MINISTERIO DE EDUCACIÓN PÚBLICA | GOBIERNO DE COSTA RICA

unicef
para cada infancia

RECOMENDACIONES PARA EL ABORDAJE DE LA SEGURIDAD DIGITAL

STEAM

Esta obra ha sido publicada gracias al patrocinio de UNICEF Costa Rica, para la iniciativa “Voces de cambio: hacia entornos educativos seguros y resilientes” del Ministerio de Educación Pública de Costa Rica.

Ministerio de Educación Pública de Costa Rica.

Departamento de Orientación Educativa y Vocacional, DVE (Unidad ejecutora de la estrategia nacional de educación STEAM).

Departamento de Tercer Ciclo y Educación Diversificada, DDC.

Dirección de Recursos Tecnológicos en Educación.

Dirección de Asuntos Internacionales y Cooperación.

Comisión Nacional de Educación STEAM, MEP.

Producción educativa: EduTech de Centroamérica

Diseño y maquetación: EduTech de Centroamérica

Primera edición: octubre, 2025

Tabla de contenido

Introducción 4

La importancia de la seguridad digital como parte de la ciudadanía digital y la formación integral 6

I. Marco conceptual 11

- Definiciones clave 12
- Principios rectores 20

II. Riesgos comunes por nivel educativo 26

- Personas estudiantes de preescolar y primaria 26
- Personas estudiantes de secundaria 29
- Personas jóvenes y adultas 33

III. Recomendaciones pedagógicas diferenciadas por nivel educativo 38

- Actividades sugeridas por nivel 38
- Ciudadanía digital, seguridad y bienestar en la educación 68
- Recursos digitales recomendados 75

IV. Señales de riesgo en la conducta digital educativa 77

- Cambios de comportamiento y consecuencias en el bienestar 78
- Uso de dispositivos, contenido inapropiado y la privacidad 79
- ¿Cómo actuar en caso de incidentes? 81
- Casos hipotéticos 85

Anexos 87

- Plantilla de planificación con enfoque de seguridad digital 87
- Glosario 89
- Material visual adicional 90

Referencias bibliográficas 94

Introducción

El presente documento de orientaciones para el abordaje de la seguridad digital nace del compromiso interinstitucional establecido entre el Ministerio de Educación Pública (MEP) y el Fondo de Naciones Unidas para la Infancia (UNICEF) en Costa Rica, orientado a robustecer entornos educativos que sean seguros, inclusivos y resilientes para toda la comunidad estudiantil. Este esfuerzo ha conducido a la priorización de intervenciones educativas que contribuyen activamente a la prevención de distintas formas de violencia y al fortalecimiento de competencias fundamentales para la vida.

En el contexto de la iniciativa "**Voces de cambio: hacia entornos educativos seguros y resilientes**" se reconoce la importancia de dotar a las personas estudiantes de herramientas socioemocionales, comunicativas, cognitivas y ciudadanas, necesarias para afrontar los desafíos del siglo XXI y participar plenamente en la construcción de espacios de respeto y convivencia.

Como respuesta a estas necesidades, el documento de orientaciones ofrece un amplio detalle de las recomendaciones claras y aplicables para abordar la seguridad digital en la educación. Este documento técnico-pedagógico, está dirigido a las personas docentes que laboran en los diferentes niveles educativos y tiene como finalidad brindar una guía para el abordaje de la seguridad digital en el ambiente de aprendizaje.

En concordancia con los compromisos nacionales e internacionales para una educación de calidad, equitativa y pertinente, la Estrategia Nacional de Educación STEAM liderada por el MEP articula los objetivos de la Agenda 2030 y el ODS 4, promoviendo que la persona estudiante sea protagonista de su aprendizaje y agente de transformación social. Este modelo de inmersión se implementa en los distintos niveles educativos y se distingue por potenciar habilidades, autoeficacia vocacional, toma de decisiones informadas y colaborativas, con equidad de género y atención a la diversidad territorial y cultural.

Por todo lo anterior, el presente documento pretende cumplir a cabalidad con el marco teórico y normativo de la estrategia de Educación STEAM del Ministerio de Educación Pública de Costa Rica, el proyecto “Voces de Cambio” y la Política Nacional de Niñez y Adolescencia.

Este documento ha sido desarrollado a partir de una amplia variedad de fuentes nacionales e internacionales vigentes que desarrollan ampliamente el tema de la seguridad educativa y se orientan por el enfoque de derechos. Para su elaboración, se realizó una investigación documental, con la herramienta NotebookLM de Google como apoyo a la sistematización, análisis y síntesis de la información.

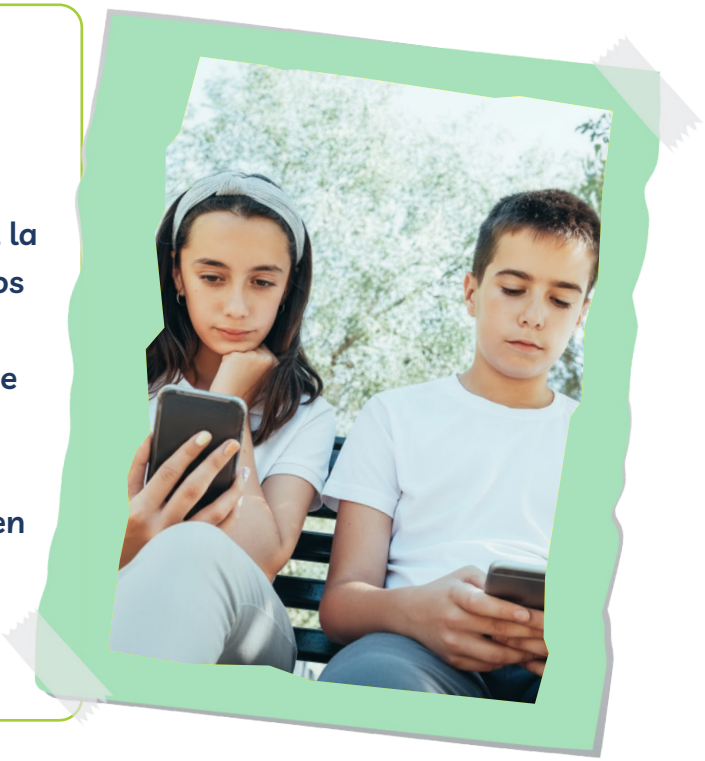
1 LA IMPORTANCIA DE LA SEGURIDAD DIGITAL COMO PARTE DE LA CIUDADANÍA DIGITAL Y LA FORMACIÓN INTEGRAL

En una sociedad cada vez más mediada por tecnologías digitales, la formación en seguridad digital se ha convertido en un eje transversal para el ejercicio pleno de la ciudadanía.

La digitalización de la vida cotidiana, incluida la educación, ha abierto múltiples oportunidades, pero también ha expuesto a las personas usuarias, especialmente a personas estudiantes, a riesgos importantes relacionados con la privacidad, la seguridad de la información y la exposición a amenazas en línea. Por ello, la seguridad digital no puede verse únicamente como una habilidad técnica, sino como un componente esencial dentro de una ciudadanía digital crítica, ética y responsable (Capuno et al., 2022).

Este tema constituye uno de los elementos fundamentales de la ciudadanía digital. No se trata únicamente de proteger los datos personales, sino también de promover comportamientos adecuados y éticos en los espacios virtuales (Capuno et al., 2022). Desde el ámbito educativo, formar en seguridad digital implica enseñar a gestionar la identidad digital, cuidar la información personal y aplicar buenas prácticas de protección. Algunas de estas prácticas incluyen el uso de contraseñas seguras, la verificación de sitios web confiables y la protección de dispositivos personales (Guevara-Andino & Delgado-Salas, 2024). Por definición, "la seguridad digital implica que el uso de Internet por parte del individuo no afecte negativamente otras partes de su vida" (Capuno et al., 2022), lo cual evidencia la dimensión ética y preventiva de esta competencia.

Además, la seguridad digital cumple un rol clave en la prevención de distintas formas de violencia digital, como el ciberacoso, el fraude, el grooming, la desinformación o la exposición a contenidos inapropiados. Estas amenazas no solo vulneran derechos fundamentales, sino que también afectan el bienestar emocional y psicológico de las personas estudiantes. Si no se abordan de manera oportuna, pueden comprometer su desarrollo integral y perjudicar su trayectoria académica.

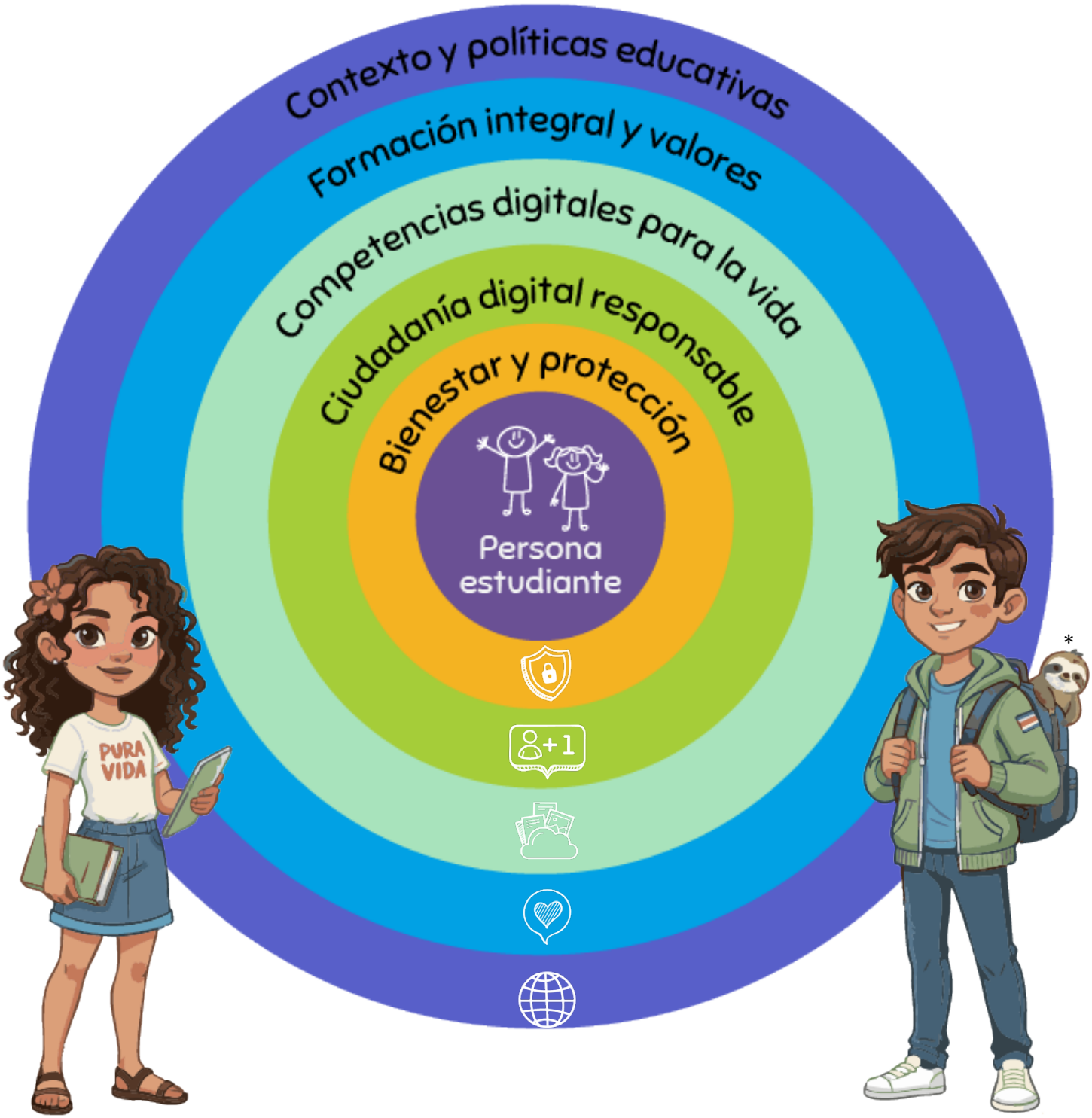


En este contexto, la normativa vigente del Ministerio de Educación Pública de Costa Rica reconoce que la violencia digital puede tener consecuencias psicoemocionales significativas.

Por esta razón, establece mecanismos claros de prevención, detección, intervención y acompañamiento, con el fin de proteger el bienestar estudiantil y fomentar un entorno educativo más seguro.

El siguiente diagrama sintetiza las diversas dimensiones y los temas que se deben considerar para abordar con las personas estudiantes la seguridad digital en los centros educativos costarricenses.

Diagrama 1
¿Dimensiones a considerar para enseñar seguridad digital en los centros educativos?



* El perezoso, símbolo nacional de la fauna silvestre de Costa Rica (Ley N.° 10007, 2021). Su uso en este material tiene fines educativos y de sensibilización ambiental.

Persona estudiante

- El eje central del proceso educativo y de la formación en seguridad digital.
- Todo lo demás gira en torno a su bienestar, desarrollo y protección.

Bienestar y protección

¿Qué representa?

Los motivos inmediatos y más personales para enseñar seguridad digital.

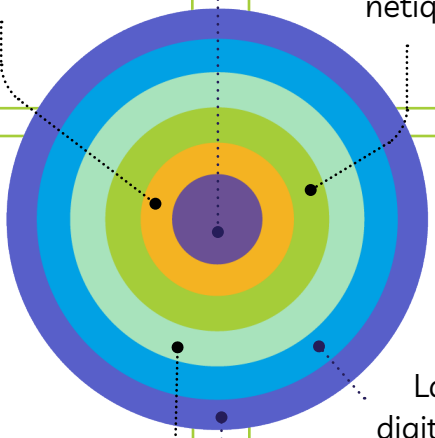
- Prevención del ciberacoso, grooming, fraude y desinformación.
- Protección emocional y psicológica.
- Generación de entornos digitales seguros.

Ciudadanía digital responsable

¿Qué representa?

La dimensión ética, crítica y participativa del uso digital.

- Uso responsable de la tecnología.
- Comportamiento ético en línea.
- Conocimiento de derechos, deberes, netiqueta y obligaciones digitales.



Competencias digitales para la vida

¿Qué representa?

Las habilidades prácticas que las personas estudiantes deben desarrollar.

- Gestión de la identidad digital.
- Protección de datos personales.
- Uso de contraseñas seguras.
- Identificación de sitios confiables.
- Manejo seguro de dispositivos.

Formación integral y valores

¿Qué representa?

La contribución de la seguridad digital al desarrollo completo de la persona estudiante.

- Autonomía y autocuidado.
- Pensamiento crítico.
- Toma de decisiones informadas.
- Respeto, empatía y convivencia digital.

Contexto y políticas educativas ¿Qué representa?

El marco institucional y social que respalda su enseñanza.

- Protocolo de actuación ante acoso cibernético (MEP).
- Transformación digital de la sociedad y la educación.
- Demandas del entorno actual.
- Rol del centro educativo como espacio preventivo y formativo.

Desde una perspectiva tanto pedagógica como institucional, integrar la seguridad digital en los procesos educativos no solo responde a una necesidad urgente, sino que también representa una estrategia clave para transformar la cultura educativa y proteger los derechos de niñas, niños y adolescentes. Así como también, de personas estudiantes adultas de la educación formal.
Esta integración permite construir entornos de aprendizaje más seguros, éticos y acordes con los desafíos del mundo digital.

De acuerdo con el Modelo para la Inclusión de las Tecnologías Digitales en Educación (MITDE), propuesto por el Ministerio de Educación Pública de Costa Rica, esta tarea implica varios compromisos importantes:

- Asegurar la formación continua del personal docente en competencias digitales.
- Establecer protocolos claros a nivel institucional para el uso seguro y responsable de la tecnología.
- Promover una cultura de corresponsabilidad entre personas estudiantes, personas docentes, familias y comunidades educativas, en relación con el uso de las tecnologías.

En el contexto costarricense actual, donde la política educativa impulsa activamente el uso reflexivo, ético y democrático de las tecnologías digitales, la seguridad digital se reconoce como un derecho fundamental y una responsabilidad colectiva. Su promoción es indispensable para proteger los derechos de las población infantil y juvenil, fomentar la participación ciudadana en entornos digitales y contribuir al desarrollo de una cultura educativa más inclusiva, crítica y segura.

2 MARCO CONCEPTUAL

Este marco conceptual ofrece una base clara y fundamentada para comprender la ciudadanía digital dentro del ámbito educativo. En un contexto donde las tecnologías digitales están cada vez más presentes en la vida personal, social y educativa, es necesario conocer los conceptos clave que permiten una participación segura, crítica y responsable en los entornos digitales. Además, se busca alinear este enfoque con principios de derechos, equidad y seguridad, en sintonía con los desafíos actuales de la transformación digital en la educación costarricense y las políticas públicas que promueven entornos educativos inclusivos, seguros y éticos.

1. Definiciones clave

La creciente presencia de las tecnologías digitales (TD) en la vida diaria y en los espacios educativos plantea nuevas necesidades formativas. Para acompañar adecuadamente a la persona estudiante, es necesario que el personal docente conozca ciertos conceptos fundamentales que favorecen una convivencia sana, ética y segura en los entornos digitales.

A continuación, en el siguiente diagrama se presentan siete conceptos centrales, junto con su definición y sus principales implicaciones educativas: ciudadanía digital, seguridad digital, autocuidado digital, huella digital, privacidad, ciberacoso y desinformación.

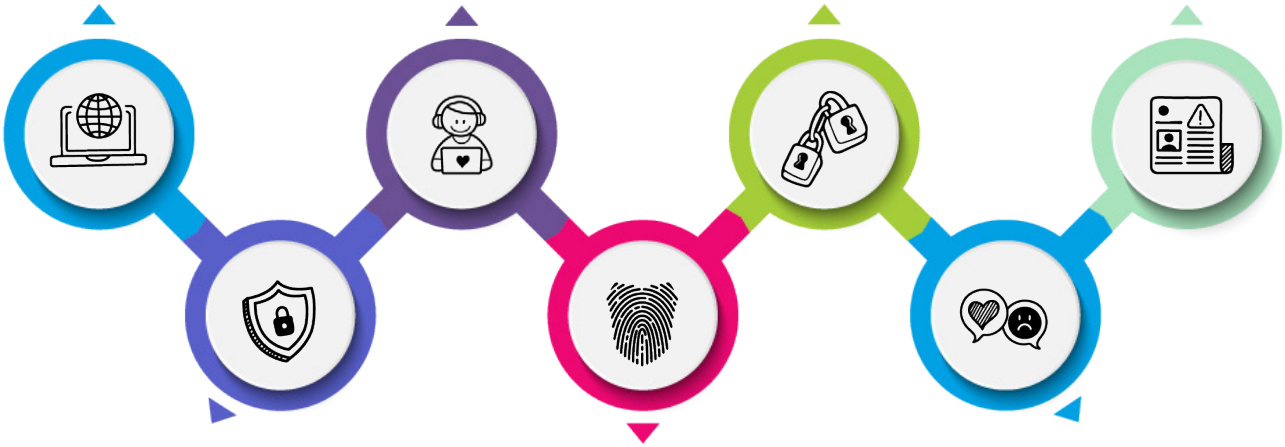
Diagrama 2. Definiciones clave

Ciudadanía digital
Capacidad para participar en entornos digitales de forma ética, crítica y responsable.

