

WHITEPAPER
**Tecnología al Servicio
de la Infancia:
Corresponsabilidad y
Evidencias**

Contenidos

1	Resumen Ejecutivo	pag. 03
2	Introducción y contexto	pag. 05
2.1	Objeto y enfoque del documento	pag. 06
2.2	Contexto de uso digital en la infancia	pag. 07
2.3	Uso de plataformas y servicios digitales	pag. 09
2.4	Riesgos, preocupaciones y percepción social	pag. 13
3	Posición de AMETIC	pag. 15
3.1	La tecnología como parte de la solución	pag. 16
3.2	Principios clave del sector	pag. 17
4	Evidencias: capacidades y desarrollos del sector tecnológico	pag. 20
4.1	Nivel de madurez del sector	pag. 21
4.2	Soluciones tecnológicas desplegadas	pag. 23
4.3	Educación y sensibilización	pag. 26
4.4	Buenas prácticas identificadas	pag. 29
4.5	Brechas y retos identificados	pag. 31
5	Corresponsabilidad en la protección de los menores	pag. 32
5.1	La protección de los menores como responsabilidad compartida	pag. 33
5.2	Principios para una actuación efectiva	pag. 35
6	Recomendaciones	pag. 36
6.1	Impulsar un modelo integral basado en la corresponsabilidad	pag. 37
6.2	Reforzar la educación y alfabetización digital	pag. 37
6.3	Favorecer la adopción efectiva de herramientas de protección	pag. 38
6.4	Impulsar la innovación para la protección de menores	pag. 38
6.5	Promover una regulación armonizada y basada en evidencia	pag. 39
7	Conclusiones	pag. 40
8	Fuentes y referencias	pag. 43

01

RESUMEN EJECUTIVO



01

La tecnología forma parte de la vida cotidiana de niños, niñas y adolescentes y constituye un espacio esencial para el aprendizaje, la socialización, la creatividad y el ejercicio de derechos relacionados con la educación, la información y la participación.

02

Los estudios analizados muestran una **elevada digitalización de la infancia y la adolescencia en España**, caracterizada por un acceso cada vez más temprano a dispositivos y servicios digitales y por un uso intensivo de plataformas y aplicaciones en múltiples ámbitos de la vida cotidiana.

03

Junto a las oportunidades que ofrece la tecnología, **existen riesgos reales relacionados** con la exposición a contenidos inapropiados, el ciberacoso, las interacciones con desconocidos, la privacidad, el bienestar emocional y determinados usos problemáticos de los servicios digitales.

04

La existencia de riesgos no implica necesariamente la materialización de daños. La mayoría de los menores utiliza la tecnología de forma habitual para aprender, relacionarse y desarrollar competencias, lo que exige **respuestas equilibradas basadas en la gestión de riesgos y no únicamente en la restricción del acceso**.

05

La evidencia disponible muestra que la protección efectiva de los menores depende tanto de las herramientas tecnológicas como del acompañamiento familiar, la educación digital, el pensamiento crítico y el desarrollo de hábitos saludables de uso.

06

Las empresas tecnológicas han incorporado de forma creciente medidas de protección mediante enfoques de privacy by design y safety by design, desarrollando controles parentales, sistemas de verificación de edad, herramientas de moderación de contenidos, configuraciones seguras y mecanismos de gestión de riesgos.

07

No obstante, **persiste una brecha significativa entre la disponibilidad de estas soluciones y su utilización efectiva** por parte de familias y menores, lo que pone de manifiesto la necesidad de reforzar la difusión, la formación y el acompañamiento.

08

La educación digital, la alfabetización mediática y el desarrollo de competencias críticas deben considerarse elementos centrales de cualquier estrategia de protección de la infancia en los entornos digitales.

09

La protección de los menores requiere un modelo de **corresponsabilidad** que implique de forma coordinada a administraciones públicas, familias, sistema educativo, sector tecnológico y sociedad civil, evitando trasladar la responsabilidad exclusivamente a un único actor.

10

Las políticas públicas deben promover un enfoque basado en evidencia, proporcionalidad, innovación y armonización regulatoria, combinando protección, capacitación y desarrollo tecnológico para garantizar que los menores puedan beneficiarse de las oportunidades de la sociedad digital de forma segura y responsable.

02

INTRODUCCIÓN Y CONTEXTO





2.1

OBJETO Y ENFOQUE DEL DOCUMENTO

La protección de niños, niñas y adolescentes en los entornos digitales se ha convertido en una de las principales prioridades sociales, educativas y regulatorias de los últimos años. La creciente digitalización de la sociedad, el acceso cada vez más temprano a dispositivos conectados y la incorporación de nuevas tecnologías y servicios digitales al día a día de los menores han intensificado el debate sobre cómo garantizar un entorno digital seguro, inclusivo y beneficioso para su desarrollo.

En este contexto, el presente documento tiene como finalidad contribuir al análisis de la protección de los menores en los entornos digitales desde una perspectiva amplia y constructiva, identificando tanto los riesgos y desafíos existentes como las oportunidades que ofrece la tecnología para el aprendizaje, la creatividad, la participación y el desarrollo personal. Asimismo, pretende aportar evidencias sobre las capacidades y soluciones que el sector tecnológico ya está desplegando para reforzar la seguridad y el bienestar de los menores.

El alcance del documento se centra en la interacción de niños, niñas y adolescentes con los servicios, plataformas y tecnologías digitales, prestando especial atención a aspectos relacionados con la seguridad, la privacidad, el bienestar digital, la educación, la participación familiar y la prevención de riesgos. El documento analiza igualmente el papel desempeñado por los diferentes actores implicados —administraciones públicas, sector tecnoló-

gico, familias, sistema educativo y sociedad civil— y la necesidad de avanzar hacia modelos de actuación basados en la corresponsabilidad.

El análisis se realiza desde un enfoque basado en la evidencia, apoyándose en estudios y fuentes de referencia nacionales e internacionales, entre ellos los informes elaborados por UNICEF, ONTSI-Red.es, Google y Fundación Fad Juventud y Amazon, así como en los resultados de la encuesta realizada entre empresas asociadas a AMETIC. Este enfoque permite fundamentar las conclusiones y recomendaciones en datos contrastados y en experiencias reales, evitando visiones simplificadas de un fenómeno complejo y en constante evolución.

Partiendo de esta base, el documento defiende la necesidad de abordar la protección de los menores desde una perspectiva equilibrada que combine protección y oportunidades, innovación y seguridad, derechos y responsabilidades. El objetivo último es contribuir a la construcción de un ecosistema digital que permita a los menores aprovechar plenamente los beneficios de la transformación digital minimizando al mismo tiempo los riesgos asociados a ella.



