (ej. simulando ser la dirección académica solicitando credenciales). Esto eleva la barrera de entrada para la detección, haciendo que la alfabetización digital tradicional sea insuficiente si no se entrena el pensamiento crítico y la verificación de fuentes.
- **El Factor Neuropsicológico en la Adolescencia.** Para comprender la vulnerabilidad del estudiante de EMS, es necesario analizar el factor biológico. Durante la adolescencia (15-18 años), la corteza prefrontal —encargada del control de impulsos y la evaluación de riesgos a largo plazo— aún se encuentra en desarrollo, mientras que el sistema límbico —que procesa las recompensas inmediatas y la validación social— está hiperactivo.

  Esto explica por qué, a pesar de conocer teóricamente los riesgos, los estudiantes priorizan la gratificación inmediata (un like, acceder a un juego, compartir un meme viral) sobre la seguridad. La "brecha de intención-comportamiento" es, por tanto, una característica evolutiva que los ciberdelincuentes explotan mediante ingeniería social diseñada para activar emociones fuertes (miedo, urgencia o curiosidad).

Alfabetización digital

La alfabetización digital no solo implica la capacidad de usar dispositivos, sino también comprender la lógica de funcionamiento de los sistemas, identificar riesgos y actuar de forma segura. Para tener una alfabetización digital adecuada, se debe de integrar:

- **Conciencia Situacional:** Entender el entorno de amenazas actual.
- **Higiene Digital:** Rutinas diarias de mantenimiento de seguridad (actualizaciones, respaldos).
- **Resiliencia:** Capacidad de recuperación ante un incidente (saber a quién reportar y cómo mitigar el daño).

Competencias digitales

Según el marco de referencia establecido por la Comisión Europea, conocido como DigComp, la competencia digital se define como "el uso seguro, crítico y responsable de las

tecnologías digitales para el aprendizaje, en el trabajo y para la participación en la sociedad" (Vuorikari et al., 2022).

El Marco Europeo de Competencias Digitales y modelos latinoamericanos coinciden en la importancia de desarrollar habilidades en cinco áreas: información, comunicación, creación de contenido, seguridad y resolución de problemas.

Entornos Escolares Digitales

El entorno escolar digital (o ciberentorno escolar) se refiere al conjunto de recursos, sistemas, redes y espacios virtuales que la institución pone a disposición de la comunidad educativa, así como las interacciones que ocurren en ellos. Este entorno incluye:

- **Infraestructura de Redes:** El acceso a Internet, las redes Wi-Fi escolares y la seguridad perimetral (firewalls, filtros).
- **Sistemas de Gestión Educativa (LMS**): Plataformas como Moodle, Google Classroom o sistemas internos para la administración de calificaciones, horarios y materiales didácticos.
- **Dispositivos:** Los equipos de cómputo en laboratorios, tabletas o laptops institucionales, y la gestión de los dispositivos personales de los estudiantes (BYOD - Bring Your Own Device) cuando se permite su uso en la red escolar.
- **Canales de Comunicación:** Correo electrónico institucional, plataformas de videoconferencia y otros canales oficiales de difusión de información.

Rol del Entorno en la Ciberseguridad:

1. **Zona de Riesgo Controlado:** El entorno es el principal punto donde los estudiantes acceden a la red. Si la red es vulnerable, el riesgo de infecciones de malware o accesos no autorizados a datos se incrementa.
2. **Laboratorio de Buenas Prácticas:** La configuración de la red escolar (ej. obligatoriedad de contraseñas fuertes, filtros de contenido inapropiado) es la primera oportunidad para que los estudiantes experimenten y adopten prácticas de seguridad robustas.
3. **Protección de Datos:** El entorno es el custodio de la información personal y académica de los estudiantes.

