Navegando juntos

Guía Integral para un Mundo Digital Seguro

Coordinadores:
Arturo Cavanna
Diego Granja

Autores:
Melchor Gómez-García
Arturo Cavanna
Moussa Boumadan
Roberto Soto-Varela
Miguel Ángel Savall

Coordinadora jurídica:
Leticia Mata Mayrand

UAM Universidad Autónoma de Madrid
foredu
EDI EDUCACIÓN DIGITAL E INNOVACIÓN
SAMSUNG

Coordinación Guía

Arturo Cavanna
Fundador de Notecalles / NotecalleX
Profesor de Tecnología Educativa / Educación Especial UAM

Diego Granja
Sales Manager Educación Samsung España

Autores

Melchor Gómez-García
Profesor de Tecnología Educativa UAM

Arturo Cavanna
Fundador de Notecalles / NotecalleX
Profesor de Tecnología Educativa / Educación Especial UAM

Moussa Boumadan
Profesor de Tecnología Educativa UAM

Roberto Soto-Varela
Profesor de Tecnología Educativa de la Universidad de Valladolid

Miguel Ángel Savall
Profesor de Máster de Tecnología Educativa en UNIR

Coordinadora Jurídica

Leticia Mata Mayrand
Abogada especializada en protección de la infancia,
familia y derechos humanos

Introducción

En el mundo actual, la tecnología ha cambiado radicalmente la forma en que vivimos, aprendemos y nos conectamos. Aunque nos ofrece oportunidades increíbles para acceder a información, aprender de manera innovadora y mantenernos conectados, también conlleva riesgos significativos si no se utiliza de manera adecuada.

El mal uso de la tecnología puede tener consecuencias muy graves para estudiantes, docentes y familias. Y eso tiene que quedar muy claro desde el principio. Llevo años observando proyectos educativos impresionantes gracias al buen uso de la tecnología y en paralelo, otros muchos años analizando y viendo lo peor del ser humano escondido y respaldado a través de la tecnología.

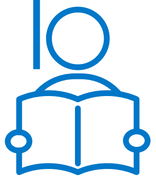
Por lo tanto, estamos viviendo un momento increíble de avances tecnológicos, pero a la par un momento muy complicado para la infancia. Los niños y jóvenes son muy vulnerables a todos estos riesgos.

Tengamos en cuenta cómo nos influye a los adultos la tecnología; las redes sociales, la digitalización, la inteligencia artificial... pues imaginemos cómo repercute en personitas que están todavía desarrollando su cerebro.

Esta guía ha sido creada para ayudar a toda la comunidad educativa a enfrentar estos desafíos y asegurar un uso responsable de la tecnología.

La hemos dividido en tres grandes bloques:

1. Docentes: aquí encontrarás herramientas para garantizar un uso seguro de la tecnología en el aula, proteger la privacidad de los estudiantes, y fomentar un entorno digital ético y respetuoso.



2. Estudiantes: este bloque les ayudará a aprender cómo protegerse en línea, manejar su presencia digital de manera consciente y a utilizar la tecnología para su aprendizaje sin caer en riesgos como el ciberacoso o el acceso a contenido inapropiado.

3. Familias: los padres juegan un papel clave en la protección de sus hijos en el hogar. En este bloque, se proporcionan consejos y recursos para supervisar y acompañar el uso de la tecnología de manera segura y saludable.

El mal uso de la tecnología puede tener un impacto negativo en la vida emocional y social de los estudiantes, y muchas veces, estos peligros no son fácilmente visibles. A través de esta guía, queremos brindarles herramientas claras para que, juntos, podamos crear un entorno digital más seguro, donde todos, desde docentes hasta alumnos y familias, se sientan protegidos y preparados para aprovechar al máximo las oportunidades que ofrece la tecnología, sin poner en riesgo su bienestar.

Docentes

+índice

1. Introducción: el rol del docente en la seguridad digital 8

- Importancia de la protección digital en el aula 9
- Los docentes como modelos a seguir 9
- Desafíos digitales en el aula 9
- Objetivos de la guía para docentes 9
- La importancia de la seguridad digital en el aula 9
- El docente como guía en el entorno digital 10
- Retos del uso de la tecnología en el aula 10
- Fomentar la ciudadanía digital 10
- Herramientas para docentes en seguridad digital 11
- El rol de la formación continua 11
- Promoción de la colaboración con familias 11
- Objetivos de la seguridad digital en el aula 11

2. Marco legal y normativoaplicable a la protección de los derechos de las personas menores de edad en el ámbito digital 13

- La convencion sobre los derechos del niño de Naciones Unidas. 14
- La labor de supervisión del comité de derechos del niño. 14
- Observación general n.º 25, relativa a los derechos de los niños en relación con el entorno digital, aprobada el 2 de marzo de 2021. 15
- A nivel europeo 15
- Nivel nacional. 15
- Educación inclusiva. 17
- Normativa y buenas prácticas dirigidas a la protección de datos personales en el ámbito escolar. 20
- Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación. 20
- Delegado de Protección de Datos en Centros Educativos 20
- La Necesidad de Normas Claras en el Uso de la Tecnología 21
- Normas Básicas para el Uso de la Tecnología en el Aula 21
- Involucrar a los Estudiantes en la Creación de Normas 22
- Comunicación de las Normas a las Familias 23
- El uso adecuado de dispositivos. 23
- Ley Orgánica de Protección Integral a la Infancia y Adolescencia frente a la Violencia (LOPIVI) 23
- Reglamento General de Protección de Datos (RGPD) 29

Docentes

+índice

- Normativa de Protección de Datos en el Entorno Escolar 30
- Delegado de Protección de Datos en Centros Educativos 30
- La Necesidad de Normas Claras en el Uso de la Tecnología 30
- Normas Básicas para el Uso de la Tecnología en el Aula 31
- Involucrar a los Estudiantes en la Creación de Normas 31
- Ejemplos de Normas Digitales en el Aula 32
- Reforzar el Cumplimiento de las Normas 32
- Comunicación de las Normas a las Familias 32

3. Establecimiento de normas y buenas prácticas 34

- Creación de un entorno digital seguro desde el inicio del curso 35
- Inclusión de los alumnos en la creación de normas 35
- Ejemplos de normas digitales en el aula 35
- Comunicación clara con las familias 35
- Uso de contratos o acuerdos digitales 35
- Acuerdo digital para estudiantes 36
- Herramientas para establecer normas y supervisar el uso de tecnología 37
- La importancia de la privacidad en el entorno escolar 37
- ¿Qué Información Personal Debe Protegerse? 38
- Consentimiento para el Uso de Datos Personales 38
- Uso seguro de plataformas educativas 38
- Protección de la privacidad en el aula 39
- Prevención de violaciones de datos 39
- Formación continua en protección de datos 39
- Implicación de las familias en la protección de la privacidad 40

4. Tecnologías seguras en el aula 41

- Uso responsable de plataformas educativas 42
- Evaluación y selección de herramientas tecnológicas 42
- Implementación de dispositivos seguros 42
- Controles parentales y restricciones de acceso 42
- Uso seguro de redes wi-fi en el aula 42
- Introducción al uso de software de monitoreo 42
- Protección contra malware y ataques cibernéticos 43

Docentes

+índice

- Ejemplos prácticos de tecnologías seguras 43
- ¿Qué es el ciberacoso y por qué es importante prevenirlo? 43
- Señales de alarma del ciberacoso en el aula 43
- ¿Cómo pueden los docentes prevenir el ciberacoso? 44
- Actuar rápidamente ante un caso de ciberacoso 45
- Fomentar un entorno digital seguro y positivo 46

5. Detección y prevención de riesgos digitales 47

- Identificación temprana de ciberacoso 48
- Prevención del grooming 48
- Sexting: prevención y actuación 48
- Prevención de tecnoadicciones 48
- Recursos para la detección y prevención 49

6. Protocolos de actuación ante incidentes 50

- Pasos generales a seguir 51
- Actuación frente a ciberacoso 51
- Manejo de casos de grooming y sexting 51
- Recursos para la intervención 52
- Seguimiento y evaluación post-incidente 52

7. Protección de datos y privacidad en el aula 53

- El manejo de información sensible en el aula 54
- Consentimiento para el uso de datos personales 54
- Políticas de uso de imágenes y vídeos en actividades escolares 54
- Uso de plataformas digitales con normas de privacidad 55
- Prevención de violaciones de datos 55
- Colaboración con el delegado de protección de datos 55

8. Promoción del bienestar digital 56

- Importancia del bienestar digital 57
- Estrategias para fomentar el uso responsable de la tecnología 57
- Prevención de tecnoadicciones 57
- Ejemplos prácticos de bienestar digital en el aula 57

Docentes

- Incorporación de la educación sobre salud digital 58
- Recursos para docentes 58

9. Herramientas y recursos de apoyo 59

- Plataformas y aplicaciones para la seguridad digital 60
- Herramientas de monitoreo en tiempo real 60
- Guías y recursos educativos en línea 60
- Formación continua para docentes 60
- uso de materiales didácticos y recursos audiovisuales 60

10. Colaboración con familias y comunidad escolar 62

- Importancia de la colaboración 63
- Comunicación abierta y continua con las familias 63
- Coordinación con el coordinador de bienestar 63
- Actividades de sensibilización para la comunidad escolar 63
- Involucrar a los estudiantes en la creación de un entorno seguro 63
- Recursos para las familias 64

Navegando Juntos:
Guía Integral para un Mundo Digital Seguro

DOCENTES

ESTUDIANTES

FAMILIAS

01 Introducción: el rol del docente en la seguridad digital

Introducción: el rol del docente en la seguridad digital

Importancia de la protección digital en el aula

El docente no solo es responsable del bienestar físico y emocional de sus alumnos, sino también de su **seguridad digital**. En un mundo cada vez más conectado, los riesgos asociados al uso de internet y dispositivos digitales se han convertido en una preocupación importante en el entorno escolar. Ciberacoso, grooming, sexting, shareting y la exposición a contenido inapropiado son algunos de los peligros a los que los menores están expuestos en línea. Por lo tanto, los profesores juegan un papel esencial en la **educación digital segura**.

Los docentes como modelos a seguir

Los niños tienden a seguir el ejemplo de los adultos en su vida. Por eso, los docentes deben actuar como **modelos de comportamiento responsable** en el uso de la tecnología. Esto incluye el uso adecuado de las redes sociales, la protección de la privacidad y la promoción del respeto en línea. Al demostrar hábitos digitales saludables, los profesores no solo protegen a sus estudiantes, sino que también los preparan para ser **ciudadanos digitales responsables**.

Desafíos digitales en el aula

Con la introducción de herramientas digitales en la educación, como plataformas de aprendizaje en línea, aplicaciones y dispositivos conectados, se abren nuevas posibilidades para la enseñanza, pero también **nuevas vulnerabilidades**. Los docentes deben estar capacitados para reconocer y gestionar estos riesgos. Desde establecer reglas claras sobre el uso de dispositivos hasta intervenir cuando se detecten comportamientos inadecuados, su labor es crucial para **crear un entorno digital seguro** y educativo.

Objetivos de la guía para docentes

Este primer bloque busca proporcionar a los docentes una visión general de su papel en la **seguridad digital** de los estudiantes y cómo pueden implementar **buenas prácticas** en el aula. También introduce la importancia de la **formación continua** en el ámbito de la ciberseguridad y cómo colaborar con las familias para ofrecer un enfoque integral a la protección de los menores en línea.

La importancia de la seguridad digital en el aula

El entorno digital ha cambiado radicalmente la forma en que se aprende y enseña, ofreciendo grandes oportunidades, pero también exponiendo a los estudiantes a **riesgos digitales** como el ciberacoso, el grooming, el phishing, y el acceso a contenido inapropiado. Como docentes, es crucial comprender estos riesgos y saber cómo abordarlos de manera proactiva para proteger a los estudiantes y fomentar un **uso responsable de la tecnología**.

La seguridad digital no es solo un conjunto de reglas; es una responsabilidad compartida por todo el equipo educativo. Los docentes tienen el deber de **crear un ambiente seguro** para sus estudiantes no solo físicamente, sino también digitalmente. Esto implica enseñarles a proteger su

Introducción: el rol del docente en la seguridad digital

01

información personal, navegar de manera crítica por internet y comprender los riesgos asociados al uso de dispositivos conectados.

El docente como guía en el entorno digital

En un mundo donde la tecnología se utiliza en casi todos los aspectos de la vida diaria, los docentes deben actuar como **modelos de comportamiento digital responsable**. Esto no solo significa saber usar herramientas tecnológicas, sino también educar a los estudiantes sobre cómo hacerlo de forma **segura, ética y saludable**.

Los docentes son los primeros en **identificar señales de riesgo** en los estudiantes, como problemas de ciberacoso o comportamientos adictivos relacionados con la tecnología. Al promover un enfoque de **prevención**, los docentes pueden intervenir antes de que los problemas se agraven, trabajando en conjunto con las familias y el equipo educativo para proporcionar el apoyo necesario.

Este punto es crucial ya que l@s alumn@s se encuentran la mayor parte de su tiempo en la escuela; por lo tanto los docentes deberíamos ser termómetros de nuestros alumn@s. Es clave que podamos estar alerta para prevenir y proteger cualquier riesgo de cualquier índole.

Retos del uso de la tecnología en el aula

Aunque la tecnología es una herramienta poderosa para el aprendizaje, también presenta desafíos únicos en términos de seguridad. Los dispositivos digitales permiten a los estudiantes **acceder a información de forma instantánea**, pero también pueden distraerlos o exponerlos a contenidos inapropiados. Para los docentes, gestionar estos dispositivos puede ser complicado, ya que no siempre tienen control total sobre lo que los estudiantes hacen en línea.

Es fundamental que los docentes establezcan **normas claras** sobre el uso de dispositivos en el aula y utilicen herramientas de control, como aplicaciones de monitoreo de actividad digital, que les permitan supervisar el uso de internet en tiempo real.

Fomentar la ciudadanía digital

Un elemento clave en el rol del docente es educar a los estudiantes sobre la **ciudadanía digital**. Ser un ciudadano digital implica no solo saber utilizar las tecnologías, sino también **comprender las implicaciones éticas** de sus acciones en línea.

Los docentes deben enseñar a los estudiantes sobre la importancia de:

- **Respetar** la privacidad de los demás.
- **Evitar** la difusión de información falsa o dañina.
- **Denunciar** situaciones de ciberacoso y apoyar a compañeros que puedan estar enfrentando problemas en línea.
- **Proteger** su propia información personal y la de sus compañeros.

Introducción: el rol del docente en la seguridad digital

Incorporar la educación sobre ciudadanía digital en el plan de estudios es fundamental para preparar a los estudiantes para ser **responsables y respetuosos en línea**.

Herramientas para docentes en seguridad digital

Existen muchas herramientas que los docentes pueden utilizar para **garantizar la seguridad digital** en sus aulas. Algunas de estas incluyen:

- **Plataformas de monitoreo de actividad en tiempo real:** ayudan a los docentes a supervisar lo que los estudiantes hacen en línea, permitiendo intervenir si se detecta un comportamiento inapropiado.
- **Aplicaciones de control parental:** aunque tradicionalmente se utilizan en el hogar, pueden aplicarse en entornos educativos para limitar el acceso a contenido inapropiado en dispositivos usados en clase.
- **Recursos educativos sobre seguridad digital:** guías y programas, como los ofrecidos por **incibe** o **pantallas amigas**, proporcionan materiales que los docentes pueden integrar en sus lecciones para enseñar a los estudiantes a navegar de forma segura por internet.

El rol de la formación continua

Dado que las tecnologías y los riesgos asociados evolucionan constantemente, es esencial que los docentes participen en **programas de formación continua** relacionados con la seguridad digital. Mantenerse al día con las mejores prácticas, las nuevas herramientas de seguridad y los últimos desafíos permite a los docentes proteger mejor a sus estudiantes y ofrecer una enseñanza de calidad en el entorno digital.

La colaboración con **especialistas en ciberseguridad** o la participación en **talleres de formación** organizados por instituciones educativas y tecnológicas es una excelente forma de mejorar las competencias de los docentes en este ámbito.

Promoción de la colaboración con familias

La seguridad digital no es solo un asunto del aula; es una responsabilidad compartida entre docentes, estudiantes y familias. Los docentes deben **fomentar la colaboración con los padres / madres** para garantizar que las normas y hábitos de seguridad digital que se implementan en la escuela también se respeten en casa. Las reuniones con las familias, el envío de guías y la recomendación de herramientas de control parental son formas eficaces de involucrar a las familias en este proceso.

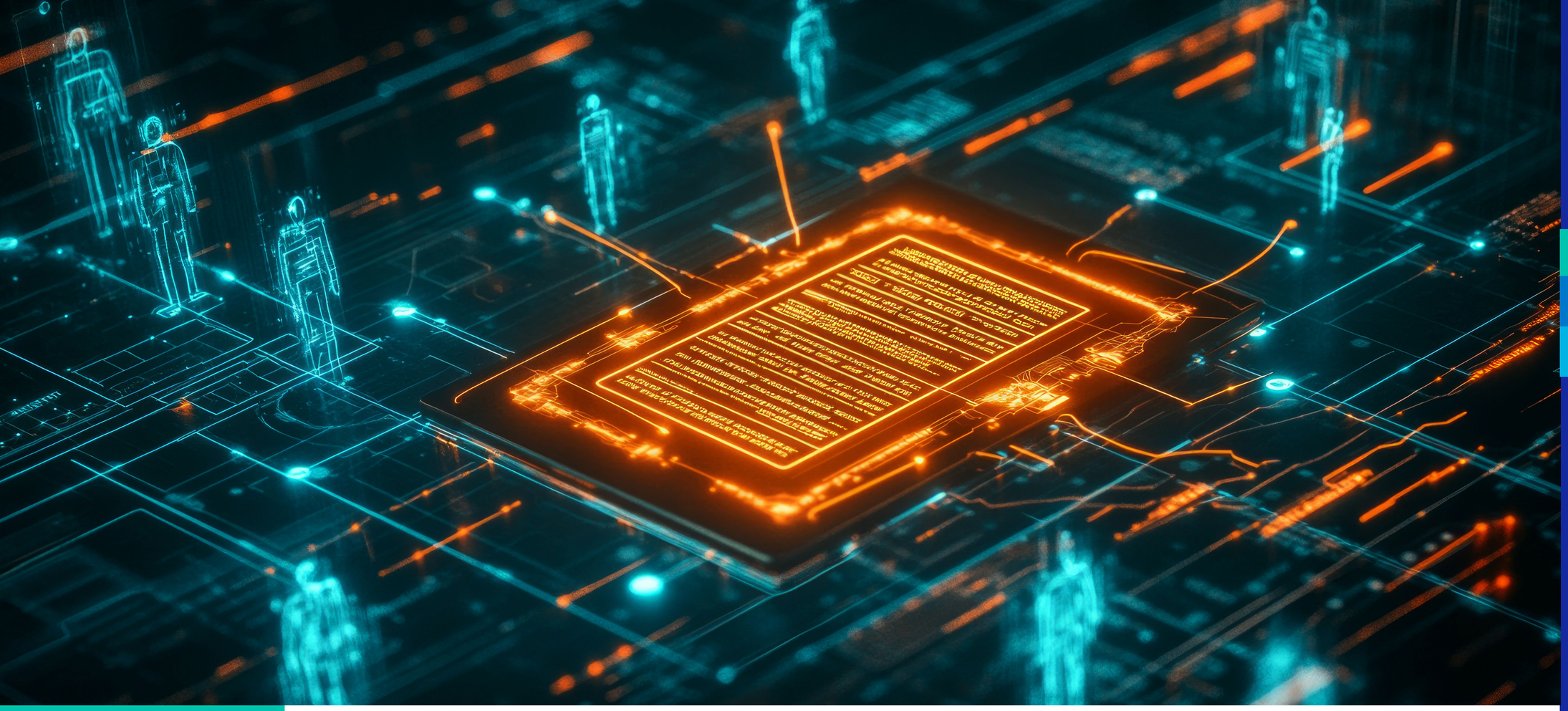
Objetivos de la seguridad digital en el aula

En resumen, los objetivos clave que los docentes deben tener en cuenta al fomentar la seguridad digital en el aula son:

- **Proteger a los estudiantes** de los peligros en línea, como el ciberacoso, el grooming y la exposición a contenido inapropiado.

Introducción: el rol del docente en la seguridad digital

- **Enseñarles a ser ciudadanos digitales responsables**, promoviendo el respeto, la ética y la seguridad en línea.
- **Establecer normas claras** sobre el uso de la tecnología y asegurarse de que se sigan en el aula.
- **Fomentar la colaboración con las familias** para que el entorno digital seguro también se mantenga fuera de la escuela.
- **Mantenerse actualizados** en las últimas tendencias y riesgos en seguridad digital mediante formación continua.



02

Marco legal y normativo

aplicable a la protección de los derechos de las personas menores de edad en el ámbito digital

Marco legal y normativo aplicable a la protección de los derechos de las personas menores de edad en el ámbito digital.

02

La convencion sobre los derechos del niño de Naciones Unidas.

cuando nos referimos al marco legal que regula la protección de los derechos de niños y niñas y adolescentes (en adelante NNA) en nuestro país, debemos siempre nombrar, en primer lugar, la Convención sobre los Derechos del Niño de Naciones Unidas (en adelante CDN).

La CDN es el instrumento de los derechos humanos más aceptado universalmente, ratificado por todos los países del mundo excepto dos. Fue adoptada por la Asamblea General de la ONU el 20 de noviembre de 1989, y España la ratificó un año después de su aprobación, en 1990. La CDN reconoce por primera vez al niño o niña como sujeto de derechos fundamentales y, a lo largo de sus 54 artículos, incorpora todo el rango de sus derechos inalienables, pero también las obligaciones de los Estados y los poderes públicos para garantizar el respeto de esos derechos.

La CDN se completa con tres Protocolos facultativos. Los dos primeros, se aprobaron en el año 2000 por la Asamblea General de Naciones Unidas y refuerzan la protección de la infancia contra la venta de niños, la prostitución y la pornografía infantil, y la participación de los niños en los conflictos armados. El tercero fue aprobado en 2011 y establece un procedimiento de comunicaciones que permite a los propios niños y niñas, o a un adulto en su nombre y representación, presentar ante el Comité de Derechos del Niño (en adelante el Comité) quejas o denuncias individuales por la posible vulneración de sus derechos reconocidos en la CDN por parte de las administraciones, instituciones, autoridades públicas y privadas, cuando el propio Estado parte no de una respuesta eficaz y, por ello, no sea posible encontrar una posible solución en su propio país.

La labor de supervisión del comité de derechos del niño.

tanto la CDN como sus Protocolos facultativos son instrumentos jurídicamente vinculantes y, como tal, en el momento que un Estado se adhiere o ratifica los mismos, su cumplimiento es obligatorio, si bien el Comité no puede imponer sanciones a los Estados por no cumplir sus preceptos. Para verificar el cumplimiento de la CDN por los Estados parte, estos deben presentar al Comité, periódicamente, informes explicando la situación de los derechos de los niños y niñas en su territorio y las políticas, medidas o leyes adoptadas durante ese tiempo para garantizar el cumplimiento de tales derechos reconocidos en la CDN 1 .

El Comité analiza estos informes y elabora unas recomendaciones para que cada país mejore su forma de proteger a los niños y las niñas. Es lo que se llaman observaciones finales. Las últimas observaciones finales del Comité al Estado español fueron aprobadas en febrero del 2018.

El Comité también elabora y publica sus observaciones generales. A través de ellas, trata de facilitar a los Estados parte la interpretación y la dimensión de cada uno de los derechos contemplados en la CDN. Son muchas las observaciones generales aplicables a los derechos de los NNA.

Marco legal y normativo aplicable a la protección de los derechos de las personas menores de edad en el ámbito digital.

02

No obstante, por lo que se refiere a la protección de sus derechos en el ámbito digital, debemos destacar la Observación General N.º 25 (2021), relativa a los derechos de los niños en relación con el entorno digital 2 .

Observación general n.° 25, relativa a los derechos de los niños en relación con el entorno digital, aprobada el 2 de marzo de 2021.

Ante la preocupación por la situación actual de los derechos de los NNA en el entorno digital, ante la necesidad de proteger su privacidad y prevenir, detectar y actuar frente a los riesgos para su integridad y salud en ese entorno, el Comité aprobó esta Observación General, que supuso un hito en la protección de los NNA en el ámbito digital.

Esta Observación General tiene como objetivo explicar a los Estados parte de la CDN la forma en que la misma y sus Protocolos Facultativos deben ser aplicados en relación con el entorno digital. En este sentido propone medidas legislativas, administrativas y preventivas dirigidas a los Estados parte, pero también al sector privado y, en concreto, las empresas proveedoras de servicios tecnológicos.

A nivel europeo

Actualmente España se encuentra en el VII Ciclo de revisión.

En Europa, dentro del marco de la Unión Europea y del Consejo de Europa, existe ya un elenco importante de normas que, dentro de su articulado, prevén regulación sobre la protección de la privacidad y seguridad de los NNA en el entorno digital y la prevención de la violencia ejercida a través de las nuevas tecnologías. Sin entrar a enumerar toda esta normativa, debido a su extensión, sí caber referenciar, sin embargo, tres Estrategias aprobadas recientemente por la UE que han impulsado una serie de medidas y propuestas a llevar a cabo por la propia UE como por los Estados parte y las empresas del sector privado, especialmente, las empresas proveedoras de servicios digitales, para garantizar que los NNA puedan navegar con seguridad en el entorno digital y aprovechar sus oportunidades:

- La Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores, aprobada en 2020.
- La Estrategia de la UE sobre los Derechos del Niño y la Garantía Infantil Europea, aprobada en 2021.
- La nueva Estrategia de la UE para una mejor Internet para los niños (BIK+), aprobada en 2022.

Nivel nacional.

Dentro del marco jurídico aplicable en el territorio español a los NNAMNA la primera norma a tener en cuenta es la Constitución Española y dentro de la misma, sus artículos 18.4 donde se reconoce como derecho fundamental a la protección de los datos personales y el artículo 39 que impone a los poderes públicos el deber de asegurar a todos los niños y niñas que se hallen en nuestro país, una protección integral y conforme a los acuerdos internacionales que velan por sus derechos.

Marco legal y normativo aplicable a la protección de los derechos de las personas menores de edad en el ámbito digital.

02

Debemos citar la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor. Su texto consolidado recoge una serie de derechos consagrados ya en la CDN de los que serán sujetos activos todas las personas menores de edad que se hallen en territorio español. Entre estos derechos está el derecho al honor, a la intimidad personal y familiar y a la propia imagen y el derecho a la protección frente a cualquier tipo de violencia (incluyendo la violencia ejercida en el entorno digital).

Por otro lado, y en lo que se refiere al derecho fundamental a la protección de los datos personales, cabe citar la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantías de Derechos Digitales. En este sentido, es elogiable la especial atención de la Agencia Estatal de Protección de Datos (AEPD) a la protección de los derechos de los NNA en el entorno digital, así como todas sus iniciativas y actuaciones que ha llevado a cabo en este sentido, cono la creación del Canal Prioritario, para la denuncia y retirada urgente de contenidos ilícitos en internet que vulneren el derecho a la protección de datos personales o la presentación hace ya casi un año de sistema de verificación de edad para proteger a los menores de edad ante el acceso a contenidos de adultos en Internet.

A) ley orgánica 8/2021, de protección integral a la infancia y adolescencia frente a la violencia (LOPIVI).

La LOPIVI constituye una ley pionera al no existir referentes en ningún otro país del mundo en el momento de su aprobación. Ninguna Ley aborda como lo hace ésta, de una forma integral la violencia hacia la infancia y, por ello, sitúa a España a la vanguardia de la protección de los derechos de los niños y en la cultura del buentrato.

Su objetivo es luchar contra la violencia que pueda sufrir un menor de edad, violencia que muchas veces permanece oculta y silenciosa y, por ello, es difícil detectar y que siempre produce en mayor o menor medida un daño psicológico en el niño o niña que la sufre, pudiéndole dejar secuelas en su desarrollo intelectual y emocional.

Esta Ley combate la violencia hacia la infancia y adolescencia de una forma integral y multidimensional, incluidas las violencias que se producen en el entorno digital, estableciendo medidas de sensibilización, de prevención, de detección precoz y denuncia, así como, medidas de asistencia, protección y recuperación de las víctimas, e implica y compromete en esta lucha frente a la violencia no solo a los poderes públicos, sino también, a todos los ciudadanos.

La LOPIVI recoge una definición del concepto de violencia sobre la infancia y la adolescencia, así como de buen trato, estableciendo medidas para la protección integral de los NNA frente a la violencia en los diferentes ámbitos en los que interactúan: familiar, educativo, de los servicios sociales, sanitario, digital, ocio y deportes y policial.

Por lo que se refiere al ÁMBITO EDUCATIVO, su capítulo IV desarrolla diversas medidas de prevención y detec-

02

ción precoz de la violencia en los centros educativos. La actuación de los centros educativos en esa prevención y detección precoz es imprescindible estos centros son imprescindibles si se tiene en cuenta que se trata de un entorno de socialización clave en la vida de los NNA. La LOPIVI establece la obligación para los centros escolares de que, junto al plan de convivencia, se aprueben protocolos de actuación frente a indicios de abuso y maltrato, acoso escolar, ciberacoso, acoso sexual, violencia de género, violencia doméstica, suicidio, autolesión y cualquier otra forma de violencia. Para el correcto funcionamiento de estos protocolos se crea la figura del Coordinador/a de Bienestar y Protección, en todos los centros educativos. También se refleja la necesaria capacitación de las personas menores de edad en materia de seguridad digital.