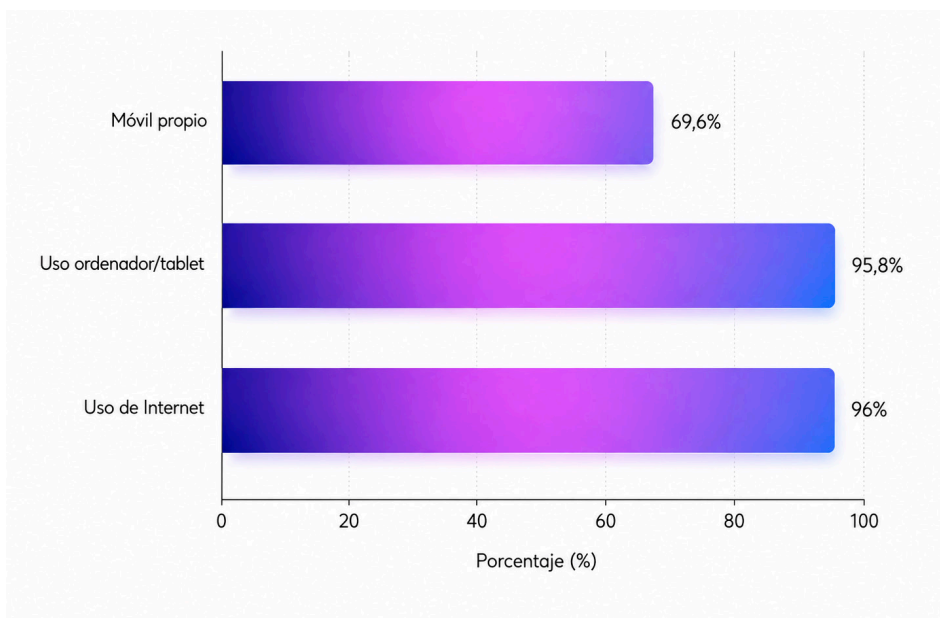
2.2

CONTEXTO DE USO DIGITAL EN LA INFANCIA

La transformación digital se ha convertido en uno de los procesos más relevantes de las últimas décadas, modificando profundamente la manera en que las personas se relacionan, acceden a la información, consumen contenidos, aprenden, trabajan y participan en la sociedad. La conectividad, los dispositivos digitales y las plataformas en línea forman parte ya de la vida cotidiana de millones de personas y constituyen infraestructuras esenciales para el desarrollo económico, social y cultural. En este contexto, la infancia y la adolescencia no permanecen ajenas a esta realidad, sino que crecen y se desarrollan en un entorno cada vez más digitalizado en el que las tecnologías están presentes desde edades tempranas.

La digitalización forma parte del entorno cotidiano de la infancia y adolescencia en España. Según el informe **“Uso de la tecnología en la infancia y adolescencia”** de ONTSI-Red.es, el **96% de los menores utiliza Internet, el 95,8% utiliza ordenador o tableta y el 69,6% dispone de teléfono móvil**, evidenciando una penetración prácticamente universal de las tecnologías digitales entre la población menor de edad¹.

Acceso a tecnologías por menores (%)

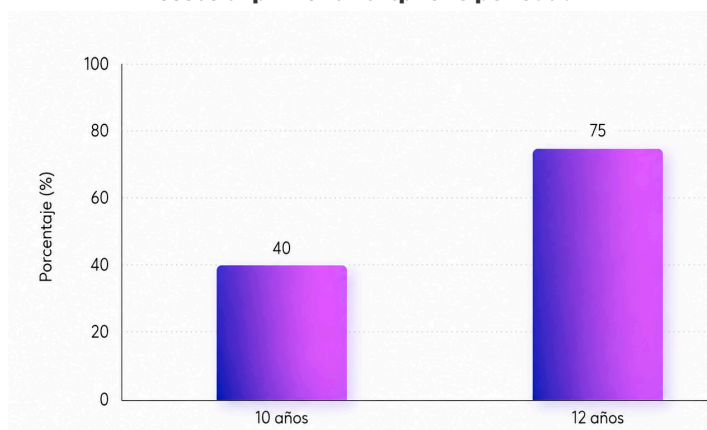


ONTSI - Red.es (2025). Uso de las tecnologías por niños, niñas y adolescentes en España.

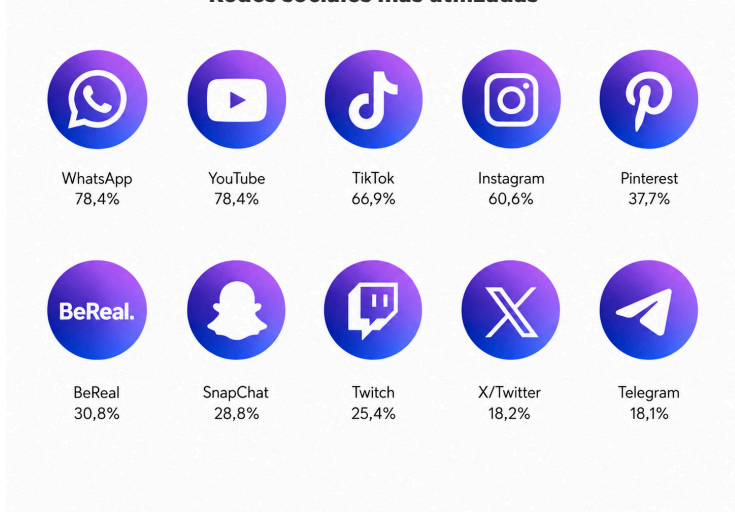
Los datos muestran además una incorporación cada vez más temprana a los entornos digitales. Según UNICEF España, el **41% de los menores dispone de teléfono móvil a los 10 años**, porcentaje que alcanza el **76% a los 12 años**, situándose la edad media de acceso al primer smartphone en torno a los **10,8 años**².

Esta presencia temprana se acompaña de una intensa actividad en redes y plataformas digitales. UNICEF señala que el **92,5% de los adolescentes tiene presencia en al menos una red social** y que el **75,8% participa en tres o más plataformas simultáneamente**, consolidando los espacios digitales como entornos habituales de relación, aprendizaje y participación.

Acceso al primer smartphone por edad



Redes sociales más utilizadas



UNICEF España. Infancia, adolescencia y bienestar digital. Una aproximación desde el bienestar integral.