Autocuidado digital
Habilidades para prevenir riesgos, protegerse emocionalmente y mantener el bienestar digital.

Privacidad
Derecho a controlar la información personal y decidir cómo, cuándo y con quién se comparte.

Desinformación
Difusión de información falsa o engañosa que busca confundir, manipular o afectar decisiones.



Seguridad digital
Conjunto de prácticas para proteger dispositivos, datos personales y actividades en línea.

Huella digital
Registro que dejamos al interactuar en internet, que puede influir en nuestra identidad y reputación.

Ciberacoso
Forma de violencia ejercida a través de medios digitales que causa daño psicológico o emocional.

a. Ciudadanía digital

La ciudadanía digital hace referencia a las habilidades, conocimientos y actitudes necesarias para participar de forma activa, crítica, ética y responsable en los espacios digitales (Gutiérrez-Aguilar et al., 2024). Esto implica la capacidad de comunicarse, informarse, colaborar y crear contenido de manera segura y respetuosa, comprendiendo el impacto de la tecnología en la vida cotidiana y ejerciendo plenamente los derechos digitales. Tal como lo establece la normativa vigente, también conlleva el ejercicio de derechos y el cumplimiento de responsabilidades en los entornos virtuales, concibiendo internet como un espacio público.

En el ámbito educativo, educar en ciudadanía digital implica promover un uso seguro, reflexivo y ético de la tecnología. Los marcos educativos actuales organizan este tema en cuatro ejes: comunicación y colaboración en línea, privacidad y seguridad, alfabetización mediática y digital, y bienestar personal (Walsh et al., 2022). Todo esto, con la intención de promover el pensamiento crítico, el compromiso cívico y la preparación de las personas estudiantes para participar de manera responsable en la sociedad digital actual.

b. Seguridad digital y ciberseguridad

La seguridad digital implica adoptar medidas preventivas para protegerse de riesgos relacionados con el uso de dispositivos, aplicaciones y plataformas en línea. Esto incluye la protección de datos personales, el uso de contraseñas seguras, la instalación de software de protección, y la evaluación de la confiabilidad de los sitios web. Además, resalta la importancia de la acción humana en la prevención de vulnerabilidades, promoviendo una cultura de cuidado personal y colectivo en los entornos digitales.

En el contexto educativo, la seguridad digital debe ser formativa y ética, ya que los centros educativos no solo deben garantizar entornos tecnológicos protegidos sino también formar a las personas estudiantes y al personal docente y administrativo en prácticas seguras, responsables y sostenibles en el uso de las tecnologías (Capuno et al., 2022).

Esto implica integrar la seguridad digital como parte del currículo y de las competencias transversales, fomentando el pensamiento crítico, el manejo adecuado de la información y el reconocimiento de posibles amenazas como virus, fraudes, suplantaciones de identidad, o el acceso a contenidos inapropiados.

c. Autocuidado digital

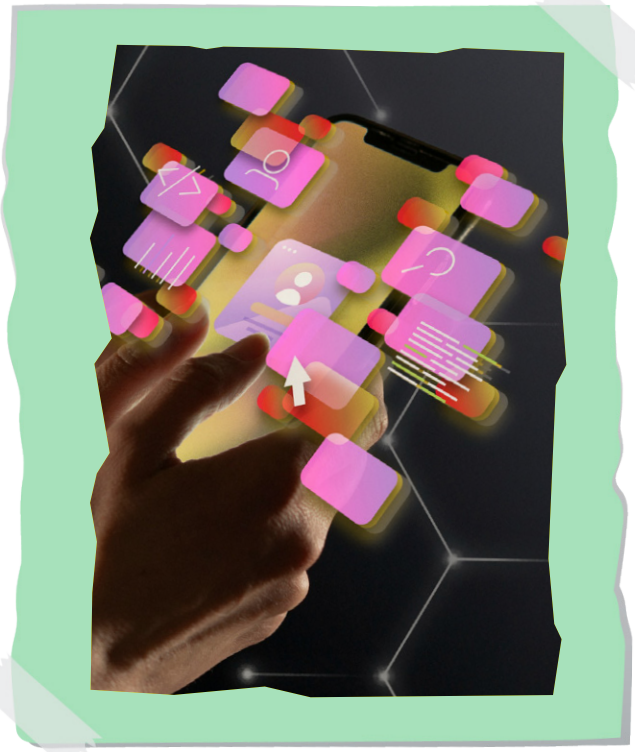
El autocuidado en el entorno digital se refiere a las acciones que permiten reducir riesgos y proteger los derechos individuales durante el uso de tecnologías (Walsh et al., 2022). Este concepto es clave para la prevención de situaciones como el ciberacoso, el acceso a contenidos inapropiados o la exposición de información personal. Las familias y los centros educativos tienen la responsabilidad de brindar acompañamiento, información y orientación a las personas menores de edad para fortalecer su capacidad de identificar alertas, tomar decisiones responsables y mantener prácticas digitales seguras.

El autocuidado digital es un pilar fundamental de la ciudadanía digital, ya que fortalece la autonomía de la persona estudiante al permitirle reconocer riesgos, tomar decisiones informadas y actuar con criterio en entornos digitales. Su desarrollo no solo contribuye a formar personas conscientes de sus derechos, deberes y responsabilidades en el uso de la tecnología, sino que también abarca aspectos esenciales como el manejo del tiempo frente a las pantallas, la desconexión digital, la salud mental, el descanso y el equilibrio entre la vida en línea y fuera de línea.

d. Huella digital

La huella digital es el rastro que una persona deja al interactuar en internet: páginas visitadas, búsquedas realizadas, publicaciones, comentarios y archivos compartidos (Ministerio de Educación Pública de Costa Rica, 2016). Cada acción en el entorno digital por más mínima que parezca, contribuye a construir un perfil personal que puede ser accesible por terceros con buenas o malas intenciones.

Esta huella, en muchos casos, es pública, persistente y difícil de borrar, ya que los contenidos pueden ser almacenados, copiados o viralizados rápidamente sin el control del usuario. Su alcance puede tener implicaciones importantes en la vida presente y futura de una persona, afectando su reputación, sus relaciones personales, sus oportunidades laborales e incluso su seguridad.



La comprensión y gestión responsable de la huella digital es fundamental, especialmente en el caso de niñas, niños y adolescentes, quienes muchas veces no son plenamente conscientes de las consecuencias de su actividad en línea. El educar sobre la huella digital desde edades tempranas es clave para prevenir situaciones de exposición no deseada, acoso en línea o suplantación de identidad, y para fomentar una ciudadanía digital ética, empática y segura.

e. Privacidad

La privacidad en el entorno digital se refiere al derecho de las personas a controlar la información que comparten, así como a decidir quién puede acceder a ella y cómo se utiliza (Liu & Khalil, 2023). Este principio implica que las personas estudiantes deben tener control sobre sus datos personales, los cuales deben ser gestionados con responsabilidad y confidencialidad. La protección de estos datos no solo es una práctica ética, sino también un derecho reconocido en los entornos digitales (Liu & Khalil, 2023).

En el contexto educativo, la privacidad significa que las personas estudiantes conservan ese control sobre sus datos y que esta información no debe ser compartida sin su consentimiento durante la recolección, el análisis o la presentación de informes. Además, la protección de estos datos es un derecho fundamental que debe garantizarse de manera justa y equitativa para todos.

Sin embargo, este derecho se ve constantemente desafiado por tecnologías que recopilan, almacenan y procesan grandes volúmenes de información, muchas veces sin que los usuarios conozcan con claridad cómo se usa esa información (Kumar, 2024). Por eso, es fundamental que las comunidades educativas comprendan los riesgos asociados al uso de plataformas digitales y promuevan una cultura del consentimiento, la transparencia y el manejo ético de los datos.

La educación en privacidad digital debe ser parte del enfoque formativo de los centros educativos no solo para enseñar prácticas responsables, sino también para ayudar a las personas estudiantes a reconocer las consecuencias de compartir en exceso su información personal y a valorar la importancia de proteger su intimidad en línea (Kumar, 2024). Además, es necesario aprender a diferenciar entre lo íntimo, lo privado y lo público, entendiendo que el respeto por la privacidad cambia según el contexto y que su protección debe ser un derecho accesible para todos.

f. Ciberacoso

El ciberacoso es una forma de violencia que se produce a través de medios digitales y que puede manifestarse mediante insultos, amenazas, exclusión o la difusión de contenido ofensivo dirigido a una persona. Este fenómeno afecta principalmente a la población infantil y juvenil, y se caracteriza por acciones reiteradas de humillación, hostigamiento o acoso con la intención de causar daño emocional (Walsh et al., 2022). Las formas comunes de ciberacoso incluyen la difusión de rumores, suplantación de identidad, exclusión virtual, publicación de imágenes sin consentimiento y mensajes agresivos a través de redes sociales, videojuegos en línea u otros espacios digitales.

Estas situaciones suelen originarse en contextos educativos presenciales y extenderse al ámbito virtual, o viceversa, generando un ciclo de violencia que trasciende los límites físicos del centro educativo. Debido a su gravedad, el ciberacoso puede provocar consecuencias serias como ansiedad, aislamiento, baja autoestima, pérdida de interés académico y afectaciones severas a la salud mental, incluyendo depresión y pensamientos suicidas.

En Costa Rica, este tipo de violencia está contemplado en la legislación mediante las Leyes N.° 9404, N.° 10020 (2021) y N.° 10487 (2024)[1] que promueven entornos educativos libres de acoso, incluyendo el cibernético. Por ello, los centros educativos, junto con el personal docente y administrativo, deben asumir un rol activo y comprometido en la prevención, detección temprana, atención integral y sanción de estas conductas. Esto implica implementar protocolos claros de actuación, fomentar una cultura de respeto y empatía, incorporar la educación emocional y digital en el currículo, y establecer canales seguros para la denuncia.

1 Ley N°. 9404: Ley para la prevención y el establecimiento de medidas correctivas y formativas frente al acoso escolar o bullying.

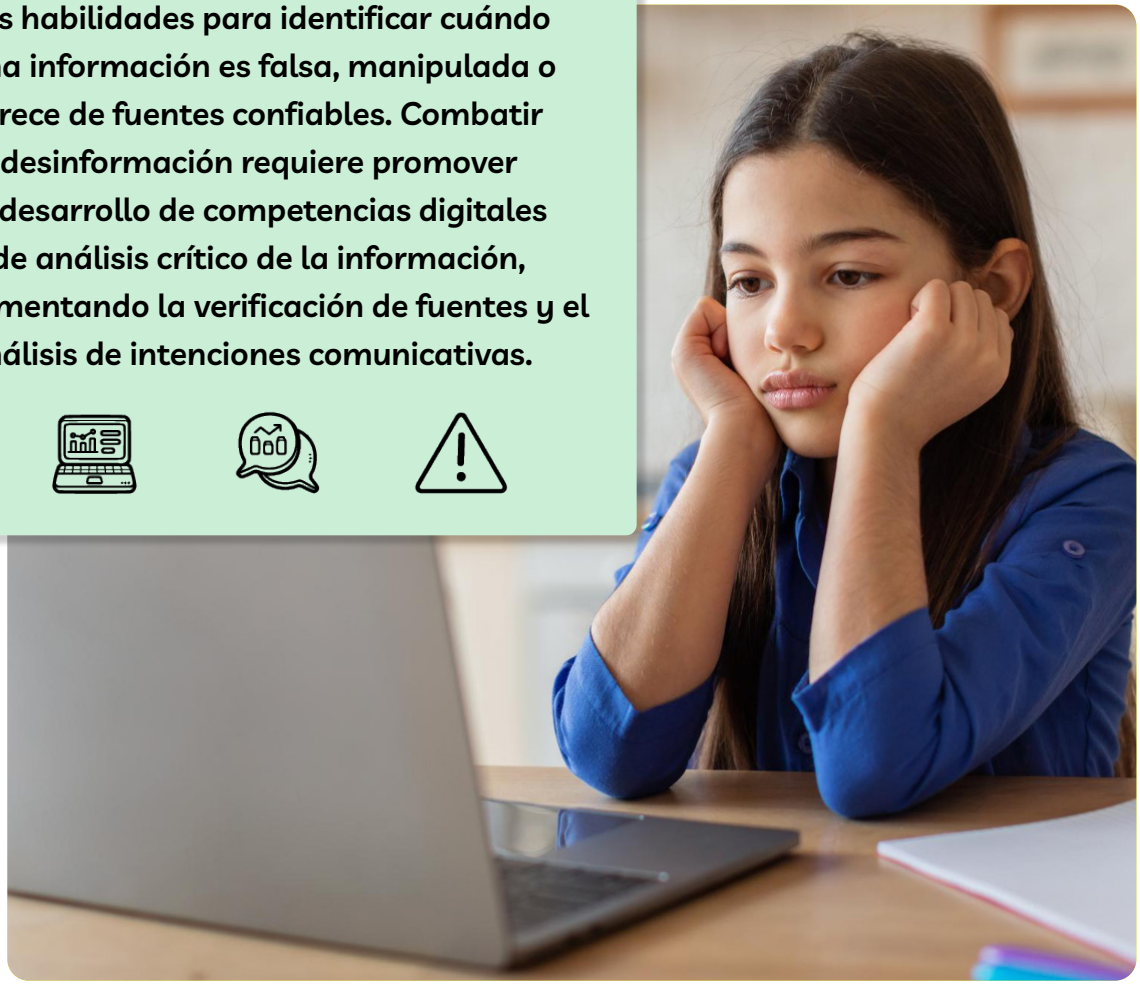
Ley N.° 10020 (2021): Ley para la prevención del acoso a personas menores de edad por medios electrónicos o virtuales (grooming).

Ley N.° 10487 (2024): Ley contra el acoso predatorio.

9. Desinformación

La desinformación es la difusión deliberada de contenido falso o engañoso que busca manipular percepciones, provocar confusión o influir en el comportamiento de las personas. Su rápida propagación en línea dificulta su control y puede afectar la percepción de la realidad, las decisiones cotidianas, la confianza y la convivencia en los centros educativos (Gutiérrez-Aguilar et al., 2024).

La persona menor de edad puede estar particularmente expuesta a estos contenidos y es necesario fortalecer sus habilidades para identificar cuándo una información es falsa, manipulada o carece de fuentes confiables. Combatir la desinformación requiere promover el desarrollo de competencias digitales y de análisis crítico de la información, fomentando la verificación de fuentes y el análisis de intenciones comunicativas.



2. Principios rectores

La integración de la ciudadanía digital en los entornos educativos requiere una base ética y normativa que oriente las decisiones pedagógicas y administrativas. En este sentido, los principios rectores constituyen guías fundamentales para el diseño, implementación y evaluación de políticas, programas y acciones relacionados con la vida digital de niñas, niños, adolescentes, personas jóvenes y adultas.

Estos principios aseguran que toda intervención en el ámbito digital respete los derechos humanos y promueva la equidad, la inclusión y el bienestar. A través de su aplicación transversal, se busca consolidar una cultura digital basada en el respeto a la diversidad, la protección de la dignidad humana y el ejercicio pleno de los derechos en línea.

a. Enfoque de derechos humanos y derechos digitales

Las niñas, niños y adolescentes así como las personas jóvenes y adultas son sujetos activos de derechos, también en los entornos digitales. Esto implica que las políticas de ciberseguridad en educación deben estar fundamentadas en los derechos humanos universales, garantizando su aplicación en los espacios virtuales de aprendizaje. La educación, al ser un derecho humano esencial, debe brindarse en condiciones de seguridad, equidad e inclusión, tanto en el ambiente físico como en el digital.

En la práctica, este enfoque se traduce en los siguientes compromisos:

Asegurar el acceso equitativo y seguro a tecnologías digitales como parte del derecho a una educación de calidad. Esto incluye garantizar la conectividad, el acceso a dispositivos y a contenidos relevantes, sin distinción por género, condición socioeconómica o territorio (Ministerio de Educación Pública de Costa Rica, 2022).

Promover entornos virtuales libres de violencia digital, reconociendo que formas como el ciberacoso, el hostigamiento en línea o la exposición a contenidos nocivos constituyen violaciones a los derechos fundamentales del estudiantado. El Estado tiene la responsabilidad de proteger a niños, niñas y adolescentes contra todo tipo de perjuicio, abuso o explotación, también en el ámbito digital (Ministerio de Educación Pública de Costa Rica, 2016).

Garantizar la participación activa de las personas estudiantes en el diseño e implementación de políticas, programas y normas que afectan su experiencia en entornos digitales. La participación debe ser ética, legítima, significativa y acorde con su nivel de desarrollo, fortaleciendo su rol como ciudadanos digitales críticos.

Fomentar una ciudadanía digital ética, segura e inclusiva, basada en principios de respeto, responsabilidad, igualdad y solidaridad. Esto implica desarrollar en las personas estudiantes las competencias necesarias para ejercer sus derechos y deberes digitales, participar en comunidades virtuales, y actuar con criterio frente a los riesgos en línea.

b. Protección de datos personales

La protección de los datos personales en el entorno educativo es un principio esencial dentro de cualquier política de ciberseguridad. En los centros educativos, tanto públicos como privados, se maneja información sensible relacionada con personas estudiantes, personas docentes y personal administrativo. Esta información incluye datos académicos, identificaciones, imágenes, resultados de evaluaciones, historial médico, entre otros. El tratamiento inadecuado de estos datos puede tener consecuencias graves en la vida de las personas, especialmente en la población estudiantil, por lo que es fundamental contar con normas claras y mecanismos eficaces para su protección (Correia de Barros & Vilela, 2025).