Por otro lado, su artículo 5 establece la obligación para las administraciones públicas de promover y garantizar un formación especializada, inicial y continua al personal docente y educador, al ser profesionales en contacto habitual con personas menores de edad. Dicha formación deberá comprender como mínimo los siguientes puntos:

- La prevención y detección precoz de toda forma de violencia;
- La actuación a llevar a cabo una vez se han detectado indicios de violencia;
- Uso seguro y responsable de Internet, incluyendo cuestiones relativas al uso intensivo y generación de trastornos conductuales;
- EL buen trato a los NNA;
- La identificación de los factores de riesgo y de una mayor exposición y vulnerabilidad ante la violencia;
- Los mecanismos para evitar la victimización secundaria;
- El impacto de los roles y estereotipos de género en la violencia que sufren NNA.

Educación inclusiva.

De conformidad con su artículo 16, el personal de los centros educativos tendrá un deber de comunicación cualificado, de tal forma que: Cuando tuvieran conocimiento o advirtieran indicios de la existencia de una posible situación de violencia de un NNA, deberán comunicarlo de forma inmediata a los servicios sociales competentes y, cuando proceda, a las Fuerzas y Cuerpos de Seguridad y/o al Ministerio Fiscal. Cuando adviertan una posible infracción de la normativa sobre protección de datos personales de una persona menor de edad, deberán comunicarlo de forma inmediata a la Agencia Española de Protección de Datos.

Cuando adviertan la existencia de contenidos disponibles en Internet que constituyan una forma de violencia contra cualquier NNA. En todo caso, deberán prestar a la víctima la atención inmediata que precise, facilitar toda la información de que dispongan, así como prestar su máxima colaboración a las autoridades competentes.

Por otro lado, el art. 18 establece la obligación de que todos los centros educativos, al inicio de cada curso escolar,

Marco legal y normativo aplicable a la protección de los derechos de las personas menores de edad en el ámbito digital.

02

facilitarán a los NNA toda la información sobre los procedimientos de comunicación de situaciones de violencia, de las personas responsables en este ámbito, así como de las líneas telefónicas de ayuda a los NNA (como las líneas 116111, o las líneas de ayuda de la Fundación ANAR 900202010). Los centros educativos deben mantener siempre actualizada esa información y en un lugar visible y accesible, para que los NNA puedan consultarla libremente en cualquier momento.

En este sentido, el art. 22.2 señala que los centros educativos deberán adoptar todas las medidas necesarias para garantizar la protección seguridad de los NNA que comuniquen una situación de violencia.

Por lo que respecta al ÁMBITO DIGITAL, el art. 8.2 establece la obligación para las administraciones públicas de adoptar las medidas necesarias que aseguren su colaboración con el sector de las nuevas tecnologías. En especial, con las empresas de tecnologías de la información y comunicación, con la Agencia de Protección de Datos, con las Fuerzas y Cuerpos de Seguridad y con la Administración de Justicia con el fin de detectar y retirar, a la mayor brevedad posible, los contenidos ilegales en las redes que supongan una forma de violencia sobre los NNA. Por otro lado, su capítulo VIII, regula las actuaciones que deben realizar y promover las administraciones públicas para garantizar el uso seguro y responsable de Internet por parte de los NNA, familias, personal educador y profesionales que trabajen con personas menores de edad. En este sentido sus artículos 45 y 46 establecen las siguientes líneas de actuación:

- Desarrollar campañas de educación, sensibilización y difusión sobre el uso seguro y responsable de Internet y las tecnologías de la información y la comunicación, así como sobre los riesgos derivados de un uso inadecuado que puedan generar fenómenos de violencia sexual contra los NNA; Fomentar medidas de acompañamiento a las familias, reforzando y apoyando el rol de los progenitores a través del desarrollo de competencias y habilidades que favorezcan el cumplimiento de sus obligaciones legales;
- Poner a disposición de los NNA, familias, personal educador y otros profesionales que trabajen habitualmente con personas menores de edad una línea de ayuda que ofrezca a los usuarios asistencia y asesoramiento ante situaciones potenciales de riesgo y emergencia de las personas menores de edad en Internet; Adoptar medidas para incentivar la responsabilidad social de las empresas en materia de uso seguro y responsable de Internet por la infancia y la adolescencia.
- Realizar periódicamente diagnósticos, sobre el uso seguro de Internet entre los NNA y las problemáticas de riesgo asociadas, así como de las nuevas tendencias.
- Fomentar la colaboración con el sector privado, para la creación de entornos digitales seguros, una mayor estandarización en el uso de la clasificación por edades y el etiquetado inteligente de contenidos digitales.
- Fomentar la implementación y el uso de mecanismos de control parental y los mecanismos de verificación de edad, denuncia y bloqueo.

- Impulsar entre la industria códigos de autorregulación para el uso seguro y responsable en el desarrollo de productos y servicios destinados al público infantil y adolescente.

2.5.B) Anteproyecto de ley organica para la protección de las personas menores de edad en los entornos digitales.

Este Anteproyecto de Ley, aprobado por el Consejo de ministros el 4 de junio de 2024 y, actualmente, en trámite parlamentario, introduce medidas dirigidas al sector público y a las empresas tecnológicas para garantizar la seguridad de los NNA en el mundo digital, protegiendo sus derechos en este entorno, especialmente el derecho a la intimidad, al honor y a la propia imagen, así como el derecho a la protección de sus datos personales y al acceso a contenidos adecuados para su edad. Asimismo, introduce algunas modificaciones legales, entre otras, en el Código Penal.

Entre todas las medidas establecidas en el Anteproyecto de Ley para la creación de entornos digitales seguros y saludables para los NNA, caben destacar las siguientes:

- Obliga a los poderes públicos a elaborar una Estrategia Nacional sobre la protección a la infancia y la adolescencia en el entorno y, de manera más específica, a impulsar campañas de sensibilización sobre los derechos de los menores en la esfera digital y los riesgos que esta entraña, con especial atención al consumo de material pornográfico, e investigar sobre los efectos de la tecnología en el desarrollo cognitivo de niños, niñas y adolescentes; En el ámbito sanitario, incluye medidas para el fomento de la detección precoz, la prevención y la atención especializadas a menores con patologías asociadas al uso inadecuado de dispositivos; En el ámbito educativo, contempla la inclusión en los currículos escolares desde la primaria hasta la segundaria de formación en ciudadanía digital y alfabetización mediática, privacidad y propiedad intelectual. Por otro lado, establece la obligación para todos los centros educativos, independientemente de su titularidad, de regular el uso de dispositivos móviles y digitales en las aulas, en las actividades extraescolares y en lugares y tiempos de descanso que tengan lugar bajo su supervisión, conforme a lo dispuesto en la normativa de la comunidad autónoma. Respecto a las empresas del sector tecnológico, establece la obligación para los fabricantes de que los dispositivos digitales cuenten con sistemas de control parental activados por defecto y con un etiquetado informativo sobre sus riesgos. Asimismo, prohíbe con carácter general el acceso de las personas menores de edad a las plataformas loot boxes (cajas de recompensa) en los videojuegos, que funcionan como mecanismos similares a los juegos de azar y pueden producir comportamientos adictivos.
- Prevé la implantación de sistemas de verificación de la edad «efectivos y obligatorios», para evitar el acceso por parte de los NNA a contenidos inadecuados y nocivos para su desarrollo.
- Tipifica como delitos los deepfakes con contenido sexual y/o vejatorio (difusión, sin autorización, de imágenes

o audios generados por inteligencia artificial o cualquier otra tecnología); regula la orden de alejamiento online; introduce el denominado grooming (engaño online a menores) como circunstancia agravante en diferentes delitos contra la libertad sexual de menores; y refuerza la tipificación de la difusión de material pornográfico a los niños y niñas, para evitar algunas conductas impunes.

- Eleva de 14 a 16 años la edad mínima a la que se puede dar consentimiento al tratamiento de datos personales.

Junto a este Anteproyecto de Ley, en trámite parlamentario, cabe citar que el Gobierno constituyó mediante Acuerdo del Consejo de ministros de 30 de enero de 2024, un Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia. Este Comité ha venido trabajando sobre los entornos digitales con el fin de realizar un informe que analice buenas prácticas y elabore recomendaciones, medidas y actuaciones para una hoja de ruta con el objetico de generar un entorno digital seguro, que contribuya a la mejor protección del desarrollo integral de la infancia y la adolescencia. Este informe saldrá a la luz en las próximas semanas.

NORMATIVA y BUENAS PRÁCTICAS DIRIGIDAS A LA PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO ESCOLAR.

Los centros educativos tienen la obligación ineludible de cumplir con la normativa de protección de datos de carácter personal, más si se tiene presente el volumen de datos que manejan y la categoría especial de alguno de esos datos que, además de poder corresponder a personas menores de edad, pueden referirse, por ejemplo, a la salud.

La normativa de protección de datos para centros educativos la constituyen:

- El Reglamento Europeo General de Protección de Datos vigente desde 2016.
- La Ley Orgánica 3/2018, de Protección de Datos Personales y Garantías de Derechos.

Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación.

Esta normativa exige que los docentes, junto con la administración del centro, implementen medidas que aseguren que los datos de los estudiantes, incluidos sus nombres, imágenes y otros datos sensibles, se manejen de manera segura y conforme a la ley. Esto incluye garantizar que no se publiquen sin autorización y que se utilicen exclusivamente para los fines educativos que se han comunicado a los padres o tutores.

Delegado de Protección de Datos en Centros Educativos

Los centros educativos deben contar con un Delegado de Protección de Datos (DPD), quien es responsable de asegurar el cumplimiento de la normativa en el manejo de los datos de los alumnos. El DPD supervisa que se implementen medidas adecuadas para garantizar la seguridad

02

de los datos, asesora al personal sobre cómo gestionar correctamente la información personal y actúa como punto de contacto con las autoridades de protección de datos. Es importante que los docentes estén familiarizados con las funciones del DPD y trabajen en coordinación con él para asegurar el cumplimiento de las normativas.

La Necesidad de Normas Claras en el Uso de la Tecnología

El uso de dispositivos tecnológicos en el aula, como portátiles, tablets y smartphones, se ha convertido en una parte esencial del proceso de enseñanza y aprendizaje. Sin embargo, para garantizar que estos dispositivos se utilicen de manera segura y productiva, es crucial que los docentes establezcan normas claras sobre su uso. Estas normas no solo deben proteger a los estudiantes de los riesgos digitales, sino también fomentar una cultura de respeto y responsabilidad en el entorno digital.

Establecer reglas claras desde el principio del curso ayudará a crear un marco de comportamiento que evite distracciones, garantice un aprendizaje efectivo y proteja la seguridad de los estudiantes. Los docentes deben asegurarse de que estas normas sean entendidas y aceptadas por los estudiantes, y adaptarse a la edad y las necesidades del grupo.

Normas Básicas para el Uso de la Tecnología en el Aula

1. **Uso limitado de dispositivos para fines educativos:**

- Los dispositivos deben utilizarse exclusivamente para actividades educativas. Se debe evitar el acceso a redes sociales, juegos, y cualquier otro contenido que no esté relacionado con las tareas de clase, a menos que se indique lo contrario por parte del docente.
- Para fomentar este comportamiento, los docentes pueden integrar software de monitoreo que les permita supervisar el uso de dispositivos y restringir el acceso a sitios web no autorizados durante el horario de clase.

2. **Respetar la privacidad y la seguridad de los demás:**

- Los estudiantes deben aprender a no compartir fotos o videos de compañeros sin su consentimiento. El respeto por la privacidad de los demás es esencial para crear un ambiente seguro.
- Además, se debe educar a los estudiantes sobre la importancia de proteger su información personal y no compartir contraseñas, datos sensibles o detalles privados con personas que no conocen.

3. **Uso responsable del correo electrónico y otras plataformas de comunicación:**

- El correo electrónico y las plataformas de chat escolar, como Google Classroom o Microsoft Teams, deben ser utilizados con responsabilidad. Los estudiantes deben entender que estas herramientas están diseñadas para la comunicación educativa y no para el envío de mensajes personales o inapropiados.

02

4. Mantener un comportamiento respetuoso en línea:

- El respeto en el entorno digital es tan importante como en el mundo real. El ciberacoso, los comentarios hirientes o los ataques personales no deben ser tolerados bajo ninguna circunstancia.
- Los docentes deben establecer un código de conducta para el comportamiento en línea que los estudiantes deben cumplir, incluyendo cómo interactuar respetuosamente en foros y plataformas colaborativas.

Involucrar a los Estudiantes en la Creación de Normas

Un enfoque muy eficaz para asegurar que las normas sean respetadas es involucrar a los estudiantes en su creación. Los estudiantes son más propensos a seguir reglas cuando han participado activamente en su desarrollo. Los docentes pueden abrir un diálogo al inicio del curso para discutir cuáles deberían ser las normas de uso de dispositivos, la privacidad y el respeto en línea.

Este proceso participativo ayuda a que los estudiantes comprendan mejor la importancia de las normas y sientan una mayor responsabilidad al cumplirlas. Además, se pueden realizar acuerdos digitales o contratos de comportamiento en línea, en los que los estudiantes firman su compromiso de seguir las reglas acordadas.

Ejemplos de Normas Digitales en el Aula

Algunos ejemplos de normas que pueden establecerse son:

- Limitar el uso de teléfonos móviles durante la clase, permitiendo su uso solo en actividades específicas que lo requieran.
- Evitar multitareas: Los estudiantes deben concentrarse en una sola tarea a la vez, para mejorar la atención y la comprensión del contenido.
- Pedir permiso antes de grabar cualquier contenido o tomar fotos en clase.
- Apagar los dispositivos al finalizar las actividades que lo requieran para evitar distracciones.
- Reforzar el Cumplimiento de las Normas

Para que las normas sean efectivas, es fundamental que los docentes refuercen el cumplimiento de las mismas de manera consistente. Esto implica:

1. Recordatorios regulares sobre las normas al inicio de las clases.

2. Monitoreo activo: Supervisar el uso de dispositivos y las actividades en línea de los estudiantes para asegurarse de que se sigan las normas. Los docentes pueden utilizar software de gestión de aula digital para monitorizar las pantallas de los estudiantes en tiempo real y asegurarse de que estén trabajando en las actividades correctas.

3. Consecuencias claras y coherentes: Los estudiantes deben ser conscientes de las consecuencias de no seguir las normas. Estas consecuencias deben ser justas, consistentes y proporcionadas al tipo de infracción. Por ejemplo, si

02

un estudiante utiliza su dispositivo para jugar durante la clase, puede perder el privilegio de usarlo por el resto de la sesión.

Comunicación de las Normas a las Familias

- Es fundamental que los docentes también involucren a las familias en el proceso de establecimiento de normas. Informar a los padres sobre las reglas digitales que se aplican en el aula les permite apoyarlas en casa. Los padres pueden reforzar estas normas y supervisar el uso que los estudiantes hacen de los dispositivos fuera del horario escolar.
- El envío de un documento con las normas o la organización de una reunión informativa al inicio del curso puede ser una buena manera de asegurarse de que las familias estén al tanto de las expectativas digitales del aula.
- Uso de Contratos Digitales o Acuerdos de Uso

Un enfoque eficaz para formalizar las normas y asegurar que los estudiantes comprendan su importancia es el uso de contratos digitales. Estos contratos o acuerdos pueden incluir reglas sobre:

El uso adecuado de dispositivos.

- La protección de la privacidad personal y de los compañeros.
- El comportamiento adecuado en plataformas de comunicación en línea. Los contratos pueden ser revisados y firmados tanto por los estudiantes como por los padres, lo que refuerza la idea de que la seguridad digital es una responsabilidad compartida.

Ley Orgánica de Protección Integral a la Infancia y Adolescencia frente a la Violencia (LOPIVI)

La **LOPIVI** establece medidas específicas para garantizar la seguridad y protección de los menores frente a todas las formas de violencia, incluidas las que ocurren en entornos digitales. En el ámbito escolar, los docentes tienen un papel clave en la detección y prevención de la violencia digital, como el ciberacoso, grooming y otras situaciones de riesgo que puedan afectar a los alumnos. Esta ley también exige la **formación del profesorado** en la identificación y gestión de estos casos, lo que subraya la necesidad de que los docentes estén al día con las normativas que protegen a los menores en el entorno digital.

Te resumimos los puntos clave de la **Ley Orgánica de Protección Integral a la Infancia y la Adolescencia frente a la Violencia (LOPIVI)**:

1. Protección integral frente a la violencia

La LOPIVI tiene un enfoque integral, abarcando múltiples ámbitos en los que los menores interactúan. Busca prevenir, detectar y actuar frente a cualquier forma de violencia, ya sea física, emocional o sexual, asegurando un entorno seguro en los ámbitos:

- **Familiar**: Se prevé la protección de los menores frente a cualquier tipo de maltrato o abuso por parte de familiares.
- **Educativo**: Los centros educativos deben implementar **protocolos de actuación** para prevenir y detectar el acoso escolar y otros tipos de violencia.
- **Social**: Se contempla la intervención en contextos comunitarios y sociales donde los menores puedan estar expuestos a situaciones de riesgo.
- **Sanitario**: El sector salud se involucra en la detección temprana de señales de maltrato y abuso, con protocolos para proteger a los menores y garantizar su bienestar físico y psicológico.
- **Digital**: Se protegen a los menores frente a riesgos como el ciberacoso, el grooming y el acceso a contenidos inapropiados en el entorno digital.
- **Ocio y deportes**: Los entornos recreativos deben adoptar medidas para prevenir la violencia, con figuras de protección específicas para este ámbito.
- **Policial**: Las fuerzas de seguridad deben contar con **formación especializada** para actuar en casos de violencia contra menores, con un enfoque de respeto hacia los derechos infantiles.

2. Enfoque preventivo

La ley pone un énfasis particular en la **prevención de la violencia**. Para ello, se requiere que todos los sectores, desde la educación hasta la sanidad, establezcan **programas preventivos** que minimicen la posibilidad de que los menores sufran violencia. Algunas medidas preventivas incluyen:

- **Educación en valores**: En el ámbito educativo, se introducen programas para educar a los menores en valores como la igualdad, el respeto y la resolución pacífica de conflictos.
- **Entornos protectores**: La ley promueve la creación de entornos físicos y emocionales seguros para los menores, tanto en sus hogares como en las instituciones públicas y privadas.
- **Identificación temprana**: Se busca identificar situaciones de riesgo en las primeras etapas para intervenir antes de que se desarrollen casos graves de violencia.

3. Principio del buen trato

Este principio va más allá de prevenir la violencia. La ley fomenta el **buen trato** hacia los menores, promoviendo su desarrollo integral en un entorno de respeto y cariño. Esto implica:

- Asegurar que los niños y adolescentes sean tratados con dignidad y respeto en todas las interacciones.
- Promover una **participación activa de los menores** en las decisiones que afecten su vida, especialmente en contextos de educación, salud y bienestar.
- Crear programas que promuevan el bienestar emocional y psicológico de los menores, reconociendo la importancia de un entorno afectivo positivo para su desarrollo.

4. Refuerzo del derecho a ser escuchado

La LOPIVI refuerza el derecho de los menores a ser **escuchados y tenidos en cuenta** en los procedimientos legales y administrativos que les afecten, especialmente en casos de violencia. Este derecho incluye:

- La posibilidad de que los menores puedan **denunciar situaciones de violencia sin la presencia de sus tutores** si estos están involucrados o si el menor teme represalias.
- El reconocimiento de que la opinión de los menores debe ser valorada en decisiones importantes, como cambios de custodia o situaciones de conflicto familiar.
- Se asegura que los menores reciban un trato adecuado durante su testimonio, evitando la revictimización.

5. Coordinadores de bienestar y delegados de protección

La ley introduce la figura de los **coordinadores de bienestar** en las escuelas y otras instituciones que trabajan con menores. Estos profesionales son responsables de:

- **Prevenir situaciones de violencia** en el ámbito educativo, deportivo y de ocio.
- Supervisar la **implementación de protocolos** de actuación frente a situaciones de riesgo.
- Actuar como punto de referencia para los menores, padres y profesionales ante cualquier señal de alerta sobre posibles casos de violencia.
- Los **delegados de protección** cumplen un rol similar en entornos fuera del ámbito escolar, asegurando que los derechos de los menores sean respetados en actividades de ocio y deportes.

6. Prohibición de prácticas que atentan contra la integridad infantil

La ley prohíbe explícitamente ciertas prácticas que, aunque anteriormente toleradas en algunos contextos, son consideradas **inaceptables** porque atentan contra la dignidad y la integridad de los menores. Entre estas prácticas están:

- **Contención mecánica en centros de protección**: Se prohíbe el uso de dispositivos de contención física (como esposas o cinturones) en centros de protección para menores, salvo en situaciones extremas y con supervisión.
- **Desnudos integrales o pruebas invasivas**: Se prohíbe la realización de desnudos integrales y de pruebas médicas innecesarias que puedan resultar humillantes para los menores, salvo que sean absolutamente imprescindibles para su salud.

7. Creación de la Conferencia Sectorial de Infancia

Se crea un órgano de cooperación llamado Conferencia Sectorial de Infancia, que tiene como objetivo:

- **Coordinar políticas** de protección de la infancia a nivel estatal y autonómico.
- Compartir **buenas prácticas** entre las diferentes comunidades autónomas.
- **Diseñar estrategias** conjuntas para la prevención y protección de la infancia y adolescencia frente a la violencia, asegurando que las políticas sean coherentes y efectivas en todo el país.

8. Registros unificados

La ley establece la creación de **registros unificados** sobre

la violencia infantil para mejorar la formulación de políticas y la intervención en estos casos:

- **Registro Unificado de Violencia contra la Infancia (RUSSVI)**: Un registro nacional que recopila datos de todas las denuncias y casos confirmados de violencia contra menores, permitiendo un seguimiento centralizado.
- Estos registros ayudarán a **detectar patrones de violencia**, a realizar estudios sobre el impacto de las políticas preventivas y a coordinar la respuesta de las distintas administraciones públicas.

9. Prueba preconstituida

La ley incluye la figura de la **prueba preconstituida** para evitar que los menores tengan que declarar múltiples veces en procesos judiciales, lo que podría resultar en **revictimización**. Esta medida implica:

- Grabar de manera anticipada el testimonio de los menores, especialmente aquellos de menos de 14 años o con discapacidad, para evitar que tengan que repetir sus declaraciones en distintas fases del proceso judicial.
- Este sistema también asegura que los menores puedan testificar en condiciones adecuadas, en espacios amigables y con personal especializado.

10. Ampliación de los plazos de prescripción

La LOPIVI extiende los **plazos de prescripción de los delitos graves** cometidos contra menores, como el abuso sexual y la explotación, para que las víctimas tengan más tiempo para denunciar. Según la ley:

- Los delitos comenzarán a prescribir cuando la víctima cumpla **35 años**, lo que les ofrece más tiempo para procesar el trauma y decidir si desean emprender acciones legales.
- Esta medida reconoce que muchas víctimas de abuso infantil no se sienten capaces de denunciar hasta la edad adulta, por lo que amplía el plazo para permitir que busquen justicia.

El **Anteproyecto de Ley Orgánica para la Protección de las Personas Menores de Edad en los Entornos Digitales** introduce medidas clave para **garantizar la seguridad infantil** en el mundo digital.

1. Protección contra contenidos inapropiados

El anteproyecto establece medidas específicas para evitar que los menores de edad accedan a contenido perjudicial en línea, como material violento, pornográfico o relacionado con el consumo de drogas y apuestas. Estas medidas incluyen:

- **Filtros de contenido obligatorios** en plataformas y servicios que ofrezcan acceso a Internet, tanto en navegadores como en aplicaciones, para bloquear contenido inapropiado.
- La **responsabilidad de las plataformas** de redes sociales, sitios web de streaming, y videojuegos de implemen-

tar mecanismos que restrinjan el acceso de menores a este tipo de contenido, con sanciones en caso de incumplimiento.

- Los proveedores de servicios de Internet también deberán ofrecer a las familias **herramientas para controlar y monitorear** el contenido al que acceden los menores.

2. Fomento del uso responsable de la tecnología

- El anteproyecto promueve que los menores desarrollen **competencias digitales** que les permitan hacer un uso seguro y responsable de la tecnología. Para ello, se implementarán en los centros educativos programas que incluyan:
- **Educación en ciudadanía digital**: Los niños y adolescentes aprenderán sobre los riesgos del ciberacoso, grooming, y la difusión de contenido inadecuado, así como sobre cómo actuar en estas situaciones.
- **Promoción del pensamiento crítico en línea**: Se fomentará la capacidad de los menores para identificar noticias falsas, publicidad engañosa y comportamientos manipuladores en las redes sociales.
- **Apoyo al uso productivo de la tecnología**: Además de prevenir riesgos, se fomentará el uso positivo de la tecnología para el aprendizaje y el desarrollo de habilidades digitales.

3. Mecanismos de verificación de edad

Una de las disposiciones más relevantes del anteproyecto es la **implementación obligatoria de mecanismos de verificación de edad** en plataformas digitales que ofrecen contenido sensible o servicios que puedan no ser apropiados para menores. Esto incluye:

- **Requerir la verificación de la edad del usuario** mediante métodos confiables antes de permitir el acceso a contenido o servicios no aptos para menores, como las redes sociales o plataformas de videojuegos que incluyan compras dentro de la aplicación.
- Se establece una **responsabilidad directa para las plataformas** que no cumplan con estos requisitos, con la posibilidad de recibir sanciones económicas si no implementan controles efectivos.

4. Control parental

El anteproyecto también destaca la importancia de dotar a los padres y tutores de herramientas eficaces para supervisar y controlar el uso de la tecnología por parte de los menores. Entre las medidas propuestas se incluyen:

- **Obligación para los fabricantes de dispositivos conectados a Internet** (tabletas, smartphones, consolas de videojuegos, etc.) de incorporar de manera gratuita sistemas de control parental que permitan restringir el acceso a ciertas aplicaciones o páginas web.
- Los sistemas de control parental deberán ser **fáciles de activar y configurar** para que los padres puedan supervisar el tiempo de uso, bloquear aplicaciones o limitar el acceso a determinados tipos de contenido.
- Se fomentará que los **proveedores de servicios de In-**

02

ternet y plataformas digitales incluyan guías y recursos informativos para padres sobre cómo utilizar estas herramientas de control de manera efectiva.

5. Protección de los datos personales

Uno de los pilares del anteproyecto es la protección de los datos personales de los menores, especialmente en el entorno digital. Se refuerzan las normativas existentes, proponiendo:

- **Elevar la edad mínima para el consentimiento del tratamiento de datos** personales a los 16 años. Esto significa que los menores de esa edad no podrán proporcionar su consentimiento sin la autorización de sus padres o tutores para el tratamiento de datos personales en plataformas digitales.
- Establecer mayores controles para que las plataformas y servicios digitales **limiten la recolección de datos de los menores**, protegiendo su privacidad en todo momento.
- Promover que los proveedores de servicios informen de manera clara y accesible a los menores y sus familias sobre **qué datos se recopilan** y cómo se utilizan, asegurando que los menores tengan pleno conocimiento de los riesgos de compartir información personal en línea.

6. Medidas educativas y de formación

La **formación de docentes y alumnos** es otro pilar del anteproyecto. Se plantea que las escuelas tengan la obligación de incluir dentro de su currículum programas específicos que enseñen competencias digitales seguras. Estas medidas incluyen:

- **Formación obligatoria** para los docentes, a fin de que estén capacitados para enseñar a los alumnos sobre los riesgos y oportunidades del entorno digital.
- **Programas de educación digital** en los que los alumnos aprendan a utilizar la tecnología de manera productiva y a detectar situaciones de riesgo como el acoso en línea o la manipulación digital.
- Los centros educativos deberán establecer **políticas de protección digital** que incluyan medidas para proteger a los menores dentro del entorno escolar, como la supervisión del uso de dispositivos conectados a Internet.

7. Medidas en el ámbito sanitario

El anteproyecto contempla la importancia de la salud digital, proponiendo medidas para prevenir problemas de salud derivados del uso excesivo de la tecnología. Esto incluye:

- **Prevención de la adicción a la tecnología**: Se desarrollarán campañas y programas de educación dirigidos a menores y sus familias para prevenir la adicción a los videojuegos, redes sociales y otros dispositivos electrónicos.
- **Atención especializada para menores** con problemas de salud relacionados con el uso excesivo de pantallas, como el insomnio, la ansiedad o la depresión.

- Los centros escolares, en colaboración con el sistema sanitario, deberán **monitorear el impacto de la tecnología en la salud física y mental** de los estudiantes y proporcionar intervenciones cuando sea necesario.

8. Sanciones y supervisión

Para garantizar el cumplimiento de las medidas, el anteproyecto establece un **régimen de sanciones** para las plataformas que no implementen adecuadamente las medidas de seguridad y verificación de edad. Se prevén sanciones como:

- **Multas económicas** para las plataformas que incumplan las normativas de verificación de edad, control parental o recolección de datos.
- La **supervisión por parte de la Comisión Nacional de los Mercados y la Competencia (CNMC)**, que se encargará de asegurar que los proveedores de servicios digitales y plataformas cumplan con sus obligaciones legales.
- Se fortalecerán los mecanismos de denuncia y vigilancia de **contenidos inapropiados y acoso** a través de las redes sociales y otras plataformas.

9. Colaboración público-privada

El anteproyecto fomenta la colaboración entre los sectores público y privado para crear un **entorno digital seguro para los menores**. Algunas medidas incluyen:

- La creación de un **código de conducta** para las empresas tecnológicas, con el objetivo de proteger a los menores en sus servicios.
- Fomentar la participación activa de empresas tecnológicas en la **Estrategia Nacional sobre Protección de la Infancia en el Entorno Digital**, asegurando que desarrollen herramientas y políticas que faciliten la seguridad de los menores.
- Establecer alianzas con ONG y expertos en seguridad digital para diseñar campañas de concienciación dirigidas a menores, familias y educadores.