Desde una perspectiva de bienestar, los estudios destacan que la tecnología constituye hoy un entorno donde los menores ejercen derechos fundamentales relacionados con la educación, el acceso a la información y la participación social. Los entornos digitales ofrecen oportunidades significativas para el aprendizaje, el desarrollo de competencias digitales, la creatividad, la expresión personal y el acceso a recursos educativos y culturales.

Por ello, el debate ya no se centra en el acceso, sino en cómo garantizar experiencias digitales seguras, equilibradas y orientadas al desarrollo integral de niños y adolescentes.

Al mismo tiempo, ONTSI advierte que persisten diferencias asociadas al contexto socioeconómico y al nivel de acompañamiento familiar, lo que pone de manifiesto que la brecha digital ya no se define únicamente por el acceso, sino también por la capacidad para realizar un uso seguro, crítico y beneficioso de la tecnología. Del mismo modo, la creciente presencia de dispositivos conectados y servicios digitales en la vida de los menores plantea nuevos desafíos relacionados con la privacidad, la seguridad, la gestión del tiempo de uso y la exposición a riesgos en línea.

Los datos de estos informes, así como el enfoque de bienestar digital planteado por 3202, la protección de los menores en entornos digitales debe abordarse desde una perspectiva integral que combine seguridad, acompañamiento, educación y participación. Este enfoque implica la actuación coordinada de familias, centros educativos, administraciones públicas y sector tecnológico para garantizar que los menores puedan beneficiarse de las oportunidades que ofrece la tecnología de forma segura y acorde con su desarrollo.



2.3

USO DE PLATAFORMAS Y SERVICIOS DIGITALES

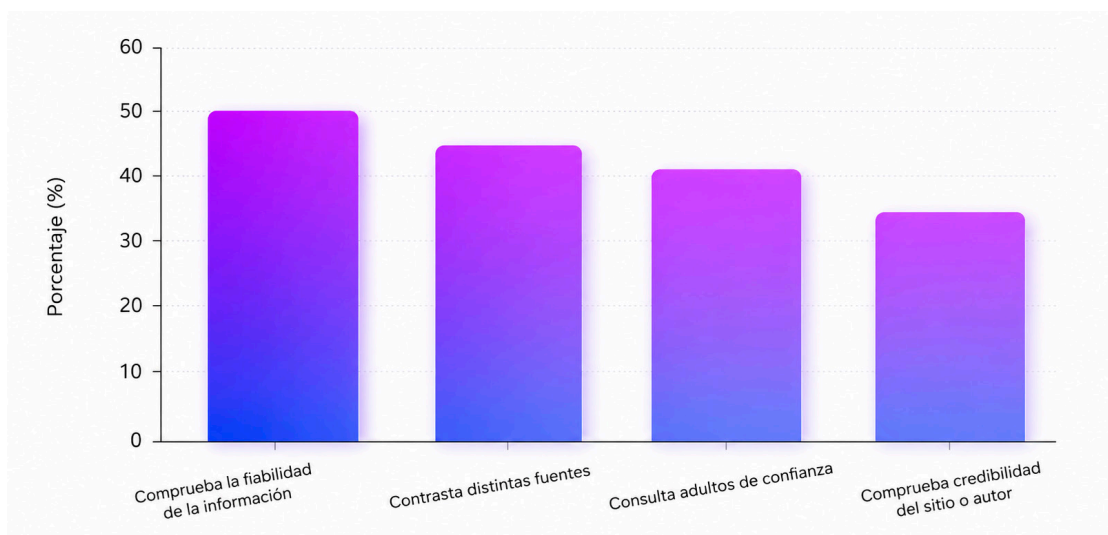
Tras constatar la amplia presencia de la tecnología en la vida cotidiana de niños, niñas y adolescentes, resulta necesario analizar cómo utilizan estos entornos digitales y cuál es la percepción que tienen sobre su propia experiencia digital. Comprender los hábitos de uso resulta fundamental para disponer de una visión completa del fenómeno y para identificar tanto las oportunidades como los desafíos asociados al entorno digital.

Los estudios analizados muestran que la relación de los menores con la tecnología es cada vez más diversa y compleja. El entorno digital constituye un espacio de socialización, aprendizaje, entretenimiento, creatividad y participación, en el que los adolescentes desarrollan buena parte de sus actividades diarias.

En este contexto, el estudio **The Future Report** de Google refleja una elevada adopción de tecnologías emergentes entre los jóvenes. Entre el **91% y el 96% de los adolescentes afirma haber utilizado herramientas de inteligencia artificial durante el último año**, principalmente para el aprendizaje, la realización de tareas escolares y actividades creativas³.

Asimismo, el estudio apunta al desarrollo de determinadas competencias digitales, ya que el **50% afirma comprobar habitualmente la fiabilidad de la información que consulta**, mientras que el **45% contrasta distintas fuentes**, el **41% recurre a personas adultas de confianza** para validar contenidos o resolver dudas y el 34% comprueba la credibilidad del sitio web o del autor. Estos datos sugieren una creciente incorporación de prácticas asociadas al pensamiento crítico y a la alfabetización mediática.

Competencias de verificación de información



Fuente: **Google & Livity (2025)**. The Future Report Spain 2025. Google Safety Engineering Center, 2025

Los resultados también ofrecen información relevante sobre cómo perciben los propios adolescentes su relación con la tecnología. El **68% considera que mantiene un equilibrio adecuado entre su vida online y offline**, y el **77% afirma gestionar correctamente sus hábitos digitales**. Estos datos sugieren que una parte importante de los jóvenes percibe la tecnología como una herramienta integrada de forma natural en su vida cotidiana y no necesariamente como un elemento que interfiera en otras actividades.

No obstante, esta percepción debe analizarse junto con otros indicadores disponibles. Los estudios de UNICEF muestran que el uso de dispositivos y servicios digitales ocupa una parte muy significativa del tiempo diario de los adolescentes. La elevada presencia en redes sociales, plataformas de mensajería y espacios de consumo audiovisual revela que la actividad digital constituye uno de los principales ámbitos de interacción y ocio de los jóvenes. Asimismo, UNICEF advierte de que determinados patrones de uso intensivo pueden relacionarse con efectos negativos sobre aspectos como la calidad del sueño, la gestión del tiempo, la actividad física, el bienestar emocional o las relaciones sociales presenciales.