Políticas Institucionales de Ciberseguridad

Las políticas institucionales son el conjunto de normas, procedimientos y directrices formalmente adoptadas por la escuela o el sistema educativo para gestionar y proteger sus activos digitales, así como para regular el comportamiento de los usuarios. Estas políticas son esenciales porque establecen las expectativas de comportamiento y las consecuencias del incumplimiento; tales como:

- **Política de Uso Aceptable (PUA).** Son reglas que definen el uso permitido de los recursos tecnológicos, incluyendo internet, correo y equipos. Lo cual implicaría en los estudiantes prohibir la descarga de software no autorizado o el acceso a sitios web inapropiados o maliciosos.
- **Política de Contraseñas**. Establece los requisitos mínimos de longitud, complejidad y frecuencia de cambio de las contraseñas institucionales. Lo cual, obliga al uso de contraseñas robustas y a no compartirlas.
- **Política de Privacidad y Protección de Datos.** Describe cómo la institución recolecta, usa, almacena y protege los datos personales (ej. calificaciones, direcciones, historiales médicos). Generando una conciencia sobre el valor de sus datos y la necesidad de su protección.
- **Política Anti-acoso (Ciberacoso).** Define y sanciona el acoso o la intimidación digital dentro o fuera del entorno escolar que afecte a la comunidad. Fomentando el uso ético y responsable de las comunicaciones digitales.
- **Política de Respuesta a Incidentes.** Establece los pasos a seguir ante un evento de seguridad (ej. detección de malware, robo de información, phishing). Indicando a quién y cómo reportar una vulneración o un ataque cibernético.

Políticas Institucionales de Ciberseguridad de la UAEH

Las políticas institucionales de la Universidad Autónoma del Estado de Hidalgo (UAEH), especialmente aquellas relacionadas con la tecnología y los sistemas de información, buscan garantizar la seguridad, integridad y uso adecuado de sus recursos digitales por parte de toda la comunidad universitaria (funcionarios, docentes, investigadores, no-docentes y estudiantes).

Estas políticas están centralizadas principalmente a través de la Dirección de Información y Sistemas (DIS) y establecen un marco de acción para proteger los activos informáticos y la información.

Política General para el Uso Adecuado de Tecnología de Información y Comunicaciones

Esta política es el eje rector y su alcance se extiende a todos los usuarios de la UAEH, incluyendo a los estudiantes. Sus objetivos principales son:

- **Preservar la Integridad:** Mantener la información segura y contrarrestar interrupciones en las actividades críticas de la universidad, alineándose

con estándares internacionales de seguridad.

- **Control de Acceso:** Controlar el acceso a la información y a las instalaciones de activos informáticos y de comunicaciones.
- **Reducción del Riesgo Humano:** Utilizar los sistemas de información de manera segura para reducir el riesgo de error humano y prevenir pérdida, robo, abuso o modificación de software o datos.
- **Cumplimiento Legal y Ético:** Evitar infringir cualquier norma civil o penal, ley, obligación contractual, o cualquier reglamento sobre el uso de la información y derechos de autor.

Lineamientos Aplicables a los Sistemas de Información

En el contexto de los estudiantes de Educación Media Superior (Preparatorias de la UAEH), los lineamientos de uso de los sistemas son cruciales:

1. **Uso Institucional Exclusivo:** Los Sistemas de Información y herramientas asociadas (como el correo electrónico y el acceso a Internet) son propiedad de la UAEH y solo deben utilizarse para fines estrictamente institucionales.
2. **Autorización:** El uso de estos recursos solo está permitido para el personal y los estudiantes debidamente autorizados (a través de sus cuentas institucionales).
3. **Seguridad y Privacidad:** Se exige el uso responsable del software, evitando actividades que comprometan la seguridad de la red o la privacidad de otros usuarios. Esto incluye:
    - Evitar la descarga de archivos maliciosos o el acceso a sitios web no seguros.
    - Reportar inmediatamente cualquier situación de riesgo o incidente de seguridad al personal responsable (como el personal del Centro Integral de Servicios Académicos o CISA).