10. Modificaciones legales

El anteproyecto propone realizar modificaciones en varias leyes importantes para ajustarlas a las nuevas realidades del entorno digital:

- **Código Penal**: Se endurecen las penas relacionadas con el acoso y explotación sexual de menores a través de medios digitales.
- **Ley General de Comunicación Audiovisual**: Se introducen disposiciones para garantizar la protección de los menores en medios de comunicación y plataformas de video bajo demanda.
- **Ley Orgánica de Protección de Datos**: Se actualiza para incluir mayores protecciones para los menores en cuanto al tratamiento y uso de sus datos personales.

Reglamento General de Protección de Datos (RGPD)

El **RGPD** regula cómo deben ser tratados los datos perso-

nales en la Unión Europea, y tiene implicaciones directas en el manejo de la información de los estudiantes en los centros educativos. Los docentes deben comprender cómo el RGPD impacta la **recogida, almacenamiento y uso de datos** de los alumnos, incluidos los datos que se manejan a través de plataformas educativas, correos electrónicos o redes sociales del centro. Los centros educativos son responsables de garantizar que los datos se utilicen solo con fines educativos y bajo medidas de seguridad que protejan la privacidad de los menores.

Normativa de Protección de Datos en el Entorno Escolar

En los centros educativos, la protección de datos personales es esencial, ya que los menores son uno de los colectivos más vulnerables. La normativa exige que los docentes, junto con la administración del centro, implementen medidas que aseguren que los datos de los estudiantes, incluidos sus nombres, imágenes y otros datos sensibles, se manejen de manera **segura y conforme a la ley**. Esto incluye garantizar que no se publiquen sin autorización y que se utilicen exclusivamente para los fines educativos que se han comunicado a los padres o tutores.

Delegado de Protección de Datos en Centros Educativos

Los centros educativos deben contar con un **Delegado de Protección de Datos (DPD)**, quien es responsable de asegurar el cumplimiento del RGPD en el manejo de los datos de los alumnos. El DPD supervisa que se implementen medidas adecuadas para garantizar la seguridad de los datos, asesora al personal sobre cómo gestionar correctamente la información personal y actúa como punto de contacto con las autoridades de protección de datos. Es importante que los docentes estén familiarizados con las funciones del DPD y trabajen en coordinación con él para asegurar el cumplimiento de las normativas.

La Necesidad de Normas Claras en el Uso de la Tecnología

El uso de dispositivos tecnológicos en el aula, como portátiles, tablets y smartphones, se ha convertido en una parte esencial del proceso de enseñanza y aprendizaje. Sin embargo, para garantizar que estos dispositivos se utilicen de manera segura y productiva, es crucial que los docentes establezcan **normas claras** sobre su uso. Estas normas no solo deben proteger a los estudiantes de los riesgos digitales, sino también fomentar una **cultura de respeto y responsabilidad** en el entorno digital.

Establecer reglas claras desde el principio del curso ayudará a crear un marco de comportamiento que evite distracciones, garantice un aprendizaje efectivo y proteja la seguridad de los estudiantes. Los docentes deben asegurarse de que estas normas sean **entendidas y aceptadas por los estudiantes**, y adaptarse a la edad y las necesidades del grupo.

02

Normas Básicas para el Uso de la Tecnología en el Aula

1. **Uso limitado de dispositivos para fines educativos:**
   - Los dispositivos deben utilizarse exclusivamente para actividades educativas. Se debe evitar el acceso a redes sociales, juegos, y cualquier otro contenido que no esté relacionado con las tareas de clase, a menos que se indique lo contrario por parte del docente.
   - Para fomentar este comportamiento, los docentes pueden integrar **software de monitoreo** que les permita supervisar el uso de dispositivos y restringir el acceso a sitios web no autorizados durante el horario de clase.

2. **Respetar la privacidad y la seguridad de los demás:**
   - Los estudiantes deben aprender a **no compartir fotos o videos de compañeros** sin su consentimiento. El respeto por la privacidad de los demás es esencial para crear un ambiente seguro.
   - Además, se debe educar a los estudiantes sobre la importancia de **proteger su información personal** y no compartir contraseñas, datos sensibles o detalles privados con personas que no conocen.

3. **Uso responsable del correo electrónico y otras plataformas de comunicación:**
   - El correo electrónico y las plataformas de chat escolar, como Google Classroom o Microsoft Teams, deben ser utilizados con responsabilidad. Los estudiantes deben entender que estas herramientas están diseñadas para la comunicación educativa y no para el envío de mensajes personales o inapropiados.

4. **Mantener un comportamiento respetuoso en línea:**
   - El **respeto en el entorno digital** es tan importante como en el mundo real. El ciberacoso, los comentarios hirientes o los ataques personales no deben ser tolerados bajo ninguna circunstancia.
   - Los docentes deben establecer un **código de conducta** para el comportamiento en línea que los estudiantes deben cumplir, incluyendo cómo interactuar respetuosamente en foros y plataformas colaborativas.

Involucrar a los Estudiantes en la Creación de Normas

Un enfoque muy eficaz para asegurar que las normas sean respetadas es **involucrar a los estudiantes** en su creación. Los estudiantes son más propensos a seguir reglas cuando han participado activamente en su desarrollo. Los docentes pueden abrir un diálogo al inicio del curso para discutir cuáles deberían ser las normas de uso de dispositivos, la privacidad y el respeto en línea.

Este proceso participativo ayuda a que los estudiantes comprendan mejor la **importancia de las normas** y sientan una mayor responsabilidad al cumplirlas. Además, se pueden realizar **acuerdos digitales** o **contratos de comportamiento en línea**, en los que los estudiantes firman su compromiso de seguir las reglas acordadas.

Ejemplos de Normas Digitales en el Aula

Algunos ejemplos de normas que pueden establecerse son:

- **Limitar el uso de teléfonos móviles** durante la clase, permitiendo su uso solo en actividades específicas que lo requieran.
- **Evitar multitareas**: Los estudiantes deben concentrarse en una sola tarea a la vez, para mejorar la atención y la comprensión del contenido.
- **Pedir permiso antes de grabar** cualquier contenido o tomar fotos en clase.
- **Apagar los dispositivos** al finalizar las actividades que lo requieran para evitar distracciones.

Reforzar el Cumplimiento de las Normas

Para que las normas sean efectivas, es fundamental que los docentes **refuercen el cumplimiento** de las mismas de manera consistente. Esto implica:

- **Recordatorios regulares** sobre las normas al inicio de las clases.
- **Monitoreo activo**: Supervisar el uso de dispositivos y las actividades en línea de los estudiantes para asegurarse de que se sigan las normas. Los docentes pueden utilizar **software de gestión de aula digital** para monitorizar las pantallas de los estudiantes en tiempo real y asegurarse de que estén trabajando en las actividades correctas.
- **Consecuencias claras y coherentes**: Los estudiantes deben ser conscientes de las consecuencias de no seguir las normas. Estas consecuencias deben ser **justas, consistentes y proporcionadas** al tipo de infracción. Por ejemplo, si un estudiante utiliza su dispositivo para jugar durante la clase, puede perder el privilegio de usarlo por el resto de la sesión.

Comunicación de las Normas a las Familias

Es fundamental que los docentes también involucren a las familias en el **proceso de establecimiento de normas**. Informar a los padres sobre las reglas digitales que se aplican en el aula les permite apoyarlas en casa. Los padres pueden reforzar estas normas y supervisar el uso que los estudiantes hacen de los dispositivos fuera del horario escolar.

El envío de un **documento con las normas** o la organización de una reunión informativa al inicio del curso puede ser una buena manera de asegurarse de que las familias estén al tanto de las expectativas digitales del aula.

Uso de Contratos Digitales o Acuerdos de Uso

Un enfoque eficaz para formalizar las normas y asegurar que los estudiantes comprendan su importancia es el uso de **contratos digitales**. Estos contratos o acuerdos pueden incluir reglas sobre:

- **El uso adecuado de dispositivos**.
- **La protección de la privacidad personal y de los compañeros**.
- **El comportamiento adecuado en plataformas de comunicación en línea**.

Los contratos pueden ser revisados y firmados tanto por los estudiantes como por los padres, lo que refuerza la idea de que la seguridad digital es una responsabilidad compartida.

05 Establecimiento de normas y buenas prácticas

Creación de un entorno digital seguro desde el inicio del curso

Es fundamental que los docentes establezcan reglas claras sobre el uso de la tecnología desde el comienzo del curso. Al crear un ambiente digital seguro, los estudiantes entienden cuáles son los comportamientos aceptables y los límites en el uso de dispositivos electrónicos y plataformas en línea. Estas reglas pueden incluir:

- Restricciones en el uso de teléfonos móviles en clase.
- Normas sobre la privacidad y el respeto a los compañeros en entornos digitales.
- Políticas sobre la utilización de dispositivos del colegio (tablets, ordenadores).

Inclusión de los alumnos en la creación de normas

Involucrar a los estudiantes en la creación de estas reglas es una buena práctica para que se sientan comprometidos con su cumplimiento. Los docentes pueden guiar discusiones sobre qué comportamientos online son apropiados y por qué es importante respetar la privacidad y la seguridad digital. Este enfoque participativo no sólo fomenta un mayor respeto por las reglas, sino que también educa a los alumnos sobre las mejores prácticas de seguridad en línea.

Ejemplos de normas digitales en el aula

Algunas de las normas que se pueden establecer incluyen:

- Prohibir la publicación de imágenes o videos de compañeros sin su consentimiento.
- Fomentar el uso respetuoso de correos electrónicos o plataformas de chat del aula.
- Establecer tiempos de uso para las actividades digitales en clase, promoviendo pausas para evitar la fatiga digital.

Comunicación clara con las familias

Es esencial que las familias estén al tanto de las normas digitales del aula para poder reforzarlas en casa. El establecimiento de una **política digital del aula** que se comunique de manera clara a los padres o tutores garantiza que todos los involucrados trabajen juntos para crear un entorno digital seguro y respetuoso. Esta política puede presentarse en una reunión de inicio de curso o mediante una circular que explique las reglas y las expectativas.

Uso de contratos o acuerdos digitales

Una práctica útil es hacer que los estudiantes firmen un **acuerdo digital**, un contrato en el que se comprometen a seguir las normas establecidas sobre el uso de la tecnología en el aula. Estos acuerdos pueden incluir compromisos sobre el respeto en línea, la protección de la privacidad y el uso adecuado de dispositivos, lo que ayuda a que los alumnos sean conscientes de su responsabilidad en el espacio digital.

Te incluimos un ejemplo para que podáis personalizar vuestro propio acuerdo digital:

Acuerdo digital para estudiantes

Yo, [nombre del estudiante], me comprometo a seguir las siguientes normas sobre el uso de la tecnología en el aula y en mi vida diaria, entendiendo la importancia de ser un ciudadano digital responsable.

Compromisos sobre el Uso de la Tecnología

1. **Uso adecuado de dispositivos**
   - Utilizaré los dispositivos electrónicos (tablets, ordenadores, smartphones) únicamente para fines educativos durante el horario escolar.
   - No utilizaré mi dispositivo para enviar mensajes personales, jugar o visitar sitios web no relacionados con el aprendizaje sin el permiso de un docente.

2. **Protección de la privacidad**
   - No compartiré información personal (nombre completo, dirección, número de teléfono, fotos) mía o de otros compañeros en línea sin el consentimiento correspondiente.
   - Configuraré las **opciones de privacidad** en redes sociales y aplicaciones para proteger mi información personal.
   - No compartiré mis contraseñas con nadie, excepto con mis padres o tutores.

3. **Respeto en línea**
   - Me comprometo a **ser respetuoso** con mis compañeros, profesores y otras personas en todas mis interacciones en línea.
   - No participaré en **actos de ciberacoso** ni en la difusión de contenido ofensivo o inapropiado. Informaré de inmediato a un adulto de confianza si veo que algún compañero está siendo acosado o si recibo contenido ofensivo.

4. **Responsabilidad en el uso de redes sociales y plataformas digitales**
   - No publicaré ni compartiré imágenes, vídeos o mensajes que puedan ser ofensivos o inapropiados.
   - Seré responsable de **lo que publico** en redes sociales y me aseguraré de que cualquier contenido compartido sea respetuoso y adecuado.
   - No compartiré información que no esté verificada o que pueda dañar a otras personas.

5. **Seguridad en línea**
   - No haré clic en enlaces sospechosos ni descargaré archivos de fuentes no confiables.
   - Informaré de inmediato a mis profesores o a un adulto de confianza si veo algo en línea que me haga sentir incómodo o inseguro.

6. **Uso equilibrado de la tecnología**
   - Me comprometo a **equilibrar el tiempo que paso en línea** con otras actividades saludables, como el deporte, el estudio o pasar tiempo con mi familia y amigos.
   - Seguiré las indicaciones de mis padres y profesores sobre el tiempo de uso de dispositivos, incluyendo momentos de desconexión.

Compromiso Final

Al firmar este acuerdo, entiendo que mi comportamiento

en línea tiene **consecuencias** y que debo actuar con responsabilidad y respeto en todos los entornos digitales. Me comprometo a respetar estas normas para garantizar un uso adecuado de la tecnología y contribuir a un entorno digital seguro y respetuoso.

Nombre del estudiante: _____

Firma del estudiante: _____

Fecha: _____

Nombre del padre/tutor: _____

Firma del padre/tutor: _____

Fecha: _____

Herramientas para establecer normas y supervisar el uso de tecnología

Los docentes pueden utilizar herramientas como controles parentales, plataformas de monitoreo de actividad en línea o sistemas de gestión del aula que les permitan supervisar el uso que los alumnos hacen de las tecnologías en tiempo real. Por ejemplo, aplicaciones que limitan el acceso a ciertos contenidos o que alertan al docente sobre comportamientos inapropiados pueden ser de gran utilidad para mantener el orden y la seguridad.

La importancia de la privacidad en el entorno escolar

En el contexto digital actual, la **privacidad y la protección de los datos personales** de los estudiantes se han vuelto una prioridad clave para los docentes. Las escuelas y los educadores están manejando más información digital que nunca: datos de contacto, evaluaciones, fotos y videos de actividades escolares, y otros tipos de información sensible. A medida que las plataformas educativas y los entornos en línea se integran más en el proceso de enseñanza, garantizar la privacidad de los estudiantes se convierte en una responsabilidad crítica.

Los docentes deben comprender no sólo la importancia de proteger esta información, sino también las normativas legales que la regulan, como el Reglamento General de Protección de Datos (RGPD) en Europa y otras normativas locales. Estas leyes establecen que la información personal de los menores debe ser tratada con el máximo cuidado, y

cualquier uso indebido o fuga de datos puede tener consecuencias legales graves.

¿Qué Información Personal Debe Protegerse?

Los docentes deben ser conscientes de los distintos tipos de información personal que deben proteger en el entorno escolar digital. Entre los datos sensibles que es fundamental salvaguardar, se incluyen:

- **Datos personales de identificación:** nombres completos, fechas de nacimiento, direcciones, números de teléfono, y otros datos que puedan identificar a un estudiante.
- **Información académica:** calificaciones, informes de progreso, y cualquier detalle relacionado con el rendimiento escolar del estudiante.
- **Imágenes y videos:** fotos o videos de estudiantes que se tomen en el contexto escolar, por ejemplo, durante actividades en el aula, eventos o salidas escolares.
- **Datos relacionados con la salud o la familia:** cualquier información relacionada con la salud de los estudiantes o su contexto familiar es altamente sensible y debe manejarse con un cuidado extremo.

Consentimiento para el Uso de Datos Personales

Es esencial que los docentes comprendan la necesidad de obtener el **consentimiento explícito** de los padres o tutores antes de recopilar, utilizar o compartir cualquier tipo de dato personal de los estudiantes. Esto incluye:

- El uso de imágenes o videos de los estudiantes en redes sociales, sitios web de la escuela o publicaciones de la comunidad.
- La inscripción de los estudiantes en plataformas educativas que requieran el uso de datos personales.

El consentimiento debe ser **claro, informado y verificable,** y los padres deben saber exactamente qué datos se van a recopilar, con qué propósito, y cómo se van a proteger.

Uso seguro de plataformas educativas

Muchas plataformas digitales que se utilizan en el entorno escolar, como **google classroom**, **microsoft teams** o **moodle**, requieren que los estudiantes creen cuentas y proporcionen cierta información personal. Es fundamental que los docentes se aseguren de que estas plataformas cumplan con las normativas de protección de datos y ofrezcan configuraciones de privacidad adecuadas.

Los docentes deben:

- **Evaluar las plataformas antes de utilizarlas**: no todas las herramientas digitales son seguras o respetan la privacidad de los usuarios. Los docentes deben asegurarse de que las plataformas que utilizan cumplan con los estándares de protección de datos, como el rgpd.
- **Configurar la privacidad en las plataformas**: a menudo,

las plataformas permiten a los docentes ajustar las configuraciones de privacidad para garantizar que solo los estudiantes y el personal autorizado puedan acceder a la información compartida.

- **Formar a los estudiantes sobre el uso seguro de las plataformas**: enseñar a los estudiantes a proteger su información personal en estas plataformas, usando contraseñas seguras y no compartiendo datos sensibles en chats públicos o foros abiertos.

Protección de la privacidad en el aula

La privacidad también debe protegerse en las actividades diarias dentro del aula, tanto en el entorno digital como en el físico. Algunas prácticas esenciales incluyen:

- **No compartir información personal innecesaria**: por ejemplo, no es necesario que todos los estudiantes conozcan detalles personales de un compañero que no están relacionados con el aprendizaje.
- **Respetar la privacidad en proyectos y presentaciones**: si se pide a los estudiantes que compartan proyectos en línea, asegúrate de que no incluyan información personal sin el debido consentimiento.

Prevención de violaciones de datos

Las **violaciones de datos** pueden tener consecuencias graves para los estudiantes y para la escuela. Los docentes deben tomar medidas proactivas para evitar que ocurran:

- **Usar contraseñas seguras y autenticación de dos factores**: esto no solo debe aplicarse a las cuentas personales de los docentes, sino también a las plataformas que los estudiantes utilizan en el aula.
- **Mantener el software actualizado**: el uso de software obsoleto puede hacer que los dispositivos sean más vulnerables a ciberataques. Asegúrate de que todos los dispositivos estén protegidos con **antivirus actualizados** y que se utilicen **firewalls** para bloquear accesos no autorizados.
- **Realizar copias de seguridad regulares**: la información de los estudiantes debe estar siempre respaldada en sistemas seguros, evitando el riesgo de pérdida de datos en caso de fallos técnicos o ciberataques.

Formación continua en protección de datos

Dado que las normativas y los riesgos relacionados con la privacidad digital cambian constantemente, es esencial que los docentes reciban **formación continua** en este ámbito. Los colegios pueden organizar talleres sobre protección de datos o colaborar con expertos en ciberseguridad para formar al personal educativo sobre cómo proteger eficazmente la información de los estudiantes.

Además, los docentes deben estar al tanto de las herramientas y recursos disponibles para ayudarlos a cumplir con las normativas de protección de datos y garantizar la seguridad en el aula digital.

Implicación de las familias en la protección de la privacidad

La colaboración con las familias es esencial para garantizar que la **privacidad y los datos personales** de los estudiantes se protejan tanto dentro como fuera del aula. Los docentes deben:

- **Informar a las familias sobre las medidas de privacidad** implementadas en la escuela y las plataformas digitales que se utilizan.
- **Fomentar buenas prácticas en el hogar**: proporcionar guías o recomendaciones a los padres sobre cómo proteger la información personal de sus hijos en internet y cómo supervisar su actividad digital de manera segura.

04 Tecnologías seguras en el aula

04

Uso responsable de plataformas educativas

Las plataformas educativas en línea, como **google classroom**, **microsoft teams** o **moodle**, ofrecen grandes beneficios para la enseñanza, pero también requieren un uso adecuado para asegurar la privacidad de los alumnos. Los docentes deben conocer las políticas de privacidad y configuraciones de seguridad de las plataformas que utilizan, asegurando que:

- Solo los estudiantes y personal autorizado tengan acceso.
- Los datos personales y el rendimiento académico se mantengan protegidos.

Evaluación y selección de herramientas tecnológicas

Antes de implementar una nueva tecnología en el aula, los docentes deben evaluar su seguridad. Algunas preguntas clave incluyen:

- ¿La plataforma cumple con el **rgpd** y las normativas de protección de datos?
- ¿Permite la creación de contraseñas seguras y protege la información personal de los estudiantes?
- ¿La herramienta cuenta con opciones de control para limitar el acceso a contenido inapropiado?

Implementación de dispositivos seguros

Los dispositivos utilizados en el aula, como tablets o portátiles, deben contar con medidas de seguridad integradas. Herramientas como **samsung knox** ofrecen un entorno protegido que permite a los docentes gestionar los dispositivos de los estudiantes, controlar las aplicaciones que se pueden instalar y supervisar el uso en tiempo real. Esto garantiza que los estudiantes solo accedan a contenido educativo y no a sitios potencialmente dañinos.

Controles parentales y restricciones de acceso

El uso de dispositivos digitales por parte de los estudiantes requiere la implementación de **controles parentales** o configuraciones de restricción de acceso. Los docentes pueden aprovechar herramientas que limiten el acceso a ciertos sitios web, aplicaciones o incluso redes sociales durante las horas de clase. Estas configuraciones no solo previenen distracciones, sino que también protegen a los estudiantes de riesgos en línea.

Uso seguro de redes wi-fi en el aula

Las redes wi-fi en los centros educativos deben contar con medidas de seguridad robustas, como **autenticación de usuario** y **encriptación**. El acceso debe estar restringido a personal autorizado y estudiantes, y es importante que los docentes monitoreen el tráfico de la red para detectar posibles amenazas o actividades no permitidas. La conexión debe configurarse para que los estudiantes no puedan acceder a redes públicas no seguras.

Introducción al uso de software de monitoreo

Existen diversas herramientas de **monitoreo de actividad**

digital que permiten a los docentes supervisar en tiempo real lo que los estudiantes hacen en sus dispositivos durante las clases. Estas herramientas alertan sobre el acceso a contenido inapropiado, permiten compartir pantallas y bloquear aplicaciones o sitios web.

Protección contra malware y ataques cibernéticos

Los dispositivos y plataformas que se utilicen en el aula deben estar protegidos contra malware y otras amenazas cibernéticas. Esto incluye:

- Mantener actualizado el software de seguridad en todos los dispositivos.
- Usar **firewalls** y **antivirus** robustos.
- Capacitar a los alumnos en la identificación de correos electrónicos fraudulentos (phishing) o sitios web maliciosos.

Ejemplos prácticos de tecnologías seguras

Un buen ejemplo de tecnología segura en el aula es el uso de dispositivos **samsung** gestionados por **knox**, así como **chromebooks u ordenadores** con **controles parentales integrados** y **supervisión remota**. Los docentes pueden configurar las actividades que los estudiantes deben realizar, bloquear el acceso a ciertas aplicaciones o sitios web, y monitorear el progreso de cada alumno de manera individual. Además, estas herramientas ofrecen la posibilidad de enviar alertas en caso de detectar comportamientos inadecuados o riesgos en línea.

¿Qué es el ciberacoso y por qué es importante prevenirlo?

El **ciberacoso** es una forma de acoso que se realiza a través de medios digitales como redes sociales, aplicaciones de mensajería, juegos en línea o cualquier otra plataforma de comunicación virtual. A diferencia del acoso tradicional, el ciberacoso puede ocurrir en cualquier momento y lugar, lo que lo convierte en un problema particularmente grave para los estudiantes. Las consecuencias emocionales y psicológicas del ciberacoso pueden ser devastadoras, afectando el bienestar de los estudiantes, su rendimiento escolar e incluso su vida social.

Es responsabilidad de los docentes **identificar, prevenir y actuar rápidamente** cuando hay casos de ciberacoso en el entorno escolar. Los estudiantes suelen pasar muchas horas en línea, lo que los expone a este tipo de riesgos. Por ello, la escuela debe ser un espacio seguro en el que los estudiantes se sientan protegidos y apoyados.

Señales de alarma del ciberacoso en el aula

El ciberacoso no siempre es fácil de detectar, ya que la mayoría de las interacciones ocurren fuera del alcance de los docentes. Sin embargo, hay ciertas **señales de alerta** que pueden indicar que un estudiante está siendo víctima de ciberacoso:

- **Cambios repentinos en el comportamiento**: si un estudiante que normalmente es activo o participativo en

clase se vuelve retraído, silencioso o ansioso, podría estar enfrentando problemas en línea.

- **Evitar el uso de dispositivos**: algunos estudiantes que están siendo acosados en línea pueden comenzar a evitar el uso de sus dispositivos, mostrando temor o ansiedad cada vez que reciben un mensaje o notificación.
- **Caída en el rendimiento académico**: el ciberacoso puede afectar profundamente la concentración y el bienestar emocional de los estudiantes, lo que a menudo se refleja en un bajo rendimiento académico o una falta de interés por las actividades escolares.
- **Cambios en las relaciones con compañeros**: si un estudiante deja de interactuar con ciertos compañeros con los que antes tenía una relación cercana, esto podría ser un indicio de que está ocurriendo algún tipo de conflicto en línea.
- **Irritabilidad o tristeza inexplicables**: el ciberacoso puede generar frustración, tristeza y sentimientos de impotencia. Si un estudiante muestra estos comportamientos sin una razón clara, es posible que esté enfrentando acoso digital.

¿Cómo pueden los docentes prevenir el ciberacoso?

La prevención del ciberacoso es clave y comienza con la creación de un ambiente escolar en el que se promueva el **respeto mutuo, la empatía y la responsabilidad digital**. Los docentes juegan un papel crucial en la construcción de este entorno seguro mediante las siguientes acciones:

1. **Fomentar la empatía y el respeto:**

- Los docentes deben enseñar a los estudiantes la importancia de ser respetuosos en línea, evitando participar en conversaciones hirientes o difundir rumores. El **respeto y la empatía** deben ser valores centrales en la cultura del aula.
- Organizar actividades que promuevan el trabajo en equipo y la colaboración puede ayudar a construir relaciones más saludables entre los estudiantes, minimizando el riesgo de conflictos en línea.

2. **Educar sobre las consecuencias del ciberacoso:**

- Es fundamental que los estudiantes comprendan las graves consecuencias que puede tener el ciberacoso, tanto para la víctima como para el acosador. Los docentes deben explicar que el ciberacoso no es solo un acto de crueldad, sino que puede tener consecuencias legales y académicas.
- Mostrar ejemplos concretos o invitar a expertos a hablar sobre los riesgos del ciberacoso puede ser una forma efectiva de hacer que los estudiantes tomen conciencia del problema.

3. **Establecer normas claras sobre el comportamiento en línea:**

- En el contexto escolar, es fundamental que existan **normas claras y explícitas** sobre el uso de dispositivos y el

comportamiento en plataformas en línea. Estas normas deben incluir la prohibición explícita del ciberacoso, la intimidación y el acoso de cualquier tipo.

- Los estudiantes deben conocer las **consecuencias** de violar estas normas. Por ejemplo, los casos de ciberacoso deben ser abordados con medidas disciplinarias, que pueden incluir desde la suspensión temporal del acceso a dispositivos hasta acciones más severas en casos graves.

4. **Enseñar a los estudiantes a proteger su privacidad:**

- Uno de los principales factores que facilita el ciberacoso es la falta de conocimiento sobre cómo proteger la información personal en línea. Los docentes deben enseñar a los estudiantes a **configurar la privacidad** en sus cuentas, a usar contraseñas seguras y a no compartir información personal con desconocidos.
- También es importante educar a los estudiantes sobre las consecuencias de compartir fotos o videos inapropiados, ya que este material puede ser utilizado para acosarlos o extorsionarlos.

Actuar rápidamente ante un caso de ciberacoso

Si un docente detecta que un estudiante está siendo víctima de ciberacoso, es crucial que actúe de inmediato para proteger al estudiante y poner fin al acoso. A continuación, se describen algunos pasos que los docentes deben seguir:

1. **Escuchar al estudiante con empatía:**

- Si un estudiante confía en el docente y reporta que está siendo acosado en línea, es vital **escucharle con empatía y sin juzgar**. Los estudiantes suelen sentirse avergonzados o culpables por el acoso que sufren, por lo que necesitan un entorno de confianza donde se les asegure que no están solos.

2. **Recopilar pruebas del acoso:**

- Si es posible, el docente debe ayudar al estudiante a recopilar **pruebas del ciberacoso** (mensajes, capturas de pantalla, publicaciones) para tener una base sólida al momento de reportar el incidente.

3. **Informar a los responsables del colegio y a los padres:**

- Los casos de ciberacoso deben ser reportados de inmediato a los **coordinadores de bienestar** o al equipo directivo del colegio. Asimismo, es importante informar a los padres del estudiante para que puedan ofrecerle apoyo adicional en casa.

4. **Tomar medidas disciplinarias adecuadas:**

- El ciberacoso no debe ser tolerado en ningún caso. Si se identifica al acosador, deben tomarse las medidas disciplinarias adecuadas, siguiendo los protocolos establecidos por el colegio y, si es necesario, involucrando a las autoridades.

5. **Proporcionar apoyo emocional a la víctima:**

- El ciberacoso puede tener un impacto emocional profundo en los estudiantes. El docente debe asegurarse de que la víctima reciba el apoyo emocional necesario, ya sea a través de charlas con el coordinador de bienestar, sesiones con un psicólogo escolar o actividades que promuevan su autoestima y confianza.

Fomentar un entorno digital seguro y positivo

Finalmente, los docentes deben fomentar un **entorno digital seguro y positivo** en el aula. Esto puede incluir el uso de **plataformas educativas controladas**, donde se supervise la interacción entre los estudiantes, así como la promoción de actividades en las que los estudiantes utilicen la tecnología de forma colaborativa y constructiva.