Por tanto, los datos dibujan una realidad compleja. Por un lado, los adolescentes perciben la tecnología como una herramienta integrada de forma natural en su vida cotidiana y consideran que gestionan adecuadamente su uso. Por otro, la evidencia disponible señala la necesidad de seguir promoviendo hábitos digitales saludables que permitan maximizar los beneficios asociados a la tecnología y reducir potenciales efectos negativos derivados de un uso excesivo o inadecuado.

El papel de las familias

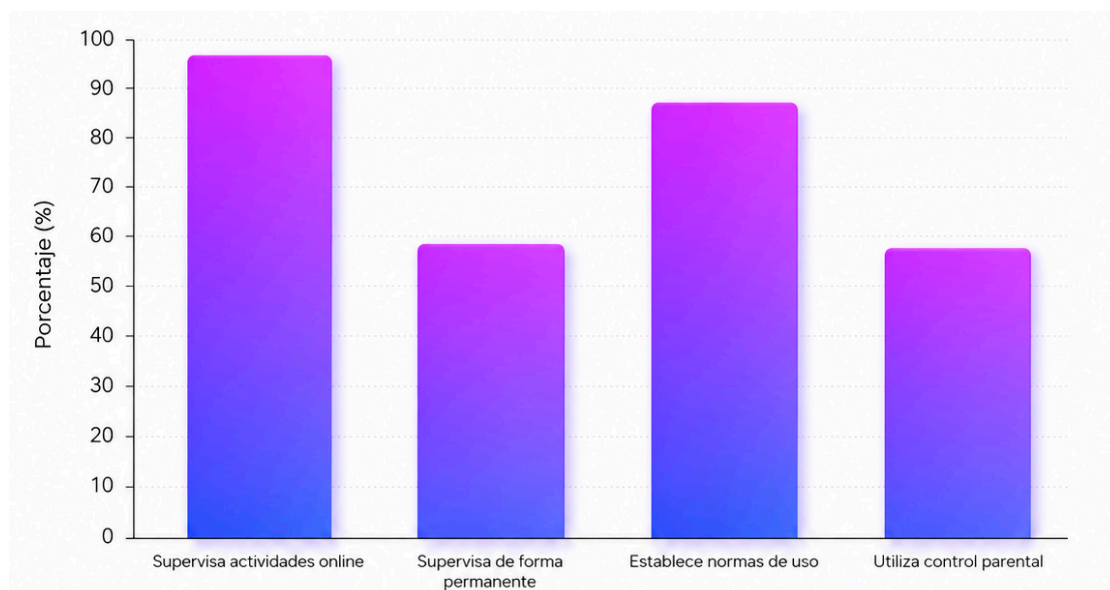
La evidencia analizada muestra que las familias continúan desempeñando un papel fundamental en la educación, supervisión y acompañamiento de niños, niñas y adolescentes en el entorno digital. En un contexto caracterizado por una presencia cada vez más temprana e intensa de la tecnología en la vida cotidiana de los menores, el entorno familiar constituye el principal espacio donde se establecen hábitos de uso, normas de comportamiento y criterios para afrontar los riesgos y oportunidades asociados al mundo digital.

Según Google, el **44% de los adolescentes identifica a padres y familiares como su principal fuente de confianza** para abordar cuestiones relacionadas con el entorno digital, mientras que el **46% afirma apoyarse en ellos para gestionar hábitos y comportamientos digitales**. Sin embargo, estos datos también po-

nen de manifiesto que más de la mitad de los adolescentes no sitúa a sus familias como referencia principal, lo que evidencia la coexistencia de diferentes modelos de acompañamiento y distintos niveles de implicación familiar.

En paralelo, el estudio de **Fundación Fad Juventud y Amazon** muestra que las familias mantienen una participación en la supervisión de las actividades digitales de sus hijos. El informe señala que aproximadamente el **98% de las familias supervisa las actividades de consumo online de los menores**, y que el **59% afirma hacerlo de manera sistemática o permanente**, porcentajes significativamente superiores a los observados en las actividades de compra realizadas en entornos físicos.

Papel de las familias en el entorno digital

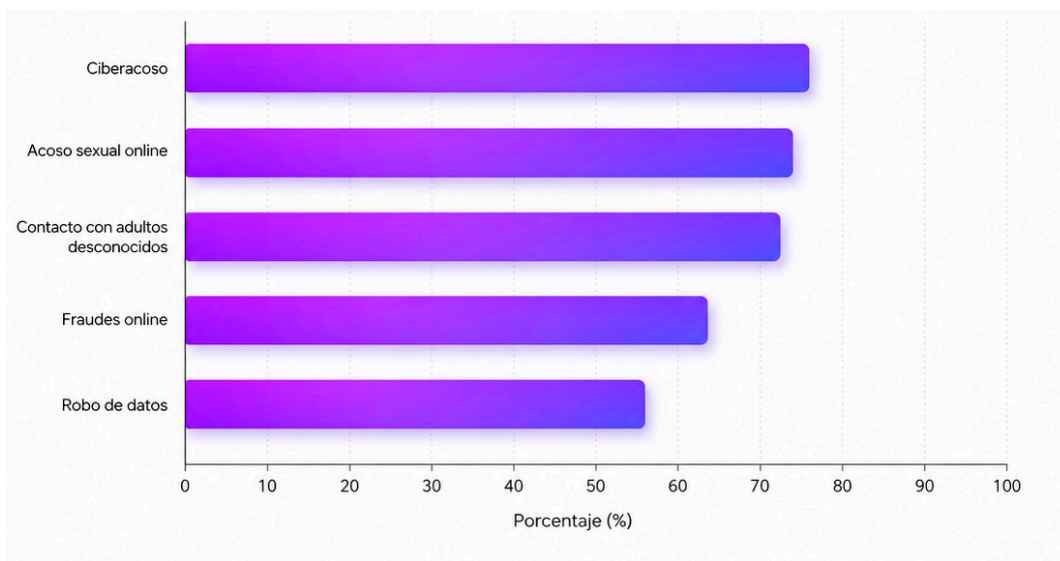


Fuente: **Google & Livity (2025)**. The Future Report Spain 2025. Google Safety Engineering Center, 2025

Asimismo, el estudio evidencia que el acompañamiento familiar no se limita exclusivamente al control. El **87,4% de las familias establece normas relacionadas con el uso de Internet y las actividades digitales**, mientras que el **58,7% utiliza herramientas de control parental** para gestionar determinados aspectos del acceso a contenidos o servicios digitales. Estos datos muestran que la mayoría de los hogares combina medidas tecnológicas con estrategias educativas y de supervisión directa.