Lineamientos de Uso en Áreas Específicas (CISA)

Los lineamientos de uso de espacios físicos y tecnológicos, como los Centros Integrales de Servicios Académicos (CISA), refuerzan las políticas de ciberseguridad a nivel operativo:

- **Uso de Dispositivos Personales (BYOD):** Se permite su uso, pero la institución no se responsabiliza por la pérdida, daño o robo de dispositivos personales, lo que fomenta la responsabilidad individual en la protección física y digital.
- **Reporte de Fallas:** Cualquier daño o mal funcionamiento de equipos debe reportarse de inmediato.
- **Conducta Digital:** Se prohíben conductas como el acoso o la discriminación que vulneren los derechos de otros usuarios, extendiendo la ética digital al entorno físico.

La UAEH ha establecido una Política General de Uso de TIC que abarca desde la protección técnica de sus sistemas hasta la regulación del comportamiento de sus usuarios. Para los estudiantes, esto se traduce en una obligación de usar los recursos tecnológicos de manera segura, ética y estrictamente institucional, con énfasis en el reporte de incidentes y el cuidado de los activos de información.

Marco Jurídico y Responsabilidad Legal en México

La ciberseguridad en el entorno escolar no opera en un vacío legal. Es imperativo que tanto estudiantes como docentes comprendan que las conductas en el ciberespacio tienen consecuencias penales en el mundo físico. En México, el marco normativo se ha endurecido significativamente en los últimos años para proteger la integridad digital.

La "Ley Olimpia" y la Violencia Digital

Un componente crítico en la educación de los estudiantes de EMS es el conocimiento de la llamada "Ley Olimpia" (un conjunto de reformas al Código Penal Federal y leyes estatales). Esta normativa tipifica como delito la violación a la intimidad sexual, sancionando la difusión, producción o almacenamiento de contenido íntimo sin consentimiento (sexting no consentido o packs).

En el contexto escolar, es común que los estudiantes compartan estos contenidos "como broma" o presión social, desconociendo que están cometiendo un delito que puede conllevar penas de prisión y antecedentes penales, incluso para menores de edad bajo el sistema de justicia para adolescentes.

Protección de Datos Personales

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (aplicable a universidades públicas como la UAEH) establecen el derecho a la privacidad. Las instituciones educativas son garantes de los datos biométricos, académicos y patrimoniales de los alumnos. Cualquier vulneración de seguridad que exponga esta información (por ejemplo, publicar listas de calificaciones con nombres completos en redes sociales abiertas) constituye una violación a la normativa que puede derivar en sanciones administrativas para la institución y el personal.

Integrar el conocimiento de estas leyes en el currículo no es solo una medida preventiva, sino una estrategia de formación ciudadana. El estudiante debe transitar de ser un usuario pasivo a un sujeto de derechos y obligaciones digitales.

Resultados: Análisis Cuantitativo de Vulnerabilidades en el Ciberentorno

En base al análisis de la literatura revisada y los informes especializados permitió identificar tendencias consistentes sobre los riesgos y vulnerabilidades que enfrentan los estudiantes de Educación Media Superior en materia de ciberseguridad. A continuación, se presentan los hallazgos basados en métricas globales y regionales:

En primer lugar, se observa una susceptibilidad significativa ante el **phishing** y la **ingeniería social**. Un informe internacional encabezado por el University College London señala que aproximadamente uno de cada cinco adolescentes evaluados en contextos de vulnerabilidad socioeducativa mostró alta probabilidad de caer en fraudes digitales, debido principalmente a la sobreconfianza y la falta de criterios de verificación. La Organización para la Cooperación y el Desarrollo Económicos (OECD), en su informe 21st-Century Readers (2021), evidenció una carencia educativa estructural. Al evaluar la capacidad de estudiantes de 15 años para distinguir hechos de opiniones y detectar correos maliciosos (phishing), los resultados fueron preocupantes:

"En promedio, en los países de la OCDE, solo el 54% de los estudiantes informó haber recibido capacitación en la escuela sobre cómo reconocer si la información es sesgada o subjetiva" (OECD, 2021).

Esto valida la hipótesis de que las instituciones educativas no están cumpliendo su rol de barrera de contención preventiva.