05 Detección y prevención de riesgos digitales

05

Identificación temprana de ciberacoso

El **ciberacoso** es una de las principales amenazas que los estudiantes enfrentan en el entorno digital. Los docentes deben estar atentos a las señales de acoso, como cambios en el comportamiento de los alumnos, la aparición de conflictos en línea o la exclusión social. Es fundamental enseñar a los estudiantes a denunciar estos incidentes de manera segura, tanto a los docentes como a sus familias, y fomentar un ambiente de respeto mutuo.

Los docentes pueden apoyarse en **plataformas seguras** que monitorean la actividad digital en tiempo real, alertando sobre posibles comportamientos de acoso o violencia digital.

Prevención del grooming

El **grooming** se refiere a la manipulación que realizan adultos hacia menores con fines de abuso sexual. Es crucial que los docentes eduquen a los estudiantes sobre cómo proteger su información personal y no entablar conversaciones con extraños en línea. Los docentes también deben capacitarse para identificar señales de grooming, como cambios en las interacciones sociales de los estudiantes o comportamientos sospechosos en línea.

Para prevenir este tipo de delitos, los docentes pueden implementar charlas educativas en clase, fomentar el diálogo abierto sobre los peligros de internet y enseñar a los alumnos a ser **críticos con las interacciones digitales**. Los recursos como **no te calles** ofrecen estrategias claras para que los estudiantes y docentes puedan identificar y actuar rápidamente frente a estos problemas. Además, otros recursos como los ofrecidos por **pantallas amigas** pueden ser de gran utilidad para educar a los niños sobre cómo evitar caer en estas situaciones.

Sexting: prevención y actuación

El **sexting** es el envío de imágenes o mensajes con contenido sexual entre menores, lo cual puede derivar en problemas graves como el acoso o la explotación. Los docentes deben educar a los estudiantes sobre los riesgos del sexting, promoviendo el respeto por la intimidad propia y de los demás. También es importante que sepan las consecuencias legales del uso y distribución de este tipo de contenido.

Se pueden ofrecer talleres y charlas sobre el respeto a la privacidad, apoyándose en recursos como **no te calles**, **pantallas amigas** e **incibe**, que proporcionan guías detalladas para abordar el tema de manera pedagógica y efectiva.

Prevención de tecnoadicciones

El **uso excesivo de dispositivos** puede derivar en tecnoadicciones, afectando tanto el rendimiento académico como la salud emocional de los estudiantes. Los docentes pueden promover hábitos saludables de uso de la tecnología en el aula, como realizar pausas tecnológicas, limitar el tiempo de pantalla en actividades no educativas y fomentar el equilibrio entre actividades digitales y físicas.

05

Además, es importante educar a los estudiantes sobre la importancia de **gestionar su tiempo en línea**, identificando señales de dependencia digital, como la necesidad constante de estar conectado o la incapacidad de desconectarse de redes sociales.

Recursos para la detección y prevención

Los docentes cuentan con múltiples herramientas para detectar y prevenir estos riesgos.

Es muy importante contar con plataformas que permiten monitorear en tiempo real lo que los estudiantes están haciendo en sus dispositivos, alertando ante comportamientos inusuales. Además, recursos educativos como **no te calles** y **pantallas amigas** ofrecen guías y materiales específicos sobre la prevención del acoso, grooming y sexting, que pueden ser utilizados en el aula para capacitar tanto a estudiantes como a docentes.

06 Protocolos de actuación ante incidentes

06

Pasos generales a seguir

Cuando ocurre un incidente digital en el aula, es fundamental que los docentes sigan un protocolo claro para garantizar la seguridad de los estudiantes y manejar la situación de manera efectiva. Los principales pasos incluyen:

- **Identificación del incidente**: lo primero es identificar y confirmar el tipo de incidente. Puede tratarse de ciberacoso, suplantación de identidad, grooming, sexting, u otra actividad que ponga en riesgo la seguridad del estudiante. Esto puede ser reportado directamente por los alumnos, detectado por el docente o alertado por alguna plataforma de monitoreo.
- **Documentación**: una vez identificado el incidente, es necesario documentar la situación de manera precisa. Esto incluye recopilar pruebas (mensajes, capturas de pantalla, correos electrónicos) que puedan ser necesarias para la investigación del caso o para actuar adecuadamente. También es importante que el incidente quede registrado en un informe interno del centro educativo.
- **Intervención inmediata**: dependiendo de la gravedad del incidente, el docente puede intervenir directamente bloqueando el acceso a la plataforma, informando al coordinador de bienestar del centro, y contactando a los padres del alumno afectado. Si la situación es grave (como en casos de grooming o amenazas), se debe notificar de inmediato a las autoridades competentes, como la **guardía civil** o **policía**.
- **Notificación al coordinador de bienestar y protección**: el **coordinador de bienestar** es la figura clave dentro del centro educativo para gestionar incidentes relacionados con la seguridad de los alumnos. Es esencial que los docentes reporten todos los casos al coordinador, quien activará los protocolos adicionales y decidirá las medidas a tomar, tanto con el alumnado afectado como con el resto de la comunidad educativa.
- **Implicación de las familias**: una vez que se ha confirmado el incidente, es importante involucrar a las familias, especialmente si el problema afecta directamente al bienestar del estudiante. Los padres deben ser informados de la situación y de las medidas que el centro está tomando para resolver el problema. También se les puede aconsejar sobre cómo actuar desde casa y qué medidas adicionales tomar, como bloquear el acceso a ciertas plataformas o denunciar a las autoridades.

Actuación frente a ciberacoso

Ante situaciones de **ciberacoso**, los docentes deben intervenir rápidamente para evitar que el problema escale. El **protocolo antibullying** debe activarse de inmediato, con la implicación del equipo directivo y, si es necesario, la policía. Las acciones inmediatas pueden incluir:

- La mediación entre las partes involucradas.
- El seguimiento de las redes sociales o plataformas donde ocurre el acoso.
- La retirada de publicaciones ofensivas y el bloqueo de perfiles si es posible.

Manejo de casos de grooming y sexting

En situaciones de **grooming** o **sexting**, los docentes deben

asegurarse de que los estudiantes reciban apoyo emocional mientras el caso es investigado. Estos incidentes requieren una intervención inmediata de las autoridades, dado que implican delitos graves que atentan contra la seguridad del menor. El personal docente debe ofrecer un entorno seguro en el que los alumnos puedan compartir sin temor, con la confianza de que la situación se gestionará de manera discreta y profesional.

Recursos para la intervención

Existen varios recursos y plataformas que pueden ayudar a los docentes a actuar de manera efectiva ante incidentes digitales. Por ejemplo:

- **Pantallas amigas** y **no te calles** ofrecen herramientas y guías prácticas para actuar ante incidentes de ciberacoso o grooming.
- **Incibe** proporciona una línea de ayuda y asesoramiento para situaciones de ciberseguridad, tanto para docentes como para alumnos.

Seguimiento y evaluación post-incidente

Después de un incidente, es crucial llevar a cabo un **seguimiento** para asegurarse de que la situación ha sido resuelta y que el alumno afectado está recibiendo el apoyo adecuado. Se debe evaluar el impacto del incidente en la clase y tomar medidas para prevenir futuros problemas, como reforzar las charlas educativas sobre el uso responsable de la tecnología o implementar nuevos controles digitales en el aula.

07 Protección de datos y privacidad en el aula

07

El manejo de información sensible en el aula

Los centros educativos y docentes están en contacto con una gran cantidad de información sensible sobre sus estudiantes, como sus nombres, imágenes, datos académicos y datos de contacto. Es fundamental que los docentes comprendan la importancia de proteger esta información para cumplir con el **Reglamento General De Protección De Datos (RGPD)** y la **Ley Orgánica De Protección De Datos Y Garantía De Los Derechos Digitales (LOPDGDD)**.

Los docentes deben asegurarse de que:

- Solo los responsables autorizados (docentes y personal administrativo) tengan acceso a los datos de los estudiantes.
- Los datos se utilicen exclusivamente para fines educativos y no se compartan sin el consentimiento explícito de los padres o tutores.

En el contexto digital actual, la privacidad y la protección de los datos personales de los estudiantes se han vuelto una prioridad clave para los docentes. Las escuelas y los educadores están manejando en el ámbito digital mucha información correspondiente a sus alumnos/as: datos de contacto, evaluaciones, fotos y videos de actividades escolares, y otros tipos de información sensible. A medida que las plataformas educativas y los entornos en línea se integran más en el proceso de enseñanza, garantizar la privacidad de los estudiantes se convierte en una responsabilidad crítica. Los docentes deben comprender no sólo la importancia de proteger esta información y la necesidad de conocer y cumplir la legislación en materia de protección de datos personales, que establece un marco de regulación ex profeso para cuando los datos personales corresponden a personas menores de edad, para exigir las máximas garantías y cuidado en su tratamiento.

Consentimiento para el uso de datos personales

El consentimiento de los padres o tutores es necesario para recoger y utilizar cualquier tipo de dato personal de los menores, especialmente para:

- Compartir imágenes de los estudiantes en redes sociales, páginas web del centro o publicaciones.
- Participar en actividades extracurriculares que requieran el uso de datos digitales, como inscripciones en plataformas educativas externas.

Los docentes deben asegurarse de que se cuente con el consentimiento por escrito antes de recopilar o compartir cualquier dato de los estudiantes. Este consentimiento debe explicar claramente los fines para los que se usarán los datos, quiénes tendrán acceso y cómo se protegerá la información.

Políticas de uso de imágenes y vídeos en actividades escolares

Es común que durante actividades escolares se tomen fo-

tografías o vídeos de los estudiantes, pero esto puede poner en riesgo su privacidad si no se manejan de manera correcta. Los docentes deben:

- Obtener el consentimiento de los padres para la toma y publicación de imágenes.
- Asegurarse de que las imágenes solo se utilicen en los entornos autorizados (por ejemplo, en comunicaciones internas o webs protegidas del colegio).
- Evitar la publicación de imágenes o vídeos que identifiquen a los estudiantes sin el debido permiso.

Uso de plataformas digitales con normas de privacidad

Los centros educativos y los docentes utilizan cada vez más plataformas digitales para gestionar el aprendizaje y la comunicación con los estudiantes y las familias. Es fundamental asegurarse de que estas plataformas cumplan con las normativas de privacidad y protección de datos. Los docentes deben:

- Verificar que las plataformas digitales que se usan en el aula (p. Ej., **Google classroom**, **microsoft teams**) tengan configuraciones de seguridad adecuadas y opciones de privacidad personalizables.
- Configurar las plataformas de manera que los datos personales de los estudiantes estén protegidos y no se compartan sin consentimiento.

Prevención de violaciones de datos

En el entorno digital, la protección de datos es especialmente crítica debido a las amenazas como el acceso no autorizado, el robo de identidad o la filtración de datos. Los docentes deben seguir estas buenas prácticas para prevenir violaciones de datos:

- Usar contraseñas seguras y fomentar que los estudiantes hagan lo mismo.
- Cifrar cualquier tipo de archivo o comunicación que contenga información sensible de los estudiantes.
- Realizar copias de seguridad de los datos y asegurarse de que se almacenen en lugares seguros, con acceso restringido solo al personal autorizado.

Colaboración con el delegado de protección de datos

El **Delegado de Protección de Datos (DPD)** en los centros educativos tiene la responsabilidad de garantizar que se cumplan las leyes de protección de datos. Los docentes deben trabajar estrechamente con el DPD para asegurar que cualquier manejo de datos de los estudiantes sea conforme con la normativa. El DPD también puede proporcionar formación y asesoramiento para que el personal docente comprenda las mejores prácticas en el manejo de la privacidad y los datos.

08 Promoción del bienestar digital

Importancia del bienestar digital

El **bienestar digital** se refiere al equilibrio entre el uso de la tecnología y la salud mental y física de los estudiantes. Con el creciente uso de dispositivos y plataformas digitales en el aula, los docentes tienen la responsabilidad de promover hábitos saludables de uso de la tecnología. Esto no solo ayuda a prevenir tecnoadicciones, sino también a mejorar el rendimiento académico y el bienestar general de los alumnos.

Estrategias para fomentar el uso responsable de la tecnología

1. **Establecer límites de tiempo**

Los docentes pueden limitar el tiempo que los estudiantes pasan utilizando dispositivos electrónicos durante las clases, promoviendo la importancia de pausas regulares. Establecer tiempos específicos para el uso de la tecnología asegura que los estudiantes no se sobreexpongan a pantallas durante largos periodos.

2. **Fomentar la desconexión activa**

La desconexión periódica de las pantallas es clave para el bienestar digital. Se pueden organizar actividades fuera de línea, como debates o trabajos en grupo, para equilibrar el aprendizaje digital con experiencias más directas y sociales.

3. **Enseñar la gestión del tiempo digital**

Los docentes pueden utilizar herramientas que monitoreen y limiten el uso de aplicaciones y redes sociales para que los estudiantes aprendan a manejar su tiempo en línea. Programas como **samsung digital wellbeing** permiten controlar y gestionar las actividades digitales de los estudiantes, promoviendo un uso más saludable de los dispositivos.

Prevención de tecnoadicciones

El uso excesivo de la tecnología puede llevar a **tecnoadicciones**, que afectan tanto el rendimiento académico como la salud emocional. Los docentes pueden fomentar una relación equilibrada con la tecnología mediante la educación y la conciencia sobre los efectos negativos de un uso desmedido. Algunas señales de tecnoadicción incluyen:

- Dificultad para concentrarse en tareas sin el uso de tecnología.
- Necesidad constante de estar conectado a redes sociales o videojuegos.
- Cambios en el comportamiento o en los patrones de sueño.

Ejemplos prácticos de bienestar digital en el aula

- **pausas activas**: durante las clases en las que se utilicen dispositivos digitales, es importante que los estudiantes tomen descansos breves y realicen actividades físicas o estiramientos para evitar la fatiga digital.
- **Concienciación sobre la privacidad**: los estudiantes deben estar educados sobre los riesgos de compartir demasiada información en línea, así como sobre la importancia de cuidar su **identidad digital**.

Incorporación de la educación sobre salud digital

El bienestar digital también incluye enseñar a los estudiantes a ser críticos con la información que consumen en línea y a establecer límites saludables en su uso de dispositivos. Se pueden incluir charlas y talleres que promuevan la **higiene digital**, incluyendo temas como la correcta postura frente a la pantalla, la ergonomía en el uso de dispositivos y el uso de aplicaciones que controlan el tiempo de pantalla.

Recursos para docentes

Los docentes pueden acceder a plataformas como **pantallas amigas** o **incibe** para encontrar guías y herramientas sobre cómo educar a los estudiantes en el bienestar digital. Además, estos recursos ofrecen recomendaciones sobre la gestión del uso de dispositivos en casa y en el aula, ayudando a involucrar también a las familias en la promoción de un entorno digital saludable.

Herramientas y recursos de apoyo

Plataformas y aplicaciones para la seguridad digital

Los docentes tienen a su disposición numerosas **plataformas y aplicaciones** diseñadas para ayudarles a mantener un entorno digital seguro. Algunas de las más útiles incluyen:

1. **Google classroom**
Permite la gestión segura del aprendizaje digital, con controles para limitar el acceso a material inapropiado.

2. **Microsoft teams**
Ofrece opciones de seguridad como la autenticación de usuarios y la restricción de acceso a personas no autorizadas.

3. **Samsung knox**
Asegura el uso de dispositivos en el aula, protegiendo los datos personales de los estudiantes y garantizando un acceso controlado a las aplicaciones.

Herramientas de monitoreo en tiempo real

Los docentes pueden utilizar herramientas de monitoreo para supervisar en tiempo real lo que los estudiantes están haciendo en sus dispositivos. Estas herramientas permiten:

- Bloquear sitios web inapropiados.
- Monitorear las actividades digitales de los alumnos.
- Enviar alertas en caso de actividades sospechosas o riesgos potenciales.

Guías y recursos educativos en línea

Existen plataformas y organizaciones que ofrecen guías completas y actualizadas para capacitar a los docentes en temas de seguridad digital. Entre ellas destacan:

- **Pantallas amigas**: ofrece guías sobre prevención del ciberacoso, grooming y sexting, además de herramientas educativas para trabajar con los estudiantes en la promoción de una ciudadanía digital responsable.
- **Incibe**: proporciona recursos sobre ciberseguridad y cómo manejar incidentes digitales en el aula. Ofrecen asesoramiento y formación tanto para docentes como para estudiantes.
- **No te calles, cuéntalo**: plataforma enfocada en la prevención del abuso sexual infantil, con recursos diseñados para ayudar a los docentes.

Formación continua para docentes

La seguridad digital es un ámbito en constante evolución. Es crucial que los docentes participen en **programas de formación continua** que les mantengan al día sobre las últimas amenazas y las mejores prácticas para prevenirlas.

uso de materiales didácticos y recursos audiovisuales

El uso de materiales didácticos, como **cómics de ciberseguridad** y vídeos educativos, puede ser muy efectivo para

enseñar a los estudiantes sobre la importancia de la seguridad digital. Recursos visuales y dinámicos facilitan la comprensión de temas complejos como el ciberacoso, el grooming y la gestión de la privacidad en línea. **Pantallas amigas** y **no te calles, cuéntalo** son buenos ejemplos de organizaciones que ofrecen este tipo de materiales.

10 Colaboración con familias y comunidad escolar

10

Importancia de la colaboración

Para garantizar la protección digital de los estudiantes, es crucial que exista una **colaboración estrecha** entre docentes, familias y otros actores de la comunidad educativa. Al trabajar juntos, se pueden establecer normas y valores comunes que fomenten un uso responsable de la tecnología dentro y fuera del aula.

Comunicación abierta y continua con las familias

Los docentes deben mantener una comunicación abierta y regular con las familias sobre los riesgos y las mejores prácticas en el entorno digital. Esto incluye:

- **Informar a las familias sobre los incidentes digitales** que ocurran en el aula, como ciberacoso o violaciones de la privacidad, y cómo se están gestionando.
- **Recomendar herramientas y recursos** que los padres puedan usar en casa para supervisar y proteger a sus hijos en línea, como **controles parentales** y plataformas de seguridad digital.
- **Compartir guías prácticas** sobre el uso seguro de dispositivos, tales como la guía del **plan digital familiar**, para que las familias comprendan cómo ayudar a los niños a equilibrar su tiempo en línea.

Coordinación con el coordinador de bienestar

El **coordinador de bienestar y protección** desempeña un papel esencial en la creación de un entorno seguro. Los docentes deben trabajar de manera cercana con este coordinador para:

- **Desarrollar protocolos claros** sobre cómo actuar ante incidentes digitales y cómo implementar estrategias preventivas.
- **Planificar actividades educativas** y talleres que involucren a las familias, fomentando la concienciación sobre la seguridad digital y la privacidad.

Actividades de sensibilización para la comunidad escolar

Es importante que las familias y la comunidad escolar participen en actividades de sensibilización sobre la seguridad digital. Los docentes pueden organizar:

- **Talleres** para padres y alumnos sobre el uso responsable de redes sociales y la protección de la privacidad.
- **Reuniones periódicas** con las familias para discutir el impacto de la tecnología en la vida de los estudiantes, compartiendo recursos de plataformas como **pantallas amigas** o **incibe**.
- **Seminarios o webinars** con expertos en ciberseguridad para educar a la comunidad escolar sobre los últimos riesgos digitales y cómo prevenirlos.

Involucrar a los estudiantes en la creación de un entorno seguro

Es fundamental que los estudiantes participen activamente

10

en la creación de un ambiente digital seguro. Los docentes pueden fomentar la participación de los alumnos al:

- **Enseñarles a ser responsables** de su propio comportamiento en línea.
- **Promover la denuncia de incidentes digitales** como el ciberacoso o la difusión de contenido inapropiado, asegurándoles que sus inquietudes serán atendidas de forma confidencial.
- **Crear comités estudiantiles de ciberseguridad**, donde los propios alumnos trabajen en proyectos para educar a sus compañeros sobre la seguridad en línea.

Recursos para las familias

Proporcionar a las familias recursos y guías prácticas sobre la **protección de datos**, el uso responsable de la tecnología y cómo identificar señales de riesgo digital es clave para extender la seguridad más allá del aula.

Estudiantes

+índice

1. Introducción a la seguridad digital 68

- ¿Qué es la seguridad digital? 69
- ¿Por qué es importante mantenerse seguro en línea? 69
- Beneficios de la seguridad digital 69
- ¿Qué aprenderás en esta guía? 69

2. Normas básicas para un uso seguro de la tecnología 71

- Reglas para el uso de dispositivos en el aula 72
- Uso responsable de la tecnología en casa 72
- Cómo proteger tu información personal 72
- ¿Cómo crear contraseñas seguras? 73
- Participación activa en la protección digital 73
- Reglas para mantener el orden y la seguridad en plataformas digitales 73

3. Prevención del ciberacoso 74

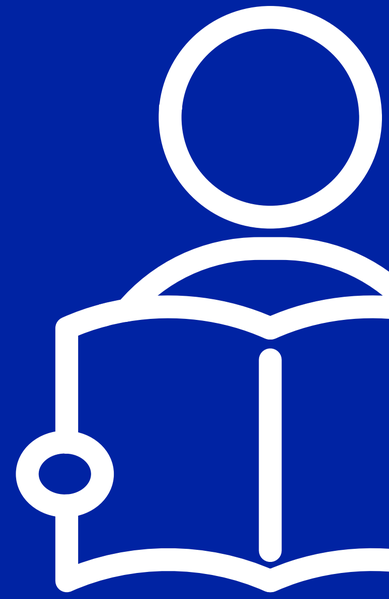
- ¿Qué es el ciberacoso? 75
- ¿Cómo saber si estás siendo víctima de ciberacoso? 75
- Cómo protegerte del ciberacoso 75
- Cómo denunciar el ciberacoso 76
- Cómo ayudar a un compañero que está sufriendo ciberacoso 76
- Ser un ciudadano digital respetuoso 76

4. Protección de la privacidad y datos personales 77

- ¿Por qué es importante proteger tu privacidad? 78
- ¿Qué información personal debes proteger? 78
- Cómo proteger tu información personal en redes sociales 78
- ¿Cómo crear contraseñas seguras? 79
- La importancia de la configuración de privacidad en aplicaciones y juegos 79
- Qué hacer si sientes que tu privacidad ha sido comprometida 79

5. Uso responsable de las redes sociales 80

- ¿Qué son las redes sociales? 81



Estudiantes

+índice

- ¿Cómo usar las redes sociales de manera responsable? 81
- Cómo protegerte en redes sociales 81
- Qué hacer si ves contenido inapropiado 82
- Uso positivo de las redes sociales 82

6. Evitar el Grooming y otros peligros online 83

- ¿Qué es el Grooming? 84
- Señales de alerta del grooming 84
- Cómo protegerte del Grooming 84
- ¿Qué hacer si sospechas de Grooming? 85
- Otros peligros online: suplantación de identidad y Phishing 85
- Consejos para navegar de manera segura 85

7. Pornografía y acceso a contenidos inadecuados 87

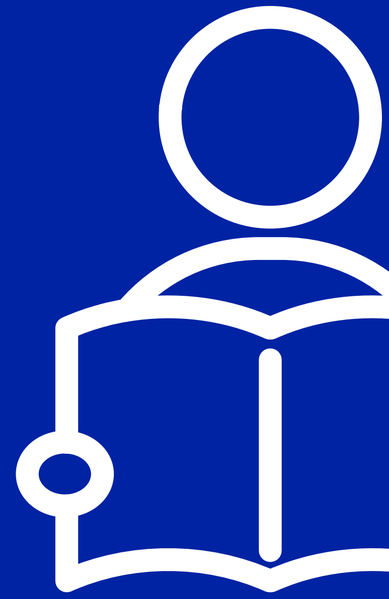
- ¿Qué es la Pornografía? 88
- Por Qué la Pornografía Puede Ser Dañina 88
- Cómo Evitar el Acceso a Contenido Inadecuado 88
- ¿Qué Hacer Si Accedes a Contenidos Inapropiados? 89
- Consecuencias de Compartir Contenido Inapropiado 89
- Fomentando Relaciones Saludables 89

8. Qué hacer ante incidentes en internet 90

- ¿Qué es un incidente en línea? 91
- Pasos a seguir si ocurre un problema en línea 91
- ¿Por qué es importante actuar rápidamente? 91
- Dónde buscar ayuda 92
- Consecuencias de ignorar el problema 92
- Recursos para manejar incidentes en línea 92

9. Pedir ayuda si necesitas apoyo 93

- ¿Por qué es importante pedir ayuda? 94
- ¿A quién puedes pedir ayuda? 94
- Cómo pedir ayuda 95
- Recursos y herramientas de apoyo 95



Estudiantes

10. Control del tiempo en pantalla y bienestar digital 96

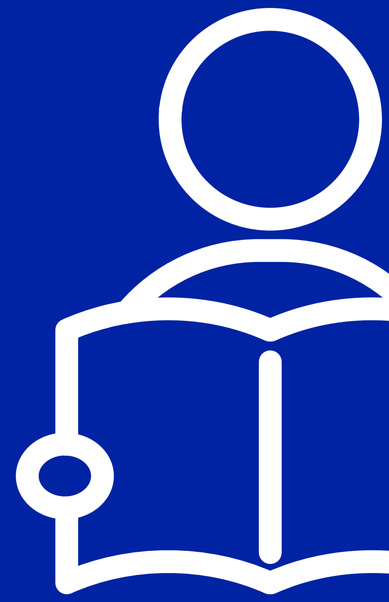
- Ser amable y respetuoso en línea 97
- Usar internet de manera positiva 97
- Cuidar tu propia huella digital 98
- Apoyar un entorno digital seguro para todos 98

11. Recursos y herramientas para mantenerte seguro 99

- Herramientas para protegerte en línea 100
- Recursos en línea para aprender más sobre seguridad 100

12. Conclusión: ser un ciudadano digital responsable 101

- Ser amable y respetuoso en línea 102
- Usar internet para el aprendizaje y crecimiento personal 102
- Mantén un equilibrio entre el mundo digital y el mundo real 102



01

Introducción a la seguridad digital

Introducción: el rol del docente en la seguridad digital

¿Qué es la seguridad digital?

La **seguridad digital** significa protegernos mientras usamos dispositivos conectados a internet, como móviles, tablets, ordenadores y consolas de videojuegos. Estos dispositivos nos permiten acceder a un mundo de información, juegos y redes sociales, pero también nos exponen a ciertos riesgos si no tomamos precauciones.

La seguridad digital implica el uso de prácticas que nos protejan del ciberacoso, robo de datos personales, virus y otros peligros que pueden afectar nuestro bienestar físico, mental y emocional. De la misma manera que nos protegemos en el mundo físico, debemos hacerlo en el mundo digital.

¿Por qué es importante mantenerse seguro en línea?

Es esencial mantenerse seguro en línea porque:

- **Proteges tu información personal**: Tu nombre, dirección, escuela, y hasta fotos tuyas son datos privados que no deben compartirse fácilmente. Cualquier persona puede usar estos datos sin que te des cuenta.
- **Previenes el ciberacoso**: Internet es un espacio donde algunos usuarios se comportan mal. Si eres víctima de ciberacoso, es importante saber cómo protegerte y qué hacer al respecto.
- **Mantienes el control sobre tu bienestar emocional**: Al navegar de manera segura, te aseguras de que tu experiencia en línea sea positiva, sin tener que lidiar con contenido inapropiado o peligroso.

Beneficios de la seguridad digital

- **Mayor control sobre tu privacidad**: Mantener la privacidad en línea es esencial para evitar que desconocidos sepan cosas sobre ti o tu vida personal. Configuraciones adecuadas de seguridad te permiten decidir quién ve tus publicaciones y qué tipo de contenido compartes.
- **Protección frente a amenazas**: Las amenazas en línea, como virus, malware y fraudes, pueden dañar tu dispositivo o comprometer tu información. Saber cómo evitarlas te mantendrá a salvo.
- **Un entorno positivo y respetuoso**: Al practicar la seguridad digital, promueves un uso más saludable y respetuoso de Internet, tanto para ti como para tus amigos y compañeros.

¿Qué aprenderás en esta guía?

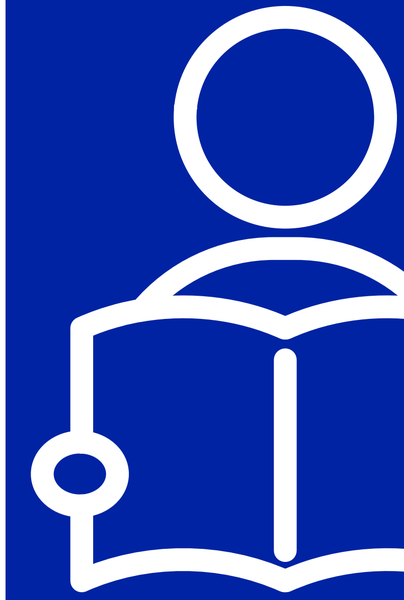
En esta guía, aprenderás:

1. **Cómo protegerte** cuando utilices dispositivos digitales.

2. **Cómo detectar y actuar** ante amenazas como el ciberacoso, el grooming o el acceso a contenido inapropiado.

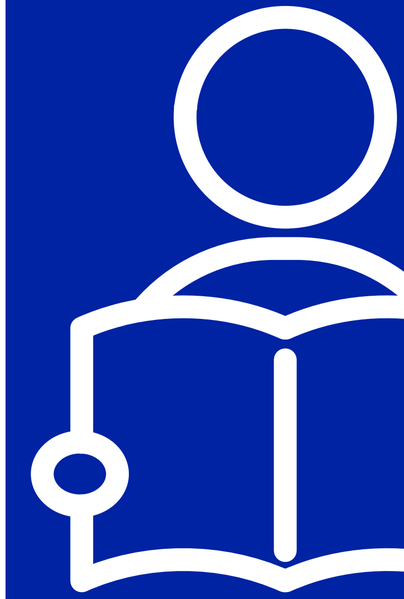
3. **Cómo establecer límites sanos** en el uso de internet, manteniendo un equilibrio entre el tiempo que pasas en línea y otras actividades.