Las preocupaciones manifestadas por las familias son coherentes con los riesgos identificados en otros estudios. Según Fundación Fad Juventud y Amazon, los aspectos que generan mayor inquietud son el **ciberacoso (76,9%)**, el **contacto con personas adultas desconocidas (76,2%)** y los **fraudes o estafas online (75,9%)**. Por su parte, ONTSI identifica también el acceso a contenidos inapropiados y las interacciones potencialmente peligrosas como algunas de las principales preocupaciones relacionadas con el uso de Internet por parte de los menores.

Principales preocupaciones de las familias



Fuente: Fundación Fad Juventud y Amazon (2026). Consumo online en familias con hijos e hijas adolescentes

Sin embargo, la evidencia disponible muestra igualmente que el acompañamiento familiar se enfrenta a importantes desafíos. La velocidad a la que evolucionan las plataformas, aplicaciones y servicios digitales dificulta que muchas familias dispongan de conocimientos suficientes para comprender en profundidad los entornos digitales utilizados por sus hijos. Esta situación puede generar diferencias significativas en la capacidad de supervisión y acompañamiento entre hogares, especialmente cuando existen brechas de competencias digitales entre generaciones.

En este sentido, los estudios sugieren que la protección efectiva de los menores no puede descansar exclusivamente en la labor de las familias. Si bien el hogar constituye el primer espacio de acompañamiento y educación digital, resulta necesario complementar esta función mediante la colaboración de centros educativos, administraciones públicas, organizaciones sociales y sector tecnológico. La construcción de un entorno digital seguro requiere, por tanto, un enfoque de corresponsabilidad que proporcione a las familias información, recursos y herramientas que les permitan ejercer de forma efectiva su papel como agentes clave de protección y acompañamiento.



2.4

RIESGOS, PREOCUPACIONES Y PERCEPCIÓN SOCIAL

La evidencia disponible muestra que los riesgos asociados al uso de tecnologías por parte de los menores son diversos y abarcan dimensiones relacionadas con la seguridad, el bienestar emocional, la salud mental, la privacidad y la convivencia digital. Los estudios analizados coinciden en que la experiencia digital de niños y adolescentes se desarrolla en un entorno que combina importantes oportunidades de aprendizaje, participación y relación social, junto con situaciones de riesgo que requieren medidas de prevención y acompañamiento adecuadas.

Entre las principales preocupaciones identificadas por las familias destacan el acceso a contenidos inapropiados, el contacto con desconocidos y el ciberacoso. Según ONTSI, alrededor del 60% de los hogares considera preocupante la posibilidad de que los menores interactúen con personas desconocidas en Internet.¹

Los datos del estudio Fundación Fad Juventud y Amazon muestran una percepción muy similar. Las preocupaciones más mencionadas por las familias son el ciberacoso (76,9%), el contacto con adultos desconocidos (76,2%), el acoso sexual online (76,7%), los fraudes o estafas online (62,3%) y el robo de datos personales o bancarios (57,1%).

Desde la perspectiva de UNICEF, los riesgos se extienden también al ámbito emocional y relacional. El informe destaca cuestiones como la sobreexposición digital, la presión social derivada del uso de redes, la construcción de la identidad digital, la violencia digital entre iguales y la pérdida de determinados hábitos saludables asociados a un uso intensivo de la tecnología.

En relación con la interacción social, UNICEF identifica que el 58,4% de los adolescentes reconoce haber mantenido conversaciones con personas desconocidas a través de Internet, mientras que el 31,3% de quienes mantienen o han mantenido relaciones afectivas declara haber sufrido de forma frecuente situaciones de violencia digital en la pareja. Asimismo, un 25% de los menores manifiesta haber sufrido victimización escolar tradicional y un 8,3% ciber-victimización.

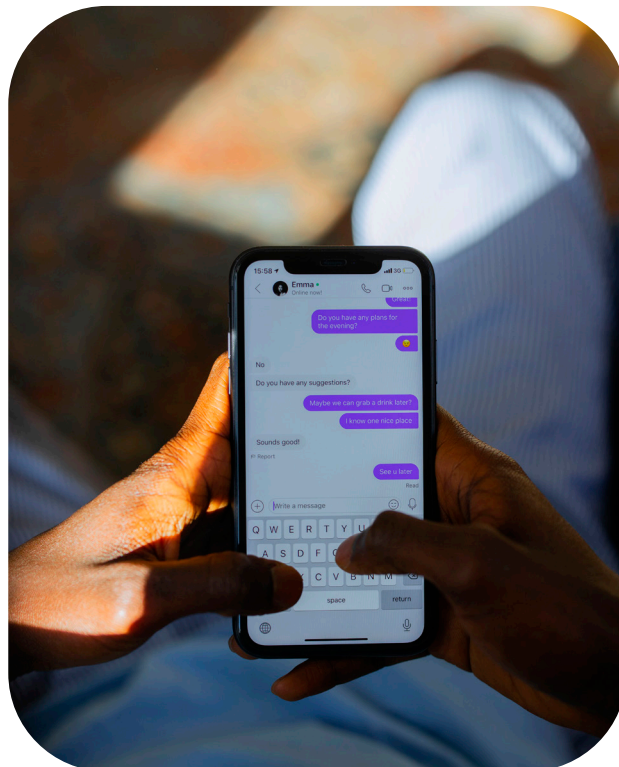


Los riesgos también se proyectan sobre determinados consumos y servicios digitales. Según UNICEF, el 29,6% de los menores ha consumido pornografía alguna vez, con una edad media de primer acceso de 11,58 años; un 7,9% presenta indicadores de consumo problemático. Asimismo, el 53,5% juega a videojuegos al menos una vez por semana, existiendo un 1,7% con posible trastorno asociado a su uso. Por otro lado, un 11,1% reconoce haber realizado apuestas con dinero, de forma presencial u online, identificándose un 2,4% de jugadores problemáticos.

Asimismo, el informe vincula determinadas experiencias digitales con indicadores de bienestar emocional, señalando que un 14,2% de los menores presenta indicadores de malestar emocional, un 13,7% síntomas de ansiedad, un 13,1% síntomas depresivos y un 7,4% muestra situaciones compatibles con riesgo suicida. No obstante, el propio estudio subraya que estos fenómenos son complejos y multifactoriales, por lo que no pueden atribuirse exclusivamente al uso de la tecnología.