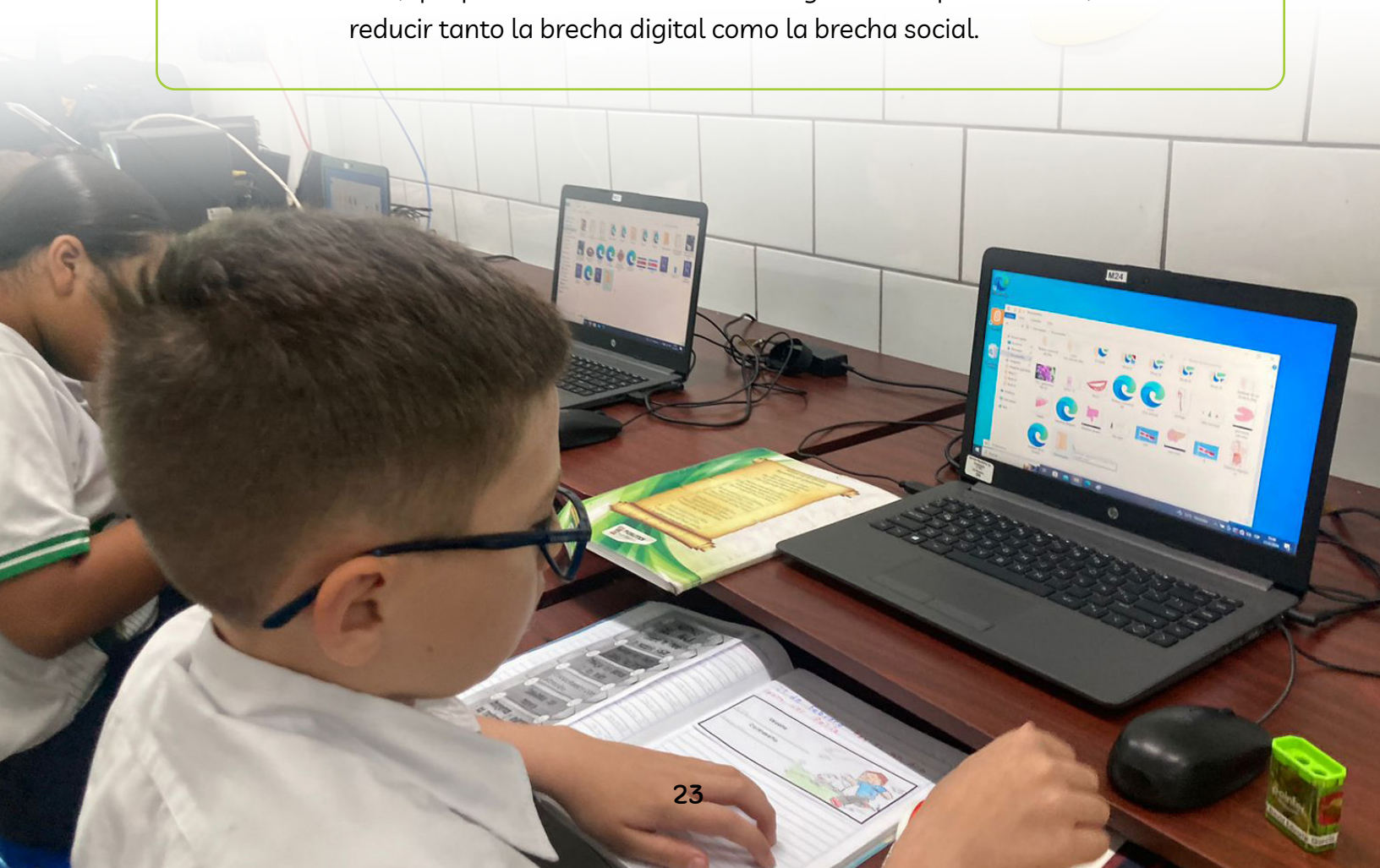
Las políticas de protección de datos deben asegurar que la información personal se utilice de forma responsable, con un propósito claro y legítimo. Es fundamental que las personas, especialmente la población estudiantil y sus familias sepan quién recopila sus datos, para qué se usarán y durante cuánto tiempo se conservarán (Correia de Barros & Vilela, 2025). Además, solo debe recolectarse la información necesaria, asegurando que sea precisa, esté actualizada y se proteja adecuadamente para evitar accesos no autorizados, pérdidas o filtraciones.

El principio de no discriminación establece que la información recopilada nunca debe utilizarse para excluir, segregar o perjudicar a una persona o grupo. Asimismo, la gestión de riesgos en ciberseguridad educativa debe incluir la formación de la comunidad educativa en el uso seguro de internet, el manejo responsable de los datos personales, y la protección de la identidad digital y la propiedad intelectual. Según el Modelo para la Inclusión de las Tecnologías Digitales en Educación (MITDE), esto requiere una revisión periódica de los protocolos institucionales relacionados con el uso de plataformas, el acceso a redes y las políticas de consentimiento informado.

c. Equidad de género e inclusión social

La equidad de género y la inclusión social son principios fundamentales en la construcción de entornos educativos digitales seguros y justos. La ciberseguridad educativa no puede abordarse desde una perspectiva neutral, ya que las desigualdades sociales, económicas y de género también se reflejan e incluso se amplifican en los espacios digitales. Las políticas deben reconocer estas diferencias y trabajar activamente para cerrar las brechas que afectan el acceso, el uso y la apropiación de las tecnologías.

El enfoque de inclusión digital propone asegurar que todas las personas, sin distinción, puedan participar plenamente en la vida digital. Esto implica garantizar que personas de comunidades rurales, con discapacidad, de distintos contextos culturales o en situación de vulnerabilidad, tengan acceso real y significativo a las herramientas tecnológicas. Un ejemplo de esta visión es el Modelo de Inclusión Digital Educativa (MITDE) en Costa Rica, que promueve una ciudadanía digital con equidad social, buscando reducir tanto la brecha digital como la brecha social.



Es esencial que las políticas de ciberseguridad contemplen las desigualdades específicas que enfrentan las personas en su diversidad de condiciones y expresiones de identidad en el entorno digital.

Asimismo, se debe considerar la necesidad de aplicar principios de accesibilidad universal. Esto implica diseñar recursos educativos digitales que se adapten a la diversidad de estilos de aprendizaje, capacidades y contextos, por medio de enfoques como el Diseño Universal de Aprendizaje (DUA) (Ministerio de Educación Pública de Costa Rica, 2021). Este diseño permite múltiples formas de representación, acción y expresión, garantizando que todas las personas estudiantes tengan oportunidades reales de participación y aprendizaje.

Finalmente, la responsabilidad social del sistema educativo frente a las tecnologías digitales implica un compromiso activo con la reducción de las desigualdades. No se trata solo de proveer dispositivos o conectividad, sino de generar condiciones para que cada persona estudiante, independientemente de su situación, pueda desarrollar sus capacidades, protegerse y ejercer plenamente su ciudadanía en el entorno digital.

d. Enfoque desarrollista y autonomía progresiva

El enfoque desarrollista parte del reconocimiento de que las personas atraviesan distintas etapas del desarrollo, cada una con necesidades, derechos y niveles de autonomía particulares. En el marco de la Política Nacional de Niñez y Adolescencia 2024–2036 (PNNA), se define como niño o niña a toda persona desde la concepción hasta los 12 años, y como adolescente a quien tiene entre 12 y 17 años. Esta categorización permite orientar de manera más precisa las políticas públicas, las estrategias educativas y las acciones de protección en entornos digitales, considerando el desarrollo progresivo de cada grupo. Lo que se vive y aprende en cada etapa influye significativamente en el bienestar futuro, por lo que es fundamental que temas como la educación digital, la ciberseguridad y el uso responsable de la tecnología se aborden con indicadores de evaluación adecuados a cada momento del desarrollo.

En este sentido, las políticas de ciberseguridad y el desarrollo de competencias digitales deben considerar tanto el nivel de madurez como las capacidades de los niños, niñas y adolescentes. El principio del interés superior del niño o niña debe ser una consideración primordial en todas las decisiones vinculadas al entorno digital, desde el diseño de plataformas hasta la regulación y gestión de los contenidos. Esto implica garantizar su protección frente a riesgos, facilitar su participación significativa y asegurar que los recursos tecnológicos sean comprensibles, seguros y apropiados para su edad y contexto.

Respetar el desarrollo, los derechos y las necesidades específicas de cada etapa no solo permite crear entornos digitales más seguros y pertinentes, sino que también contribuye a formar personas estudiantes con autonomía, criticidad y mejor preparación para enfrentar los desafíos del mundo digital. Este proceso requiere el acompañamiento activo y consciente de las personas adultas, que orienten y respalden el crecimiento progresivo de las habilidades digitales, promoviendo la protección sin limitar la participación.

3 RIESGOS COMUNES POR NIVEL EDUCATIVO

1. Personas estudiantes de preescolar y primaria

La niñez en edad preescolar y primaria se encuentra en una etapa donde la curiosidad y el aprendizaje son muy intensos, y el uso de la tecnología se vuelve cada vez más frecuente, tanto en el hogar como en el entorno educativo. Sin embargo, esta interacción con dispositivos y plataformas digitales no está exenta de riesgos que pueden afectar su desarrollo, seguridad y bienestar. Aunque muchas investigaciones se han centrado en los adolescentes, los más pequeños también enfrentan amenazas digitales específicas que requieren atención y acompañamiento adecuados por parte de los adultos responsables (Cambridge University, 2020).

Uno de los principales riesgos es la exposición a contenidos inapropiados. A pesar de los filtros y controles parentales que algunas plataformas incorporan, los menores pueden encontrarse con imágenes violentas, discursos de odio, material sexual explícito o contenidos que promueven conductas peligrosas, como retos virales que incitan a la autolesión o a dietas extremas (Walsh et al., 2022).

Esta exposición puede causar confusión, ansiedad o normalización de comportamientos dañinos. Además, muchos niños pequeños aún no tienen las herramientas cognitivas necesarias para distinguir entre la realidad y la ficción en lo que consumen digitalmente (Alsehaimi, 2018).

El uso prolongado de dispositivos también puede derivar en una sobreexposición digital, que no se limita únicamente al tiempo frente a la pantalla, sino que incluye la posibilidad de desarrollar una dependencia o incluso una adicción a la tecnología. Esta situación puede tener efectos negativos en la salud física de personas estudiantes, manifestándose en alteraciones del sueño, molestias musculares, fatiga visual y, además, en dificultades para concentrarse, regular sus emociones o relacionarse con otros (Alsehaimi, 2018). A esto se suma que, en muchos casos, los menores se distraen con facilidad debido a las constantes notificaciones, anuncios emergentes y estímulos digitales, lo que termina interfiriendo tanto en su aprendizaje como en momentos clave de juego libre o socialización presencial.

Otro riesgo importante es el contacto con personas desconocidas, que puede presentarse a través de chats, redes sociales, videojuegos en línea u otras plataformas interactivas. Existen situaciones graves como el phishing, grooming o seducción en línea, en el que adultos se hacen pasar por niños para ganarse la confianza del menor y, posteriormente, manipularlo con fines sexuales, extorsivos o delictivos. A esto se suman los intentos de solicitud no deseada, estafas, suplantación de identidad (phishing) y fraudes digitales que pueden aprovecharse del desconocimiento o la ingenuidad infantil (Alsehaimi, 2018).

La falta de conciencia sobre la privacidad y seguridad de los datos también representa un desafío ya que muchos comparten sin saberlo información sensible como su nombre, dirección, fotografías, ubicación o detalles educativos en plataformas que no siempre son seguras (Correia de Barros & Vilela, 2025). Incluso las herramientas educativas, si no cuentan con políticas de protección adecuadas, pueden recopilar una gran cantidad de datos personales, que en algunos casos se utilizan con fines poco claros. Esta información deja una huella digital que puede permanecer en línea indefinidamente y generar consecuencias a futuro, como riesgos para la seguridad o la reputación de la persona menor de edad (Correia de Barros & Vilela, 2025).

El ciberacoso es otra de las amenazas más relevantes en la vida digital de esta población y puede manifestarse en forma de insultos, exclusión, rumores, difusión no consentida de imágenes o vídeos, amenazas reiteradas o burlas que se transmiten por plataformas digitales. Este tipo de violencia tiene un fuerte impacto emocional en las víctimas, generando ansiedad, depresión, pérdida de autoestima e incluso, en casos extremos, pensamientos suicidas; y aunque muchas veces comienza en la escuela o el entorno cercano, el medio virtual amplifica su efecto debido a la rapidez con la que se difunden los contenidos y la dificultad para eliminarlos (Ministerio de Educación Pública de Costa Rica, 2016).

Además, la baja alfabetización digital en la infancia los vuelve especialmente vulnerables a creer noticias falsas, caer en desinformación o reproducir estereotipos nocivos (Alsehaimi, 2018), lo que resulta aún más preocupante en un entorno digital saturado de contenidos poco fiables o manipuladores. A esto se suman las desigualdades sociales y económicas, que pueden limitar el acceso a tecnologías seguras, a acompañamiento adulto y a una educación digital de calidad, haciendo que ciertos grupos infantiles enfrenten riesgos aún mayores.

Aunque muchos niños y niñas tienden a buscar ayuda cuando enfrentan problemas en línea, no siempre saben a quién acudir o temen ser castigados, lo que dificulta una intervención oportuna (Cambridge University, 2020).

Por ello, el rol de la persona docente es fundamental para brindar contención, orientación y apoyo, ya que los centros educativos en conjunto con las familias no solo deben enseñar el uso seguro y responsable de las tecnologías, sino también promover entornos digitales protectores donde cada uno se sienta acompañado, escuchado y respetado.

2. Personas estudiantes de secundaria

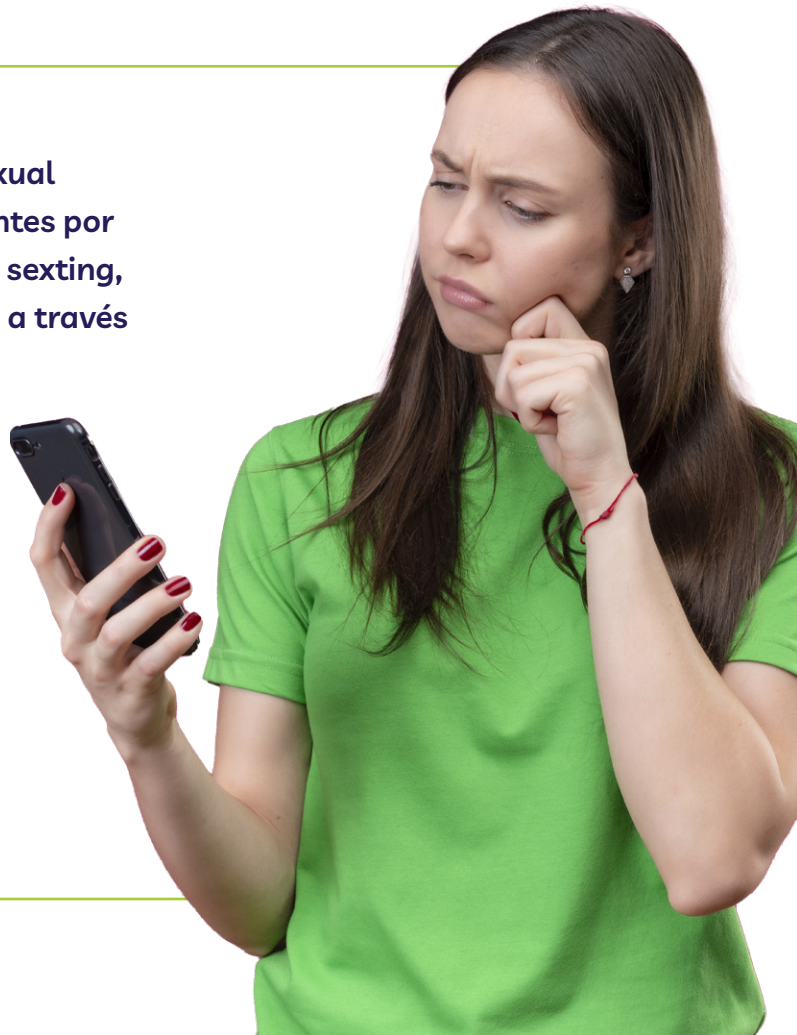
Durante la etapa de secundaria, los adolescentes amplían significativamente su participación en el entorno digital. Interactúan en redes sociales, plataformas de mensajería, videojuegos en línea y otros espacios virtuales que les permiten relacionarse con pares, explorar intereses personales y construir su identidad. Este acceso más autónomo a la tecnología los expone a una variedad de riesgos que pueden afectar su bienestar emocional, social, físico y académico. A medida que crecen, cuentan con mayor libertad y tiempo de conexión pero aún no han desarrollado completamente las habilidades necesarias para enfrentar los desafíos del entorno digital, lo que los convierte en una población especialmente vulnerable (Trinidad et al., 2025).

La combinación de independencia creciente, menor supervisión adulta y una alfabetización digital todavía en desarrollo incrementa la vulnerabilidad de esta etapa (Alsehaimi, 2018). Además, los riesgos tienden a intensificarse con la edad y con el tiempo que los adolescentes pasan conectados.

Uno de los riesgos más frecuentes en esta etapa es el ciberacoso, que se manifiesta cuando una persona es acosada, amenazada, o ridiculizada a través de medios digitales. Esta forma de violencia puede incluir comentarios ofensivos, difusión de rumores, amenazas, publicación de imágenes sin consentimiento, exclusión en redes sociales o mensajes persistentes cargados de agresividad. A diferencia del acoso tradicional, el ciberacoso puede continuar fuera del horario académico, alcanzar rápidamente a una gran audiencia y causar un daño prolongado en el tiempo (Walsh et al., 2022).

Este tipo de violencia afecta profundamente el bienestar emocional de los adolescentes, generando ansiedad, tristeza, aislamiento, baja autoestima y en muchos casos una disminución en su desempeño académico (Correia de Barros & Vilela, 2025). En los entornos digitales también se observa una alta circulación de discursos discriminatorios, dirigidos especialmente a adolescentes por razones de identidad sexual, expresión de género, origen étnico, religión o apariencia física. Muchas veces se normalizan como parte de la "interacción en redes" aunque impactan negativamente en la autoestima de quienes las reciben y afectan su sentido de pertenencia, especialmente entre quienes ya enfrentan condiciones de vulnerabilidad en sus entornos escolares o familiares.

Otro riesgo crítico es la exposición a violencia sexual digital. En esta etapa, algunas personas estudiantes por presión de grupo o desconocimiento practican el sexting, es decir, el envío voluntario de imágenes íntimas a través de plataformas digitales. Aunque pueda parecer una práctica consentida, se vuelve peligrosa cuando ese contenido es compartido sin permiso o utilizado para manipular a la persona, lo que se conoce como sextorsión. Esta forma de chantaje digital genera un fuerte impacto emocional en las víctimas, quienes ven vulnerada su intimidad y amenazada su integridad.



En muchos casos, la sextorsión se vincula con situaciones de grooming, donde una persona adulta se hace pasar por una persona adolescente y gana la confianza del menor con fines de abuso o explotación sexual (Trinidad et al., 2025). También se ha identificado la difusión no consentida de imágenes íntimas como una forma de agresión digital que afecta especialmente a mujeres adolescentes.

A esto se suma la exposición no intencionada a contenidos sexuales explícitos, pornografía o mensajes que refuerzan la hipersexualización, los cuales pueden distorsionar la forma en que los adolescentes perciben los vínculos afectivos, su cuerpo y la intimidad (Walsh et al., 2022).

El uso excesivo de tecnologías digitales es una preocupación cada vez más presente en la vida las personas estudiantes. Ellos y ellas pasan largas horas conectados a redes sociales, videojuegos o plataformas de mensajería, lo que puede impactar negativamente en su salud mental, sus relaciones sociales y su desempeño académico (Alsehaimi, 2018).

Esta relación intensa con el entorno digital puede derivar en conductas adictivas, que se manifiestan mediante irritabilidad cuando no tienen acceso a sus dispositivos, dificultades para concentrarse, alteraciones en el sueño y una fuerte dependencia emocional del mundo virtual.

La exposición constante a desinformación y contenido dañino se ha convertido en otro riesgo significativo, ya que en internet circula una enorme cantidad de información sin filtros ni garantías de veracidad, lo que dificulta que los y las adolescentes puedan distinguir entre hechos reales y falsos (Walsh et al., 2022). Muchos confían en las primeras fuentes que encuentran o comparten contenidos sin verificar su procedencia ni cuestionar su intención. Esta falta de pensamiento crítico les vuelve más vulnerables a noticias falsas, rumores o mensajes manipuladores, que pueden generar confusión, miedo o reforzar prejuicios y estereotipos ya existentes.