4. **Cómo pedir ayuda** si alguna vez te encuentras en una situación incómoda o peligrosa en internet.



Introducción: el rol del docente en la seguridad digital

La seguridad digital no es solo responsabilidad de los adultos, sino también de los propios estudiantes. Al estar informado y tomar medidas de protección, puedes disfrutar de internet de manera positiva, aprendiendo y conectando con otras personas de forma segura.



02 Normas básicas para un uso seguro de la tecnología

Reglas para el uso de dispositivos en el aula

El uso de dispositivos como tablets, ordenadores y móviles en el aula puede ser muy útil para aprender, pero también es importante seguir ciertas reglas para garantizar un entorno seguro y productivo:

1. **Usa los dispositivos solo para fines educativos**
En el aula, la tecnología debe usarse para aprender, no para jugar, enviar mensajes o acceder a redes sociales. Asegúrate de que estás siguiendo las instrucciones de tu profesor.

2. **No compartas información privada mientras usas dispositivos en clase:**
A veces, puedes necesitar iniciar sesión en plataformas educativas. Siempre protege tu nombre de usuario y contraseña, y asegúrate de cerrar sesión cuando termines de usar un dispositivo compartido.

3. **Sigue las indicaciones del profesor sobre el uso de apps y sitios web:**
Es importante que solo accedas a las aplicaciones y sitios web que el profesor ha aprobado. Acceder a otros sitios web sin autorización podría exponerte a riesgos o distraerte del aprendizaje.

Uso responsable de la tecnología en casa

Además de seguir normas en el aula, también es importante que tengas cuidado cuando uses la tecnología en casa:

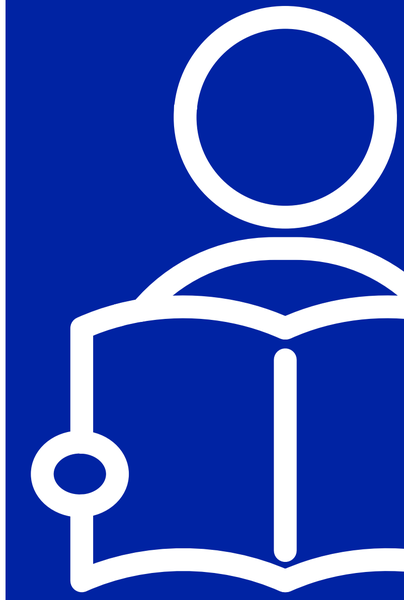
1. **Ten horarios establecidos para el uso de dispositivos:**
Pasar mucho tiempo frente a una pantalla puede afectar tu salud y concentración. Junto a tu familia, puedes establecer límites para asegurarte de que tienes tiempo para otras actividades como estudiar, hacer ejercicio o pasar tiempo con amigos.

2. **Evita el multitasking:**
Si estás haciendo los deberes, intenta concentrarte solo en esa tarea. Tener varias pestañas abiertas o revisar redes sociales mientras estudias puede hacer que te distraigas y no completes tu trabajo correctamente.

Cómo proteger tu información personal

Una de las cosas más importantes cuando usas tecnología es **proteger tu información personal**. Esto incluye detalles como tu nombre completo, dirección, fotos, y otra información privada que no debería estar disponible para extraños.

- **No compartas tu información en redes sociales**: Aunque sea tentador, nunca compartas datos personales en lugares públicos de Internet como perfiles o comentarios en redes sociales.
- **Cuidado con las fotos**: Las imágenes que subes pueden ser vistas y descargadas por personas desconocidas. Antes de compartir una foto, pregúntate si quieres que cualquiera la vea.



- **Piensa antes de publicar**: Si no te sientes cómodo compartiendo algo con tu profesor o tu familia, probablemente no sea una buena idea publicarlo en Internet. Cualquier cosa que publiques en línea puede quedarse ahí para siempre, incluso si la borras.

¿Cómo crear contraseñas seguras?

Tus contraseñas son la primera línea de defensa para proteger tu información en línea. Aquí tienes algunos consejos para crear una contraseña segura:

1. **Combina letras, números y símbolos:**
Cuantas más combinaciones uses, más difícil será que alguien adivine tu contraseña. Ejemplo: en vez de “perro123”, una mejor opción sería “p3rr0#f13l”.

2. **No uses información fácil de adivinar:**
Evita utilizar tu nombre, el nombre de tu mascota o fechas de cumpleaños. Estos son datos que otras personas pueden conocer fácilmente.

3. **Cambia tus contraseñas con regularidad:**
Es recomendable cambiar tus contraseñas cada pocos meses, sobre todo si crees que alguien podría haber tenido acceso a tus cuentas.

4. **Usa una contraseña diferente para cada cuenta:**
Si usas la misma contraseña para todas tus cuentas y alguien la descubre, podría tener acceso a toda tu información.

Participación activa en la protección digital

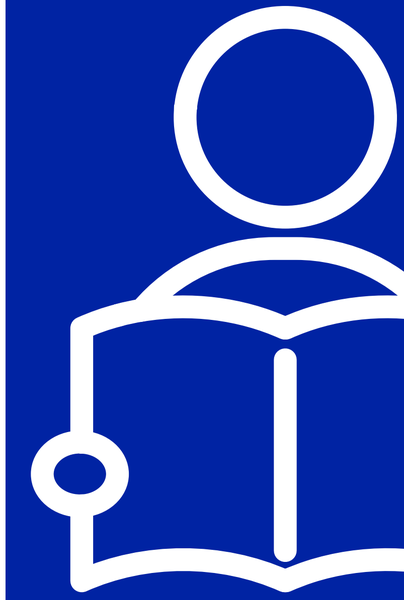
Además de protegerte a ti mismo, también puedes ayudar a proteger a tus amigos y compañeros:

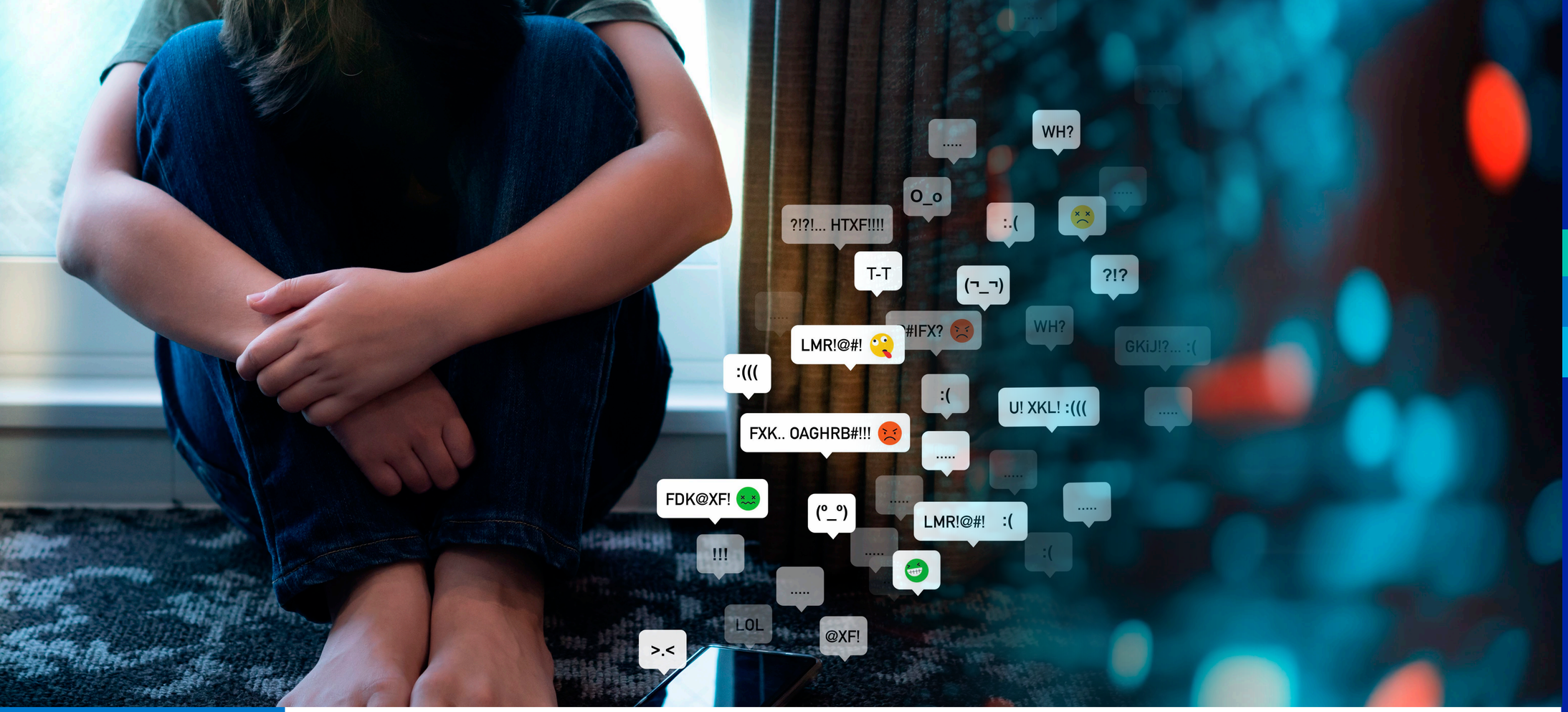
- **Si ves algo sospechoso, repórtalo**: Si notas que alguien está compartiendo información personal sin darse cuenta o accediendo a sitios web peligrosos, díselo y ayúdale a protegerse. Todos somos responsables de crear un espacio digital seguro.
- **No participes en actividades que puedan comprometer la seguridad de otros**: Publicar fotos de tus compañeros sin permiso, etiquetar a personas en fotos sin preguntarles o compartir sus contraseñas son prácticas peligrosas.

Reglas para mantener el orden y la seguridad en plataformas digitales

Muchas plataformas educativas y redes sociales tienen **reglas de seguridad** diseñadas para protegerte. Asegúrate de seguirlas para no ponerte en riesgo:

- **Configura la privacidad de tus cuentas**: Revisa la configuración de privacidad en tus redes sociales y plataformas de uso frecuente, como Google Classroom o Microsoft Teams. Limita quién puede ver tu información y publicaciones.
- **Revisa las políticas de uso de las plataformas**: Saber cómo funciona cada plataforma que utilizas y qué tipo de comportamientos están permitidos te ayudará a protegerte mejor.





05 Prevención del ciberacoso

¿Qué es el ciberacoso?

El **ciberacoso** es un comportamiento dañino en línea en el que una persona o un grupo de personas se burla, molesta o insulta repetidamente a otra persona a través de mensajes, publicaciones en redes sociales o incluso juegos en línea. A diferencia del acoso físico, el ciberacoso puede suceder en cualquier momento del día y afecta emocionalmente a las víctimas porque se extiende más allá del entorno escolar o social. Esto incluye:

- Envío de mensajes ofensivos o amenazantes.
- Compartir fotos, videos o rumores sobre alguien con la intención de herir.
- Crear perfiles falsos o hacerse pasar por otra persona para dañarla.

El ciberacoso puede causar ansiedad, estrés e incluso afectar el rendimiento escolar y la vida social de quienes lo sufren. Por eso, es importante saber cómo detectarlo y qué hacer si ocurre.

¿Cómo saber si estás siendo víctima de ciberacoso?

Aquí tienes algunas señales que pueden indicar que estás siendo víctima de ciberacoso:

1. **Mensajes repetitivos y desagradables**: si alguien te envía mensajes insultantes o amenazantes de manera constante, ya sea por redes sociales, correos electrónicos o mensajes de texto.

2. **Publicaciones que te ridiculizan**: si alguien publica comentarios, fotos o videos sobre ti que te hacen sentir incómodo o avergonzado, especialmente si lo hacen sin tu consentimiento.

3. **Exclusión de grupos en línea**: a veces, el ciberacoso también puede implicar excluir intencionadamente a alguien de grupos de chat o redes sociales, haciéndolo sentir aislado y solo.

4. **Suplantación de identidad**: si alguien crea un perfil falso haciéndose pasar por ti o por otra persona, para engañar o manipular a otros o causar daño a tu reputación.

Cómo protegerte del ciberacoso

Si estás experimentando ciberacoso o crees que podrías ser víctima de ello, es importante que sigas estas estrategias:

- **no respondas a los mensajes ofensivos**: Si te involucras en una discusión o respondes a las provocaciones, es posible que el acosador se sienta motivado para seguir molestándote. Ignorar estos mensajes suele ser la mejor opción.
- **Bloquea al acosador**: La mayoría de las plataformas de redes sociales y aplicaciones de mensajería permiten bloquear a usuarios molestos. Esto evita que puedan enviarte más mensajes o interactuar contigo.
- **Guarda pruebas del acoso**: Es importante hacer capturas de pantalla de los mensajes, fotos o publicaciones

ofensivas para tener pruebas en caso de que decidas informar del incidente. Esto será útil cuando hables con un adulto o las autoridades.

- **Informa a los adultos**: Siempre es importante contarle a un adulto de confianza, como tus padres, un maestro o el coordinador de bienestar de tu escuela. Ellos pueden ayudarte a resolver el problema y ofrecer apoyo emocional si lo necesitas.

Cómo denunciar el ciberacoso

Si eres víctima de ciberacoso, es importante que **denuncies el comportamiento**. Muchas plataformas en línea, como instagram, tiktok, youtube, y videojuegos en línea, tienen herramientas para reportar conductas inapropiadas. Al denunciar, la plataforma revisa el comportamiento y puede tomar medidas, como suspender la cuenta del acosador.

Además, es crucial que hables con tus padres o tutores sobre lo que está sucediendo para que puedan brindarte apoyo y, si es necesario, tomar acciones adicionales, como reportarlo a la escuela o a las autoridades locales.

Cómo ayudar a un compañero que está sufriendo ciberacoso

Si ves que un compañero está siendo acosado en línea, puedes marcar una gran diferencia al ofrecerle apoyo. Aquí tienes algunas maneras de ayudar:

- **No te quedes callado**: Si presencias ciberacoso, no apoyes al acosador ni te mantengas en silencio. Puedes hablar con el acosador y decirle que su comportamiento es inaceptable, o informar del incidente a un adulto.
- **Sé un amigo de apoyo**: Si ves que un amigo está siendo víctima de ciberacoso, escúchale y ofrécele tu apoyo. A veces, saber que no están solos puede hacer una gran diferencia para quienes lo sufren.
- **Informa a un adulto de confianza**: Si tienes miedo de intervenir directamente, puedes hablar con un adulto de confianza (padre, profesor, o el coordinador de bienestar) y contarles lo que está sucediendo para que puedan actuar.

Ser un ciudadano digital respetuoso

La mejor manera de prevenir el ciberacoso es **ser siempre respetuoso en línea**. Tratar a los demás con amabilidad y no participar en comportamientos dañinos como compartir rumores o insultar a otros te ayudará a crear un entorno digital más positivo. Recuerda que lo que dices y haces en internet tiene consecuencias reales para otras personas.

Al seguir estas pautas, no solo te proteges a ti mismo del ciberacoso, sino que también ayudas a que el entorno digital sea más seguro y agradable para todos.

04 Protección de la privacidad y datos personales

04

¿Por qué es importante proteger tu privacidad?

En la vida diaria, no le contarías tus secretos o detalles personales a alguien que acabas de conocer. Del mismo modo, en internet, es crucial que protejas tu información para evitar que personas desconocidas o malintencionadas accedan a ella. Mantener tu **privacidad digital** significa tener control sobre qué información compartes y con quién la compartes. Esto es importante para:

- **Protegerte del robo de identidad**: Si alguien consigue información personal sobre ti, como tu nombre completo, dirección o contraseñas, podría hacerse pasar por ti y causar problemas.
- **Evitar el acoso en línea**: Compartir demasiada información personal puede permitir que extraños te molesten o intenten contactar contigo sin tu consentimiento.
- **Mantener tu reputación en línea**: Lo que publicas en Internet puede quedarse ahí para siempre. Si no cuidas lo que compartes, podrías poner en riesgo tu reputación o sentirte incómodo más adelante por contenido que publicaste en el pasado.

¿Qué información personal debes proteger?

Al usar internet, hay varios tipos de información que debes mantener en privado. Aquí tienes algunos ejemplos de información que nunca debes compartir públicamente:

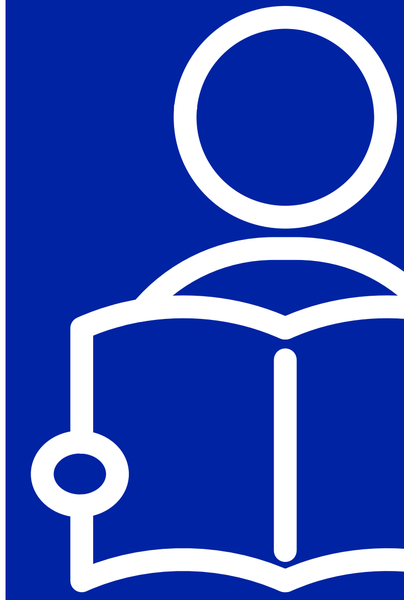
- **Nombre completo**: Usa sólo tu primer nombre en redes sociales o en perfiles públicos.
- **Dirección y ubicación**: No digas dónde vives, tu colegio o lugares que frecuentas. Algunas aplicaciones pueden rastrear tu ubicación, así que asegúrate de desactivar estas funciones cuando no sean necesarias.
- **Número de teléfono y correo electrónico**: Comparte esta información sólo con personas de confianza.
- **Contraseñas**: Nunca compartas tus contraseñas con nadie, ni siquiera con amigos. Las contraseñas son la llave de tu privacidad en línea.
- **Fotos personales**: Piensa antes de publicar fotos, especialmente si muestran información sobre dónde vives o detalles sobre ti.

Cómo proteger tu información personal en redes sociales

Las redes sociales son una herramienta divertida para compartir momentos con amigos, pero también pueden ser un espacio donde tu privacidad está en riesgo. Aquí tienes algunos consejos para proteger tu información:

1. **Configura la privacidad de tu perfil**: asegúrate de que solo las personas que conoces puedan ver tu perfil y lo que publicas. Configura tus cuentas para que sean privadas, y revisa regularmente quién tiene acceso a tu contenido.

2. **No aceptes solicitudes de amistad de desconocidos**: aunque pueda parecer emocionante tener muchos seguidores, es importante que solo aceptes solicitudes de per-



sonas que conoces en la vida real. Los extraños podrían tener malas intenciones o intentar obtener tu información.

3. **Controla lo que publicas**: antes de publicar una foto o un comentario, pregúntate si estás cómodo con que otras personas lo vean. Recuerda que lo que publicas puede permanecer en internet mucho tiempo, incluso si lo borras.

¿Cómo crear contraseñas seguras?

Una contraseña segura es una de las mejores formas de proteger tu información en línea. Aquí tienes algunos consejos sobre cómo crear y gestionar tus contraseñas:

- **Hazlas difíciles de adivinar**: Utiliza una combinación de letras mayúsculas y minúsculas, números y símbolos. Evita usar palabras simples como «contraseña» o tu nombre.
- **Cambia tus contraseñas regularmente**: Cambia tus contraseñas cada pocos meses para asegurarte de que tus cuentas sigan siendo seguras.
- **No reutilices contraseñas**: Usa una contraseña diferente para cada cuenta. Si alguien descubre una de tus contraseñas, no podrá acceder a todas tus cuentas.

La importancia de la configuración de privacidad en aplicaciones y juegos

Muchos juegos y aplicaciones te piden información personal para crear una cuenta. Aunque esto es normal, es importante revisar cómo se utiliza esta información. Asegúrate de:

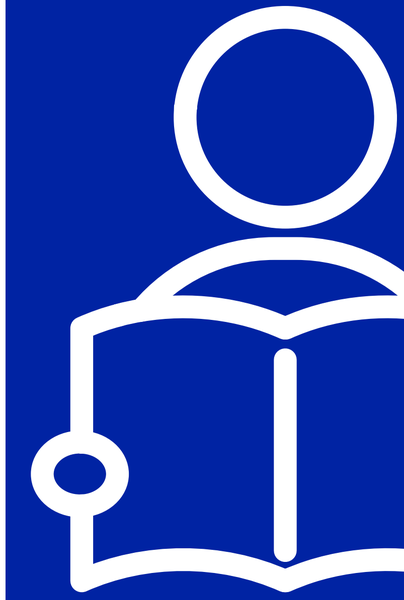
1. **Leer las políticas de privacidad**: antes de registrarte en un nuevo juego o aplicación, revisa su política de privacidad para entender qué datos recopilan y cómo los usan.

2. **Revisar los permisos de las aplicaciones**: algunas aplicaciones pueden pedir permisos innecesarios, como acceso a tu ubicación o contactos. Si no es necesario para la función de la aplicación, desactiva esos permisos.

Qué hacer si sientes que tu privacidad ha sido comprometida

Si alguna vez sientes que alguien está accediendo a tu información personal sin tu consentimiento o te encuentras en una situación en la que tu privacidad está en peligro, debes:

- **Cambiar tus contraseñas inmediatamente**: Si sospechas que alguien más conoce tu contraseña, cámbiala rápidamente.
- **Habla con un adulto de confianza**: Cuéntale a tus padres, profesores o a un coordinador de bienestar lo que está pasando. Ellos te ayudarán a manejar la situación y tomar las medidas necesarias para protegerte.
- **Reporta el problema a la plataforma**: Si alguien está accediendo a tu cuenta o compartiendo tu información sin tu consentimiento, puedes reportar la situación a la plataforma (red social, juego, etc.) para que tomen medidas.



05 Uso responsable de las redes sociales

05

¿Qué son las redes sociales?

Las **redes sociales** son plataformas en línea donde puedes compartir fotos, pensamientos, interactuar con amigos y conocer a nuevas personas. Las redes más populares entre los jóvenes incluyen **instagram**, **tiktok**, **snapchat**, **whatsapp** y **youtube**. Aunque pueden ser muy divertidas y útiles para conectarse, también tienen riesgos si no las usas de manera responsable.

¿Cómo usar las redes sociales de manera responsable?

El uso responsable de las redes sociales significa **ser cuidadoso con lo que publicas y con quién interactúas**. Aquí tienes algunos consejos importantes para mantenerte seguro y evitar problemas:

1. **Piensa Antes de Publicar:**
   - ¿Te sentirías cómodo si todo el mundo lo viera?: Recuerda que, una vez que publicas algo en Internet, puede ser muy difícil eliminarlo completamente. Incluso si borras una publicación, alguien pudo haber hecho una captura de pantalla.
   - **Evita publicar información personal**: No publiques tu dirección, número de teléfono o detalles de tu ubicación. Esta información puede ser utilizada por personas malintencionadas para localizarte o acosarte.
   - **Sé respetuoso**: Publica contenido que sea amable y positivo. Evita compartir mensajes ofensivos, comentarios crueles o imágenes que puedan herir a otros.

2. **No Compartas Fotos de Otras Personas Sin Su Permiso:**
   - Aunque parezca inofensivo compartir fotos con tus amigos, siempre es importante pedirles permiso antes de hacerlo. Lo que es cómodo para ti puede no serlo para otra persona, y todos tienen derecho a controlar su imagen en línea.

3. **Limita el Número de Seguidores:**
   - A veces es emocionante tener muchos seguidores, pero **es mejor que solo aceptes solicitudes de amistad de personas que conoces en la vida real**. Esto te ayudará a evitar interactuar con extraños que podrían tener malas intenciones.
   - Además, configura tu cuenta como privada para que solo tus amigos cercanos puedan ver lo que publicas.

4. **Evita las Discusiones o Peleas en Línea:**
   - Las redes sociales no son el lugar adecuado para resolver peleas o discusiones. Si alguien te provoca o intenta comenzar una pelea, **ignora los comentarios y habla con un adulto** si te sientes incómodo. Las discusiones en línea pueden salirse de control rápidamente y hacerte sentir peor.

Cómo protegerte en redes sociales

Las plataformas de redes sociales tienen configuraciones de **privacidad y seguridad** que te permiten controlar quién puede ver tu perfil y lo que publicas. Asegúrate de:

1. **Configurar la privacidad**: revisa y ajusta tus configuraciones de privacidad para asegurarte de que solo tus amigos puedan ver lo que compartes.

2. **Bloquear y reportar comportamientos inapropiados**: si alguien te acosa o publica contenido que te hace sentir incómodo, **bloquéalo y rep**órtalo a la plataforma. Todas las redes sociales tienen herramientas para reportar conductas inapropiadas.

3. **Evitar compartir tu ubicación**: algunas aplicaciones pueden mostrar tu ubicación exacta cuando publicas una foto o mensaje. Asegúrate de desactivar esta función a menos que sea necesario.

4. **Usar contraseñas seguras y no compartirlas**: protege tu cuenta con una contraseña fuerte y no la compartas con nadie, ni siquiera con tus amigos. Esto evitará que alguien entre a tu cuenta y haga publicaciones sin tu consentimiento.

Qué hacer si ves contenido inapropiado

A veces, aunque seas cuidadoso con lo que ves y compartes, puedes encontrarte con contenido que te haga sentir incómodo o sea inapropiado para tu edad. Aquí tienes algunas acciones que puedes tomar:

1. **No interactúes con el contenido**: no comentes ni compartas contenido inapropiado. Lo mejor es ignorarlo.

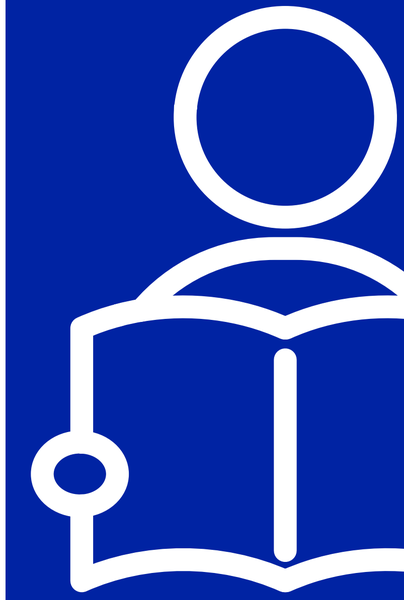
2. **Reporta el contenido a la plataforma**: la mayoría de las redes sociales te permiten reportar publicaciones, videos o comentarios que violen sus normas. Esto puede incluir contenido ofensivo, acosador o explícito.

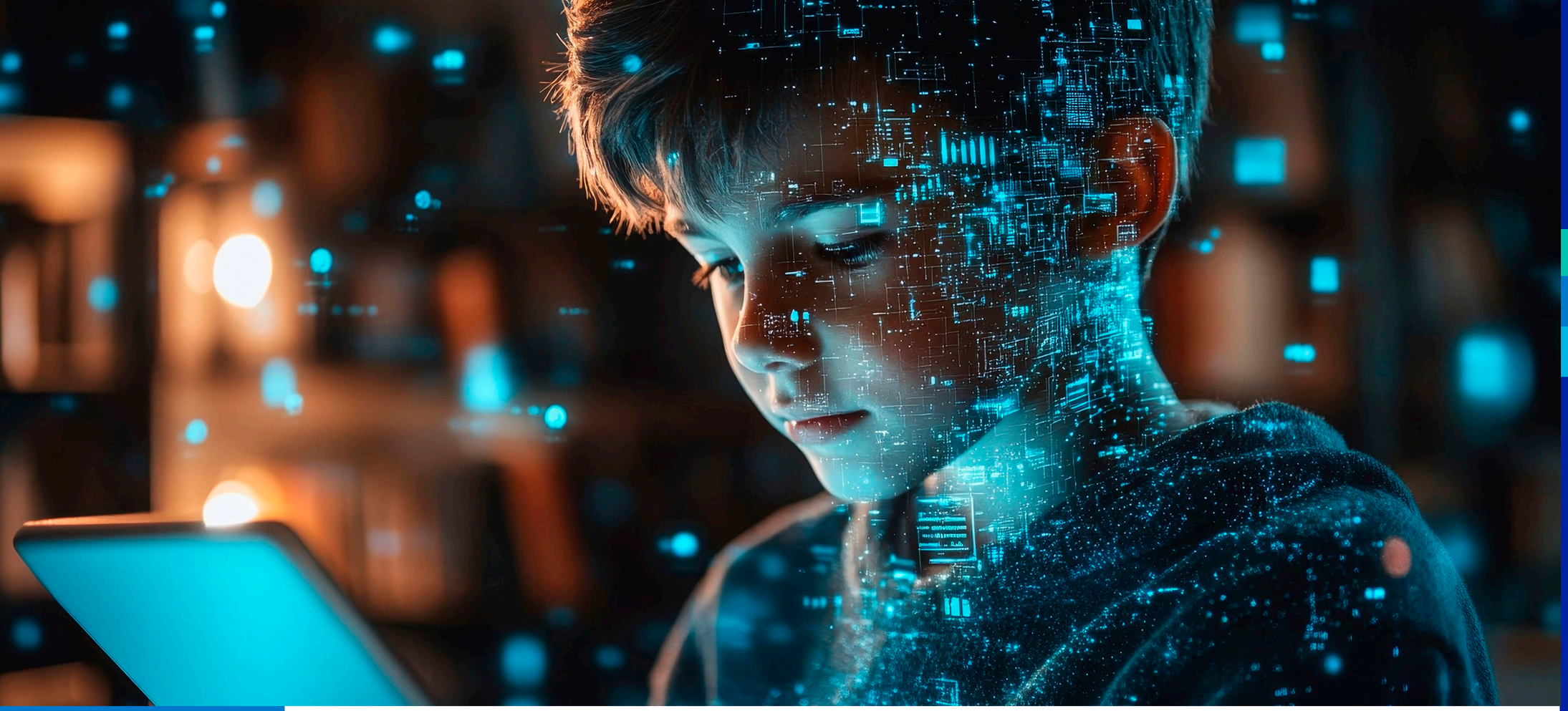
3. **Habla con un adulto**: si el contenido te hace sentir incómodo o te preocupa, es importante que lo hables con un adulto de confianza, como tus padres o un maestro. Ellos te pueden ayudar a manejar la situación y tomar las medidas adecuadas.