En cuanto a la **intensidad de Uso y Redes Sociales.** La posibilidad de ataques se amplía con el tiempo de exposición. Common Sense Media (2021), en su censo sobre el uso de medios, reportó un crecimiento sin precedentes en el uso de pantallas tras la pandemia:

"El uso de medios de entretenimiento en pantalla creció un 17% entre los adolescentes (de 13 a 18 años) entre 2019 y 2021... llegando a una media de 8 horas y 39 minutos diarios" (Common Sense, 2021).

Además, el informe destaca que el 84% de los adolescentes utiliza redes sociales, espacios donde la supervisión parental y docente es mínima.

Respecto a la **gestión de contraseñas**, diversos estudios confirman que las prácticas inseguras son comunes entre jóvenes. El reporte “World Password Day 2025” de Bitwarden indica que cerca del 70 % de la Generación Z reutiliza contraseñas en múltiples servicios digitales, lo que incrementa la exposición ante ataques de relleno de credenciales. Estos datos coinciden con encuestas históricas realizadas por Google y Enzoic, que muestran patrones similares.

En cuanto a la **exposición de información personal en redes sociales**, los datos del Pew Research Center muestran que más del 95 % de los adolescentes utiliza Internet diariamente, y una gran proporción comparte fotografías, contenido personal o información sensible en plataformas sociales. Informes como el Common Sense Census confirman que los adolescentes interactúan con redes sociales a edades cada vez más tempranas, con poca revisión de configuraciones de privacidad.

Y hablando de la **civilidad digital**, la inmersión digital de los estudiantes es casi total, pero el entorno es hostil. Según el Global Online Safety Survey de Microsoft (2023), que evalúa el estado de la civilidad digital, el 69% de los encuestados a nivel global experimentó algún riesgo en línea en el último año. El informe detalla que:

"Los riesgos más comunes encontrados fueron la desinformación, con un 50%, seguidos por riesgos personales como el discurso de odio y el acoso, que afectaron a un 47% de los usuarios" (Microsoft, 2025).

Esta cifra subraya que la mayoría de los estudiantes de EMS navegan en un ecosistema donde la probabilidad de encuentro con amenazas es la norma, no la excepción.

Otra incidencia es el **Ciberacoso** y **Violencia Digital.** La violencia entre pares ha migrado al entorno virtual. UNICEF (2022) advierte sobre la normalización de la violencia digital, señalando que, en 30 países encuestados, 1 de cada 3 jóvenes reportó haber sido víctima de ciberacoso. Microsoft (2025) violencia digital está en un 37%, mientras que los riesgos sexuales entre 20% y 23%.

A nivel regional, el Instituto Nacional de Ciberseguridad de España (INCIBE) reportó en su balance de 2023 cifras récord que reflejan la magnitud del problema en el ámbito hispanohablante:

"INCIBE gestionó 118.820 incidentes de ciberseguridad durante el año, de los cuales un porcentaje significativo afectó a la ciudadanía y a menores, destacando el fraude online y el contenido abusivo" (INCIBE, 2024).

Respecto a las **amenazas técnicas (Ransomware y Malware). L**a Agencia de la Unión Europea para la Ciberseguridad (ENISA) en su Threat Landscape Report (2023), identifica que el sector educativo es un objetivo prioritario para los ciberdelincuentes debido a la gran cantidad de datos personales que maneja (PII):

"El sector de la administración pública y la educación experimentó el 19% de todos los ataques de ransomware dirigidos reportados a nivel global" (ENISA, 2023).

Estos datos confirman que la Educación Media Superior enfrenta una "tormenta perfecta": alta exposición (Common Sense), riesgos elevados (Microsoft), objetivos vulnerables (ENISA) y escasa preparación educativa (OECD).

En el **ámbito institucional**, los reportes de organizaciones como MS-ISAC, CIS y CoSN indican que una proporción significativa de escuelas carece de planes documentados de respuesta a incidentes. En estudios recientes, entre el 30 % y el 40 % de los centros educativos reportaron no contar con protocolos formales, mientras que otros informes documentan una alta incidencia de ataques sin

una estructura institucional adecuada para afrontarlos.