Finalmente, todos estos riesgos están profundamente vinculados con la privacidad y el manejo de la identidad digital. Muchas personas adolescentes comparten en línea información personal como su nombre completo, dirección, rutinas diarias, fotografías o ubicación, sin pensar en las consecuencias que esto puede tener.

Esta exposición los deja en una posición vulnerable frente a situaciones como el robo de identidad, la suplantación de perfiles o el uso indebido de sus datos con fines comerciales o incluso delictivos (Correia de Barros & Vilela, 2025).

Una vez que la información se publica en internet, deja de estar completamente bajo el control de la persona, ya que puede replicarse y difundirse sin límites, generando una huella digital que persiste en el tiempo y es muy difícil de eliminar por completo. Esto incluye el contenido personal, la información privada y la imagen de la persona, por lo que es fundamental ser consciente de los derechos digitales y del derecho de imagen al compartir cualquier tipo de información en línea.

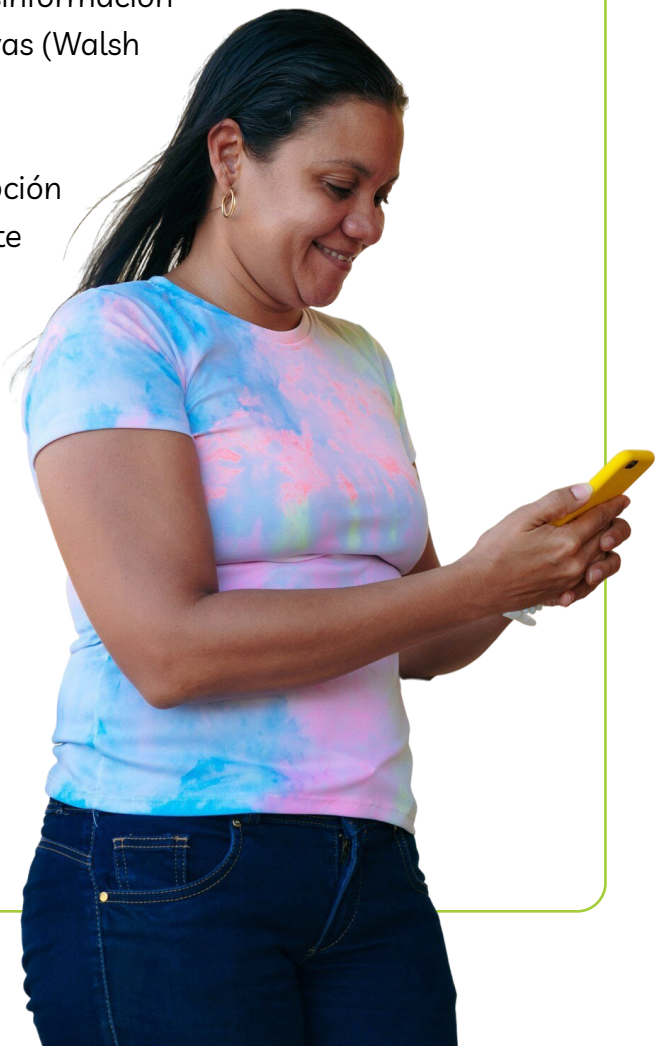
3. Personas jóvenes y adultas

El uso intensivo de tecnologías digitales entre personas jóvenes y adultas ha transformado profundamente la forma en que se comunican, acceden a información, trabajan, estudian y se entretienen. Aunque estas herramientas ofrecen múltiples beneficios, también presentan riesgos que, si no se gestionan adecuadamente, pueden afectar la seguridad, el bienestar y la reputación de quienes las utilizan.

Uno de los riesgos más comunes es el fraude en línea, que abarca desde estafas simples hasta esquemas complejos de engaño digital. La pérdida de dinero por sitios falsos, plataformas de compra engañosas o enlaces maliciosos es cada vez más habitual, especialmente cuando no se aplican precauciones básicas como verificar la autenticidad de los sitios, proteger los métodos de pago o evitar compartir datos personales en entornos inseguros (Correia de Barros & Vilela, 2025). El phishing, por ejemplo, consiste en correos o mensajes que aparentan ser legítimos pero que buscan robar contraseñas, instalar software malicioso o acceder a información sensible (Kumar, 2024). También existen casos de extorsión o chantaje digital en los que las personas son presionadas mediante amenazas o manipulación para entregar información privada o realizar pagos. Este tipo de delitos no solo genera consecuencias económicas, sino que también puede afectar la seguridad personal, la reputación y la estabilidad emocional de las víctimas.

El uso de datos personales sin consentimiento o su filtración, ya sea por negligencia o por vulnerabilidades de seguridad es un riesgo constante en la vida digital. La exposición de información como nombres, direcciones, documentos académicos o rutinas diarias puede ser aprovechada para fraudes, suplantación de identidad u otros delitos (GAT Labs for Education, n.d.). A esto se suma la falta de transparencia en el uso de los datos por parte de algunas plataformas, lo que ha generado desconfianza entre usuarios adultos, incluidas personas docentes, sobre cómo se recopila y procesa su información. Muchos usuarios tampoco aplican prácticas de protección básica como el uso de contraseñas seguras, antivirus o copias de seguridad, lo que agrava la vulnerabilidad ante amenazas externas (Capuno et al., 2022).

Por otra parte, el acceso libre a internet sin criterios de selección expone a las personas jóvenes y adultas a una gran cantidad de contenido dañino, que va desde imágenes violentas o sexualizadas hasta discursos de odio, desinformación o mensajes que promueven prácticas autodestructivas (Walsh et al., 2022).
Este contenido, muchas veces viralizado en redes o presentado sin advertencias, puede alterar la percepción de la realidad, generar ansiedad o insensibilizar frente a situaciones de violencia.



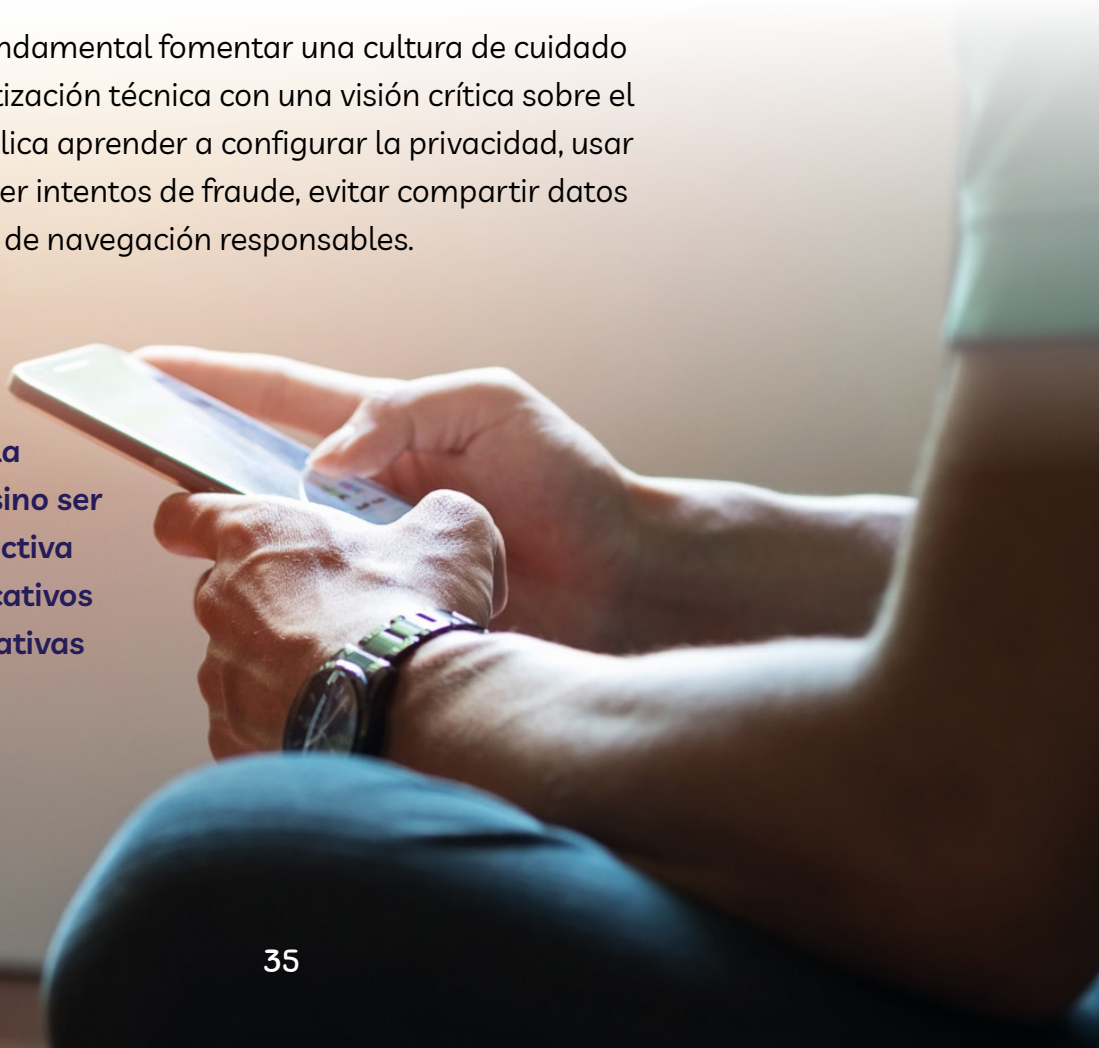
Aunque se suele asociar el grooming con menores, también se han documentado casos en personas adultas jóvenes que fueron manipulados por desconocidos que fingían empatía o interés emocional con fines de explotación sexual o financiera (Trinidad et al., 2025). En paralelo, el ciberacoso no es exclusivo de adolescentes: en entornos sociales, académicos o laborales, las personas adultas pueden ser blanco de insultos, amenazas, humillaciones públicas o campañas de desprestigio digital.

El uso excesivo de pantallas y tecnologías digitales también representa un riesgo importante, muchas personas pasan varias horas conectadas por trabajo, estudio o entretenimiento, lo que puede afectar la salud física, la calidad del sueño, la concentración y el bienestar emocional. En ciertos casos, esta relación desbalanceada con la tecnología puede evolucionar hacia una adicción digital, con impactos en el desempeño laboral o académico y en la vida personal.

Un aspecto clave que atraviesa todos estos riesgos es el manejo de la reputación y la huella digital, las personas adultas suelen compartir en línea fotografías, opiniones o aspectos íntimos sin considerar que ese contenido puede permanecer disponible indefinidamente y ser visualizado por personas fuera de su círculo de confianza. Esta exposición puede generar consecuencias a largo plazo cómo la pérdida de oportunidades laborales, conflictos interpersonales o afectaciones en la imagen pública (Stopbullying.gov, 2021). Una de las formas más graves de este tipo de daño es la difusión no consentida de imágenes íntimas, una práctica que afecta especialmente a mujeres jóvenes y que puede derivar en acoso, amenazas o aislamiento, con un fuerte impacto en la salud emocional.

Frente a este panorama es fundamental fomentar una cultura de cuidado digital que combine la alfabetización técnica con una visión crítica sobre el uso de la tecnología. Esto implica aprender a configurar la privacidad, usar contraseñas seguras, reconocer intentos de fraude, evitar compartir datos sensibles y mantener hábitos de navegación responsables.

La protección digital no debe recaer únicamente en la responsabilidad individual, sino ser parte de una estrategia colectiva que involucre a centros educativos familias, comunidades educativas y plataformas tecnológicas.



A continuación, en el siguiente diagrama se presentan las acciones y recomendaciones clave diferenciadas por grupo de edad, esenciales para abordar de manera efectiva los riesgos educativos y de seguridad en el entorno digital, promoviendo un uso responsable, crítico y seguro de la tecnología.

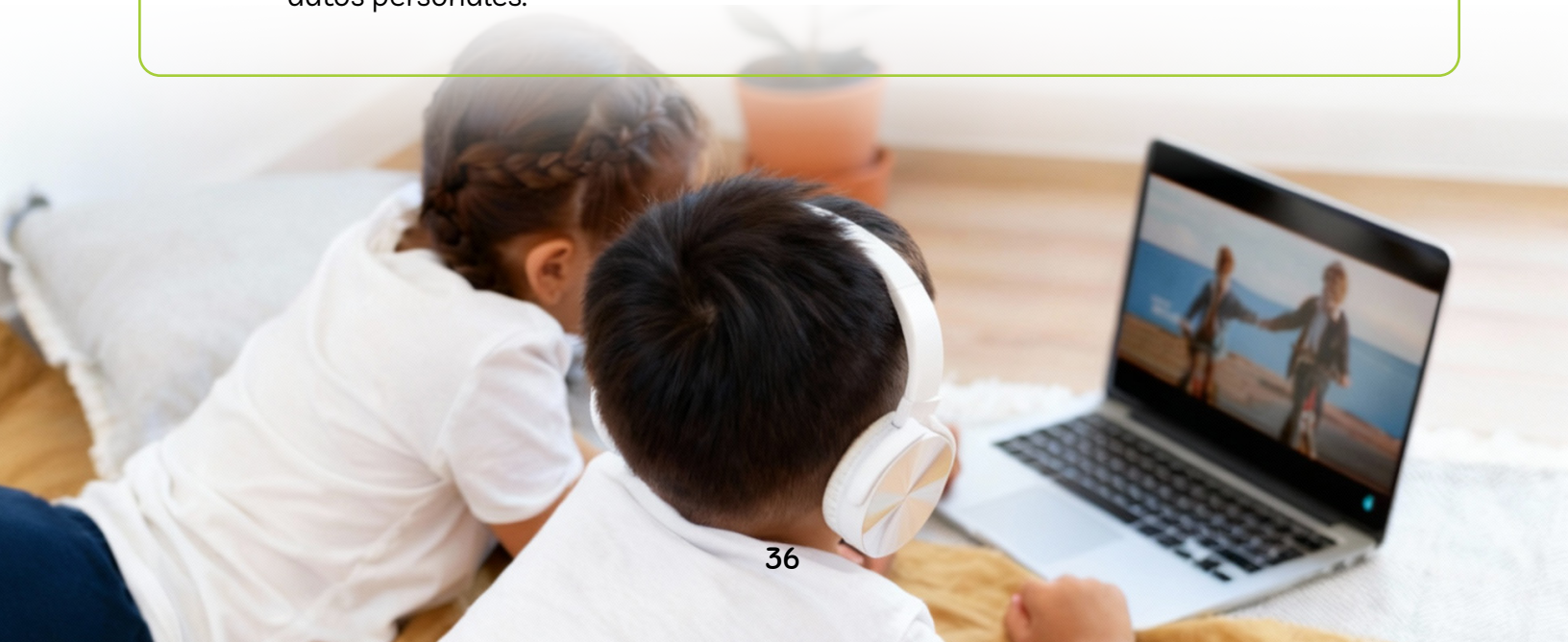
Diagrama 3. Acciones recomendadas para abordar los riesgos educativos

GRUPO 1:

Personas estudiantes de preescolar y primaria

Acompañamiento y rutinas

- **Acompañamiento confiable:** Mantener una supervisión cercana del uso de pantallas, promoviendo un espacio de confianza donde los niños y niñas puedan solicitar ayuda cuando lo requieran.
- **Control parental activo**: Configurar filtros, límites de tiempo y restricciones adecuadas según la edad, en todos los dispositivos y plataformas.
- **Rutinas digitales saludables:** Establecer horarios de conexión, pausas activas y espacios sin tecnología (como durante las comidas o antes de dormir).
- **Educación digital temprana:** Introducir conceptos básicos como el respeto en línea, la empatía, la privacidad y la importancia de ser cuidadosos con los datos personales.



GRUPO 2:

Personas estudiantes de secundaria

Diálogo y empatía

Educación crítica y empática: Enseñar a reconocer, enfrentar y prevenir situaciones de violencia digital como el ciberacoso o la sextorsión, sin culpabilizar.

Espacios de diálogo seguro: Fomentar conversaciones abiertas sobre temas complejos (sexualidad, redes sociales, autoestima) sin juicios ni prejuicios.

Trabajo con familias: Brindar a padres, madres o persona encargada legal herramientas para reconocer los riesgos y saber cómo abordarlos de manera efectiva.

Protección legal y emocional: Informar sobre derechos digitales, vías de denuncia y redes de apoyo cuando se vulnera la intimidad o se sufre acoso.

Pensamiento crítico digital: Promover el análisis de fuentes, la verificación de información y la identificación de estereotipos o manipulaciones en línea, ofreciendo asesoría y apoyo a las personas estudiantes frente a la violencia digital.

GRUPO 3:

Personas jóvenes y adultas

Responsabilidad personal y profesional

Cuidados básicos: Aplicar medidas de seguridad como contraseñas robustas, copias de seguridad, actualizaciones de software y uso de antivirus.

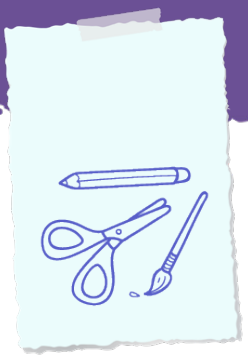
Gestión de identidad digital: Ser consciente de lo que se comparte, proteger la privacidad y cuidar la reputación personal y profesional en línea.

Alfabetización digital: Participar en capacitaciones o formaciones sobre ciberseguridad, netiqueta, privacidad y uso ético de las tecnologías en distintos ámbitos.

Manejo saludable del tiempo digital: Establecer límites, practicar desconexión consciente y cuidar la salud mental.

Apoyo ante violencia digital: Conocer y aplicar protocolos de denuncia, acceder a apoyo psicosocial, y construir entornos laborales o educativos seguros.

4 RECOMENDACIONES PEDAGÓGICAS DIFERENCIADAS POR NIVEL EDUCATIVO



1. Actividades sugeridas por nivel

A continuación, se presenta, para cada nivel educativo, una serie de orientaciones y recomendaciones pedagógicas para el abordaje educativo de la seguridad digital con personas estudiantes. Cada una de estas estrategias se presenta de acuerdo a una ruta didáctica sugerida que debe ser adaptada y contextualizada de acuerdo a las necesidades e intereses del estudiantado con que se desarrolle.

a. Preescolar

Mis huellas digitales

Objetivo

Comprender la relación entre nuestras actividades en línea y la huella digital que generan para el uso seguro de la tecnología con apoyo de una persona adulta.

Materiales sugeridos

- Hojas impresas con una huella digital, será el espacio de trabajo donde representarán sus acciones digitales.
- Lápices de escribir, crayolas, marcadores o lápices de colores.
- Goma y tijeras.
- Una pizarra con la frase “¡Lo que hago en internet deja huella!”, que sirva como guía visual y refuerzo del mensaje principal de la actividad.
- Revistas con imágenes diversas que puedan recortar y agregar en el espacio de trabajo.

Preguntar (Identificar la necesidad o problema inicial)

Se inicia una conversación con las personas estudiantes sobre el significado de huella, partiendo de ejemplos cotidianos como las marcas que deja la pintura en las manos o los pies. Se les plantea la pregunta “¿qué pasa cuando usamos el celular o la computadora? ¿será que también dejamos alguna marca?”. A partir de sus ideas se introduce el concepto de huella digital como una marca invisible que dejamos cuando usamos la tecnología e interactuamos en línea.