Resulta importante señalar que la existencia de riesgos no implica necesariamente la materialización de daños o perjuicios. La mayoría de los menores utiliza diariamente la tecnología sin experimentar consecuencias graves derivadas de su actividad digital y, como muestran los estudios analizados, muchos perciben el entorno digital como un espacio de aprendizaje, relación y desarrollo personal. Sin embargo, la elevada frecuencia de exposición a determinadas situaciones de riesgo, unida a la especial vulnerabilidad de niños, niñas y adolescentes durante su proceso de desarrollo, justifica la adopción de medidas preventivas orientadas a minimizar posibles impactos negativos.

Por otro lado, ONTSI detecta una brecha relevante entre la preocupación de las familias y la adopción efectiva de medidas de protección. Aunque existe un amplio consenso sobre la necesidad de proteger a los menores, el estudio indica que el 23,2% de las familias no utiliza ninguna medida específica de protección digital, mientras que el 94% muestra apoyo a mecanismos como la verificación de edad o los controles parentales. Asimismo, UNICEF señala que únicamente el 30,7% de los progenitores limita los contenidos a los que acceden o suben sus hijos a Internet, aunque también evidencia que determinadas prácticas de mediación familiar pueden reducir significativamente las conductas de riesgo y los usos problemáticos.



En conjunto, la evidencia apunta a que los riesgos no derivan exclusivamente de la tecnología, sino de la interacción entre factores tecnológicos, educativos, familiares y sociales. Por ello, la protección efectiva de los menores requiere enfoques integrales que combinen alfabetización digital, acompañamiento familiar, herramientas tecnológicas, entornos digitales seguros y la colaboración entre administraciones públicas, sistema educativo, familias y sector tecnológico. El objetivo no debe ser restringir las oportunidades que ofrece el entorno digital, sino garantizar que los menores puedan beneficiarse de ellas de forma segura, responsable y acorde con su grado de desarrollo y madurez.

03

POSICIÓN DE AMETIC





3.1

LA TECNOLOGÍA COMO PARTE DE LA SOLUCIÓN

Los datos analizados en los apartados anteriores muestran que la tecnología ocupa un lugar central en la vida de niños, niñas y adolescentes. Los entornos digitales son espacios donde los menores aprenden, se informan, se relacionan, desarrollan su creatividad y ejercen una parte creciente de su participación social. La tecnología representa también una herramienta esencial para el acceso al conocimiento, la reducción de barreras, la inclusión social y el desarrollo de competencias cada vez más relevantes para su futuro personal y profesional. No obstante, junto a estas oportunidades, existen riesgos que deben ser comprendidos, evaluados y abordados adecuadamente. Por ello, resulta necesario impulsar medidas que contribuyan a crear entornos digitales más seguros, favorezcan el bienestar de los menores y les doten de los conocimientos, competencias y herramientas necesarias para desenvolverse de forma responsable, crítica y autónoma en una sociedad cada vez más digitalizada.

Desde esta perspectiva, AMETIC considera que **la tecnología debe entenderse como parte de la solución a los desafíos asociados**

La tecnología debe entenderse como parte de la solución a los desafíos asociados a la protección de los menores en el entorno digital. Los propios estudios analizados muestran que los jóvenes utilizan cada vez más las herramientas digitales para aprender, desarrollar pensamiento crítico, expresarse creativamente y acceder a nuevas oportunidades de formación. El uso generalizado de tecnologías emergentes como la inteligencia artificial para actividades educativas constituye un ejemplo de la capacidad transformadora de estas herramientas cuando son utilizadas de forma adecuada.

Esta visión resulta especialmente relevante en un contexto en el que el debate público se centra con frecuencia en los riesgos asociados al entorno digital. La existencia de dichos riesgos es indiscutible y exige respuestas firmes, pero ello no debe conducir a planteamientos que identifiquen la tecnología como el origen exclusivo de los problemas o que limiten las oportunidades derivadas de su utilización. La evidencia disponible muestra que la realidad es más compleja y requiere respuestas equilibradas

capaces de proteger a los menores sin privarles de las oportunidades que ofrece la sociedad digital.

El sector tecnológico ha desarrollado durante los últimos años un amplio conjunto de soluciones orientadas a reforzar la seguridad de los menores. Herramientas de control parental, configuraciones reforzadas de privacidad, sistemas de moderación de contenidos, limitaciones de determinadas funcionalidades, mecanismos de denuncia y plataformas adaptadas a diferentes edades forman parte ya de muchos servicios y dispositivos utilizados diariamente por millones de familias.

Por ello, AMETIC defiende que la industria tecnológica debe ser considerada un actor comprometido con la protección de la infancia y parte activa en el desarrollo de soluciones eficaces, proporcionales y sostenibles para mejorar la seguridad de los menores en los entornos digitales.





3.2

PRINCIPIOS CLAVE DEL SECTOR

La posición de AMETIC se articula sobre una serie de principios que buscan compatibilizar la protección de los menores con el aprovechamiento de las oportunidades que ofrece la transformación digital.

Uso responsable y equilibrado

La protección efectiva de los menores requiere fomentar una relación saludable con la tecnología. Los datos muestran que una gran mayoría de adolescentes percibe la tecnología como una parte natural de su vida y considera que gestiona adecuadamente sus hábitos digitales. Sin embargo, también existen situaciones de uso intensivo o problemático que requieren atención.

Por ello, el objetivo debe centrarse en promover hábitos digitales saludables, desarrollar capacidades de autocuidado y proporcionar a los menores herramientas que les permitan desenvolverse de forma progresivamente autónoma en los entornos digitales. La educación digital y el pensamiento crítico constituyen elementos esenciales para que niños y adolescentes aprendan a gestionar riesgos, identificar contenidos inadecuados, proteger su privacidad y utilizar las tecnologías de forma responsable.

Un enfoque centrado exclusivamente en la limitación o restricción del acceso difícilmente permitirá desarrollar estas competencias a largo plazo.

Seguridad y privacidad desde el diseño

La protección de los menores debe incorporarse desde el origen en el diseño de productos y servicios digitales. El sector tecnológico ha avanzado de forma significativa en la aplicación de principios de safety by design y privacy by design, integrando mecanismos de protección desde las fases iniciales de desarrollo.

Este enfoque permite incorporar funcionalidades como controles parentales, perfiles adaptados por edad, configuraciones de privacidad reforzadas, herramientas de supervisión, sistemas de reporte y mecanismos de mitigación de riesgos que facilitan una experiencia más segura para los menores.

La mejora continua de estas herramientas constituye una prioridad para la industria, especialmente en un ecosistema digital caracterizado por la rápida evolución tecnológica y la aparición constante de nuevos servicios y modelos de interacción.