Finalmente, los datos del State of Cybersecurity Education Report elaborado por CYBER.ORG y el EdWeek Research Center revelan una brecha clara entre uso y formación digital. Aunque el uso diario de Internet entre adolescentes es prácticamente universal, menos de la mitad de las instituciones educativas reportan impartir formación sistemática en ciberseguridad. Esta asimetría evidencia un desfase crítico entre la intensidad del uso tecnológico y la adquisición de competencias de seguridad digital.

Estrategias de Fortalecimiento Institucional y Curricular en Ciberseguridad

A partir de los hallazgos evidenciados en el diagnóstico de competencias, se articula una propuesta integral de intervención. Esta propuesta no se limita a la implementación de talleres aislados, sino que plantea una reingeniería en la forma en que la Educación Media Superior (EMS) aborda la seguridad digital. La estrategia se estructura en cuatro ejes fundamentales: transversalidad curricular, formación docente, metodologías activas y gobernanza institucional.

Eje 1: Transversalidad Curricular (El Enfoque Holístico)

La ciberseguridad no debe relegarse a una asignatura optativa de informática. Dada la naturaleza ubicua de la tecnología, se propone su integración transversal en el Marco Curricular Común (MCC). Esto implica que las competencias de seguridad se desarrollen a través de diversas áreas del conocimiento:

- **Matemáticas y Pensamiento Lógico:** Se sugiere la enseñanza de conceptos de criptografía básica, probabilidad y combinatoria aplicados a la fortaleza de contraseñas. El estudiante debe comprender matemáticamente por qué una contraseña de 6 caracteres es vulnerable a un ataque de fuerza bruta en comparación con una de 12.
- **Ética y Ciencias Sociales:** Abordaje de dilemas éticos digitales, privacidad como derecho humano, legislación de protección de datos y las consecuencias sociales del ciberacoso y la desinformación (fake news).
- **Lectura y Redacción:** Análisis crítico del discurso para la detección de ingeniería social. Se busca desarrollar habilidades lingüísticas que permitan al estudiante identificar inconsistencias semánticas y sintácticas en correos de phishing o mensajes fraudulentos.

Eje 2: Profesionalización y Actualización Docente

Uno de los hallazgos críticos es la brecha generacional y técnica entre docentes y estudiantes. Para fortalecer la EMS, es imperativo implementar un programa de "**Formación de Formadores en Ciberhigiene**".

El docente no necesita ser un experto en programación, pero sí un gestor de riesgos competente. La propuesta incluye:

1. **Capacitación Continua:** Cursos semestrales sobre las últimas amenazas (ransomware, estafas en redes sociales emergentes).
2. **Protocolos de Respuesta:** Dotar al profesorado de guías claras sobre cómo actuar si un alumno reporta un caso de sexting o ciberacoso, vinculando la acción pedagógica con el apoyo psicológico y legal.
3. **Cambio de Rol:** El docente pasa de ser un transmisor de información técnica a un mediador de la cultura digital, guiando a los estudiantes en el uso ético de las herramientas que ya dominan operativamente.

Eje 3: Implementación de Metodologías Activas (Gamificación)

La enseñanza tradicional teórica resulta ineficaz para la ciberseguridad, un campo dinámico y práctico. Se propone la adopción de la **Gamificación** y el **Aprendizaje Basado en Retos (ABR)** como estrategias didácticas centrales.

- **Capture The Flag (CTF**): Organización de competiciones internas tipo CTF, donde los estudiantes deben resolver retos de seguridad (encontrar vulnerabilidades simuladas, descifrar códigos) en un entorno controlado y seguro. Esto canaliza la curiosidad técnica hacia la defensa ética (Blue Teaming) en lugar del ataque malicioso.
- **Simulacros de Phishing:** Realización de campañas de phishing ético institucional. La escuela envía correos falsos simulados a los alumnos; aquellos que hacen clic no son castigados, sino redirigidos automáticamente a una micro-lección ("Momento de aprendizaje") que les explica su error en tiempo real.

Eje 4: Gobernanza y Ecosistema de Seguridad Escolar

El fortalecimiento de la EMS requiere que la institución misma sea un modelo de seguridad. No se puede enseñar seguridad en una red escolar vulnerable.