Imaginar (Generar soluciones y conceptos)

Se invita a imaginar qué actividades realizan con la tecnología que podrían formar parte de esa huella invisible. A través del diálogo se exploran sus experiencias cotidianas con preguntas como por ejemplo “¿qué te gusta hacer en la tableta?”, “¿con quién ves videos?”, “¿qué juegos usas en el celular?”. Estas preguntas permiten conectar el concepto abstracto de la huella digital con su realidad cercana.

Planificar (Diseñar la representación)

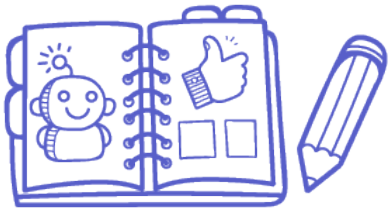
Se entrega a cada persona estudiante una hoja con el dibujo de una gran huella en el centro. Se les invita a pensar qué acciones relacionadas con la tecnología quieren representar dentro de esa huella. Pueden decidir si van a dibujar sus actividades o si van a buscar imágenes que las representen según los recursos disponibles.

Crear (Construir el modelo)

Con los materiales disponibles se les solicita que dibujen o peguen dentro de la huella aquellas actividades tecnológicas que forman parte de su vida digital como ver videos, jugar en línea, hacer videollamadas, usar aplicaciones, entre otras. Este ejercicio busca hacer visible lo invisible, transformar en imagen lo que normalmente no se ve pero que deja rastro.

Experimentar (Probar y evaluar el diseño)

Una vez que han completado su huella se realiza una breve conversación individual o en grupo donde pueden explicar su trabajo, "¿por qué dibujaste ese juego?", "¿qué representa esa parte de tu huella digital?". Esta etapa permite profundizar en la comprensión de sus elecciones y evaluar cómo reconocen su presencia en el entorno digital.



Mejorar (Reflexionar y corregir)

Se promueve la reflexión sobre su trabajo al preguntar “¿crees que te faltó algo por incluir?”, “¿hay algo que haces en internet y no recordaste poner?”. Se refuerza la idea de que todo lo que hacemos en línea, sea divertido, cotidiano o incluso sin darnos cuenta, forma parte de nuestra huella digital y deja una marca que otros podrían ver o guardar.

Compartir (Comunicar resultados y conclusiones)

Para cerrar la actividad se propone compartir los trabajos realizados entre todas las personas participantes. Se comentan las similitudes y diferencias entre las huellas digitales representadas, reforzando el mensaje clave, así como una huella física deja rastro, todo lo que hacemos en internet también lo deja. Por eso es importante actuar con cuidado y siempre con el acompañamiento de una persona adulta de confianza.

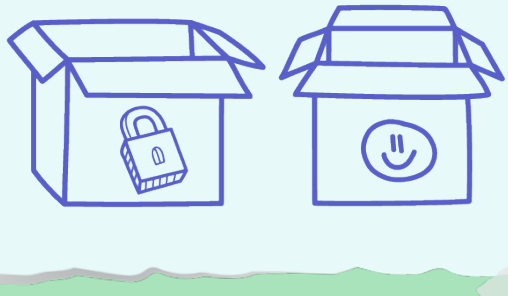
¿Puedo compartirlo?

Objetivo

Aprender a diferenciar la información que se puede compartir y la que no, analizando con la ayuda de la familia ejemplos de datos seguros y privados, para tomar decisiones responsables y proteger la privacidad en línea.

Materiales sugeridos

- Una variedad de imágenes o tarjetas con nombres que representen diferentes tipos de información personal y no personal. Algunas sugerencias incluyen una fotografía familiar, una imagen que simbolice una dirección (como una casa con un número), su comida favorita, un dibujo infantil, entre otros.
- Dos cajas grandes o recipientes similares para clasificar la información. Una de ellas debe tener un dibujo de un candado (para representar la información privada o que no debe compartirse), y la otra puede tener una imagen amigable como una carita sonriente (para representar información pública o que sí se puede compartir).



Preguntar (Identificar la necesidad o problema inicial)

Se inicia una conversación guiada con las personas estudiantes sobre los secretos y la información que no se debe contar a cualquier persona. Se les pregunta: "¿qué cosas les gusta contar solo a su familia o amigos cercanos?", "¿está bien contarle a cualquier persona dónde vivimos o cómo se llama nuestra mascota?". A través del diálogo se introduce la idea de que así como cuidamos algunos secretos en la vida cotidiana también debemos aprender a proteger cierta información cuando usamos internet.

Imaginar (Generar soluciones y conceptos)

Se propone una situación imaginaria "vamos a pensar que estamos usando una aplicación, viendo videos o jugando en línea, y de repente alguien empieza a hacernos preguntas. ¿qué cosas podríamos responder sin problema y cuáles no deberíamos decir?". Se invita a reflexionar sobre los distintos tipos de información que compartimos y a imaginar cómo nos sentiríamos si alguien desconocido supiera cosas personales nuestras.

Planificar (Diseñar la representación)

Se presentan dos cajas, una con un candado cerrado que representa la información privada y otra con una cara amigable que representa la información pública. Se muestran tarjetas o imágenes con diferentes tipos de datos: nombre completo, dirección, foto familiar, comida favorita, dibujo personal, nombre de su mascota, entre otros. Se explica que deberán pensar muy bien en cuál de las dos cajas debería ir cada imagen según si es algo que se puede compartir o no.

Crear (Construir el modelo)

Las personas estudiantes clasifican las tarjetas colocándolas en la caja correspondiente. Esta actividad les permite construir una representación visual de la información que consideran privada o pública. Pueden trabajar individualmente, en parejas o en pequeños grupos fomentando el diálogo y la toma de decisiones en conjunto.

Experimentar (Probar y evaluar el diseño)

Mientras realizan la actividad, se abre un espacio para comentar las decisiones tomadas "¿por qué pusiste esa tarjeta en la caja del candado?", "¿crees que esa información es segura para compartir en internet?". A través de estas preguntas, se analiza el criterio de cada grupo y se promueve la evaluación crítica de sus elecciones.

Mejorar (Reflexionar y corregir)

Al terminar, se invita a revisar las elecciones hechas: "¿hay alguna tarjeta que ahora piensan que debería ir en otra caja?", "¿cambiarían algo después de escuchar a sus compañeros?". Esta reflexión permite reforzar el criterio de protección de datos personales y comprender mejor los riesgos de compartir información privada en espacios digitales.

Compartir (Comunicar resultados y conclusiones)

Para finalizar se propone que cada grupo o persona estudiante comparta una conclusión o algo nuevo que aprendió. Se retoma el mensaje clave de la actividad, así como en la vida real no le contamos todo a cualquier persona, en internet también debemos cuidar qué compartimos y con quién. Algunas cosas son solo nuestras y está bien protegerlas.

La pantalla se apaga

Objetivo

Incentivar el uso consciente y equilibrado de la tecnología, desde un acompañamiento a las personas estudiantes, en la identificación de buenas prácticas, que fomenten la responsabilidad y el aprovechamiento positivo de las herramientas digitales.

Materiales sugeridos

- Dispositivo tecnológico (puede ser una tablet de juguete o imágenes impresas).
- Espacio amplio para moverse dentro del escenario educativo.
- Elemento sonoro o visual que indique la señal para “apagar la pantalla” (puede ser una campana, palmas o una imagen con el ícono de encendido/apagado).
- Una pizarra con la frase: “Después de la pantalla, también se juega”, que refuerce el mensaje de la actividad.

Preguntar (Identificar la necesidad o problema inicial)

Se inicia una conversación con las personas estudiantes sobre lo que suelen hacer frente a una pantalla, como ver videos, jugar, hacer videollamadas, escuchar música o usar aplicaciones. A partir de sus respuestas, se plantea una reflexión "¿está bien usar pantallas todo el tiempo?", "¿cómo se siente nuestro cuerpo después de estar mucho rato sentados frente a una pantalla?". A través del diálogo se introduce la idea de que las pantallas pueden ser divertidas pero también es necesario equilibrar su uso con otras actividades importantes para el bienestar físico y mental.

Imaginar (Generar soluciones y conceptos)

Se invita a imaginar cómo podrían ser esas pausas saludables durante el uso de pantallas. Se les pregunta "¿qué podríamos hacer cuando sentimos que ya hemos estado mucho tiempo frente a una pantalla?", "¿qué movimientos o juegos nos ayudarían a sentirnos mejor?". Se anima a compartir ideas sobre cómo cuidar el cuerpo mientras se disfruta de la tecnología.

Planificar (Diseñar la representación)

Se explica que harán un juego para representar momentos con "pantalla encendida" y "pantalla apagada". Antes de empezar se acuerda una señal que puede ser una palabra clave o un sonido que indicará cuándo deben hacer una pausa. Se organiza el espacio para permitir movimiento libre y se anticipan las acciones que podrán realizar cuando se apague la pantalla como estirarse, caminar, saltar u otra pausa activa.

Crear (Construir el modelo)

Se desarrolla el juego, las personas estudiantes imitan el uso de diferentes dispositivos (mirar televisión, usar una tableta, jugar en una computadora). Cuando escuchan la señal acordada, deben simular que apagan su pantalla, separarse del dispositivo imaginario y realizar una pequeña actividad física. Al reiniciarse la pantalla, vuelven a su posición y continúan la simulación. Esta dinámica puede repetirse varias veces, alternando entre momentos activos y momentos frente a la pantalla.

Experimentar (Probar y evaluar el diseño)

Durante el juego, se observan las reacciones del grupo, cómo responden al cambio, qué actividades físicas prefieren y cómo equilibran ambos momentos. Se conversa brevemente entre rondas: "¿cómo se sintieron al moverse?", "¿qué parte les gustó más?". Esta evaluación ayuda a identificar qué tan conscientes están del impacto del tiempo de pantalla en su bienestar.

Mejorar (Reflexionar y corregir)

Al finalizar se promueve una reflexión grupal "¿creen que sería bueno hacer esto en casa?", "¿qué podrían hacer diferente cuando usan mucho el celular o la tableta?". Se anima a pensar en pequeñas acciones que pueden aplicar en su vida cotidiana para cuidar el cuerpo y la mente mientras disfrutan de la tecnología.

Compartir (Comunicar resultados y conclusiones)

Se invita a cada persona estudiante a compartir una idea o consejo que podrían dar a otras personas sobre cómo hacer pausas cuando usan pantallas. Se cierra la actividad reforzando el mensaje principal: la tecnología es parte de nuestra vida y puede ser divertida pero también es importante saber cuándo parar, moverse y disfrutar de otros juegos y momentos sin pantallas.

b. Primaria

Mi primer contrato digital

Objetivo

Fomentar el compromiso con el uso responsable de la tecnología mediante la creación de un contrato visual y participativo, para establecer acuerdos sobre el uso seguro y consciente de internet, dispositivos y aplicaciones.

Materiales sugeridos

- Cartulina o papel periódico para el contrato colectivo.
- Lápices de escribir, crayolas, marcadores o lápices de colores.
- Imágenes impresas o dibujos hechos para ilustrar las normas.
- Almohadilla con tinta o pintura para firmar con huellas dactilares (opcional).
- Copias individuales del contrato en formato pequeño para que lo lleven a casa y lo firmen con su familia (opcional).

Preguntar (Identificar la necesidad o problema inicial)

Se inicia una conversación grupal sobre las normas que las personas estudiantes ya conocen y aplican en casa o en la escuela como reglas para cruzar la calle, para cuidar los juguetes o para compartir con los demás. A partir de sus respuestas, se plantea una nueva pregunta "¿y qué pasa cuando usamos una tablet, un celular o la computadora? ¿deberíamos tener reglas también para eso?". Se abre el diálogo hacia la idea de que el uso de la tecnología como cualquier otra actividad requiere cuidado, respeto y límites.

Imaginar (Generar soluciones y conceptos)

Se invita a imaginar cuáles serían esas reglas que nos ayudarían a usar la tecnología de forma segura, respetuosa y divertida. A través de preguntas como por ejemplo: "¿qué cosas harías siempre antes de usar un dispositivo?", "¿qué reglas crees que te ayudan a estar más seguro en internet?", se generan ideas que serán la base para construir acuerdos colectivos.

Planificar (Diseñar la representación)

A partir de lo conversado se propone crear un contrato digital donde se reúnan las reglas básicas que todos consideran importantes para un uso responsable de la tecnología. Se planifica cómo lo representarán, se usarán frases simples, claras y acompañadas por imágenes o dibujos que ilustran cada acuerdo. Esto facilita la comprensión para las personas más pequeñas y fortalece el vínculo entre palabra e imagen.

Crear (Construir el modelo)

En conjunto, el grupo redacta los acuerdos y los ilustra. Algunas frases pueden ser como “pido permiso antes de usar la tablet”, “uso la computadora con un adulto cerca”, “no comparto fotos ni datos con personas que no conozco”, “trato bien a los demás en los juegos”. Luego, se firma el contrato de manera colectiva, ya sea escribiendo su nombre, inicial o colocando su huella dactilar como símbolo de compromiso con las normas acordadas.

Experimentar (Probar y evaluar el diseño)

Durante la creación del contrato se generan espacios de intercambio para revisar y evaluar lo que están incluyendo como “¿esta regla nos ayuda a cuidarnos entre todos?”, “¿creen que falta alguna?”, “¿es clara para todos?”. Este momento permite reforzar la comprensión del sentido de cada norma y evaluar si representa realmente lo que quieren comprometerse a cumplir.

Mejorar (Reflexionar y corregir)

Una vez terminado el contrato se hace una revisión final con todo el grupo. Se invita a reflexionar, “¿creen que podrán cumplir con estas reglas en casa también?”, “¿qué pueden hacer si alguien no cumple alguna?”. Si es necesario se ajustan frases o se agregan nuevas ideas. Se refuerza la noción de que este contrato no es para castigar sino para acompañar y cuidar el uso de la tecnología.

Compartir (Comunicar resultados y conclusiones)

El contrato se exhibe en un lugar visible del escenario educativo como recordatorio colectivo. Además se puede entregar una versión reducida y personalizada para que cada persona estudiante la lleve a casa donde podrá firmarla junto con su familia. Así se promueve la continuidad del compromiso también en el hogar, fortaleciendo el vínculo entre el centro educativo y la familia en torno al uso saludable de la tecnología.

Superhéroes y Superheroínas digitales

Objetivo

Fortalecer las habilidades sociales y la convivencia positiva en línea mediante un comportamiento respetuoso y responsable en entornos digitales que incluya la empatía, el buen trato y la resolución pacífica de conflictos en juegos, redes y otros espacios virtuales.

Materiales sugeridos

- Cartulina, lámina de Foam o tela para crear capas, máscaras o insignias de “superhéroes digitales”.
- Lápices de escribir, crayolas, marcadores o lápices de colores.
- Goma y tijeras.
- Tarjetas con situaciones problemáticas o comunes en línea (por ejemplo, recibir un mensaje grosero, ver a alguien que molesta a otro en un juego, encontrar una imagen desagradable, no saber qué hacer al recibir una solicitud de amistad).
- Espacio amplio para dramatizar o compartir las soluciones en grupo.

Preguntar (Identificar la necesidad o problema inicial)

La actividad comienza con una conversación sobre cómo nos comportamos en el mundo real, cómo saludamos, cómo pedimos ayuda, qué hacemos cuando jugamos con otros compañeros y otras compañeras. Luego se plantea una comparación "¿y cuando estamos en internet o jugamos en línea, nos comportamos igual?", "¿creen que también hay reglas o formas correctas de tratar a los demás en esos espacios?". A partir de este diálogo se introduce la idea de que en el mundo digital también podemos ser personas respetuosas, amables y valientes, y que todos tenemos el poder de ser superhéroes y superheroínas digitales.

Imaginar (Generar soluciones y conceptos)

Se invita a imaginar cómo sería un superhéroe o una superheroína digital, "¿qué cosas haría?", "¿cómo ayudaría a otros cuando alguien no se porta bien en un juego o en un chat?", "¿qué haría si ve algo que lo hace sentir incómodo o triste en internet?". Se conversa sobre valores como el respeto, la empatía, la valentía, la responsabilidad o la honestidad y cómo estos pueden guiar nuestro comportamiento en línea.

Planificar (Diseñar la representación)

El grupo se prepara para crear su personaje de superhéroe o superheroína digital. Se les propone pensar en un nombre, un símbolo, un valor principal que representen (por ejemplo, Super Respeto, Valiente Digital, Capitana Empatía) y cómo podrían representarlo visualmente. Se planifica la elaboración de elementos como una insignia, una capa, una máscara o cualquier otro accesorio que les ayude a representar su identidad digital positiva.

Crear (Construir el modelo)

Cada persona estudiante diseña su personaje de superhéroe o superheroína digital utilizando materiales disponibles como cartulina, marcadores, telas, stickers, entre otros. Representan gráficamente su valor (por ejemplo, con un rayo que simboliza acción rápida para ayudar, o un corazón que representa cuidado por los demás). Este personaje es una forma simbólica de comprometerse con un comportamiento positivo en entornos digitales.

Experimentar (Probar y evaluar el diseño)

Se presentan tarjetas con situaciones problemáticas que pueden ocurrir en contextos digitales como un mensaje irrespetuoso, una solicitud de datos personales, una persona que molesta a otra en un chat, entre otras. De forma individual o en grupo, cada persona estudiante debe responder como su superhéroe o superheroína "¿qué harías vos en esta situación?", "¿cómo usarías tu poder digital para ayudar?". Se promueve que expresen acciones como ignorar mensajes dañinos, pedir ayuda a una persona adulta, proteger su información o apoyar a un amigo que está siendo molestado.

Mejorar (Reflexionar y corregir)

Luego de discutir varias situaciones se reflexiona en grupo, "¿alguna situación fue difícil de resolver?", "¿creen que podrían actuar así en la vida real, no solo en el juego?", "¿qué podrían hacer si se equivocan y no actúan como su superhéroe?". Esta etapa permite fortalecer el pensamiento crítico y reconocer que aprender a comportarse en el mundo digital también es un proceso que requiere práctica y apoyo.

Compartir (Comunicar resultados y conclusiones)

Para cerrar cada persona estudiante se presenta con su nombre de superhéroe o superheroína y el valor que representa, explicando brevemente cómo ayudará a los demás en el mundo digital. Se puede hacer una pequeña ceremonia donde se reconozca a cada uno como defensor o defensora de una buena convivencia en línea. Se refuerza el mensaje final, tener buenos comportamientos digitales no es solo una elección personal sino una forma de cuidar a los demás, construir espacios seguros y hacer del mundo digital un lugar mejor.