Uso positivo de las redes sociales

Las redes sociales no solo son un lugar para compartir fotos y videos, también pueden ser una herramienta poderosa para aprender, expresarte y conectar con otros de forma positiva:

- **Usa las redes para aprender**: Sigue cuentas educativas, científicas o artísticas que te enseñen cosas nuevas y te inspiren.
- **Apoya a los demás**: Las redes sociales pueden ser una excelente forma de apoyar a tus amigos o a personas que lo necesitan, compartiendo mensajes positivos o ayudando a causas que te importan.
- **Sé un buen ejemplo**: Publica contenido respetuoso y apropiado que inspire a otros a ser amables y responsables en línea.





06

Evitar el Grooming y otros peligros online

06

¿Qué es el Grooming?

El **grooming** es cuando un adulto intenta ganarse tu confianza en internet para aprovecharse de ti o hacerte daño. A menudo, los groomers (como se les llama) fingen ser más jóvenes o alguien con intereses similares a los tuyos para hacerte sentir cómodo. Al principio, pueden parecer amigables y agradables, pero su objetivo final es engañarte y manipularte.

El grooming puede empezar en redes sociales, juegos en línea, chats, aplicaciones de mensajería o cualquier plataforma donde interactúes con desconocidos. A medida que te van conociendo más, pueden pedirte información personal, fotos, o incluso intentar encontrarse contigo en persona.

Señales de alerta del grooming

Es importante que reconozcas algunas señales que pueden indicar que alguien podría estar intentando hacer grooming:

1. **Te piden mantener la relación en secreto**: si alguien en línea te pide que no le cuentes a nadie, ni a tus padres ni a tus amigos, sobre la relación o las conversaciones que tienen, esto es una señal clara de que algo no está bien. Las personas que se preocupan por ti no te piden secretos.

2. **Te hacen preguntas personales**: preguntar detalles sobre tu vida, como tu dirección, número de teléfono, el nombre de tu escuela o incluso pedirte fotos privadas, es una señal de peligro. No compartas esta información con personas que no conoces en la vida real.

3. **Intentan ser muy cercanos muy rápido**: si una persona que acabas de conocer en línea te trata como si fueran mejores amigos o incluso como si tuvieran una relación sentimental, y te llenan de cumplidos o regalos virtuales, puede ser una estrategia para ganarse tu confianza.

4. **Te envían contenido inapropiado**: si alguien te envía fotos, videos o mensajes con contenido sexual o inapropiado, es un signo claro de que no tienen buenas intenciones.

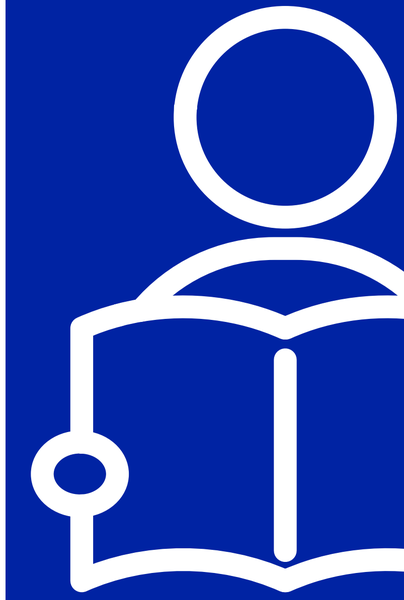
Cómo protegerte del Grooming

La mejor manera de protegerte es evitar interactuar con personas que no conoces en la vida real y seguir estos consejos:

1. **No hables con extraños**: así como no hablarías con desconocidos en la calle, tampoco deberías hacerlo en internet. Aunque alguien parezca amigable, si no lo conoces en la vida real, es mejor no entablar conversación.

2. **No compartas información personal**: nunca des detalles sobre ti, como tu nombre completo, edad, dirección, teléfono o dónde estudias. Los groomers pueden usar esta información para encontrarte o manipularte.

3. **Desconfía si alguien te hace sentir incómodo**: si alguna vez una conversación te hace sentir extraño o incómodo,



confía en tu instinto. Detén la conversación inmediatamente y cuéntale a un adulto de confianza.

4. **Reporta y bloquea**: si alguien te hace sentir incómodo, bloquea a esa persona y repórtala en la plataforma que estés usando. La mayoría de las redes sociales y aplicaciones tienen opciones para denunciar usuarios que se comporten de manera inapropiada.

¿Qué hacer si sospechas de Grooming?

Si sospechas que estás siendo víctima de grooming, es esencial que actúes rápidamente:

- **Deja de comunicarte inmediatamente**: Si alguien te está pidiendo cosas que te hacen sentir incómodo, deja de responderle y bloquea a esa persona.
- **Guarda pruebas**: Si has recibido mensajes o fotos inapropiadas, toma capturas de pantalla y guárdalas. Estas pruebas pueden ser útiles si decides denunciar el caso.
- **Habla con un adulto de confianza**: Cuéntale a tus padres, a un profesor o a cualquier adulto de confianza lo que está sucediendo. Ellos podrán ayudarte a gestionar la situación y protegerte.
- **Denuncia el incidente a las autoridades**: Si crees que alguien te está acosando o te está haciendo grooming, puedes denunciarlo a las autoridades locales 062 ó 091 o a servicios en línea como **INCIBE** (Instituto Nacional de Ciberseguridad) que tiene recursos para ayudarte.

Otros peligros online: suplantación de identidad y Phishing

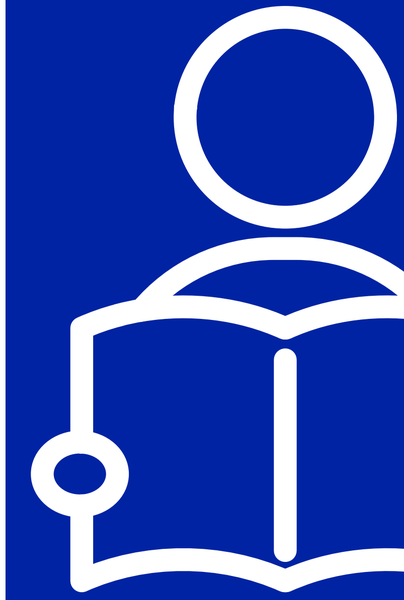
Además del grooming, existen otros peligros en línea de los que debes protegerte:

- **Suplantación de Identidad**: Esto ocurre cuando alguien finge ser otra persona, como un amigo o un compañero de clase, para obtener información personal o acosarte. Asegúrate de verificar siempre con quién hablas y si dudas, confirma con esa persona en la vida real.
- **Phishing**: Los ataques de **phishing** son intentos de engañarte para que reveles información personal, como contraseñas o detalles de tarjetas de crédito, a través de correos electrónicos o mensajes falsos. Estos mensajes pueden parecer oficiales, como de tu banco o red social, pero son falsos. Nunca hagas clic en enlaces sospechosos ni proporciones información confidencial a través de estos medios.

Consejos para navegar de manera segura

Para evitar estos peligros, sigue estas pautas:

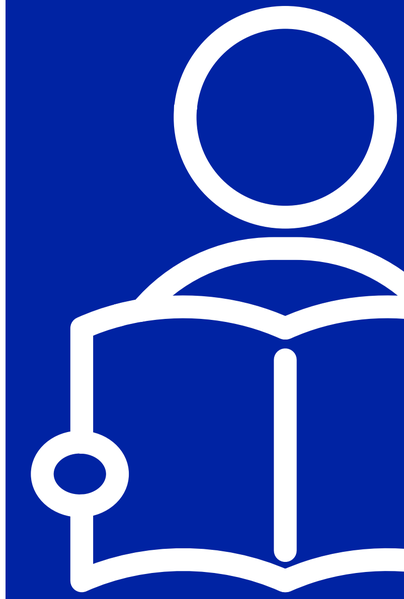
- **Mantén tu perfil en redes sociales privado**: Limita quién puede ver tu información y publicaciones. Configura tus redes sociales para que solo amigos de confianza puedan acceder a tu perfil.
- **Verifica a las personas con las que hablas**: Si recibes un mensaje de alguien que dice ser un amigo, pero te parece sospechoso, verifica su identidad antes de continuar la conversación.



06

- **No aceptes regalos ni propuestas en línea**: Si alguien en Internet te ofrece cosas gratis, como dinero, regalos o acceso a eventos, es mejor desconfiar. Muchos groomers usan regalos como una forma de manipulación.

- **Utiliza contraseñas fuertes**: Asegúrate de que tus contraseñas sean seguras y no las compartas con nadie.



07 Pornografía y acceso a contenidos inadecuados

07

¿Qué es la Pornografía?

La **pornografía** es contenido que muestra imágenes o videos de carácter sexual explícito. En Internet, este tipo de contenido es muy accesible, pero **no es apropiado para menores** y puede ser dañino tanto emocional como psicológicamente. Además, no representa las relaciones de manera realista, ya que lo que se ve en la pornografía muchas veces está manipulado y distorsiona la idea de lo que deberían ser las relaciones sanas y respetuosas.

Es fundamental que sepas que, como menor de edad, **no deberías estar expuesto a este tipo de contenido**, ya que puede generar confusión, malestar y una percepción errónea de la sexualidad y las relaciones entre las personas.

Por Qué la Pornografía Puede Ser Dañina

Existen varias razones por las que la pornografía es peligrosa para los jóvenes:

1. **Distorsiona la realidad**: La pornografía no muestra relaciones sanas ni reales. Presenta imágenes que no reflejan el respeto, el consentimiento y la igualdad que deben estar presentes en una relación saludable.

2. **Impacta en tu salud emocional**: La exposición a la pornografía puede hacerte sentir confundido, incómodo o ansioso. Además, puede afectar la manera en que ves a los demás y cómo interpretas las relaciones.

3. **Es adictiva**: Al igual que otras actividades en línea, la pornografía puede volverse adictiva. Pasar tiempo consumiendo este tipo de contenido puede distraerte de tus estudios, tus relaciones personales y tus actividades diarias.

4. **Riesgo de Explotación**: Muchas veces, la pornografía involucra a personas que no han dado su consentimiento para aparecer en esos videos o imágenes. Ver o compartir este contenido puede perpetuar la explotación de otras personas.

Cómo Evitar el Acceso a Contenido Inadecuado

Hoy en día, es fácil encontrarse con pornografía y otro contenido inadecuado sin siquiera buscarlo. Aquí tienes algunos consejos para evitar el acceso a este tipo de material:

1. **Usa filtros de contenido**: Existen herramientas y configuraciones en navegadores y dispositivos que pueden bloquear el acceso a sitios web inapropiados. **Controles parentales** pueden ayudar a filtrar el contenido inapropiado.

2. **No hagas clic en enlaces sospechosos**: A veces, puedes recibir mensajes o correos electrónicos con enlaces que parecen inofensivos, pero que te llevan a sitios de pornografía o contenido inapropiado. Nunca hagas clic en enlaces si no conoces su origen.

3. **Ten cuidado en redes sociales**: Las redes sociales pueden ser un lugar donde se comparta contenido inadecua-

do. Si ves que alguien publica algo inapropiado, puedes reportarlo a la plataforma para que lo eliminen.

¿Qué Hacer Si Accedes a Contenidos Inapropiados?

A veces, aunque tomes todas las precauciones, puedes encontrarte accidentalmente con contenido inapropiado. En ese caso, es importante que sepas cómo actuar:

1. **Cierra inmediatamente la página o aplicación**: Si accidentalmente accedes a pornografía o a contenido inapropiado, lo mejor es cerrar el sitio web o aplicación de inmediato.

2. **No sigas explorando**: Aunque sientas curiosidad, es mejor que no sigas viendo ese contenido. Puede afectar cómo te sientes o tu percepción sobre las relaciones.

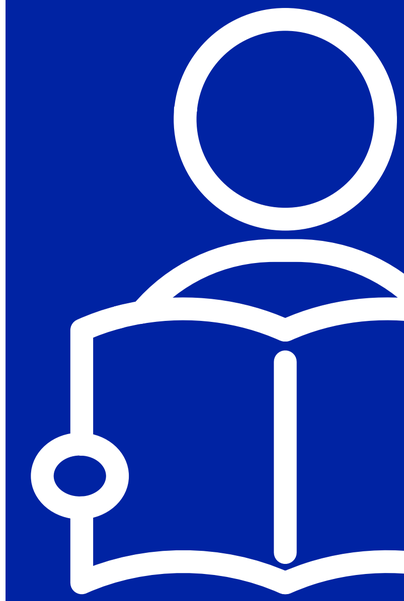
3. **Habla con un adulto de confianza**: Si te sientes incómodo o preocupado por lo que has visto, habla con tus padres, un maestro o un adulto en quien confíes. Ellos pueden orientarte y ayudarte a entender por qué es importante evitar este tipo de contenido.

Consecuencias de Compartir Contenido Inapropiado

Es importante que también sepas que compartir contenido inapropiado, como pornografía, puede tener **consecuencias legales**. Distribuir este tipo de contenido es ilegal, especialmente cuando involucra a menores de edad. Compartir imágenes o videos sin el consentimiento de los involucrados también puede ser muy dañino y perjudicial para otras personas.

Fomentando Relaciones Saludables

En lugar de recurrir a la pornografía, es fundamental aprender sobre las relaciones sanas y respetuosas. Las relaciones reales se basan en el **respeto mutuo**, el **consentimiento** y la **igualdad**. Si tienes preguntas sobre las relaciones o la sexualidad, lo mejor es hablar con adultos de confianza, como tus padres o profesores, que pueden orientarte de una manera adecuada y saludable.



08 Qué hacer ante incidentes en internet

08

¿Qué es un incidente en línea?

Un incidente en línea es cualquier situación que te hace sentir incómodo o en peligro mientras navegas por internet o interactúas con otras personas en redes sociales, juegos o aplicaciones. Esto incluye:

- **Ciberacoso**: Cuando alguien te molesta, insulta o amenaza repetidamente a través de mensajes o publicaciones.
- **Grooming**: Cuando un adulto intenta manipularte o engañarte para obtener información personal o para realizar acciones inapropiadas.
- **Suplantación de identidad**: Si alguien finge ser tú o usa tu cuenta sin permiso.
- **Acceso a contenido inapropiado**: Si accidentalmente accedes a pornografía, violencia gráfica o cualquier otro material no adecuado para tu edad.

Estos problemas pueden hacer que te sientas asustado, nervioso o inseguro. Es importante saber cómo actuar para resolver la situación lo antes posible.

Pasos a seguir si ocurre un problema en línea

1. **No reacciones ni respondas:**
   - Si alguien te está molestando o acosando en línea, evita responder. Interactuar puede empeorar la situación o darle al acosador más motivos para continuar.

2. **Guarda pruebas del incidente:**
   - Es importante que tomes capturas de pantalla o guardes los mensajes, fotos o publicaciones que te están causando problemas. Esto puede servir como prueba si decides reportarlo más adelante.

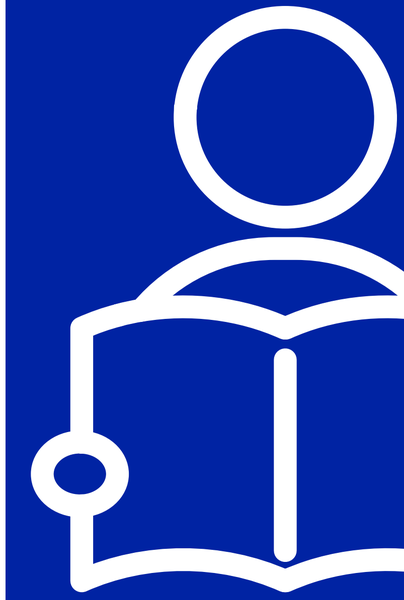
3. **Bloquea al usuario:**
   - Todas las redes sociales y aplicaciones tienen opciones para bloquear a usuarios que te están molestando. Al bloquear a alguien, esa persona ya no podrá enviarte mensajes ni ver tu perfil.

4. **Reporta el incidente en la plataforma:**
   - Muchas plataformas como Instagram, TikTok, YouTube y juegos en línea tienen opciones para reportar comportamientos inapropiados. Cuando reportas un incidente, la plataforma revisa la situación y puede tomar medidas, como suspender la cuenta del acosador o eliminar el contenido ofensivo.

5. **Habla con un adulto de confianza - No Te Calles:**
   - Si sientes que el problema es serio, no dudes en contárselo a un adulto de confianza, como tus padres, un maestro o el coordinador de bienestar de tu escuela. Ellos pueden ofrecerte el apoyo necesario para manejar la situación y protegerte.

¿Por qué es importante actuar rápidamente?

Cuando enfrentas un incidente en línea, es crucial que actúes con rapidez. Si ignoras el problema o lo dejas pasar, la situación podría empeorar o el acosador podría continuar moles-



tándote. Al tomar medidas inmediatas, puedes detener el acoso o prevenir que alguien más también se vea afectado.

Además, actuar rápidamente te ayuda a **recuperar el control** sobre la situación y evitar que siga afectando tu bienestar emocional.

Dónde buscar ayuda

Si el problema continúa o sientes que no puedes resolverlo por ti mismo, existen varias formas de buscar ayuda:

1. **Habla con tus padres**: ellos pueden ayudarte a denunciar el problema a las autoridades si es necesario o a gestionar la situación en casa.

2. **Contacta al coordinador de bienestar en tu escuela**: en la mayoría de los colegios hay coordinadores de bienestar encargados de ayudar en situaciones de acoso o problemas relacionados con la seguridad en línea. Ellos pueden guiarte en los pasos que debes seguir y ofrecerte apoyo emocional.

3. **Plataformas de denuncia en línea**: organizaciones como **pantallas amigas** o **no te calles, cuéntalo** ofrecen recursos y líneas de ayuda para reportar incidentes en internet y obtener orientación.

Consecuencias de ignorar el problema

Si ignoras los incidentes en línea, pueden seguir afectándote de diferentes maneras:

- **Aumenta el impacto emocional**: Sentirte acosado o inseguro en línea puede causar estrés, ansiedad e incluso afectar tu rendimiento escolar y tus relaciones personales.
- **El acosador puede continuar**: Si no actúas, la persona que te está acosando o molestando puede sentir que no hay consecuencias y seguir molestándote o incluso a otras personas.
- **Se pierde la oportunidad de resolver el problema**: Al no reportar el incidente, la plataforma o las personas encargadas de protegerte no pueden intervenir y detener la situación.

Recursos para manejar incidentes en línea

Hay varios recursos que te pueden ayudar a enfrentar problemas en línea:

- **Controles parentales y bloqueos**: Muchas aplicaciones y dispositivos tienen opciones para configurar controles parentales y filtros que te protegen de contenido inapropiado.
- **Guías y apoyo en línea**: Plataformas como **INCIBE, No Te Calles** y **Pantallas Amigas** ofrecen guías sobre cómo actuar ante problemas en Internet y líneas de ayuda a las que puedes acudir si te sientes inseguro.
- **Teléfono de Ayuda al Menor y Adolescente:** 116 111

Pedir ayuda si necesitas apoyo

09

¿Por qué es importante pedir ayuda?

Cuando enfrentas situaciones en línea que te hacen sentir incómodo o inseguro, **pedir ayuda** es esencial. Puede que sientas vergüenza, miedo o que creas que puedes manejar la situación por ti mismo, pero los incidentes en internet pueden ser muy complicados y requieren apoyo. Pedir ayuda a tiempo puede evitar que el problema crezca y te proporciona el apoyo emocional y práctico que necesitas para sentirte seguro.

Recuerda que no estás solo. Mucha gente, incluidos tus padres, maestros y amigos, está dispuesta a ayudarte y protegerte cuando lo necesites.

¿A quién puedes pedir ayuda?

Tienes varias personas y recursos a los que puedes acudir cuando necesites apoyo. Lo importante es que te sientas cómodo y que confíes en quienes te ayudarán. Algunas de las opciones incluyen:

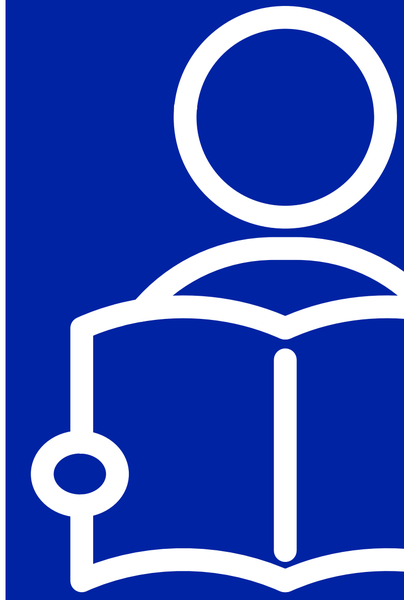
1. **Padres o tutores:**
   - Tus padres o tutores son las personas más cercanas y quienes mejor pueden ayudarte en situaciones de acoso, grooming, ciberacoso o acceso a contenido inapropiado. Ellos pueden hablar contigo, brindarte orientación, y si es necesario, contactar a las autoridades o denunciar a los responsables del incidente.
   - No tengas miedo de contarles lo que está pasando, aunque te sientas avergonzado o culpable. Lo más importante es tu bienestar y ellos siempre estarán ahí para apoyarte.

2. **Maestros o coordinadores de bienestar en la escuela:**
   - En el colegio, los maestros y los coordinadores de bienestar están capacitados para manejar problemas relacionados con la seguridad digital. Si te sientes incómodo hablando con tus padres, puedes acudir a un profesor en el que confíes. Ellos pueden guiarte sobre los pasos que debes seguir, ofrecerte apoyo emocional y tomar medidas para que el problema no continúe.
   - En algunos casos, los incidentes que ocurren en línea pueden tener repercusiones en el entorno escolar, como el ciberacoso entre compañeros. Por eso es importante que la escuela esté al tanto para intervenir adecuadamente.

3. **Amigos de confianza:**
   - Hablar con un amigo de confianza también puede ayudarte a sentirte mejor y a encontrar el valor para buscar ayuda. A veces, compartir tus preocupaciones con alguien cercano de tu edad puede darte una nueva perspectiva y motivarte a actuar.

4. **Líneas de ayuda y recursos en línea:**
   - Existen plataformas y organizaciones especializadas en brindar apoyo en situaciones de problemas en línea. Algunos ejemplos incluyen:

     Pantallas amigas: ofrecen guías y recursos educativos para mantenerte seguro en línea.
     No te calles, cuéntalo: es una plataforma en la que puedes denunciar situaciones de acoso o ciberacoso



de manera confidencial, y recibir orientación sobre cómo proceder.
Incibe (instituto nacional de ciberseguridad): ofrece asesoramiento y recursos para la protección digital. Tienen una línea de ayuda específica para menores y adolescentes en situaciones de riesgo en línea.
Teléfono de ayuda al menor y adolescente: 116 111

Cómo pedir ayuda

A veces, pedir ayuda puede ser difícil, especialmente si sientes vergüenza o culpa por lo que está ocurriendo. Aquí tienes algunos consejos para que puedas dar ese paso con confianza:

1. **Sé honesto**: cuéntales a los adultos lo que realmente está sucediendo, sin sentirte culpable. No te juzgarán, están ahí para ayudarte.

2. **Explica cómo te sientes**: no solo cuentes los hechos. Si te sientes triste, asustado o confundido, es importante que lo expreses. De esta manera, quienes te ayuden podrán entender mejor lo que estás experimentando.

3. **No esperes a que el problema empeore**: mientras más tiempo pase, más difícil puede ser resolver el problema. Pide ayuda tan pronto como sientas que algo no está bien.

Recursos y herramientas de apoyo

Hay varias herramientas que te pueden ayudar a sentirte más seguro cuando navegas por internet:

- **Controles parentales**: tus padres pueden instalar controles parentales en tus dispositivos para ayudarte a evitar contenido inapropiado o bloquear a personas que intenten molestarte.
- **Plataformas de reporte**: como se mencionó antes, plataformas como **no te calles, cuéntalo** o las herramientas de denuncia en redes sociales te permiten reportar comportamientos inapropiados de manera confidencial.
- **Líneas de ayuda**: algunas organizaciones tienen líneas telefónicas o chats donde puedes hablar con profesionales sobre tus problemas en línea, recibir asesoramiento y sentirte apoyado.
- **Teléfono de ayuda al menor y adolescente:** 116 111

10

Control del tiempo en pantalla y bienestar digital

Ser amable y respetuoso en línea

Ser un **ciudadano digital responsable** significa actuar con el mismo respeto en línea que mostrarías en la vida real. En internet, es fácil sentirse anónimo y pensar que nuestras acciones no tienen consecuencias, pero eso no es cierto. Todo lo que haces en línea, desde comentarios en redes sociales hasta los mensajes que envías, tiene un impacto en las personas.

1. **Piensa antes de publicar**: antes de compartir algo en línea, ya sea un comentario, una foto o un video, pregúntate si lo que estás diciendo es amable y respetuoso. Si no dirías algo en persona, tampoco deberías publicarlo en internet.

2. **Sé empático**: piensa en cómo tus palabras o acciones en línea pueden afectar a los demás. Si ves que alguien está siendo víctima de ciberacoso o si se está difundiendo contenido hiriente, toma una posición activa. Puedes reportar el comportamiento, ofrecer apoyo a la persona afectada o simplemente evitar participar en el daño.

3. **Evita el odio y los rumores**: internet puede ser un lugar donde los rumores se propagan rápidamente y el odio o los insultos pueden viralizarse. No contribuyas a esto. Si ves que otros están compartiendo contenido ofensivo o calumnioso, no te unas y, en su lugar, considera denunciar el comportamiento.

4. **Respeta la privacidad de los demás**: no publiques fotos, videos o información personal de otros sin su permiso. Todos tienen derecho a controlar qué se comparte sobre ellos en línea. Compartir algo sin el consentimiento de los involucrados puede hacer que se sientan incómodos o expuestos.

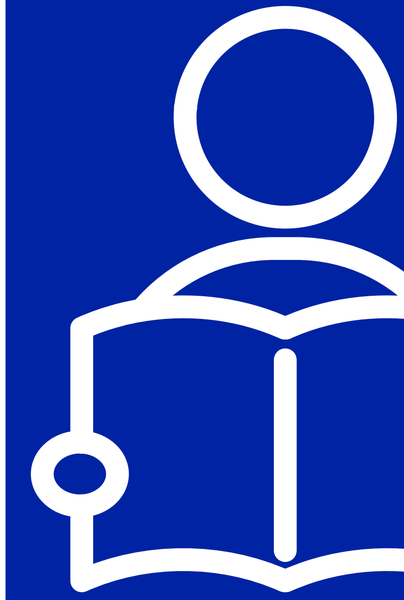
Usar internet de manera positiva

Internet no solo debe ser un lugar seguro, sino también un espacio donde puedas **crecer y aprender** de manera positiva. Ser un ciudadano digital responsable implica usar las herramientas digitales para tu beneficio y el de los demás:

1. **Saca provecho de los recursos educativos**: internet es una increíble fuente de conocimiento. Existen sitios y plataformas donde puedes aprender de todo, desde matemáticas hasta habilidades artísticas o idiomas. Usa esta herramienta para mejorar tus habilidades y expandir tu conocimiento.

2. **Participa en iniciativas positivas**: muchas redes sociales y plataformas digitales promueven campañas e iniciativas para causas sociales, medioambientales o educativas. Participar en estos proyectos puede hacer que tu experiencia en internet sea enriquecedora, además de que estarás contribuyendo a mejorar el mundo digital.

3. **Fomenta la amistad y el apoyo en línea**: al igual que en la vida real, en internet puedes crear comunidades donde todos se apoyen. Puedes organizar grupos de estudio, clubes en línea o simplemente ser un amigo positivo que ofrece palabras de aliento a quienes lo necesiten.



4. **Mantén un equilibrio saludable**: el uso responsable de internet también significa **encontrar un equilibrio entre el mundo digital y el real**. Es genial usar la tecnología para aprender y conectarte, pero también es importante que reserves tiempo para actividades fuera de línea, como hacer ejercicio, leer un libro o pasar tiempo con amigos y familia sin la distracción de los dispositivos.

Cuidar tu propia huella digital

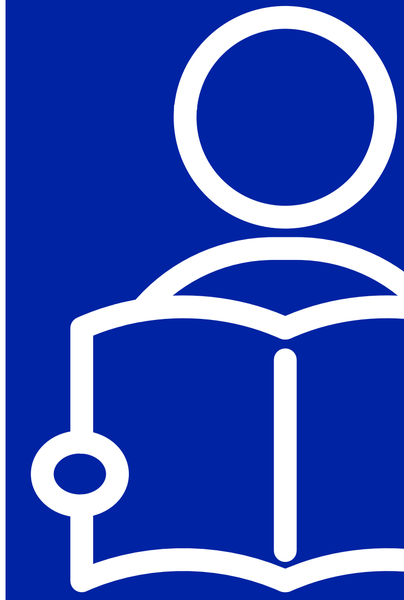
Cada vez que publicas algo en línea, estás dejando una **huella digital**. Esto es un registro de toda tu actividad en internet que puede ser visto por otros, incluidos empleadores futuros, profesores o amigos. Ser consciente de la huella digital que dejas es importante para mantener una buena reputación en línea y evitar problemas en el futuro.

- **Publica de manera responsable**: todo lo que publicas en redes sociales, blogs o foros puede quedarse en internet durante años. Asegúrate de que lo que compartes hoy no te cause vergüenza más adelante.
- **Sé consciente de la información personal que compartes**: asegúrate de proteger tus datos personales y no compartir información que pueda ser utilizada para suplantarte o poner en riesgo tu seguridad.