- **Políticas de Uso Aceptable (AUP):** Definición clara de las reglas del juego para el uso de la red escolar y dispositivos personales (BYOD). El estudiante debe firmar y comprender un contrato de ciudadanía digital al inicio del ciclo escolar.
- **Vinculación con Padres de Familia:** Dado que gran parte de la actividad digital ocurre fuera del horario escolar, se propone la creación de la "Escuela para Padres Digitales", talleres bimestrales para alinear las estrategias de supervisión en el hogar con las de la escuela.
- **Infraestructura Resiliente:** Inversión en filtrado de

contenido y seguridad perimetral en las redes de las escuelas, garantizando que el entorno de aprendizaje proteja a los menores de contenidos nocivos.

La implementación de estos cuatro ejes transforma a la escuela de un mero proveedor de acceso a internet a un entorno de inmunidad digital. El objetivo final es desarrollar en el estudiante la "Resiliencia Cibernética": la capacidad no solo de resistir ataques, sino de recuperarse, aprender y adaptarse a un entorno tecnológico hostil y cambiante.

Conclusiones

La presente investigación confirma que la ciberseguridad en la Educación Media Superior constituye un desafío pedagógico, institucional y social que exige una intervención estructural. Aunque el estudiantado demuestra una competencia operativa elevada en el uso cotidiano de tecnologías digitales, esta habilidad no se acompaña de una madurez equivalente en prácticas de protección. Persiste una brecha significativa entre la familiaridad técnica y la capacidad para comprender y gestionar riesgos vinculados con amenazas como el malware, el phishing, el ciberacoso, el grooming y la sextorsión. Esta situación refleja una vulnerabilidad doble: cognitiva, por la subestimación del riesgo, y formativa, por la ausencia de una alfabetización digital orientada a la seguridad.

Los hallazgos evidencian que la gobernanza institucional, si bien indispensable, no es suficiente para consolidar una cultura de seguridad digital. La existencia de políticas, lineamientos o normativas —como las implementadas por la UAEH— constituye solo la base de un proceso que requiere la participación activa del estudiantado y del personal docente. La ciberseguridad escolar no se fortalece únicamente mediante restricciones o controles técnicos, sino a través del desarrollo del criterio personal, el pensamiento crítico y la conciencia situacional.

En este sentido, la propuesta basada en cuatro ejes estratégicos: transversalidad curricular, profesionalización docente, metodologías activas y gobernanza institucional, representa una ruta pertinente para articular la ciberseguridad como una competencia de vida. La integración de contenidos de seguridad digital en diversas asignaturas, el uso de experiencias prácticas como la gamificación, y la capacitación continua del profesorado contribuyen a reducir la brecha generacional y a promover aprendizajes significativos.

Finalmente, el estudio concluye que la construcción de resiliencia cibernética debe consolidarse como un objetivo formativo prioritario en la EMS. La resiliencia no solo implica prevenir incidentes, sino comprenderlos, afrontarlos y aprender de ellos. Este enfoque integral permite que la tecnología sea un medio para el desarrollo personal, académico y social, y no un factor de riesgo. De esta manera, se reafirma que la ciberseguridad es, ante todo, una responsabilidad compartida que debe integrarse de forma permanente en la práctica educativa y en la vida digital del estudiantado. Solo a través de la capacitación docente continua y la implementación de metodologías activas (como simulacros y gamificación) se podrá construir una ciudadanía digital responsable, capaz de transitar de la vulnerabilidad a la resiliencia en un ciberentorno cada vez más complejo.

References

Aldawood, H., & Skinner, G. (2019). *Reviewing cyber security social engineering training and awareness programs*—Pitfalls and ongoing issues. Future Internet, 11(3), 73. https://doi.org/10.3390/fi11030073

Álvarez-García, D., Núñez, J., Pérez, J. C., & Torres, J. (2022). *Risk perception and digital security behaviors in adolescents.* Computers & Education, 185, 104524.

Berríos, L., & Luengo, R. (2020). *Alfabetización digital crítica en contextos escolares.* Revista Latinoamericana de Tecnología Educativa, 19(2), 45–60.