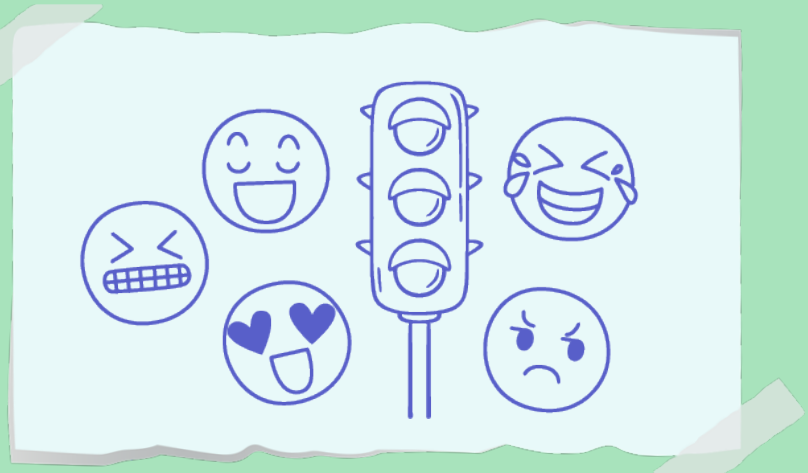
Semáforo de emociones digitales

Objetivo

Identificar las emociones y sentimientos durante la interacción con dispositivos, juegos en línea o redes sociales, para el fomento del autocuidado emocional y la gestión responsable de las experiencias digitales.

Materiales sugeridos

- Cartel de un semáforo con tres colores (verde, amarillo, rojo).
- Tarjetas con situaciones digitales cotidianas (ej. ganar en un juego, que alguien no me responda un mensaje, que mi internet se corte, que un amigo me felicite en línea).
- Emojis impresos o fichas con caritas que representen diferentes emociones.
- Hojas individuales para que cada persona estudiante cree su propio "termómetro de emociones" (opcional).



Preguntar (Identificar la necesidad o problema inicial)

Se inicia la actividad presentando una pregunta clave al grupo "¿alguna vez algo en internet o en un juego te hizo sentir raro, incómodo o muy feliz?" A partir de sus respuestas se introduce el concepto de que las emociones también aparecen cuando usamos tecnología, y que es importante aprender a reconocerlas. Para ayudarnos con esto, se presenta el semáforo como una herramienta que nos guía según cómo nos sentimos, el verde representa emociones agradables o seguras, el amarillo emociones de duda o alerta, y el rojo emociones negativas o de peligro.

Imaginar (Generar soluciones y conceptos)

Se invita a imaginar cómo reaccionarían ante distintas situaciones digitales. Se conversa con preguntas como "¿qué pasaría si un mensaje te hace sentir incómodo?", "¿y si ves algo que no entiendes o te asusta?", "¿cómo sabrías que es momento de pedir ayuda?". Se anima a pensar que, así como usamos un semáforo para saber cuándo avanzar o detenernos en la calle también podemos usarlo para escuchar nuestras emociones cuando estamos frente a una pantalla.

Planificar (Diseñar la representación)

Se prepara un semáforo visual, ya sea en formato físico o en una pizarra, con los tres colores claramente diferenciados, se explica el significado de cada uno y se presentan tarjetas con diferentes situaciones relacionadas con el uso de tecnología como ver un video divertido, recibir un mensaje de un desconocido, jugar con amigos en línea, encontrar algo que da miedo, entre otros. Se explica que cada persona estudiante o grupo deberá decidir en qué color del semáforo colocar cada situación, según cómo creen que se sentirían.

Crear (Construir el modelo)

Durante la dinámica, la persona docente lee una por una las tarjetas en voz alta. Luego de escuchar cada situación, el grupo decide colectivamente o por turnos dónde ubicarla en el semáforo. Esta representación visual permite construir un modelo claro de clasificación emocional vinculado a contextos digitales reales o posibles.

Experimentar (Probar y evaluar el diseño)

Una vez clasificadas varias tarjetas se abre un espacio de diálogo para reflexionar "¿por qué pusiste esta situación en el amarillo?", "¿qué te haría sentir más seguro en esa situación?", "¿creen que todos se sentirían igual?". Este intercambio enriquece la comprensión de las emociones propias y ajenas, y permite evaluar cómo las situaciones digitales impactan emocionalmente a cada persona de forma distinta.

Mejorar (Reflexionar y corregir)

Se promueve la autorreflexión sobre lo que se sintió durante la actividad: "¿hubo alguna tarjeta que cambiarías de color?", "¿qué puedes hacer cuando una emoción te incomoda frente a una pantalla?", "¿a quién podrías pedir ayuda?". Esta etapa busca fortalecer la autorregulación emocional y la capacidad de tomar decisiones más conscientes ante señales de malestar.

Compartir (Comunicar resultados y conclusiones)

Para finalizar se destaca que todas las emociones son válidas y que prestarles atención nos ayuda a cuidarnos. Se invita a cada persona estudiante a compartir una idea o consejo sobre qué hacer cuando algo en internet los hace sentir mal o inseguros. Se refuerza el mensaje clave, si algo nos incomoda podemos parar, pedir ayuda o elegir otra actividad que nos haga sentir mejor.

c. Secundaria

Objetivo

Desarrollar pensamiento crítico frente a la información falsa que circula en internet y redes sociales, para tomar decisiones responsables y fundamentadas en datos verificados.

Materiales sugeridos

- Fragmentos de noticias reales, noticias falsas y titulares manipulados (impresos o proyectados).

Preguntar (Identificar la necesidad o problema inicial)

La actividad comienza con una pregunta generadora: "¿todo lo que ves en internet es verdad?", seguida de ejemplos reales o cercanos de noticias dudosas, rumores virales o desinformación en redes. Se plantea la necesidad de aprender a distinguir entre información confiable y contenidos falsos o manipulados, y se introduce la idea de que en el mundo digital, compartir sin verificar también tiene consecuencias.

Imaginar (Generar soluciones y conceptos)

Se invita a imaginar distintas formas en que podríamos comprobar si una información es verdadera como buscar fuentes, contrastar datos, analizar quién la publica, entre otros. A través de preguntas como "¿qué harías si te llega esta noticia por WhatsApp?" o "¿cómo podrías saber si es real?" Se fomenta la generación de estrategias para enfrentar la desinformación desde una actitud crítica y activa.

Planificar (Diseñar la representación)

La persona docente presenta una serie de fragmentos de información, pueden ser capturas de pantalla, titulares llamativos, mensajes virales o extractos de noticias. Algunos serán verdaderos, otros falsos o manipulados. Se organizan equipos o se trabaja de forma individual y se plantea el desafío de analizar cada fragmento y decidir su nivel de veracidad (real, falso, manipulado) justificando cada decisión con argumentos claros.

Crear (Construir el modelo)

Los grupos examinan los fragmentos de información utilizando criterios como fuente, redacción, fecha, imágenes, y tono del mensaje. Luego elaboran una tabla, afiche o presentación donde clasifican cada caso e incluyen su justificación. Este proceso permite construir una representación organizada del análisis crítico que han hecho, visualizando cómo se llega a una conclusión fundamentada.

Experimentar (Probar y evaluar el diseño)

Cada grupo expone sus decisiones y justificaciones, comparando resultados con los de sus compañeros y compañeras. Se analiza si hubo desacuerdos, qué argumentos fueron más sólidos y cómo se pueden mejorar los criterios de verificación. Este intercambio permite validar el razonamiento crítico, identificar sesgos y evaluar la solidez de las fuentes utilizadas.

Mejorar (Reflexionar y corregir)

Se promueve la autorreflexión sobre lo que se sintió durante la actividad: "¿hubo alguna tarjeta que cambiarías de color?", "¿qué puedes hacer cuando una emoción te incomoda frente a una pantalla?", "¿a quién podrías pedir ayuda?". Esta etapa busca fortalecer la autorregulación emocional y la capacidad de tomar decisiones más conscientes ante señales de malestar.

Compartir (Comunicar resultados y conclusiones)

Para cerrar, se construye colectivamente una lista de buenas prácticas para verificar información antes de compartirla, que puede exponerse en el ambiente de aprendizaje o compartirse digitalmente. Se refuerza el mensaje de que en tiempos de sobreinformación, ser un usuario crítico y consciente es tan importante como tener acceso a la tecnología. Cada persona puede ser parte del cambio hacia una comunidad digital más segura, ética y reflexiva.

Objetivo

Favorecer una relación saludable y consciente con la tecnología mediante la autorregulación emocional, el autocuidado y una reflexión crítica frente al uso de redes sociales.

Materiales sugeridos

- Tarjetas con frases o situaciones comunes en redes (por ejemplo "No recibí likes", "Todos tienen mejor vida que yo", "Tengo miedo de perderme algo").
- Cartulina con columnas: "Me hace bien / Me afecta / Me presiona".
- Lápices de escribir, crayolas, marcadores o lápices de colores.

Preguntar (Identificar la necesidad o problema inicial)

La actividad inicia con una conversación guiada sobre cómo nos sentimos al usar redes sociales. Se plantea una pregunta inicial: "¿alguna vez sentiste presión, comparaciones o malestar al ver lo que otros publican?" A partir de esto se entregan tarjetas con situaciones comunes en redes como recibir pocos likes, sentir que hay que responder siempre, seguir modas y se invita a clasificarlas según cómo les hacen sentir, ya sean positivas, negativas o que generan presión emocional.

Imaginar (Generar soluciones y conceptos)

Después de clasificar las tarjetas, se abre un espacio para imaginar qué se podría hacer en cada caso para cuidar el bienestar personal. Se proponen preguntas como por ejemplo: "¿qué podrías hacer si te sentís mal con lo que ves en redes?", "¿cómo te gustaría que fueran las redes sociales para que te hagan bien?", "¿qué tipos de cuentas o contenidos te inspiran y te hacen sentir bien contigo mismo o contigo misma?"

Planificar (Diseñar la representación)

Según los intereses del grupo, se elige una forma de profundizar el análisis colectivo:

- Una mesa redonda o debate sobre los efectos emocionales del uso de redes.
- La creación de un podcast breve, donde se compartan testimonios, consejos o reflexiones.
- Un afiche o campaña visual con mensajes sobre autocuidado digital.
- Un muro digital con frases que promuevan el bienestar, los límites y el pensamiento crítico frente a lo que vemos en línea.

Se organizan roles, temas y tiempos para desarrollar la actividad elegida.

Crear (Construir el modelo)

Las personas estudiantes desarrollan el producto seleccionado. Para acompañar esta actividad se sugiere el uso de herramientas digitales que potencien la expresión creativa y colaborativa. Por ejemplo, se puede utilizar una herramienta interactiva para dinamizar una mesa redonda o debate, permitiendo que el grupo participe con encuestas o preguntas en tiempo real. En caso de elegir la creación de un podcast breve se pueden emplear herramientas digitales para grabar y editar testimonios o reflexiones, así como programas de diseño para crear la portada del episodio. Para quienes opten por una campaña visual, existen plataformas que ofrecen plantillas dinámicas para crear mensajes sobre autocuidado digital. Finalmente, si se desea construir un muro digital colaborativo, se pueden utilizar herramientas en línea que permitan reunir frases, ideas y recursos compartidos por el grupo, promoviendo la reflexión colectiva en torno al bienestar emocional en entornos digitales. La creación debe reflejar tanto el análisis emocional como las posibles soluciones que cada grupo propone.

Experimentar (Probar y evaluar el diseño)

Se presentan los productos al grupo, se escuchan los podcasts, se realiza el debate o se exponen los afiches. A partir de estas presentaciones se invita a la evaluación colectiva “¿qué ideas les resonaron más?”, “¿qué propuesta les pareció útil o aplicable?”, “¿qué emociones reconocieron en común?”. Esta instancia permite validar los aprendizajes y valorar la diversidad de experiencias.

Mejorar (Reflexionar y corregir)

Se promueve una reflexión detallada sobre el uso que cada persona hace de las redes sociales. Se pregunta: "¿hay algo que podrías cambiar o mejorar en tu relación con las redes?", "¿qué cuentas deberías dejar de seguir?", "¿qué hábitos digitales podrías implementar para sentirte mejor?". Se refuerza que cuidarse emocionalmente también es parte de ser usuarios responsables y conscientes.

Compartir (Comunicar resultados y conclusiones)

Para cerrar se elaboran propuestas concretas para fortalecer el bienestar digital, que pueden escribirse en un mural, grabarse en formato audiovisual o compartirse por medios escolares. Algunas ideas que pueden surgir:

- Hacer pausas conscientes de redes.
- Seguir cuentas que inspiren o promuevan bienestar.
- Dejar de seguir contenido que genera comparación o malestar.
- Hablar con alguien de confianza si algo en redes afecta emocionalmente.

Se concluye reforzando que las redes pueden ser herramientas positivas, siempre que se usen con conciencia, límites y cuidado emocional.

Mi yo digital ideal

Objetivo

Fomentar la responsabilidad personal y la coherencia entre su identidad digital y sus acciones en línea, mediante la imaginación y proyección de una versión digital de sí mismos que desean construir, en concordancia con sus valores, intereses y el impacto que quieren tener en su entorno digital.

Materiales sugeridos

- Hojas en blanco o plantilla con silueta de perfil digital.
- Lápices de escribir, crayolas, marcadores o lápices de colores.
- Una pizarra con la frase: "¿Cómo quiero que me vean en internet?"

Preguntar (Identificar la necesidad o problema inicial)

La actividad comienza con una pregunta que invita a la introspección: "¿cómo te gustaría que te vean las demás personas cuando estás en internet? ¿qué imagen estás construyendo con lo que publicás, comentás o compartís?". Se propone reflexionar sobre la identidad digital como una parte de quiénes somos, que también se proyecta en redes sociales, plataformas y espacios digitales. Se plantea el desafío de construir una presencia en línea auténtica, positiva y coherente con los propios valores.

Imaginar (Generar soluciones y conceptos)

Se invita a imaginar un yo digital ideal, no en términos de apariencia sino desde los intereses, talentos, valores y acciones que les gustaría reflejar en el mundo digital. Se motiva a pensar más allá de la popularidad o los likes, y a enfocarse en quiénes desean ser, cómo quieren expresarse y qué impacto desean tener en su comunidad digital.

Planificar (Diseñar la representación)

Cada persona estudiante recibe una hoja o plantilla con el título “Mi yo digital ideal” donde podrán escribir palabras clave, valores que los representen como respeto, empatía, creatividad, acciones que desearían llevar adelante en internet, cómo crear contenido útil, compartir ideas, ayudar a otros o incluso diseñar un perfil simulado con sus intereses, metas y estilo de comunicación en línea. También pueden incluir íconos, hashtags, colores o imágenes que identifiquen esa versión de sí mismos y de sí mismas.

Crear (Construir el modelo)

Durante el desarrollo de la actividad las personas estudiantes plasman sus ideas en la hoja entregada, combinando texto, símbolos o elementos gráficos que representen su identidad digital ideal. Esta creación les permite tomar distancia del “yo actual” para visualizar hacia dónde quieren avanzar en el entorno digital y qué decisiones los acercan a esa versión más alineada con sus valores y propósito personal.

Experimentar (Probar y evaluar el diseño)

Quienes deseen compartir voluntariamente su representación pueden hacerlo en grupo. A través del intercambio se genera un diálogo sobre las diferencias, coincidencias e inspiraciones que surgen al ver los perfiles de los demás. Se pregunta: "¿qué te llamó la atención del perfil de tu compañero o de tu compañera?", "¿qué parte de tu perfil ya estás mostrando en redes?", "¿qué podrías cambiar para acercarte a ese ideal?".

Mejorar (Reflexionar y corregir)

Se promueve una reflexión personal sobre cómo las decisiones que se toman hoy en internet contribuyen a construir ese "yo digital ideal". Se alienta a identificar cambios concretos que podrían implementar como cuidar el lenguaje, pensar antes de publicar, compartir cosas que los representen de forma auténtica, entre otros. La mejora no se plantea como una corrección obligatoria sino como una evolución consciente.

Compartir (Comunicar resultados y conclusiones)

Para cerrar, se pueden colgar las representaciones en el escenario educativo o subirlas a un muro digital a modo de galería reflexiva. También se pueden emplear herramientas de diseño en línea para transformar el perfil ideal en una pieza visual más elaborada. Se refuerza la idea de que la identidad digital no es algo que se actúa, sino que se construye a diario con cada acción en línea y que proyectar una versión auténtica y respetuosa de uno mismo fortalece el bienestar personal y colectivo en los entornos digitales.

2. Ciudadanía digital, seguridad y bienestar en la educación

En la actualidad, la educación no solo se centra en el aprendizaje académico, sino también en formar personas estudiantes críticas, responsables y capaces de desenvolverse de manera segura en entornos digitales. La integración de competencias digitales, pensamiento crítico, ética, ciudadanía digital y bienestar socioemocional se convierte en un pilar fundamental para preparar a esta población frente a los retos tecnológicos y sociales del siglo XXI.

El enfoque STEAM (Ciencia, Tecnología, Ingeniería, Arte y Matemáticas) y las metodologías activas junto con el Aprendizaje Socioemocional (SEL), permiten abordar estos desafíos de forma interdisciplinaria, promoviendo habilidades cognitivas, socioemocionales y éticas, esenciales para el desarrollo integral de las personas estudiantes (Walsh et al., 2022).

a. Competencias digitales

La educación digital no puede limitarse al uso técnico de herramientas, sino que debe promover habilidades de pensamiento crítico, análisis de información y juicio ético (Cambridge University, 2020). Esto incluye enseñar a las personas estudiantes a evaluar fuentes, identificar sesgos, juzgar la intención detrás de los mensajes y aplicar un pensamiento reflexivo al interactuar con medios digitales. Por ejemplo, al leer una noticia en línea las personas estudiantes deben ser capaces de preguntarse: ¿quién está detrás de esta información?, ¿es confiable?, ¿cuál es el propósito de compartirla?

La integración de la alfabetización digital crítica y reflexiva en el ambiente de aprendizaje permite que las personas estudiantes sean participantes activas y responsables, capaces de tomar decisiones informadas que protejan su bienestar y el de su comunidad (Kumar, 2024). La educación ética digital incluye enseñar principios clave como la privacidad, la seguridad y la propiedad intelectual, así como asumir responsabilidades en el ámbito virtual.

Es fundamental también el desarrollo de habilidades socioemocionales como la empatía, la resiliencia y la autorregulación, que les permitan gestionar conflictos y prevenir riesgos como el ciberacoso. De esta forma, si una persona estudiante presencia un caso de acoso en línea, debe saber cómo intervenir de manera respetuosa y si es necesario, cómo buscar ayuda.

De este modo, la educación digital no solo se trata de aprender a usar la tecnología, sino de formar ciudadanos digitales responsables que promuevan una convivencia sana y segura en los espacios virtuales.

b. Integración STEAM y metodologías activas

El enfoque STEAM permite abordar la ciudadanía digital de manera interdisciplinaria. Aprovechando la tecnología, la ingeniería y la apropiación tecnológica, para enseñar seguridad digital y gestión de información, y desarrollando el pensamiento analítico a través de las ciencias y matemáticas. Las artes complementan esta formación al fomentar la creatividad, la autoexpresión y la reflexión. De esta manera, las personas estudiantes no solo aprenden contenidos específicos, sino que también desarrollan habilidades para resolver problemas complejos y evaluar los riesgos de sus decisiones en entornos digitales.

Por otro lado, las metodologías activas como el aprendizaje basado en proyectos, aprendizaje basado en retos, aprendizaje basado en juegos, la indagación guiada, el análisis de casos y simulaciones de escenarios permiten que las personas estudiantes participen de manera práctica y reflexiva en situaciones que requieren evaluación crítica, resolución de problemas y toma de decisiones éticas (Guevara-Andino & Delgado-Salas, 2024).