Apoyar un entorno digital seguro para todos

Finalmente, ser un ciudadano digital responsable no solo significa cuidar de ti mismo, sino también contribuir a que internet sea un lugar seguro y positivo para todos. Puedes ayudar a:

- **Denunciar conductas inapropiadas**: si ves que alguien está siendo acosado o está difundiendo contenido inadecuado, repórtalo. Muchas plataformas permiten denunciar comportamientos inapropiados y ayudan a proteger a la comunidad en línea.
- **Educar a otros**: comparte lo que has aprendido sobre la seguridad y el uso responsable de internet con tus amigos y familiares. Si todos practican un comportamiento digital responsable, el entorno en línea será más seguro y saludable para todos.



Navegando Juntos:
Guía Integral para un Mundo Digital Seguro

DOCENTES

ESTUDIANTES

FAMILIAS

1 Recursos y herramientas para mantenerte seguro

Herramientas para protegerte en línea

Existen muchas herramientas y aplicaciones diseñadas para mantenerte seguro en internet. Aquí te presentamos algunas que pueden ayudarte a evitar peligros y navegar con tranquilidad:

1. **Controles parentales:**
   - Los controles parentales son aplicaciones o configuraciones que permiten a tus padres supervisar y limitar el contenido al que puedes acceder en línea. También pueden establecer límites de tiempo de uso. Esto ayuda a asegurarte de que no entres accidentalmente en sitios peligrosos o inapropiados.
   - Ejemplos incluyen **Google Family Link** y **Apple Screen Time**, que permiten a los padres controlar qué aplicaciones puedes usar y durante cuánto tiempo.

2. **Safesearch:**
   - **Google safesearch** es una opción que puedes activar para filtrar los resultados de búsqueda y bloquear contenido inapropiado, como violencia o pornografía. Este filtro es especialmente útil cuando navegas por internet para buscar información para tus deberes o proyectos escolares.

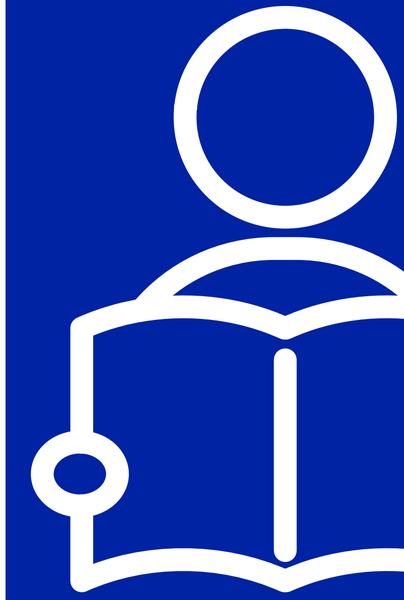
3. **Aplicaciones de bienestar digital:**
   - Aplicaciones como **Samsung Digital Wellbeing** o **Forest** te permiten controlar el tiempo que pasas en línea, especialmente en redes sociales o jugando. Estas apps te ayudan a desarrollar un uso más consciente y equilibrado de la tecnología, evitando que pases demasiado tiempo frente a la pantalla.

4. **Antivirus y software de seguridad:**
   - Mantener un antivirus actualizado en tus dispositivos es una excelente manera de protegerte de virus, malware y ataques cibernéticos. Estos programas también pueden ayudarte a detectar sitios web peligrosos antes de que accedas a ellos.

Recursos en línea para aprender más sobre seguridad

Además de las herramientas de protección, existen sitios web y recursos en línea que te enseñan cómo mantenerte seguro y cómo actuar si enfrentas problemas en internet. Algunos de los recursos más recomendados son:

- **Pantallas amigas**: este sitio ofrece videos y guías educativas sobre cómo navegar de manera segura en redes sociales, cómo evitar el ciberacoso y cómo proteger tu privacidad.
- **Incibe (Instituto Nacional de Ciberseguridad)**: tiene una línea de ayuda para adolescentes y una serie de recursos dedicados a la seguridad digital. Puedes encontrar información sobre cómo evitar riesgos en línea y qué hacer en caso de un problema.



12 Conclusión: ser un ciudadano digital responsable

Ser amable y respetuoso en línea

Ser un buen ciudadano digital significa usar internet de manera **responsable, respetuosa y ética**. Aquí tienes algunas pautas para asegurarte de que siempre te comportas de la mejor manera en línea:

- **Sé amable en tus interacciones**: al igual que en la vida real, es importante ser respetuoso y amable con las personas en internet. Evita hacer comentarios hirientes, difundir rumores o compartir contenido que pueda molestar a otros.
- **Respeta la diversidad**: en internet, te encontrarás con personas de diferentes culturas, países y formas de pensar. Es importante respetar estas diferencias y no juzgar ni discriminar a nadie.

Usar internet para el aprendizaje y crecimiento personal

Internet puede ser una herramienta increíble para aprender, compartir ideas y mejorar como persona. Aquí tienes algunas formas de usarlo positivamente:

1. **Sigue cuentas educativas:** hay miles de cuentas en redes sociales que comparten información útil y educativa sobre ciencia, tecnología, arte, literatura, y muchos otros temas. Usa internet para aprender algo nuevo cada día.

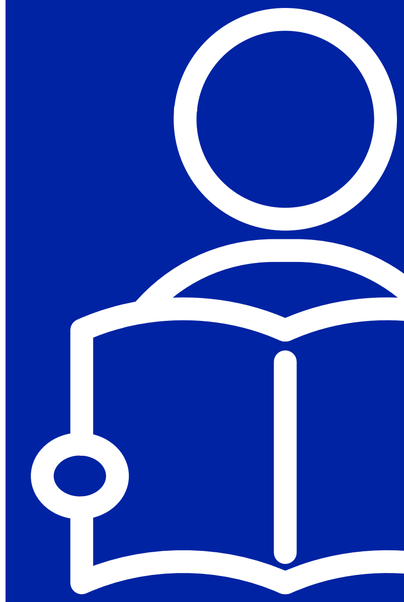
2. **Participa en proyectos colaborativos:** puedes unirte a iniciativas que promuevan el cambio social o ambiental, como campañas para proteger el medio ambiente o ayudar a los demás. Estas actividades te permiten usar internet como una fuerza positiva para el bien común.

3. **Inspira a otros**: publica contenido que sea útil y positivo para las personas. Ya sea un consejo de estudio, un logro personal o algo inspirador, puedes ser una influencia positiva para tus amigos y seguidores.

Mantén un equilibrio entre el mundo digital y el mundo real

Si bien internet es una excelente herramienta para conectarte y aprender, es importante **mantener un equilibrio** entre el tiempo que pasas en línea y el que dedicas a otras actividades. Algunas ideas para lograr este equilibrio son:

- **Haz ejercicio físico**: después de pasar tiempo en el ordenador o en el móvil, sal a caminar, juega deportes o simplemente muévete. Esto te ayudará a mantener tu cuerpo y mente saludables.
- **Pasa tiempo con tu familia y amigos sin dispositivos**: dedica tiempo a actividades sin tecnología, como juegos de mesa, salidas al parque o cocinar juntos.
- **Desconéctate antes de dormir**: deja de usar dispositivos al menos una hora antes de irte a la cama. Esto te ayudará a descansar mejor y evitar la fatiga digital.



Familias

+índice

1. Introducción a la Seguridad Digital en el Hogar 105

- ¿Por qué es tan importante la seguridad digital en el hogar? 106
- Cómo empezar con la seguridad digital en casa 106
- Educación continua para padres e hijos 107

2. Establecer normas y reglas digitales en casa 108

- Crear un plan familiar digital 109
- El valor del acuerdo familiar 110
- Contrato familiar digital 110
- Ajustando las reglas a la edad 112
- Supervisión y flexibilidad 112

3. Protección de la privacidad y datos personales 113

- La importancia de enseñar la protección de datos 114
- Enseñar a los niños a reconocer peligros 115
- Uso de contraseñas seguras 115
- Supervisión activa y herramientas de protección 115
- Reforzar el valor del consentimiento 115

4. Fomentar el respeto y la empatía en el entorno digital 116

- ¿Por qué es tan importante el respeto en línea? 117
- Fomentar la empatía en línea 117
- Qué hacer en caso de ciberacoso 118
- Establecer un código de conducta digital 118
- Predicar con el ejemplo 118

5. Uso de herramientas de control parental 119

- ¿Qué son las herramientas de control parental? 120
- ¿Por qué es importante el control parental? 120
- Funcionalidades comunes de las herramientas de control parental 120
- Herramientas recomendadas para el control parental 121
- Cómo implementar el control parental de manera efectiva 121
- Flexibilidad y confianza 122

6. Fomentar un uso equilibrado de la tecnología 123

- Impacto del uso excesivo de la tecnología 124
- Cómo fomentar un uso equilibrado de la tecnología 124

Familias

- Herramientas para gestionar el tiempo de pantalla 125
- Incentivar el auto-gestión del tiempo 125
- Equilibrar la tecnología y la vida familiar 125

7. Cómo hablar con los niños sobre los riesgos en línea 126

- Crear un entorno de confianza 127
- Temas claves a tratar 127
- Escuchar sus experiencias 128
- Estrategias para hablar con niños de diferentes edades 128

8. Promover una comunicación abierta y sostenida 129

- La importancia de la comunicación abierta 130
- Fomentar el diálogo en lugar de imponer normas 131
- Herramientas para facilitar la comunicación 131
- Hablar sobre las consecuencias del mal uso de la tecnología 131

9. Cómo actuar ante problemas en línea 132

- Primeros pasos al enfrentarse a un problema en línea 133
- Hablar con un adulto de confianza 133
- Reportar el incidente 134
- Buscar ayuda especializada 134
- Recuperar el control emocional 134

10. Conclusión: el rol de las familias en la educación digital 135

- La importancia de la educación continua 136
- Crear un entorno familiar seguro 136
- Empoderar a los niños 136
- La tecnología como aliada, no enemiga 136

01 Introducción a la Seguridad Digital en el Hogar

La tecnología forma parte de nuestra vida cotidiana, y en muchos hogares, los dispositivos digitales están presentes en casi todas las actividades diarias: desde el entretenimiento hasta el aprendizaje, pasando por la comunicación familiar. Pero, con el acceso a esta tecnología, también surgen riesgos que pueden afectar la seguridad y el bienestar de los niños si no se gestionan adecuadamente.

La **seguridad digital en el hogar** no se trata solo de restringir o supervisar el acceso a Internet, sino de crear un entorno donde los niños aprendan a **navegar de manera segura, consciente y responsable**. Como padres, desempeñamos un papel esencial en esta tarea, ya que somos los primeros modelos a seguir en el uso de la tecnología. Es fundamental que los hijos entiendan los beneficios de Internet, pero también los peligros, como el **ciberacoso**, la **exposición a contenido inapropiado** o los **riesgos de compartir información personal** sin control.

¿Por qué es tan importante la seguridad digital en el hogar?

- **Protección frente a riesgos en línea**: A diferencia de las generaciones anteriores, los niños de hoy crecen en un entorno donde Internet es omnipresente. Las plataformas que usan pueden ser educativas, pero también pueden exponerlos a **ciberacoso**, **fraudes**, **suplantación de identidad** o **grooming**. Mantenerse alerta y enseñarles a identificar estos riesgos es clave para evitar daños.
- **Desarrollo de hábitos saludables**: Los niños necesitan aprender desde pequeños cómo **gestionar su tiempo frente a la pantalla** y equilibrar el uso de la tecnología con actividades offline. El uso excesivo de dispositivos puede afectar su rendimiento académico, sus relaciones interpersonales y hasta su salud física (problemas de sueño, sedentarismo, etc.).
- **Educación sobre el respeto y la empatía en línea**: Además de protegerse a sí mismos, es importante enseñarles a ser **ciudadanos digitales responsables**. La tecnología no sólo debe utilizarse de manera segura, sino también de forma respetuosa, promoviendo interacciones positivas y empáticas en sus redes sociales o en los juegos en línea. Evitar que ellos mismos se conviertan en acosadores o difundan contenido inapropiado es tan importante como protegerlos del ciberacoso.

Cómo empezar con la seguridad digital en casa

1. Crear un ambiente de confianza: Fomentar una **comunicación abierta** en el hogar es el primer paso para que los niños se sientan seguros compartiendo sus experiencias en línea. Preguntarles regularmente qué sitios visitan, qué juegos juegan y con quién se comunican puede ayudarte a identificar posibles problemas antes de que escalen.

2. Ser ejemplos a seguir: Los niños aprenden de lo que ven. Si los padres usamos la tecnología de manera responsable (no pasando horas frente a la pantalla, gestionando bien el tiempo en redes sociales, protegiendo nuestra información personal), los niños imitarán esos comportamientos.

3. Uso de herramientas de control parental: En los primeros años de interacción digital de los niños, el uso de **herramientas de control parental** puede ayudar a restringir el acceso a sitios web o aplicaciones no adecuadas. Sin embargo, no basta con la supervisión; es crucial que los niños comprendan por qué se establecen estas reglas y cómo pueden protegerse a medida que crecen y adquieren más independencia en su navegación.

4. Establecer normas familiares sobre el uso de la tecnología: El uso de dispositivos no debe interferir con la vida familiar. Establecer límites claros sobre **cuándo** y **dónde** se pueden usar los dispositivos ayuda a evitar que la tecnología invada momentos importantes como las comidas familiares o las horas de descanso. Por ejemplo, puede ser útil implementar la "norma de la desconexión", donde todos los dispositivos se apagan una hora antes de dormir para favorecer un descanso saludable.

Educación continua para padres e hijos

La seguridad digital es un proceso que evoluciona a medida que lo hace la tecnología. Nuevas amenazas y riesgos pueden surgir, y tanto los padres como los niños deben **estar informados y actualizados**. Participar en charlas escolares sobre seguridad digital, leer guías sobre el tema y seguir recomendaciones de organizaciones especializadas (como **Pantallas Amigas** o **INCIBE**) puede ayudar a las familias a mantenerse al día con las mejores prácticas en protección digital. La seguridad digital es un proceso que evoluciona a medida que lo hace la tecnología. Nuevas amenazas y riesgos pueden surgir, y tanto los padres como los niños deben **estar informados y actualizados**. Participar en charlas escolares sobre seguridad digital, leer guías sobre el tema y seguir recomendaciones de organizaciones especializadas (como **Pantallas Amigas** o **INCIBE**) puede ayudar a las familias a mantenerse al día con las mejores prácticas en protección digital.

La seguridad digital es un proceso que evoluciona a medida que lo hace la tecnología. Nuevas amenazas y riesgos pueden surgir, y tanto los padres como los niños deben **estar informados y actualizados**. Participar en charlas escolares sobre seguridad digital, leer guías sobre el tema y seguir recomendaciones de organizaciones especializadas (como **Pantallas Amigas** o **INCIBE**) puede ayudar a las familias a mantenerse al día con las mejores prácticas en protección digital.

La seguridad digital es un proceso que evoluciona a medida que lo hace la tecnología. Nuevas amenazas y riesgos pueden surgir, y tanto los padres como los niños deben **estar informados y actualizados**. Participar en charlas escolares sobre seguridad digital, leer guías sobre el tema y seguir recomendaciones de organizaciones especializadas (como **Pantallas Amigas** o **INCIBE**) puede ayudar a las familias a mantenerse al día con las mejores prácticas en protección digital.

02 Establecer normas y reglas digitales en casa

La clave para un uso seguro y responsable de la tecnología en el hogar es **establecer normas claras** que los niños comprendan y respeten. Estas reglas deben adaptarse a la edad de los niños y a sus necesidades, pero lo más importante es que se apliquen de manera coherente.

Crear un plan familiar digital

un enfoque útil es diseñar un **plan familiar digital**, donde se establezcan las reglas sobre cuándo, dónde y cómo se puede usar la tecnología en casa. El plan debe ser conversado y acordado por todos los miembros de la familia, de modo que todos comprendan su importancia y se sientan parte de su creación. Algunos puntos clave para incluir en este plan pueden ser:

1. **Tiempo de pantalla:**
   - **Establecer límites de tiempo** para el uso de dispositivos, diferenciando entre el uso educativo y el de entretenimiento. Por ejemplo, una regla podría ser que los niños no pasen más de una o dos horas diarias en videojuegos o redes sociales, reservando el tiempo necesario para tareas escolares y actividades familiares.
   - Es importante recalcar que no todos los tiempos de pantalla son iguales: el uso educativo de la tecnología puede tener más flexibilidad, mientras que el uso recreativo debe ser limitado.

2. **Ubicaciones y momentos para usar dispositivos:**
   - **Ubicaciones controladas:** Una buena práctica es limitar el uso de dispositivos a áreas comunes de la casa, como la sala de estar o la cocina, para que el uso de la tecnología pueda ser supervisado de manera más fácil. Evitar que los dispositivos se usen en los dormitorios, especialmente antes de dormir, puede prevenir problemas de salud relacionados con el sueño.
   - **Momentos especiales:** Establecer horarios específicos para **desconectar la tecnología**, como durante las comidas familiares o una hora antes de dormir. Estos momentos son ideales para **fortalecer la comunicación familiar** y evitar que la tecnología interfiera en las relaciones personales.

3. **Uso de la tecnología durante el estudio:**
   - Si bien los dispositivos pueden ser muy útiles para hacer deberes y proyectos escolares, también pueden ser una fuente de distracción. Los padres deben ayudar a los niños a **establecer tiempos de estudio libres de distracciones**, donde no se permita el uso de redes sociales o juegos.
   - Una estrategia es utilizar aplicaciones que **bloqueen temporalmente** el acceso a ciertas páginas o apps durante las horas de estudio, lo que fomenta un ambiente más concentrado y productivo.

4. **Revisión periódica de los sitios web y aplicaciones:**
   - Mantener una conversación abierta y regular sobre **qué sitios web visitan** y **qué aplicaciones usan** es fundamental. Los padres deben revisar qué aplicaciones se descargan y entender para qué sirven, asegurándose de que sean apropiadas para la edad de sus hijos.

02

- Es importante que los padres exploren junto con los niños las plataformas que usan, para comprender sus funciones y establecer límites claros. Por ejemplo, redes sociales como TikTok o Instagram pueden ser adecuadas en ciertos contextos, pero deben ser utilizadas bajo normas específicas de seguridad y privacidad.
- Es crucial que naveguemos juntos y usemos la tecnología y especialmente el acceso a Internet juntos. Igual que has acompañado a tus hijos a cruzar un semáforo, a caminar por la calle... No le dejes sólo ante nada de esto. Existen peligros en la Red que no puedes imaginar y si les dejas solos les expondrás ante ellos.

El valor del acuerdo familiar

una de las formas más efectivas de hacer cumplir estas reglas es **involucrar a los niños en la creación del plan familiar digital**. Cuando los niños participan en la elaboración de estas normas, son más propensos a respetarlas. Además, esto fomenta el **diálogo abierto sobre el uso de la tecnología**, lo que permite que los niños se sientan escuchados y comprendidos.

Puedes formalizar este acuerdo mediante un **"contrato familiar digital"**, que todos firmen para reforzar el compromiso con las normas. El contrato podría incluir compromisos como "No usaré mi dispositivo en la mesa" o "No descargaré aplicaciones sin hablar con mis padres".

Te adjunto un modelo de Contrato Familiar Digital para que puedas personalizar y diseñar con tus hij@s.

Contrato familiar digital

nosotros, la familia [Apellido], reconocemos la importancia de la tecnología en nuestras vidas diarias, tanto para el trabajo como para la educación y el entretenimiento. Al mismo tiempo, entendemos que el uso responsable de la tecnología es esencial para mantener una buena convivencia, proteger nuestra privacidad y garantizar la seguridad en línea.

Por lo tanto, como familia, acordamos cumplir con las siguientes normas sobre el uso de la tecnología en nuestro hogar:

1. **Uso responsable de la tecnología**

uso en áreas comunes: Los dispositivos electrónicos (teléfonos, tablets, ordenadores) se utilizarán preferentemente en las áreas comunes de la casa (sala de estar, comedor) para facilitar la supervisión y evitar el aislamiento.

- **Horarios de uso:** Acordamos limitar el uso de dispositivos durante las comidas y a la hora de dormir. Nos desconectaremos una hora antes de acostarnos para promover un descanso saludable.
- **Tiempo de pantalla:** Se establecerán límites de tiempo diarios para el uso recreativo de la tecnología, equilibrando este tiempo con actividades como el deporte, la lectura y las tareas del hogar.

2. Protección de la privacidad

- **Datos personales:** Nos comprometemos a no compartir información personal, como la dirección, números de teléfono o fotos, en redes sociales o con personas desconocidas sin el consentimiento familiar.
- **Configuración de privacidad:** Revisaremos juntos las configuraciones de privacidad en redes sociales y aplicaciones para asegurarnos de que nuestra información esté protegida.
- **Contraseñas seguras:** Cada miembro de la familia se compromete a utilizar contraseñas seguras y únicas para sus cuentas y a no compartirlas con otras personas, excepto con un adulto de confianza en caso necesario.

3. Respeto en línea

- **Ciberacoso:** Nos comprometemos a tratar a todos con respeto en línea. No participaremos en comportamientos de ciberacoso ni compartiremos contenido que pueda dañar a otras personas. Si alguno de nosotros se enfrenta a una situación incómoda o de acoso en línea, lo compartirá con la familia para recibir apoyo.
- **Contenido apropiado:** Nos aseguraremos de que el contenido que compartimos, publicamos o comentamos en redes sociales o plataformas en línea sea respetuoso y adecuado para todos los públicos.

4. Supervisión y control parental

- **Uso supervisado:** Los miembros más jóvenes de la familia utilizarán la tecnología bajo la supervisión de los padres. Los padres tendrán acceso a las cuentas y dispositivos de los menores para garantizar que el uso de la tecnología sea seguro.
- **Control parental:** Se implementarán herramientas de control parental en dispositivos y aplicaciones para limitar el acceso a contenido inapropiado o peligroso, y para establecer límites de tiempo en el uso de la tecnología.

5. Equilibrio entre el mundo digital y el real

- **Actividades sin pantallas:** Acordamos equilibrar nuestro tiempo de uso de dispositivos con actividades sin tecnología, como salidas al aire libre, juegos en familia y otras actividades que fomenten el bienestar físico y emocional.
- **Momentos de desconexión:** Durante ciertos momentos del día, como las comidas o reuniones familiares, todos los miembros de la familia guardarán sus dispositivos para poder disfrutar del tiempo juntos sin interrupciones.

6. Seguridad en línea

- **Navegación segura:** Nos comprometemos a navegar por sitios web y plataformas seguras, evitando hacer clic en enlaces sospechosos o descargar archivos de fuentes no confiables.
- **Denuncia de comportamientos sospechosos:** Si alguno de nosotros detecta comportamientos o contenidos sospechosos o peligrosos en línea, lo compartiremos de inmediato con la familia y, si es necesario, con las autoridades competentes.

7. Revisión del contrato

Este contrato será revisado cada [intervalo de tiempo: 6 meses, un año] para asegurar que las normas sigan siendo adecuadas para nuestra familia y para ajustarlas a las nuevas necesidades y circunstancias que puedan surgir.

Firmas del contrato

Padre/Madre/Tutor 1: _____

Padre/Madre/Tutor 2: _____

Hijo/a 1: _____

Hijo/a 2 _____

Hijo/a 3 _____

Fecha: _____

Ajustando las reglas a la edad

a medida que los niños crecen, las reglas sobre el uso de la tecnología deben **evolucionar**. Los adolescentes, por ejemplo, pueden necesitar más independencia, pero eso no significa que no deban seguir algunas reglas. En lugar de limitarse a imponer restricciones, es importante que los padres actúen como **guías**, ayudando a los adolescentes a desarrollar hábitos tecnológicos saludables y responsables por sí mismos. Esto podría incluir:

- Discutir los **riesgos de las redes sociales** y cómo gestionar su presencia digital de manera segura.
- Enséñales a **equilibrar su tiempo en línea** con otras actividades como el deporte, la lectura o las relaciones cara a cara.

Supervisión y flexibilidad

Si bien las reglas son importantes, también es fundamental ser **flexibles y comprensivos**. Los padres deben supervisar de manera adecuada, pero sin generar un entorno de control extremo. Las reglas deben ajustarse según las necesidades y la madurez de los niños, siempre manteniendo la **comunicación abierta** para que se sientan cómodos compartiendo sus experiencias digitales.

05 Protección de la privacidad y datos personales

Protección de la privacidad y datos personales

En la era digital, la protección de la privacidad y los datos personales es uno de los temas más importantes para las familias. A menudo, los niños no son conscientes del riesgo que implica compartir información personal en línea. Desde redes sociales hasta juegos y aplicaciones educativas, muchas plataformas solicitan datos como nombres, fotos y ubicaciones, lo que puede exponer a los niños a amenazas como el robo de identidad, grooming o ciberacoso.

La importancia de enseñar la protección de datos

Es fundamental que los padres eduquen a sus hijos sobre la privacidad en línea y la importancia de proteger su información. Muchas veces, los niños comparten sin darse cuenta detalles que pueden parecer inofensivos, como su nombre o el nombre de su escuela, pero que en manos equivocadas pueden ponerlos en peligro.

Los niños deben entender que la información personal incluye no solo datos obvios como el nombre completo o la dirección, sino también detalles como:

- **Contraseñas:** No deben compartirse con nadie, ni siquiera con amigos cercanos. Las contraseñas deben ser seguras, combinando letras, números y símbolos.
- **Ubicación:** Las aplicaciones y redes sociales pueden rastrear la ubicación de los usuarios. Los padres deben enseñar a los niños a desactivar esta función cuando no sea necesaria.
- **Fotos y videos:** Las imágenes pueden proporcionar mucha información personal sin que los niños lo sepan, como dónde viven o a qué escuela asisten. Es importante que no publiquen fotos en las que aparezcan detalles como el uniforme escolar, la calle o el vecindario.
- **Configuraciones de Privacidad en Redes Sociales y Juegos**

Uno de los pasos más importantes que los padres pueden tomar para proteger la privacidad de sus hijos es revisar y ajustar las configuraciones de privacidad de todas las cuentas y aplicaciones que usan. Esto incluye:

- **Configurar las cuentas como privadas en redes sociales** como Instagram, TikTok o Facebook. De esta forma, solo personas conocidas pueden ver las publicaciones de los niños.

- **Controlar quién puede contactarlos:** Algunas plataformas permiten ajustar quién puede enviarles mensajes o agregarles como amigos. Limitar estas opciones a amigos cercanos o familiares es crucial para evitar contactos no deseados.

- **Revisar las políticas de privacidad de las aplicaciones y juegos que usan**, asegurándose de que no se recopilen datos innecesarios o se compartan con terceros sin consentimiento.

Enseñar a los niños a reconocer peligros

Además de proteger la información, los padres deben enseñar a sus hijos a reconocer situaciones sospechosas o peligrosas en línea. Esto incluye:

- **No aceptar solicitudes de amistad o mensajes de desconocidos.** Deben aprender a ser críticos con las personas que intentan contactarlos en línea y siempre consultarlo con un adulto si se sienten incómodos.
- **No compartir información personal en chats de juegos:** Muchos juegos en línea permiten chatear con otros jugadores. Asegúrate de que tus hijos sepan que no deben compartir ningún dato personal con extraños en estos espacios.
- **Detectar fraudes o estafas:** Los niños deben ser conscientes de los riesgos de hacer clic en enlaces de origen desconocido, ya que estos pueden llevar a páginas fraudulentas o descargar malware que robe información.

Uso de contraseñas seguras

un aspecto clave en la protección de datos es la gestión adecuada de contraseñas. Es esencial que los niños comprendan la importancia de:

- **Usar contraseñas complejas** que incluyan una combinación de letras mayúsculas y minúsculas, números y símbolos. Evitar el uso de contraseñas obvias como nombres de mascotas o fechas de nacimiento.
- **Cambiar las contraseñas regularmente y no reutilizar la misma contraseña** en múltiples cuentas.
- **No compartir sus contraseñas con amigos o terceros,** incluso si parecen de confianza. Esto es fundamental para mantener la seguridad de sus cuentas.

Supervisión activa y herramientas de protección

Además de educar a los niños, los padres deben utilizar herramientas que ayuden a supervisar y proteger la actividad digital de los hijos. Algunas recomendaciones incluyen:

- **Instalar software de control parental:** Herramientas como Qustodio o Google Family Link permiten a los padres monitorear el uso de aplicaciones, bloquear contenido inapropiado y recibir alertas sobre comportamientos sospechosos.
- **Revisar periódicamente la actividad en las cuentas y aplicaciones que usan los niños,** asegurándose de que todo esté bajo control y que no haya interacciones peligrosas.

Reforzar el valor del consentimiento

es importante que los niños comprendan el concepto de consentimiento digital. Deben saber que nadie tiene derecho a pedirles fotos, videos o información personal sin su permiso, y que siempre pueden negarse a compartir algo si no se sienten cómodos. Además, deben ser conscientes de que lo mismo aplica en sentido contrario: no deben compartir fotos o información de otras personas sin su consentimiento.

04 Fomentar el respeto y la empatía en el entorno digital

04

En un mundo cada vez más conectado, el respeto y la empatía en línea son tan importantes como en la vida real. Los niños deben entender que detrás de cada perfil digital hay una persona real con sentimientos y derechos. En este sentido, los padres juegan un papel crucial al fomentar comportamientos positivos y prevenir situaciones de acoso, malentendidos o la difusión de contenido inapropiado.

¿Por qué es tan importante el respeto en línea?

El respeto en línea implica tratar a los demás con cortesía y amabilidad. Al igual que en el mundo físico, los comportamientos irrespetuosos en el entorno digital, como el ciberacoso o la humillación pública, pueden causar daño emocional y psicológico. Además, las redes sociales, los chats y las plataformas de juegos pueden amplificar estos comportamientos negativos, llegando a un público mucho más amplio en muy poco tiempo.