Bond, E. (2020). *Childhood, mobile technologies and everyday experiences: Changing technologies = changing childhoods*? Palgrave Macmillan.

Cámara de Diputados del H. Congreso de la Unión. (2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Última Reforma DOF 2017. Gobierno de México.

CISA. (2023). K–12 *Cybersecurity Report*. Cybersecurity and Infrastructure Security Agency.

Common Sense Media. (2019). *The Common Sense census: Media use by tweens and teens.* Common Sense.

Common Sense Media. (2021). *The Common Sense Census: Media Use by Tweens and Teens, 2021*. Common Sense. https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens-2021

Diario Oficial de la Federación (DOF). (2021, 1 de junio). Decreto por el que se adiciona un artículo 199 Octies al Código Penal Federal (Ley Olimpia). Secretaría de Gobernación. https://www.dof.gob.mx/#gsc.tab=0

ENISA. (2021). *Cybersecurity and digital skills in education.* European Union Agency for Cybersecurity.

ENISA. (2023). *Cybersecurity Threat Landscape.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

ESET Latinoamérica. (2020). *Seguridad digital en jóvenes: Informe* 2020. ESET.

European Commission. (2022). DigComp *2.2: The Digital Competence Framework for Citizens.* Publications Office of the European Union.

FBI. (2023). Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations. Federal Bureau of Investigation, Cyber Division.

Fleming, L., & Rickwood, D. (2020). *Adolescent online behavior and the risk of cyber victimization.* School Psychology International, 41(5), 391–410.

García-Peñalvo, F. (2021). *Competencias digitales en la educación media.* Education in the Knowledge Society, 22, e23916.

Google & UNESCO. (2021). *Be Internet Awesome: Curriculum for developing safe digital habits.* UNESCO.

INAI. (2022). Guía para el Tratamiento de Datos Biométricos. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. https://home.inai.org.mx/

INCIBE. (2022). *Ciberseguridad en centros educativos: Guía integral.* Instituto Nacional de Ciberseguridad.

INEGI. (2023). *Estadísticas sobre disponibilidad y uso de*

tecnologías en adolescentes. Instituto Nacional de Estadística y Geografía.

INTERPOL. (2021). *Online child exploitation and cyber risks during the COVID-19 pandemic.* INTERPOL.

ITU. (2020). *Guidelines on Child Online Protection 2020.* International Telecommunication Union.

Livingstone, S., & Third, A. (2020). *Children and digital technologies: Risks, opportunities and rights.* London School of Economics / UNICEF.

Microsoft. (2022). *Digital Civility Index 2022*. Microsoft Corporation.

Microsoft. (2025). *Global Online Safety Survey.* Microsoft Digital Civility Index. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Global-Online-Safety-Survey-Summary-Infographic.pdf

NCSA. (2019). *CyberSecure Teens Report.* National Cyber Security Alliance.

OECD. (2021). *21st-century digital skills and cybersecurity education.* OECD Publishing. https://www.oecd.org/en/publications/21st-century-readers_a83d84cb-en.html

Pérez-Escoda, A., García-Ruiz, R., & Aguaded, I. (2022). *Digital and media literacy among adolescents: An international review.* Comunicar, 30(70), 9–20.

Sensity AI. (2024). *The State of Deepfakes: Landscape, Threats, and Impact.* Sensity Intelligence Reports. https://sensity.ai/reports/

Steinberg, L. (2010). A Social Neuroscience Perspective on Adolescent Risk-Taking. Developmental Review, 28(1), 78–106.https://www.sciencedirect.com/science/article/abs/pii/S0273229707000536?via%3Dihub

UNESCO. (2020). *Education in a post-COVID world: Nine ideas for public action.* UNESCO.

UNESCO. (2021). *Digital citizenship education: Overview and framework.* UNESCO Publishing.

Universidad Autónoma del Estado de Hidalgo (UAEH). (s.f.). Política General para el Uso Adecuado de Tecnología de Información y Comunicaciones. Dirección de Información y Sistemas.