Estas estrategias fomentan que las personas estudiantes exploren, experimenten y busquen soluciones de manera autónoma, reforzando la idea de que el aprendizaje digital no es sólo recibir información sino comprender, aplicar y cuestionar su uso.

Además, el aprendizaje colaborativo refuerza la cooperación, la autorregulación y la empatía de tal forma que se va fortaleciendo la convivencia digital y la participación responsable (Gutiérrez-Aguilar et al., 2024). En un contexto STEAM, las personas estudiantes pueden trabajar en equipo para crear prototipos o proyectos que integren principios de seguridad digital, evaluar información relevante y presentar sus resultados de manera clara y creativa, desarrollando así tanto habilidades técnicas como interpersonales.

Al combinar metodologías activas y el enfoque STEAM, se crea un espacio donde las personas estudiantes desarrollan pensamiento crítico, creatividad, colaboración y ética digital. Esto les ayuda a entender que lo que hacen en línea tiene consecuencias reales, fomentando un aprendizaje más consciente que va más allá del escenario educativo y los prepara para moverse de manera segura y responsable en el mundo digital.

c. Responsabilidad y cuidado en la vida digital

La educación digital tiene un propósito claro, formar ciudadanos y ciudadanas capaces de desenvolverse en entornos digitales con seguridad, ética y bienestar emocional. Esto implica enseñar a las personas estudiantes a proteger su información, a comportarse con respeto en línea y a tomar decisiones conscientes sobre qué tipo de información comparten y consumen.

La seguridad digital comienza con la comprensión de la privacidad y la gestión responsable de los datos. Las personas estudiantes deben aprender a crear contraseñas seguras, a reconocer correos o mensajes sospechosos y a entender que su información personal tiene valor. Integrar estos aprendizajes en proyectos STEAM como diseñar una campaña educativa sobre contraseñas o analizar cómo las aplicaciones usan nuestros datos, hace que estos conceptos tengan más relevancia en contextos reales (Walsh et al., 2022).

El autocuidado digital también incluye el bienestar emocional, lo cual se puede trabajar en clase a través de dinámicas que permitan a las personas estudiantes reflexionar sobre cómo responder ante comentarios negativos o situaciones de exclusión digital.
Esto fortalece su capacidad de actuar con calma y respeto, promoviendo el autocontrol y la empatía.

Estos valores no solo reducen conflictos y previenen el ciberacoso sino que también fomentan una convivencia sana en entornos virtuales. Además, es crucial que las personas estudiantes aprendan a pedir ayuda cuando algo les preocupa o les incomoda, sabiendo identificar las herramientas disponibles y las personas adecuadas a las que acudir.

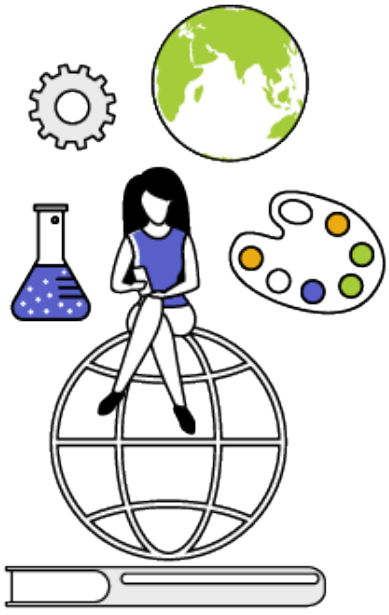
Estas competencias no se desarrollan de manera aislada, la participación activa de toda la comunidad educativa es indispensable para consolidar una cultura digital integrada. Cuando la persona docente modela comportamientos éticos y las los centros educativos apoyan la implementación, el aprendizaje se integra de manera natural en la vida cotidiana (Kumar, 2024). De este modo, se crea un entorno protector en el que la seguridad, la ética y el bienestar digital dejan de ser solo temas de clase para convertirse en valores que guían tanto la convivencia educativa como la vida en sociedad.

d. Reflexión ética y responsabilidad social

La persona docente desempeña un papel esencial al guiar al estudiantado hacia una comprensión más profunda del impacto social, ético y ambiental del uso de la tecnología. No se trata solo de enseñarles a manejar herramientas digitales sino de fomentar una reflexión sobre cómo y para qué las utilizan.

En este contexto, como se sugirió anteriormente, una de las actividades que el grupo puede realizar es el análisis de noticias para identificar si son falsas, verdaderas o manipuladas. A través de esta actividad, la persona docente promueve la reflexión sobre la veracidad de la información y la responsabilidad individual al compartir contenido. Estas conversaciones, siempre dirigidas con empatía, permiten a las personas estudiantes reconocer las implicaciones sociales de su comportamiento digital y desarrollar una conciencia crítica sobre su rol en el ambiente digital.

Integrar estas reflexiones en distintas áreas del currículo como Ciencias, Estudios Sociales, Español o incluso Artes Plásticas, refuerza el vínculo entre la tecnología y la vida cotidiana. En una clase de estudios sociales se puede debatir cómo las redes sociales han transformado la manera en que se construye la memoria colectiva o la opinión pública, en la clase de arte se podrían tratar temas como la autoría y los derechos de imagen y en español cómo el lenguaje digital puede influir en la convivencia en línea.



De este modo, las personas estudiantes no solo aprenden a utilizar las TIC de forma técnica sino que también reflexionan sobre las consecuencias humanas y sociales de sus acciones digitales. Así, el ambiente de aprendizaje se convierte en un espacio clave para construir ciudadanía digital, donde el pensamiento crítico y los valores éticos se desarrollan junto al conocimiento tecnológico.

3. Recursos digitales recomendados

Juego educativo

Interland es un juego educativo, gratuito y de fácil acceso, que enseña a la población infantil sobre seguridad en línea de manera divertida. A través de diferentes niveles y desafíos, las personas estudiantes aprenden conceptos como la gestión de contraseñas, la protección de su información personal y cómo identificar comportamientos abusivos en línea.

Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF)

Ofrece diversos cursos y materiales sobre el uso responsable de la tecnología. Es muy útil para las personas docentes que desean integrar la seguridad digital en su currículo y comprender más a fondo cómo enseñar estos temas. Los recursos están diseñados para brindar un enfoque práctico en la enseñanza.

INCIBE Menores

Ofrece recursos educativos para promover la seguridad digital entre personas estudiantes, personas docentes y familias a través de guías, consejos prácticos, juegos interactivos y materiales para proteger la privacidad en línea.

Common Sense Education

Ofrece una amplia variedad de recursos educativos sobre seguridad digital, privacidad, y bienestar en línea. La plataforma incluye lecciones interactivas, videos y guías para ayudar a las personas estudiantes a comprender la importancia de una navegación segura.

eSafety Commissioner

Agencia que proporciona recursos específicos para personas estudiantes y materiales educativos basados en evidencia para personas docentes, incluyendo formación y marcos para la seguridad en línea.

Videos recomendados

- *¿Por qué atacan a las escuelas? Ciberseguridad en educación*
- *La importancia de proteger nuestra privacidad en Internet*
- *La inteligencia artificial y la educación*

5 SEÑALES DE RIESGO EN LA CONDUCTA DIGITAL EDUCATIVA

La identificación de las señales de riesgo en la conducta de las personas estudiantes es imprescindible para promover la seguridad digital y el bienestar en línea. Estos riesgos pueden ser de contenido, contacto, conducta o contractuales, y tienden a evolucionar desde situaciones leves hasta peligrosas, especialmente cuando involucran a adultos (Ministerio de Educación Pública de Costa Rica, 2016).

Es importante que las personas docentes reconozcan cambios en el comportamiento, signos de acoso, exposición a contenido inapropiado y otras conductas que puedan indicar problemas relacionados con la tecnología.

1. Cambios de comportamiento y consecuencias en el bienestar

Las experiencias negativas en internet se asocian significativamente con una menor calidad de vida y con dificultades conductuales en las personas estudiantes. Los signos de riesgo pueden manifestarse a través de cambios emocionales y psicológicos, tales como respuestas intensas al uso de dispositivos, aislamiento social y pérdida de interés en actividades previamente disfrutadas (Stopbullying.gov, 2021). Estos cambios pueden derivar en afectaciones a la salud mental, como ansiedad, depresión e ideación suicida, ocasionando inestabilidad emocional, inseguridad y falta de confianza en sí mismos (Prkno et al., 2025).

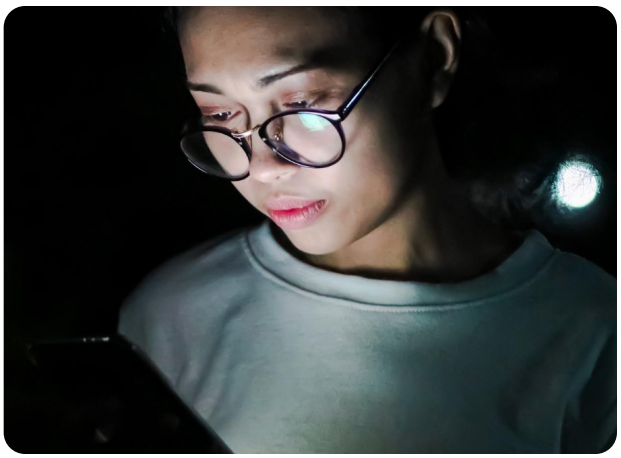
Es importante que las personas docentes y las familias estén atentas a variaciones repentinas en el estado de ánimo o en las relaciones con pares ya que estos cambios muchas veces pasan desapercibidos o se confunden con "etapas" del desarrollo. La expresión emocional en la adolescencia puede volverse más complicada por lo que las señales indirectas, como irritabilidad constante o evasión también deben considerarse.

Asimismo, las víctimas pueden presentar trastornos del sueño, fatiga, dolores de cabeza o problemas digestivos, además de cambios bruscos en su comportamiento, que van desde la agresividad hasta la pasividad o la tristeza extrema. En situaciones graves, algunas personas estudiantes pueden desarrollar conductas autolesivas o agresivas hacia otros, e incluso llegar a experimentar pensamientos suicidas (Lu, 2025). Cuando este tipo de conductas aparecen, es común que exista una dificultad para pedir ayuda o expresar lo que están viviendo, por lo que es fundamental promover un entorno de confianza y escucha activa.

2. Uso de dispositivos, contenido inapropiado y la privacidad

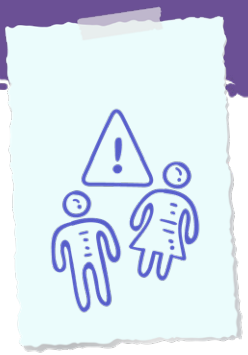
Los cambios en el uso de dispositivos y en el rendimiento académico también constituyen señales de alerta. Algunas personas estudiantes muestran una necesidad constante de estar disponibles a través del celular, incluso durante las horas de sueño. Este comportamiento puede afectar negativamente su concentración, su desempeño escolar y generar rechazo o desmotivación hacia el centro educativo (Lu, 2025). Además, el uso excesivo de pantallas puede alterar los ciclos de sueño, reducir la calidad del descanso y provocar fatiga durante el día, lo que dificulta el aprendizaje y la convivencia. El uso prolongado de dispositivos, especialmente en horas nocturnas, se asocia con un mayor riesgo de experiencias negativas en línea, aislamiento y síntomas depresivos (Prkno et al., 2025).

Además, las personas estudiantes pueden estar expuestas a contenido violento, discursos de odio, pornografía, información sobre autolesiones o drogas, y desafíos virales peligrosos, lo cual impacta negativamente en su bienestar (Ministerio de Educación Pública de Costa Rica, 2016). Muchas veces estos contenidos circulan de forma encubierta o disfrazados de entretenimiento, lo que dificulta que los adultos los identifiquen a tiempo. La circulación de imágenes sexuales, su difusión no consentida, así como la sextorsión y el chantaje, representan amenazas especialmente graves durante la adolescencia, una etapa en la que la validación social y el uso de redes tiene un peso importante.



También se identifican conductas de riesgo vinculadas a la privacidad y el manejo de datos personales así como a una alfabetización digital limitada. Compartir información personal, mantener configuraciones inseguras en redes sociales, utilizar contraseñas débiles o exponerse a fraudes en línea, incrementan la vulnerabilidad de las personas estudiantes (Alsehaimi, 2018). A menudo, esta población no comprende las implicaciones reales de sus acciones en línea, como lo que significa publicar datos personales, permitir el acceso a su ubicación o aceptar solicitudes de desconocidos.

La falta de verificación de fuentes, la descarga de aplicaciones no seguras, el uso malicioso de la tecnología, la ausencia de medidas de respaldo y el uso excesivo de dispositivos que desplazan actividades sociales y académicas, son factores adicionales que aumentan los riesgos (Capuno et al., 2022). Promover una educación digital básica que incluya hábitos seguros, pensamiento crítico y autorregulación, es una estrategia clave para reducir la exposición a estos peligros.



3. ¿Cómo actuar en caso de incidentes?

La detección y el abordaje de incidentes de riesgo digital en personas estudiantes como el ciberacoso, el contacto con desconocidos también conocido como grooming, la suplantación de identidad o la exposición de información personal, requieren un enfoque coordinado que incluya medidas preventivas, acciones inmediatas y el uso de recursos de apoyo. Es fundamental que la identificación de estos incidentes sea temprana, ya que las víctimas a veces pueden no expresar abiertamente lo que están viviendo. Las personas docentes deben estar atentas a señales indirectas de alarma como cambios en el comportamiento o el rendimiento académico para poder intervenir a tiempo y proceder en apego a la normativa vigente.

La intervención debe ser inmediata, asegurando la protección de la víctima, sin minimizar los hechos ni estigmatizar a las personas involucradas y manteniendo la confidencialidad de toda la información (Stopbullying.gov, 2021).

Es importante recordar que la confidencialidad no solo protege a las víctimas sino que también evita que los involucrados, incluidos los agresores y los testigos se sientan desprotegidos, lo que podría empeorar aún más la situación.

a. La prevención integral

La prevención integral busca modificar el entorno educativo, fortalecer las relaciones entre pares y potenciar las capacidades de las personas docentes. Para ello, los centros educativos deben aplicar los reglamentos y protocolos establecidos vigentes sobre el uso de tecnología y seguridad en línea, así como mecanismos de denuncia sólidos para que las personas estudiantes puedan reportar incidentes con confianza (Walsh et al., 2022). Las normas no solo deben ser claras, sino también accesibles y comprendidas por todos los miembros de la comunidad educativa. Los protocolos de seguridad deben ser de fácil acceso e idealmente acompañados de actividades de sensibilización periódicas para garantizar que tanto las personas estudiantes como las personas docentes comprendan las implicaciones de una mala gestión de la seguridad digital.

Además es fundamental implementar monitoreo y vigilancia constante del dominio educativo, las redes y los dispositivos, incluyendo herramientas automatizadas para detectar contenido riesgoso o actividades sospechosas. Las herramientas de monitoreo deben tener una clara justificación educativa y estar orientadas a la protección, siempre dentro de un marco que respete los derechos fundamentales de las personas estudiantes.

b. Acciones inmediatas tras la detección

Una vez identificado un incidente de riesgo digital se deben ejecutar acciones inmediatas que garanticen la protección de la persona estudiante afectada y la contención del daño. Esto incluye detener cualquier agresión digital en curso, intervenir de manera educativa y garantizar que la víctima no sea culpabilizada ni estigmatizada (Stopbullying.gov, 2021). En este sentido es útil ofrecer intervenciones educativas que promuevan la comprensión del daño emocional y psicológico que estos incidentes pueden causar.

Es fundamental escuchar a la persona estudiante para comprender qué ocurrió, cómo se siente y cuáles fueron las circunstancias del incidente. Al mismo tiempo, se debe documentar y registrar todo el incidente, incluyendo fechas, horas, descripciones y pruebas digitales, como capturas de pantalla de mensajes o publicaciones.

Esta documentación no solo es crucial para el abordaje inmediato, sino que también se convierte en una pieza clave en caso de actuación a instancias externas o investigaciones legales. Recordar que la documentación debe ser organizada y resguardada de manera segura, evitando que se filtren detalles que puedan comprometer la confidencialidad del caso.

En situaciones de alto riesgo como delitos graves o violencia sexual, los centros educativos deben realizar la comunicación inmediata a las autoridades competentes. La rapidez en la actuación no solo depende de la gravedad del incidente, sino también de los protocolos y acuerdos previos establecidos con las entidades competentes.

c. Recursos de apoyo y seguimiento

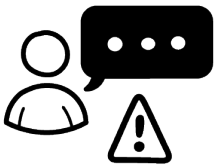
El seguimiento psicosocial es esencial para restaurar el bienestar de la persona estudiante afectada y prevenir nuevas situaciones de violencia. El personal responsable dentro de la institución educativa debe intervenir tanto con la víctima como con su familia, asegurando contención emocional, orientación y activación de rutas de apoyo. Además, es fundamental que los recursos de apoyo sean no solo accesibles sino también apropiados para la situación específica de la víctima. Un apoyo psicosocial personalizado puede marcar una gran diferencia en el proceso de recuperación y restablecimiento del bienestar.

Es fundamental que tanto las personas estudiantes como las personas docentes tengan acceso a servicios de apoyo y emergencia en situaciones de riesgo. A continuación se presenta una tabla que contiene líneas gratuitas y contactos de emergencia disponibles en Costa Rica, donde se pueden solicitar ayuda inmediata o realizar denuncias relacionadas con violencia, ciberacoso, situaciones de riesgo para menores de edad, entre otros. Estos recursos están a disposición para brindar orientación, intervención y protección en momentos críticos.

Institución / Servicio	Contacto	Detalles adicionales
Emergencias nacionales	911	Policía, Bomberos, PANI, INAMU
Ministerio de Educación Pública (MEP)	2256-7011 ext. 6206 www.vidaestudiantil.cr vidaestudiantil@mep.go.cr	Dirección de Vida Estudiantil
	2221- 4102, 2221- 4104 derechosestudiantiles@mep.go.cr	Contraloría de Derechos Estudiantiles
Patronato Nacional de la Infancia	800-2262626	Para adolescentes madres y sus familiares
	1147	Para niños, niñas y adolescentes
	https://pani.go.cr/tramites-y-servicios/denuncias-en-linea/	Denuncias en línea
Defensoría de los Habitantes de la República	https://www.dhr.go.cr/denuncias/formulario_denuncia.aspx	Denuncias en línea
	800-258-7474	Denuncias vía telefónica
Organismo de Investigación Judicial	800-8000-645	Denuncias vía telefónica

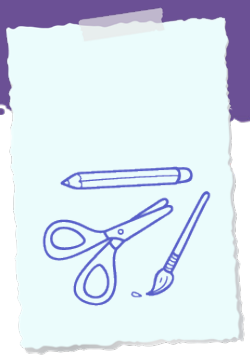
4. Casos hipotéticos

A continuación, se presentan tres casos hipotéticos que ilustran situaciones comunes de riesgo digital en contextos educativos de primaria y secundaria. Estos ejemplos permiten comprender cómo pueden manifestarse distintas problemáticas relacionadas con el uso de la tecnología y qué acciones puede tomar el personal docente ante ellas. Cada caso incluye una descripción breve, el tipo de riesgo involucrado y medidas preventivas que pueden implementarse en el entorno educativo. Su propósito es servir como guía práctica para fortalecer la capacidad de respuesta ante incidentes digitales que afectan el bienestar de las personas estudiantes.