Es esencial enseñar a los niños que lo que hacen o dicen en línea tiene un impacto directo en los demás. En muchos casos, la percepción de "anonimato" en línea lleva a los usuarios, especialmente a los más jóvenes, a actuar de manera más agresiva o insensible de lo que lo harían en persona. Este comportamiento puede dar lugar a problemas graves como el ciberacoso.

Fomentar la empatía en línea

La empatía es la capacidad de ponerse en el lugar del otro y comprender cómo se siente. En el entorno digital, es fundamental enseñar a los niños a pensar antes de comentar, publicar o compartir contenido. Algunas maneras de fomentar la empatía incluyen:

1. Reflexionar antes de actuar

Animar a los niños a pensar cómo se sentiría la otra persona antes de enviar un mensaje, publicar un comentario o compartir una imagen. Preguntarles: "¿Te gustaría que alguien te hiciera esto a ti?" es una buena forma de que consideren el impacto de sus acciones.

2. Apoyar a los demás

En lugar de sumarse a comentarios negativos o burlas, los niños deben ser alentados a apoyar a sus amigos y compañeros cuando vean que están siendo tratados injustamente en línea. Enseñarles que intervenir positivamente puede marcar una gran diferencia.

3. Evitar las burlas o la difusión de rumores

Es común que los niños participen en conversaciones que incluyen chismes o burlas. Sin embargo, en el entorno digital, estos comportamientos pueden escalar rápidamente. Los padres deben dejar claro que la difusión de rumores o la participación en burlas es inaceptable y puede tener consecuencias duraderas.

Qué hacer en caso de ciberacoso

El ciberacoso es una forma grave de maltrato en línea que puede ocurrir a través de mensajes directos, comentarios en redes sociales, juegos en línea o foros. Es crucial que los padres eduquen a sus hijos sobre cómo identificar y actuar si se enfrentan a una situación de ciberacoso. Algunas estrategias incluyen:

1. **No responder al acosador:**
Responder al ciberacoso puede empeorar la situación. Es mejor ignorar los mensajes y bloquear al acosador.

2. **Guardar pruebas**
Si un niño es víctima de ciberacoso, es importante hacer capturas de pantalla de los mensajes, comentarios o imágenes que se utilicen para acosar, ya que estas pruebas pueden ser útiles para reportar el incidente a la plataforma o a las autoridades escolares.

3. **Hablar con un adulto de confianza**
Los niños deben sentirse cómodos para acudir a sus padres o a un adulto de confianza si están siendo acosados en línea. Los padres deben reforzar la idea de que pedir ayuda no es una señal de debilidad, sino una manera de solucionar el problema.

4. **Reportar el incidente**
Muchas plataformas de redes sociales, juegos en línea y aplicaciones de mensajería tienen herramientas para reportar el ciberacoso. Los padres deben ayudar a sus hijos a reportar estos incidentes y bloquear al acosador.

Establecer un código de conducta digital

Una excelente manera de fomentar el respeto en línea es crear un código de conducta digital en el hogar. Este código puede incluir reglas como:

- **No insultar, criticar o burlarse de otros en línea.**
- **No compartir fotos, videos o información personal de otras personas sin su consentimiento.**
- **Ser amable y respetuoso en todas las interacciones digitales,** independientemente de la situación.

Los padres pueden revisar este código con sus hijos periódicamente, ajustándolo según sea necesario y asegurándose de que comprendan su importancia. Además, este código puede servir como una guía para que los niños evalúen su comportamiento en línea y aprendan a ser responsables de sus acciones.

Predicar con el ejemplo

Los padres también deben ser modelos de comportamiento positivo en línea. Los niños observan y aprenden de las interacciones de sus padres en redes sociales, correos electrónicos y otros espacios digitales. Ser respetuoso y empático en líne a, además de mantener una actitud crítica hacia el contenido que se comparte, es clave para enseñar a los hijos a comportarse de manera ética en el entorno digital.

05 Uso de herramientas de control parental

05

Las **herramientas de control parental** se han convertido en un recurso indispensable para las familias que desean mantener a sus hijos seguros en el entorno digital. Estas herramientas permiten a los padres supervisar y regular el uso de la tecnología de manera proactiva, asegurándose de que los niños tengan acceso a contenido adecuado y se mantengan protegidos frente a los riesgos en línea.

¿Qué son las herramientas de control parental?

Las herramientas de control parental son **programas o aplicaciones** que permiten a los padres monitorear y controlar cómo, cuándo y para qué se utilizan los dispositivos conectados a Internet en el hogar. Estas herramientas ofrecen una amplia gama de funcionalidades, que van desde **limitar el tiempo de pantalla** hasta bloquear el acceso a contenido inapropiado, y son útiles para supervisar tanto el uso de ordenadores como de dispositivos móviles y consolas de videojuegos.

¿Por qué es importante el control parental?

El entorno digital es vasto y puede ser difícil, incluso para los padres más atentos, supervisar constantemente lo que los niños están haciendo en línea. El control parental proporciona una capa adicional de seguridad, permitiendo a los padres:

- **Restringir el acceso a contenido no apto** para la edad del niño, como violencia o contenido sexual explícito.
- **Supervisar el tiempo de uso de los dispositivos,** evitando el uso excesivo de pantallas y asegurando que los niños realicen otras actividades importantes, como jugar al aire libre o leer.
- **Monitorear la actividad en línea**, incluyendo las interacciones en redes sociales y juegos en línea, para identificar posibles comportamientos de riesgo, como el ciberacoso o la interacción con desconocidos.

Funcionalidades comunes de las herramientas de control parental

1. Filtro de contenido

Bloquea automáticamente el acceso a sitios web o aplicaciones inapropiadas, categorizando el contenido según su naturaleza (violencia, apuestas, pornografía, etc.).

2. Límites de tiempo

Permite a los padres establecer un tiempo máximo diario o semanal para el uso de dispositivos. Algunos programas también ofrecen la opción de restringir el uso de aplicaciones específicas, como redes sociales o videojuegos.

3. Supervisión en tiempo real

Algunas herramientas permiten a los padres ver en tiempo real lo que los niños están haciendo en sus dispositivos, lo que es especialmente útil para identificar actividades de riesgo de forma temprana.

4. Bloqueo de aplicaciones

Los padres pueden bloquear aplicaciones específicas que

consideren inapropiadas para sus hijos o que se utilicen de manera excesiva.

- **Alertas de comportamiento sospechoso**: Algunas herramientas pueden enviar alertas cuando se detecta actividad inusual, como la instalación de nuevas aplicaciones, la visita a sitios bloqueados o el uso prolongado de dispositivos fuera del horario permitido.

Herramientas recomendadas para el control parental

Existen numerosas opciones de control parental que pueden adaptarse a las necesidades de cada familia. Algunas de las más populares y efectivas incluyen:

- **Google Family Link**: Una opción gratuita que permite a los padres supervisar y gestionar los dispositivos Android y Chromebooks de sus hijos. Ofrece funciones como la **supervisión de la ubicación**, el control del tiempo de pantalla y el bloqueo de aplicaciones.
- **Samsung Kids**
- **Familia Apple**
- **Qustodio**: Un software completo de control parental que funciona en múltiples plataformas (Windows, Android, iOS) y permite a los padres establecer **filtros de contenido, límites de tiempo y monitorear redes sociales**.
- **Norton Family**: Este programa de control parental es conocido por su capacidad para **filtrar contenido** y **monitorear la actividad en línea**, además de ofrecer informes detallados sobre el comportamiento digital de los niños.

Cómo implementar el control parental de manera efectiva

Si bien las herramientas de control parental son muy útiles, es importante que los padres las utilicen como parte de un enfoque más amplio de **educación digital**, y no como una medida de vigilancia rígida. Para garantizar su eficacia:

1. **Involucra a los niños en el proceso**
   - En lugar de implementar los controles de forma encubierta, los padres deben **explicar a sus hijos por qué utilizan estas herramientas** y cómo benefician su seguridad en línea. Es más probable que los niños acepten las restricciones si entienden los riesgos y la necesidad de protegerse.
2. **Actualiza y ajusta las configuraciones**

A medida que los niños crecen, sus necesidades cambian. Lo que puede ser adecuado para un niño de 8 años puede no serlo para un adolescente. Es importante **ajustar las configuraciones** regularmente para que las reglas digitales evolucionen con los hijos.

3. **No sustituyen la comunicación**

Aunque el control parental es una herramienta útil, no debe ser la única medida de protección. La **comunicación abierta y continua** sobre la seguridad digital sigue siendo esencial. Los padres deben hablar regularmente con sus hijos sobre lo que están haciendo en línea, con quién están interactuando y cómo se sienten al respecto.

05

Flexibilidad y confianza

El uso de herramientas de control parental debe ser **equilibrado y flexible**. Si bien es importante proteger a los niños, también es esencial permitirles **cierto grado de independencia** a medida que crecen y desarrollan su propio sentido de responsabilidad digital. Los padres deben estar preparados para **aflojar los controles** gradualmente a medida que los niños demuestren una mayor madurez y comprensión de los riesgos en línea.

06

Fomentar un uso equilibrado de la tecnología

Fomentar un uso equilibrado de la tecnología

06

En un mundo donde la tecnología está presente en casi todos los aspectos de la vida diaria, es crucial que las familias enseñen a sus hijos a **mantener un equilibrio** entre el tiempo que pasan frente a las pantallas y otras actividades importantes para su desarrollo. El uso excesivo de dispositivos puede afectar no solo la salud física de los niños (como la visión o el sueño), sino también su bienestar emocional y social. A continuación, te explico cómo fomentar un uso equilibrado y saludable de la tecnología en casa.

Impacto del uso excesivo de la tecnología

El tiempo prolongado frente a las pantallas puede tener varias consecuencias negativas para los niños:

1. **Problemas de salud física**

El uso constante de dispositivos puede provocar **fatiga visual**, dolores de cabeza y problemas posturales. Además, la **luz azul** emitida por las pantallas afecta la calidad del sueño, especialmente si se usan dispositivos antes de acostarse.

2. **Interferencia con el rendimiento escolar**

El uso excesivo de dispositivos para entretenimiento puede reducir el tiempo que los niños dedican a sus estudios y otras responsabilidades, afectando su rendimiento académico.

3. **Aislamiento social**

Aunque la tecnología puede conectar a las personas, el uso excesivo de dispositivos puede llevar a los niños a **desconectarse de las interacciones cara a cara**, lo que impacta negativamente en su capacidad para desarrollar habilidades sociales.

4. **Aumento de la ansiedad**

El consumo excesivo de redes sociales y la exposición constante a la vida idealizada de los demás puede generar **ansiedad, baja autoestima y presión social** en los niños y adolescentes.

Cómo fomentar un uso equilibrado de la tecnología

1. **Establecer horarios específicos**

Un buen punto de partida es **crear un horario** donde los dispositivos se utilicen solo en momentos específicos, como después de hacer los deberes o durante un tiempo limitado en la tarde. Además, es útil reservar momentos para la **desconexión total**, como durante las comidas familiares o una hora antes de acostarse, fomentando un descanso reparador.

2. **Promover actividades sin pantallas**

Fomentar hobbies que no incluyan el uso de tecnología es una excelente manera de equilibrar su uso. Estas actividades pueden incluir **lectura, deportes, juegos al aire libre, manualidades o música**. Los padres pueden involucrarse activamente en estas actividades, lo que también fortalece el vínculo familiar.

3. Ser un modelo a seguir
Los niños aprenden observando el comportamiento de sus padres. Si ven que los adultos en casa equilibran su tiempo de pantalla con otras actividades, es más probable que imiten ese comportamiento. Limitar el uso de dispositivos frente a los hijos y **participar en actividades sin pantallas** como la lectura, el ejercicio o el tiempo de calidad en familia, es clave.

4. Incluir descansos regulares durante el uso de dispositivos
Los niños deben aprender a **hacer pausas regulares** mientras usan dispositivos, especialmente durante sesiones prolongadas de videojuegos o estudio. Esto no solo previene la fatiga visual, sino que también les ayuda a mejorar su concentración y rendimiento.

5. Usar la tecnología de manera creativa y educativa
No todo el uso de la tecnología tiene que estar relacionado con el entretenimiento. Los padres pueden fomentar el uso de herramientas digitales para **proyectos creativos**, como la edición de videos, la fotografía, el aprendizaje de nuevas habilidades a través de tutoriales en línea o el uso de aplicaciones educativas que refuercen lo aprendido en la escuela.

Herramientas para gestionar el tiempo de pantalla

Hoy en día, existen múltiples herramientas que permiten a los padres **monitorear y controlar** el tiempo que los niños pasan frente a la pantalla. Algunas opciones incluyen:

- **Apple Screen Time**: Permite a los padres supervisar el uso de dispositivos, establecer límites de tiempo para aplicaciones específicas y programar períodos de desconexión.
- **Google Family Link**: Ofrece funciones similares en dispositivos Android, permitiendo a los padres **supervisar y limitar** el uso de aplicaciones y establecer límites diarios.
- **Microsoft Family Safety**: Ofrece un control exhaustivo del tiempo de uso en consolas de videojuegos y dispositivos con Windows, además de permitir el bloqueo de contenido inapropiado.

Incentivar el auto-gestión del tiempo

A medida que los niños crecen, es importante que aprendan a **gestionar su propio tiempo** de manera responsable. Los padres pueden enseñar a los niños y adolescentes a **autocontrolar su uso de la tecnología** estableciendo metas personales y revisando su progreso. Por ejemplo, animar a los niños a tomar descansos durante el uso de la tecnología o a utilizar aplicaciones que ayuden a mejorar su concentración.

Equilibrar la tecnología y la vida familiar

es importante que la tecnología no se convierta en el centro de la vida familiar. Los padres pueden crear **momentos de desconexión colectiva** donde todos los miembros de la familia guarden sus dispositivos y se dediquen a actividades conjuntas. Estas actividades pueden ser tan simples como una caminata al aire libre, cocinar juntos o ver una película, siempre y cuando no estén distraídos por teléfonos o tablets.

07 Cómo hablar con los niños sobre los riesgos en línea

Cómo hablar con los niños sobre los riesgos en línea

07

Hablar con los niños sobre los **riesgos en línea** puede ser un desafío, pero es crucial para garantizar su seguridad digital. Los niños deben saber que, aunque Internet ofrece innumerables oportunidades, también puede ser un espacio peligroso si no se usa con precaución. La mejor manera de proteger a los niños es **fomentar la comunicación abierta y constante** sobre sus experiencias en línea, para que se sientan cómodos acudiendo a sus padres ante cualquier problema.

Crear un entorno de confianza

Antes de iniciar una conversación sobre los riesgos en línea, es fundamental que los niños se sientan **seguros y confiados** para hablar de sus experiencias en Internet sin temor a represalias o castigos. Los padres deben evitar reaccionar de manera desproporcionada si los niños comparten algo incómodo o preocupante. En su lugar, deben **escuchar activamente** y asegurarse de que sus hijos comprendan que pueden acudir a ellos sin miedo, pase lo que pase.

- **Evitar el miedo excesivo**: Es importante que los niños comprendan los riesgos, pero sin sentir pánico. El objetivo es que sepan reconocer situaciones peligrosas y que actúen de manera adecuada sin dejarse paralizar por el miedo.
- **Fomentar preguntas**: Los padres deben animar a los niños a hacer preguntas sobre lo que les preocupa o lo que no entienden. Esto permite aclarar dudas y adaptar el nivel de la conversación a la edad y madurez del niño.

Temas claves a tratar

al hablar sobre los riesgos en línea, es útil abordar varios temas fundamentales para que los niños comprendan los peligros más comunes y cómo evitarlos:

1. **Ciberacoso:**
Explicar que el ciberacoso ocurre cuando alguien usa la tecnología para **molestar, insultar o intimidar** a otra persona. Los niños deben saber que el ciberacoso es serio y que no deben participar en este tipo de comportamiento, ni tolerarlo si son víctimas. Enséñales a **guardar pruebas**, bloquear al acosador y a reportar el comportamiento a un adulto de confianza.

2. **Privacidad y compartir información personal**
Enseñar a los niños la importancia de proteger su información personal, como su dirección, teléfono, escuela o fotos. Explicarles que deben **evitar compartir** esta información con desconocidos o en sitios públicos, ya que podría ser utilizada de manera indebida. También es importante enseñarles a **configurar la privacidad** en sus redes sociales.

3. **Grooming:**
El grooming es cuando un adulto se hace pasar por un amigo o alguien de confianza para **manipular o engañar** a un niño en línea. Explica que deben **nunca aceptar solicitudes de amistad** de personas que no conocen en la vida real y **nunca compartir información personal** o quedar con alguien que han conocido en línea sin la supervisión de un adulto.

4. Contenido inapropiado:
Los niños pueden encontrarse accidentalmente con **contenido inapropiado** en Internet, como violencia o material sexual. Es crucial que sepan **qué hacer si ven algo que les hace sentir incómodos**: cerrar la página, no compartirlo, y contárselo a un adulto inmediatamente. Dejar claro que no serán castigados por encontrarse con este tipo de contenido refuerza la confianza.

5. Estafas y fraudes:
Los niños deben estar alerta ante **ofertas demasiado buenas para ser verdad** o solicitudes de información personal a través de correos electrónicos o mensajes de personas desconocidas. Explicarles el concepto de **phishing** y enseñarles a no hacer clic en enlaces sospechosos ni proporcionar datos personales a extraños en línea.

Escuchar sus experiencias

Parte importante de la conversación sobre los riesgos en línea es **escuchar** lo que los niños tienen que decir sobre sus propias experiencias. Preguntarles qué sitios visitan, con quiénes hablan en línea y si alguna vez han visto algo que los haya hecho sentir incómodos es fundamental para mantener una buena comunicación. Si los padres demuestran interés y empatía, es más probable que los niños se abran y confíen en ellos cuando enfrenten una situación difícil.

Estrategias para hablar con niños de diferentes edades

- **Niños pequeños (5-8 años)**: Mantén la conversación simple, utilizando ejemplos concretos y enseñándoles conceptos básicos como **no hablar con extraños en línea** y **pedir ayuda si ven algo que no entienden**.
- **Pre-adolescentes (9-12 años)**: A esta edad, los niños comienzan a utilizar las redes sociales y aplicaciones de mensajería. Es importante hablar sobre la **privacidad**, el **respeto en línea** y el **ciberacoso**, y asegurarse de que entiendan cómo configurar correctamente la seguridad de sus cuentas.
- **Adolescentes (13-17 años)**: Los adolescentes necesitan conversaciones más avanzadas sobre temas como **grooming**, **estafas en línea** y **presión social** en redes sociales. Asegúrate de que entiendan los riesgos de compartir demasiada información y cómo manejar situaciones incómodas o peligrosas.

08 Promover una comunicación abierta y sostenida

08

Una de las mejores formas de proteger a los niños en el entorno digital es **mantener una comunicación abierta y continua** sobre lo que experimentan en línea. La tecnología evoluciona rápidamente, y con ella, los riesgos y oportunidades. Por eso, es fundamental que los padres mantengan una conversación constante con sus hijos sobre su uso de Internet, las redes sociales, los juegos en línea y cualquier inquietud que puedan tener.

La importancia de la comunicación abierta

La comunicación es clave para que los niños se sientan cómodos compartiendo sus experiencias en línea, incluyendo aquellas que les preocupan o incomodan. Muchas veces, los niños pueden dudar en contar a sus padres sobre un problema en línea por temor a ser castigados, restringidos o incomprendidos. Para evitar esta barrera, los padres deben asegurarse de que sus hijos sepan que pueden acudir a ellos sin miedo, y que **escucharán antes de juzgar**.

1. **Generar un ambiente de confianza:**
   - Los niños deben sentirse seguros para hablar sobre sus actividades en línea. Los padres deben crear un espacio donde los niños puedan expresar sus preocupaciones, errores o dudas sin temor a represalias.
   - Es importante **evitar reacciones exageradas** cuando los niños confiesan algo relacionado con un riesgo en línea. La mejor estrategia es mantener la calma y ayudarles a resolver la situación, en lugar de simplemente castigar.

2. **Conversaciones regulares:**
   - En lugar de tener una única “charla” sobre los riesgos de Internet, los padres deben incorporar conversaciones sobre el uso de la tecnología en la vida diaria. Preguntar regularmente sobre lo que están haciendo en línea, a qué juegos juegan, con quién hablan y si alguna vez se han sentido incómodos en la web.
   - Además de hablar sobre los riesgos, los padres también pueden **interesarse en los intereses digitales** de sus hijos, ya que esto ayuda a que las conversaciones sobre tecnología se sientan más naturales y menos como una “lección”.

3. **Escuchar activamente:**
   - La comunicación no solo consiste en hablar, sino también en **escuchar activamente** a los hijos. Cuando un niño comparte algo sobre sus experiencias en línea, los padres deben asegurarse de que están prestando atención y respondiendo con comprensión y apoyo.

4. **Reforzar que siempre pueden pedir ayuda:**
   - Los niños deben saber que, ante cualquier situación que les cause incomodidad o miedo en línea, **siempre pueden acudir a sus padres** para pedir ayuda. Los padres deben reforzar que no serán castigados por encontrarse en situaciones difíciles, como haber visto contenido inapropiado o haber sido contactados por desconocidos.

08

Fomentar el diálogo en lugar de imponer normas

el diálogo es más eficaz que las reglas rígidas sin explicación. Los padres deben enseñar a sus hijos **por qué es importante** seguir ciertas normas, como no compartir información personal o evitar interactuar con desconocidos en redes sociales. Cuando los niños comprenden los **motivos detrás de las reglas**, es más probable que las sigan y las respeten.

Herramientas para facilitar la comunicación

existen varias estrategias y herramientas que pueden facilitar la comunicación entre padres e hijos sobre el uso de la tecnología:

1. **Revisión conjunta de la actividad en línea**
   - Los padres pueden sentarse con sus hijos para **revisar las configuraciones de privacidad** de sus redes sociales, discutir las personas con las que interactúan y revisar los sitios web que visitan. Hacer esto de manera colaborativa genera un ambiente de confianza y aprendizaje mutuo.

2. **Aplicaciones de control parental**
   - Además de proporcionar supervisión, las **herramientas de control parental** pueden ser una excelente manera de iniciar conversaciones sobre el uso de la tecnología. Los padres pueden usar estas herramientas como una oportunidad para explicar por qué ciertas restricciones están en su lugar y cómo estas protegen a los niños de riesgos.

Hablar sobre las consecuencias del mal uso de la tecnología

Es importante que los niños entiendan que sus acciones en línea tienen **consecuencias reales**. Publicar contenido hiriente, participar en ciberacoso o compartir información privada no solo puede dañar a otros, sino que también puede tener repercusiones legales y emocionales para ellos mismos.

Los padres deben explicar que el **comportamiento en línea debe ser responsable**, respetuoso y consciente de las implicaciones a largo plazo. En este sentido, enseñar a los niños a pensar antes de publicar o compartir algo en Internet es crucial para fomentar una **ciudadanía digital responsable**.

Cómo actuar ante problemas en línea

Aunque se tomen todas las precauciones, es posible que los niños enfrenten problemas en línea, como el **ciberacoso**, el acceso a **contenido inapropiado** o la **suplantación de identidad**. Saber **cómo actuar** ante estas situaciones es crucial para proteger a los niños y reducir el impacto emocional que puedan tener.

Primeros pasos al enfrentarse a un problema en línea

1. Mantén la calma

Si los niños encuentran algo que los asusta o los hace sentir incómodos, deben aprender a **mantener la calma** y no reaccionar impulsivamente. Es natural sentir miedo o ansiedad, pero es importante recordar que hay formas efectivas de resolver el problema.

2. Cerrar la página o aplicación

Si se encuentran con contenido inapropiado o reciben mensajes ofensivos, lo mejor es **cerrar inmediatamente la página o aplicación**. Esto ayuda a cortar el contacto con la fuente del problema y evita que los niños se sientan abrumados.

3. No responder a mensajes ofensivos

Si los niños reciben mensajes de acoso o intimidación, es importante que **no respondan**. Responder puede alimentar el comportamiento del acosador y empeorar la situación. En lugar de interactuar, deben bloquear al acosador y reportar la situación a un adulto de confianza.

4. Guardar pruebas

Si el problema involucra acoso, grooming o algún otro tipo de comportamiento inapropiado, los niños deben aprender a **guardar pruebas** del incidente, como capturas de pantalla de los mensajes, publicaciones o correos electrónicos que les hayan enviado. Estas pruebas serán útiles para reportar el problema a las autoridades correspondientes.

Hablar con un adulto de confianza

Es fundamental que los niños sepan que **nunca deben manejar estos problemas solos**. Deben acudir a un adulto de confianza, ya sea un padre, un maestro o un tutor, y explicar la situación. Los padres deben asegurarse de que sus hijos entiendan que **no están solos** y que siempre habrá alguien dispuesto a ayudarles.

- **Fomentar la confianza**: Los niños pueden temer que, al contar un problema en línea, serán castigados o perderán el acceso a sus dispositivos. Los padres deben reforzar la idea de que no serán penalizados por pedir ayuda, sino que recibirán el apoyo necesario para solucionar el problema.

Reportar el incidente

Casi todas las plataformas de redes sociales, juegos en línea y aplicaciones tienen **herramientas para reportar** el comportamiento inapropiado o el contenido ofensivo. Enseñar a los niños cómo reportar estos incidentes es fundamental:

- **Reportar ciberacoso**: Las redes sociales y plataformas de mensajería permiten denunciar cuentas que hostigan o acosan. Al hacerlo, la plataforma puede investigar y tomar medidas como suspender la cuenta del acosador.
- **Bloquear al agresor**: Además de reportar el comportamiento, los niños deben aprender a **bloquear** a las personas que los acosan o envían mensajes inapropiados, para evitar cualquier contacto futuro.
- **Eliminar publicaciones inapropiadas**: Si los niños publicaron algo por error o fueron etiquetados en contenido inapropiado, deben saber cómo eliminar o solicitar la eliminación de esas publicaciones.

Buscar ayuda especializada

En casos más graves, como el **grooming** o el **robo de identidad**, puede ser necesario contactar a profesionales, como la policía o especialistas en ciberseguridad. En muchos países, hay organizaciones especializadas que ofrecen **ayuda y asesoramiento** para enfrentar estos problemas:

- **Líneas de ayuda para ciberacoso y seguridad digital**: Muchas organizaciones, como **Pantallas Amigas** o **INCIBE**, tienen líneas de ayuda confidenciales para asesorar a familias y niños sobre cómo actuar ante estos problemas en línea.
- **Coordinadores escolares de bienestar**: En muchos colegios, existen coordinadores de bienestar encargados de ayudar a los estudiantes en situaciones de acoso, tanto en línea como fuera de línea.

Recuperar el control emocional

Una vez que se ha abordado el problema, es importante ayudar a los niños a **recuperar el control emocional** y procesar lo sucedido. El acoso y otros problemas en línea pueden dejar a los niños sintiéndose asustados, inseguros o ansiosos. Los padres deben:

- **Brindar apoyo emocional**: Escuchar a los niños y validar sus emociones es esencial para que se sientan seguros y comprendidos. Ofrecerles apoyo sin juicio es clave para ayudarlos a superar el impacto de la experiencia.
- **Enseñarles estrategias de autocuidado**: Animar a los niños a realizar actividades que les gusten, como leer, hacer deporte o pasar tiempo con amigos y familiares, puede ayudar a distraerlos y recuperar la sensación de normalidad.

10 Conclusión: el rol de las familias en la educación digital

Conclusión: el rol de las familias en la educación digital

10

El entorno digital ofrece a los niños innumerables oportunidades para aprender, conectarse y divertirse, pero también presenta riesgos que pueden ser difíciles de manejar sin la guía adecuada. Es aquí donde las familias juegan un papel **fundamental**. Al proporcionar un entorno donde la tecnología se utiliza de manera segura y responsable, los padres pueden ayudar a sus hijos a **desarrollar las habilidades necesarias** para navegar por el mundo digital con confianza y seguridad.

La importancia de la educación continua

el aprendizaje sobre la seguridad en línea no es una conversación que ocurre una sola vez. A medida que los niños crecen, cambian las plataformas que usan y los riesgos a los que están expuestos. Los padres deben **mantenerse informados y actualizados** sobre las nuevas amenazas en línea, como aplicaciones emergentes, tendencias de ciberacoso o nuevas estrategias de grooming, para estar siempre preparados.

Crear un entorno familiar seguro

las familias deben trabajar juntas para crear un ambiente donde todos los miembros de la casa comprendan la importancia de la **seguridad y el respeto en línea**. Esto incluye:

- **Normas claras y coherentes** sobre el uso de la tecnología.
- Promover la **empatía y el respeto** hacia los demás, tanto en línea como fuera de línea.

Mantener una **comunicación abierta** para que los niños se sientan cómodos acudiendo a sus padres en caso de dudas o problemas en línea.

Empoderar a los niños

una de las principales metas de esta guía es **empoderar a los niños** para que se conviertan en **ciudadanos digitales responsables**. Al enseñarles sobre los riesgos en línea, cómo proteger su privacidad, cómo actuar ante problemas y la importancia del respeto y la empatía, los padres les brindan las herramientas necesarias para navegar de manera segura y confiada por el mundo digital.

La tecnología como aliada, no enemiga

Aunque esta guía pone mucho énfasis en los riesgos, la tecnología no debe ser vista como un enemigo. Es una herramienta poderosa que, utilizada de manera adecuada, puede enriquecer la vida de los niños, proporcionarles acceso a recursos educativos de calidad y facilitar la comunicación con amigos y familiares. **El objetivo no es prohibir, sino guiar, acompañar y en definitiva navegar juntos**.

UAM
Universidad Autónoma
de Madrid
foredu
EDI
EDUCACIÓN DIGITAL E INNOVACIÓN
SAMSUNG