AMETIC considera que el desarrollo de soluciones tecnológicas innovadoras debe seguir desempeñando un papel fundamental en las estrategias de protección de la infancia.

Regulación proporcionada y basada en la evidencia

La protección de los menores exige un marco regulatorio sólido y eficaz. No obstante, las medidas normativas deben construirse sobre evidencia, responder a riesgos reales identificados y ser proporcionales a los objetivos perseguidos.

Los estudios analizados muestran una realidad compleja en la que conviven oportunidades, riesgos, diferentes patrones de uso y distintos niveles de madurez digital. En consecuencia, resulta necesario evitar respuestas simplificadas que atribuyan los riesgos a una única tecnología, a un único servicio o a un único actor del ecosistema digital.

AMETIC defiende además que la protección de los menores debe desarrollarse dentro de un marco regulatorio coherente a escala europea. La existencia de instrumentos comunitarios como el Reglamento de Servicios Digitales (DSA), el Reglamento de Inteligencia Artificial o los futuros mecanismos europeos de verificación y garantía de edad evidencian la necesidad de avanzar hacia soluciones armonizadas que eviten la fragmentación regulatoria y permitan ofrecer niveles homogéneos de protección en todo el mercado único digital.

La armonización regulatoria favorece tanto la seguridad jurídica como la eficacia de las medidas de protección y contribuye a evitar que las soluciones adoptadas en un país generen distorsiones o niveles de protección diferentes respecto a otros Estados miembros.

Colaboración entre actores

Los riesgos identificados en los estudios analizados no responden exclusivamente a factores tecnológicos. Aspectos como la educación, el contexto familiar, el bienestar emocional, las relaciones sociales o el grado de acompañamiento recibido desempeñan un papel determinante.

Por ello, la protección efectiva de los menores no puede recaer exclusivamente sobre un único actor. Ni las familias pueden asumir por sí solas toda la responsabilidad, ni las empresas tecnológicas pueden resolver aisladamente problemas que tienen una dimensión educativa, social y cultural.

AMETIC considera que la protección de la infancia exige un modelo de corresponsabilidad en el que participen de forma coordinada familias, centros educativos, administraciones públicas, profesionales especializados, organizaciones de la sociedad civil y sector tecnológico.

Este enfoque colaborativo permite abordar el fenómeno desde una perspectiva integral, combinando prevención, educación, herramientas tecnológicas, acompañamiento y apoyo institucional.



Acompañamiento y educación frente la prohibición

La principal conclusión que se desprende tanto de la evidencia analizada como de la experiencia acumulada por el sector es que la protección de los menores no debe construirse únicamente desde la restricción o la prohibición, sino desde el acompañamiento y la capacitación.

La existencia de riesgos reales en el entorno digital no implica que la respuesta más eficaz sea excluir a los menores de determinados espacios digitales o limitar de forma generalizada su acceso a la tecnología. La experiencia demuestra que los enfoques basados exclusivamente en la prohibición pueden resultar insuficientes para afrontar riesgos complejos y, en algunos casos, favorecer el desplazamiento de los menores hacia entornos menos supervisados o seguros.

Por el contrario, las iniciativas orientadas a fortalecer la alfabetización digital, desarrollar competencias críticas, promover hábitos saludables y facilitar herramientas de protección permiten generar capacidades duraderas que acompañan a los menores durante todo su proceso de desarrollo.

La educación digital debe concebirse, por tanto, como un elemento central de la protección de la infancia. Educar en el uso responsable de la tecnología, en la gestión de la privacidad, en la identificación de riesgos y en el respeto a los demás usuarios resulta tan importante como disponer de herramientas técnicas de protección.

Desde esta perspectiva, AMETIC defiende que la respuesta a los desafíos del entorno digital debe combinar innovación tecnológica, educación, acompañamiento familiar, acción educativa y regulación equilibrada. La tecnología forma parte de la vida de los menores y seguirá desempeñando un papel cada vez más relevante en el futuro. El reto no consiste en aislar a niños y adolescentes del entorno digital, sino en garantizar que puedan desenvolverse en él de forma segura, responsable y acorde con su desarrollo, aprovechando todas las oportunidades que la tecnología puede ofrecer para su aprendizaje, creatividad e inclusión social.

04

EVIDENCIAS: CAPACIDADES Y DESARROLLOS DEL SECTOR TECNOLÓGICO

Las empresas asociadas a AMETIC muestran un elevado grado de compromiso del sector tecnológico con la protección de niños, niñas y adolescentes en los entornos digitales. Remarcan que la protección de los menores se ha convertido en un elemento estratégico para muchas organizaciones, que han incorporado mecanismos de prevención, herramientas específicas de protección y programas de sensibilización dirigidos a usuarios, familias y profesionales.

Asimismo, la industria tecnológica recuerda que ya dispone de soluciones técnicas y organizativas que contribuyen a reducir riesgos, mejorar la seguridad de los usuarios y facilitar el acompañamiento de los menores en el uso de los servicios digitales. No obstante, también identifica desafíos relacionados con la adopción efectiva de estas soluciones y con la necesidad de disponer de métricas que permitan evaluar mejor su impacto real.



4.1

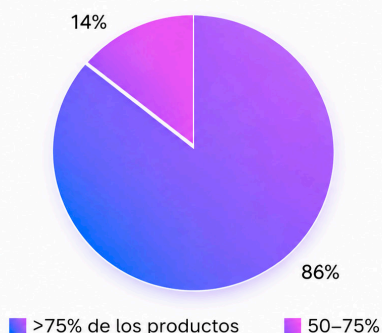
NIVEL DE MADUREZ DEL SECTOR

Nivel de integración de la protección del menor



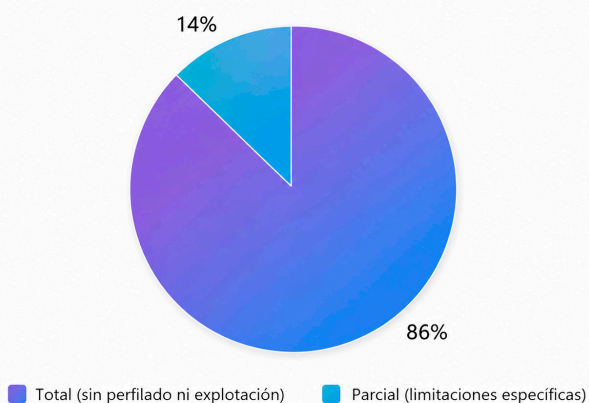
Los datos evidencian un grado significativo de madurez en materia de protección de menores. La mayoría de las organizaciones de la industria tecnológica considera este ámbito como una responsabilidad corporativa relevante e integrada en sus estrategias de desarrollo de productos y servicios.