Situación	Tipo de riesgo	Prevención
Una persona estudiante de cuarto año comienza a evitar actividades grupales, se muestra constantemente irritable y su rendimiento académico baja. Se descubre que en un grupo de WhatsApp, varios compañeros publican burlas y mensajes humillantes sobre ella, incluso utilizando stickers ofensivos con su imagen.	Ciberacoso y hostigamiento entre pares. 	Promover una cultura de respeto digital en el escenario educativo. Esto puede lograrse mediante sesiones educativas sobre el uso ético de la tecnología, el impacto del ciberacoso y la importancia de la empatía en entornos virtuales. Además, se deben establecer normas claras sobre el uso de dispositivos y redes dentro del centro educativo, así como fortalecer las habilidades socioemocionales de las personas estudiantes para mejorar la convivencia tanto presencial como digitalmente.

Situación	Tipo de riesgo	Prevención
Dos personas estudiantes de décimo año mantenían una relación sentimental. Luego de una ruptura, una de las personas comparte en un grupo de WhatsApp una captura de pantalla de una videollamada íntima que había tenido con su ex pareja. La imagen se difunde rápidamente entre otras personas estudiantes.	Sexting, imagen íntima compartida y vulneración de privacidad entre pares. 	Incorporar la educación afectivo-sexual y digital en los programas escolares. Esto debe incluir el abordaje de temas como el consentimiento, el respeto a la intimidad, los riesgos del sexting y las consecuencias legales y emocionales de compartir contenido íntimo. Asimismo, se deben establecer canales confidenciales para reportar situaciones similares, y fomentar un ambiente de confianza donde las personas estudiantes se sientan seguras de pedir ayuda.
Durante un receso, una persona docente escucha casualmente una conversación entre un grupo de personas estudiantes de octavo año. Una de ellas comenta que está saliendo con un muchacho mayor que conoció en redes sociales. Aunque nunca se han visto en persona, mantienen contacto frecuente por mensajes y videollamadas. La persona estudiante expresa dudas sobre si realmente es quien dice ser pero siente emoción y presión por seguir hablando con él.	Interacción con adulto desconocido, posible grooming y desconocimiento de riesgos en redes. 	Fortalecer la educación digital con enfoque en el pensamiento crítico y la protección emocional. Las personas estudiantes deben aprender a identificar señales de manipulación en redes sociales, reconocer que no todo lo que se muestra en línea es real y entender el valor de la privacidad y el consentimiento. Las campañas de sensibilización sobre grooming, junto con actividades prácticas sobre seguridad en redes, pueden ayudar a detectar y prevenir a tiempo este tipo de contactos engañosos.

6 ANEXOS



1. Plantilla de planificación con enfoque de seguridad digital

La siguiente plantilla se propone como una herramienta práctica para orientar la planificación de actividades o proyectos educativos que integren la seguridad digital como eje transversal. Su propósito es apoyar a las personas docentes en la identificación de riesgos, la aplicación de medidas preventivas y la promoción del autocuidado digital dentro del proceso de enseñanza y aprendizaje.

La estructura es flexible y adaptable, puede utilizarse tanto para planificar una clase específica como para diseñar proyectos interdisciplinarios de mayor alcance. Cada institución o persona docente podrá ajustarla según sus necesidades, nivel educativo y asignaturas involucradas.

<table>
<tr><td colspan="2">Nombre de la actividad o proyecto
Escriba un título claro y breve que identifique la actividad o proyecto.</td></tr>
<tr><td rowspan="2">Propósito u objetivo general
Describa la finalidad educativa y cómo se vincula con la seguridad digital.</td><td>Nivel educativo
Especifique el grupo de personas estudiantes o participantes a los que está dirigida la actividad.</td></tr>
<tr><td>Duración o fecha
Indique el tiempo estimado o el periodo del proyecto.</td></tr>
<tr><td colspan="2">Competencias o aprendizajes esperados
Enumere las habilidades y conocimientos que se espera desarrollar. Incluya competencias digitales y de seguridad.</td></tr>
<tr><td colspan="2">Desarrollo de actividades
Explique de forma clara las actividades o pasos que se desarrollarán durante la implementación de la propuesta. Incluya el propósito de cada actividad y cómo se abordarán los aspectos de seguridad digital en cada una.</td></tr>
<tr><td>Riesgos digitales identificados
Señale posibles vulnerabilidades o amenazas asociadas a la actividad.</td><td>Medidas preventivas o protocolos de seguridad
Indique acciones concretas para mitigar los riesgos.</td></tr>
<tr><td>Roles y responsabilidades
Detalle las actividades de las personas involucradas.</td><td>Recursos de apoyo
Enlaces, herramientas digitales, documentos o materiales complementarios que apoyen la actividad y la seguridad digital.</td></tr>
<tr><td colspan="2">Evaluación, retroalimentación y mejora continua
Explique cómo se medirá la comprensión y aplicación de buenas prácticas de seguridad digital, puede incluir rúbricas, autoevaluaciones o registros de observación. También utilice este espacio para registrar aprendizajes, retroalimentación o mejoras para futuras actividades.</td></tr>
</table>

2. Glosario

En el ámbito de la ciberseguridad educativa es común encontrar términos provenientes del idioma inglés que describen fenómenos, prácticas o riesgos asociados al uso de entornos digitales. Comprender su significado permite a las personas docentes y personas estudiantes reconocer conductas inapropiadas, identificar amenazas en línea y aplicar estrategias preventivas de forma más efectiva. A continuación, se presentan algunos de los conceptos más utilizados en este campo junto con una breve explicación de su relevancia en el contexto educativo.

a. Phishing

Técnica de engaño utilizada por ciberdelincuentes para obtener acceso no autorizado a información sensible o instalar software malicioso. Suele realizarse mediante correos electrónicos o mensajes falsos con enlaces o archivos adjuntos maliciosos. Es una amenaza común en entornos educativos y puede afectar especialmente a personas estudiantes. Requiere medidas de ciberseguridad para su prevención.

b. Grooming

Delito informático en el que una persona adulta se hace pasar por un menor o una menor en entornos virtuales para ganarse la confianza de niños, niñas o adolescentes con fines sexuales. Puede incluir manipulación, extorsión o explotación, tanto en línea como fuera de ella. Existen dos formas principales: obtener material íntimo sin relación previa para extorsionar, o crear un vínculo de confianza para lograr ese mismo fin.

c. Sexting

Envío voluntario de fotos o vídeos sexualmente explícitos a través de dispositivos móviles. Aunque puede ser consensuado, representa un riesgo si el contenido se difunde sin permiso, lo que constituye una forma de violencia en línea. Esta práctica puede afectar la reputación, la salud emocional y la seguridad digital, especialmente entre adolescentes. La educación debe enfocarse en el consentimiento, el respeto, y la prevención del acoso, sin culpabilizar a quienes comparten sus propias imágenes.

3. Material visual adicional

La vida en entornos digitales ofrece oportunidades de aprendizaje, comunicación y acceso a información, pero también presenta riesgos que requieren atención y manejo responsable.

Con este propósito, se presentan tres infográficos que invitan a reflexionar y actuar frente a la seguridad y el bienestar digital. Contienen información clave para reconocer riesgos, adoptar buenas prácticas y fortalecer hábitos responsables en línea.

Riesgos digitales más comunes

Todas las personas navegan por entornos digitales que pueden ser útiles y entretenidos, pero también presentan riesgos. Conocerlos es clave para protegerse y tomar decisiones seguras en línea.

Personas estudiantes de preescolar y primaria:

Exposición a contenido inapropiado: Encuentran videos, imágenes o juegos que no son adecuados para su edad.

Contacto con desconocidos: Personas desconocidas pueden intentar comunicarse o influir en ellos.

Falta de privacidad: Comparten información personal sin entender las consecuencias.

Uso excesivo de pantallas: Demasiado tiempo frente a dispositivos puede afectar su sueño, atención y bienestar.

Personas estudiantes de secundaria:

Personas estudiantes de secundaria: Ciberacoso: Intimidación, burlas o presión a través de mensajes, redes o comentarios en línea.

Sextorsión: Chantaje o presión para obtener fotos, videos o información privada.

Grooming: Adultos que buscan ganarse la confianza de adolescentes para manipulación o fines sexuales.

Desinformación: Noticias o contenidos falsos que confunden y pueden manipular opiniones.

Impacto emocional: Presión por comentarios, comparaciones y reputación en línea.

Personas jóvenes y adultas:

Fraudes y phishing: Mensajes engañosos que buscan robar dinero o datos personales.

Robo de identidad: Usan información personal para suplantar a alguien y cometer delitos.

Exposición de datos personales: Publicar información sensible sin control puede generar riesgos legales o financieros.

Adicción digital: Uso excesivo de dispositivos y redes que afecta la vida personal, académica o laboral.

Todos podemos enfrentar riesgos distintos, pero la prevención empieza con la educación digital.

Conéctate de manera segura y responsable

Todos interactuamos diariamente con entornos digitales. Adoptar hábitos seguros, responsables y equilibrados nos ayuda a proteger nuestra información, cuidar nuestra privacidad y mantener nuestro bienestar físico y emocional.

Protección de datos personales:

- Usa contraseñas únicas, fuertes y diferentes para cada cuenta.
- Activa la verificación en dos pasos siempre que sea posible.
- Evita compartir información personal sensible en redes sociales o aplicaciones.
- Revisa periódicamente los permisos de apps y servicios que utilizas.

Comportamiento ético:

- Sé respetuoso en tus interacciones. No difundas rumores, mensajes ofensivos ni contenidos privados de otros.
- Fomenta la empatía. Antes de comentar o compartir, piensa en cómo puede afectar a los demás.
- Reporta contenidos inapropiados o peligrosos en plataformas digitales.

Pensamiento crítico:

- Verifica la información antes de compartirla, identificá fuentes confiables.
- Desconfía de enlaces, mensajes o archivos sospechosos, incluso de contactos conocidos.
- Aprende a reconocer señales de fraude, desinformación o manipulación.

Autocuidado digital:

- Crea entornos digitales positivos. Sigue cuentas que eduquen, inspiren o entretienen de manera saludable.
- Cuida tu salud emocional. No te compares con lo que ves en redes y busca ayuda si sientes presión o estrés.
- Establece horarios o pausas para descansar la vista y la mente.
- Equilibra el tiempo que pasas frente a pantallas con actividades fuera de línea.

La seguridad digital no solo es proteger datos, también es cuidar personas y su bienestar.

MINISTERIO DE EDUCACIÓN PÚBLICA | GOBIERNO DE COSTA RICA

unicef para cada infancia

Educación STEAM

Lista de verificación:
seguridad digital en acción

Revisar nuestros hábitos digitales como personas guías nos ayuda a proteger la información de las personas estudiantes, fomentar una cultura de respeto en línea y mantener un entorno educativo seguro y responsable.

- [ ] Verifico la confiabilidad de los recursos digitales antes de utilizarlos en clase.
- [ ] Utilizo cuentas institucionales para actividades educativas y evito servicios personales para datos de las personas estudiantes.
- [ ] Organizo y respaldo la información importante de manera segura.
- [ ] Reviso periódicamente la configuración de privacidad de plataformas, aplicaciones y dispositivos que uso en el ambiente de aprendizaje.
- [ ] No comparto información, fotos ni videos de personas estudiantes sin el consentimiento explícito de la familia o tutores.
- [ ] Protejo mis dispositivos con contraseñas seguras y métodos de autenticación adicionales.
- [ ] Promuevo el respeto, la empatía y el autocuidado digital entre personas estudiantes y colegas.
- [ ] Abordo en clase temas como ciberacoso, desinformación y seguridad en línea de manera frecuente.
- [ ] Fomento un uso responsable y reflexivo de redes sociales y herramientas digitales.
- [ ] Conozco los protocolos institucionales ante incidentes digitales como acoso o filtración de datos.
- [ ] Sé a quién acudir dentro y fuera de la institución en caso de vulneración de información o conflictos en línea.
- [ ] Participo en capacitaciones y actualizaciones sobre seguridad digital y bienestar en línea.

4. Referencias bibliográficas

Alsehaimi, A. (2018). Psychological and social risks to children of using the internet: Literature review. Journal of Child and Adolescent Behaviour, 6(5), 1–8. https://doi.org/10.4172/2375-4494.1000380

Baltodano, M., Trejos, I., & Vargas, L. (2022). Modelo para la Inclusión de Tecnologías Digitales en Educación (MITDE). Dirección de Recursos Tecnológicos en Educación, Ministerio de Educación Pública de Costa Rica.

Barros, Y. C. de, & Vilela, J. (2025, mayo 19). Data privacy in educational contexts: Analyzing perceptions, practices and challenges in personal data protection. https://doi.org/10.5753/sbsi_estendido.2025.246754

Cambridge University. (2022, diciembre). Digital pedagogy for young learners. https://www.cambridge.org/us/files/6316/0612/8264/CambridgePapersInELT_DigitalPedagogyYLs_2020_ONLINE.PDF

Capuno, R., Suson, R., Suladay, D., Arnaiz, V., Villarin, I. J., & Jungoy, E. (2022). Digital citizenship in education and its implication. World Journal on Educational Technology: Current Issues, 14(2), 426–437. https://doi.org/10.18844/wjet.v14i2.6952

Consejo Superior de Educación. (2021). Política para el Aprovechamiento de las Tecnologías Digitales en Educación (PATDE). Dirección de Recursos Tecnológicos en Educación, Ministerio de Educación Pública de Costa Rica.

GAT Labs. (2024, mayo 27). Cyber incident response plan for school admins. https://gatlabs.com/education/wp-content/uploads/2024/05/Cyber-Incident-Response-Plan-for-K-12-Admins.pdf

Gottschalk, F., & Weise, C. (2023, agosto 8). Digital equity and inclusion in education. OECD Education Working Paper, 299. https://doi.org/10.1787/7cb15030-en

Guevara-Andino, J. H., & Delgado-Salas, J. A. (2024, junio 23). Educación para la ciudadanía digital: Preparando a los estudiantes para una participación responsable y crítica en la sociedad conectada. Journal Scientific MQRInvestigar, 8(2), 4320–4338. https://doi.org/10.56048/MQR20225.8.2.2024.4320-4338

Gutiérrez-Aguilar, O., Turpo-Gebera, O., Chicaña-Huanca, S., Laura-De La Cruz, K. M., Pérez-Postigo, G., Diaz Zavala, R., & Osorio Ccoya, I. (2024, febrero). Digital skills and digital citizenship education: An analysis based on structural equation modeling. Journal of Technology and Science Education, 14(3), 1–16. https://doi.org/10.3926/jotse.2436

Hou, Y., Chen, S., & Lin, X. (2024, febrero). Parental digital involvement in online learning: Addressing the digital divide, not redressing digital reproduction. European Journal of Education, 59(3), 1–12. https://doi.org/10.1111/ejed.12635

Instituto de Políticas Públicas en Derechos Humanos del MERCOSUR. (2022, octubre). Políticas públicas contra el acoso escolar y el ciberacoso en el MERCOSUR. https://oei.int/wp-content/uploads/2022/11/politicas-publicas-contra-el-acoso-escolar-y-el-ciberacoso-en-el-mercosur.pdf

Kumar, S. (2024, julio). Ethical considerations in digital education. En Online and Digital Education (pp. 155–177). https://www.researchgate.net/publication/382017625_Ethical_Considerations_in_Digital_Education

Liu, Q., & Khalil, M. (2023, septiembre). Understanding privacy and data protection issues in learning analytics using a systematic review. British Journal of Educational Technology, 54(6), 1–33. https://doi.org/10.1111/bjet.13388

Lu, L. (2025, mayo). Understanding cyberbullying: Causes, consequences and comprehensive intervention strategies. Trends in Sociology, 3(1), 1–20. https://doi.org/10.61187/ts.v3i1.203

Ministerio de Educación de Ecuador. (2023). Protocolo de actuación frente a situaciones de violencia digital detectadas en el Sistema Nacional de Educación. https://educacion.gob.ec/wp-content/uploads/downloads/2023/09/protocolo_frente_a_violencia_digital.pdf

Ministerio de Educación Pública de Costa Rica. (s.f.). Fundamentación teórica STEAM. Ministerio de Educación Pública de Costa Rica.

Ministerio de Educación Pública de Costa Rica. (s.f.). Manual para la ruta STEAM. Ministerio de Educación Pública de Costa Rica.

Owens, M., Ravi, V., & Hunter, E. (2023, junio 5). Digital inclusion as a lens for equitable parent engagement. TechTrends. https://doi.org/10.1007/s11528-023-00859-5

Pahira, S. H., Rinaldy, R., Al-qalbi, L. F., & Amelia, A. (2023, noviembre). Legal regulation of the use of technology in elementary school learning. Jurnal Indonesia Sosial Teknologi, 4(11), 1–8. https://doi.org/10.59141/jist.v4i11.779

Prkno, D., Grafe, N., Schulz, M. S., Kiess, W., & Poulain, T. (2025, abril 16). Children's and adolescents' negative internet experiences and the association with quality of life and behavioural difficulties: A cross-sectional study. BMJ Paediatrics Open, 9(1), e003135. https://doi.org/10.1136/bmjpo-2024-003135

Ruiz, N., & Gallagher, M. (2025, marzo). Rural education imaginaries in digital education policy: An analysis of CONPES 3988 in Colombia. International Journal of Educational Development, 113, 103222. https://doi.org/10.1016/j.ijedudev.2025.103222

Stopbullying.gov. (2021, marzo 10). How to prevent cyberbullying: A guide for parents, caregivers, and youth. https://www.stopbullying.gov/sites/default/files/documents/Cyberbullying%20Guide%20Final%20508.pdf

Trinidad, A., Marcos, V., Montes, A., & Seijo, D. (2025, abril). Negative online experiences, worry, and risk perception among adolescents: Gender differences and implications for cybercrime awareness. Cyberpsychology, Behavior, and Social Networking, 28(5), 1–12. https://doi.org/10.1089/cyber.2024.0476

UNESCO. (2023). Technology and education in light of human rights. En Paper commissioned for the 2023 Global Education Monitoring Report. https://doi.org/10.54676/XGMO8729

UNESCO & Ministerio de Educación de Chile. (2025, junio). Marco orientador de competencias digitales docentes. https://www.mineduc.cl/wp-content/uploads/sites/19/2025/06/Marco-Orientador-de-Competencias-Digitales_Docentes.pdf

UNICEF. (2024, agosto 7). Data protection in schools: Guidance for legislators, policy makers and schools. https://www.unicef.org/eca/media/35876/file/Data%20protection%20in%20schools%20.pdf

Walsh, K., Pink, E., Ayling, N., Sondergeld, A., Dallaston, E., Tournas, P., Serry, E., Trotter, S., Spanos, T., & Rogic, N. (2022, septiembre). Best practice framework for online safety education: Results from a rapid review of the international literature, expert review, and stakeholder consultation. International Journal of Child-Computer Interaction, 33, 100474. https://doi.org/10.1016/j.ijcci.2022.100474

Wang, Y.-M., Lin, Y.-C., & Wang, Y.-S. (2025, marzo 19). Implement internet ethics education: What matters most? Education and Information Technologies. https://doi.org/10.1007/s10639-025-13521-9