Grado de despliegue de “privacy & security by design” en productos con potencial uso por menores



La protección de los usuarios más vulnerables se aborda de forma creciente desde fases tempranas de diseño y desarrollo, incorporando criterios de privacidad, seguridad y gestión de riesgos como elementos estructurales de los procesos de innovación. Este enfoque está alineado con los principios de privacy and security by design y de minimización de datos, ampliamente extendidos en el sector.

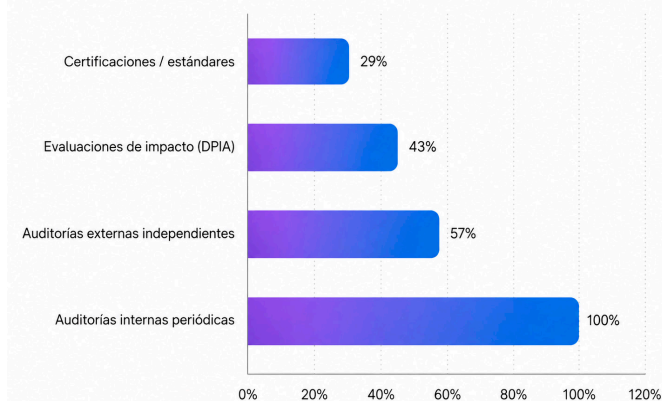
Nivel de aplicación de minimización de datos en menores



Asimismo, las empresas señalan que los requisitos relacionados con la protección de menores se tienen en cuenta tanto en los procesos tecnológicos como en la definición de políticas internas, mecanismos de supervisión y estrategias de cumplimiento normativo.

Un elemento especialmente relevante es que una parte significativa de las organizaciones ha implantado procedimientos de evaluación y revisión periódica de los riesgos asociados a sus productos y servicios. Estas actuaciones incluyen auditorías internas, procesos de revisión de cumplimiento, análisis de riesgos, evaluaciones de impacto en materia de privacidad y seguridad, así como mecanismos de seguimiento de incidentes y mejora continua. En algunos casos, estas revisiones se encuentran integradas en los ciclos de desarrollo de producto, permitiendo identificar riesgos potenciales desde fases tempranas y adoptar medidas preventivas antes de su despliegue.

Tipología de auditorías aplicadas



Se observa también una creciente incorporación de equipos multidisciplinares en los procesos de diseño y gobernanza de productos digitales, combinando perfiles tecnológicos, jurídicos, de privacidad, seguridad y experiencia de usuario. Este enfoque favorece una visión más completa de los riesgos y necesidades específicas de los menores.

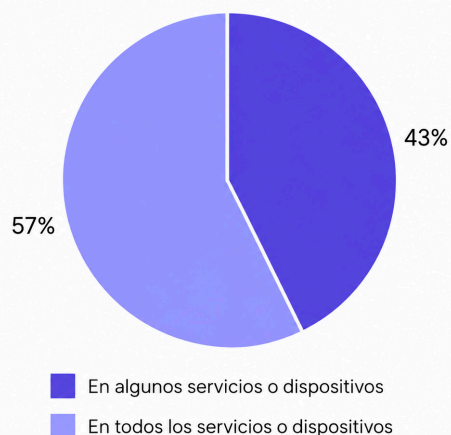
En conjunto, los resultados muestran que la protección de menores ya no se aborda únicamente como una obligación regulatoria, sino como un elemento integrado en la cultura corporativa, en los sistemas de gestión de riesgos y en el diseño de soluciones digitales.



4.2

SOLUCIONES TECNOLÓGICAS DESPLEGADAS

Alcance de las herramientas de control parental



La industria tecnológica ofrece una amplia disponibilidad de herramientas y funcionalidades orientadas a proteger a los menores en el entorno digital.

El 57% de las empresas que representa AMETIC dispone de controles parentales en todos sus servicios y que funcionalidades como la limitación de tiempo, bloqueo de contenidos, supervisión de actividad y alertas a tutores están presentes en el 100% de las soluciones analizadas.

¿Qué funcionalidades incluyen sus sistemas?



Entre las soluciones más habituales destacan:

- **Herramientas de control parental y supervisión familiar.**

- **Sistemas de verificación y estimación de edad.**

- **Configuraciones de privacidad reforzadas para menores.**

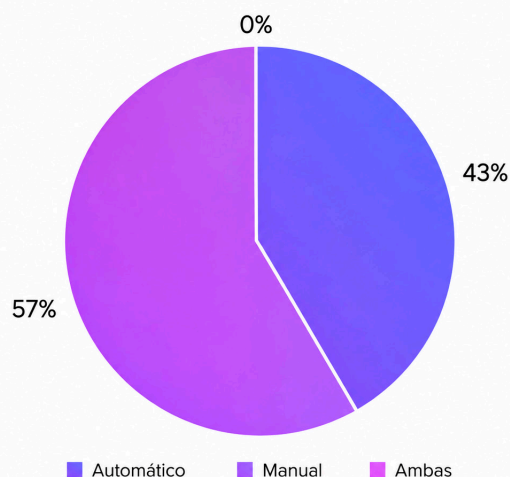
- **Mecanismos de moderación de contenidos.**

- **Sistemas de reporte y denuncia de incidencias.**

- **Herramientas de gestión de riesgos y prevención de usos indebidos.**

- **Entornos y perfiles adaptados a distintos niveles de edad y madurez.**

¿Cómo se configuran estos sistemas?

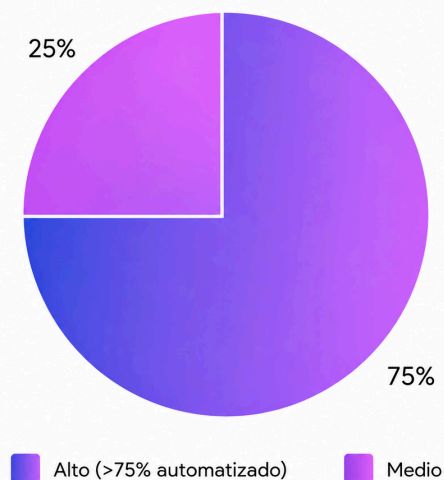


Más allá de su mera disponibilidad, las empresas han desarrollado funcionalidades específicas destinadas a reducir la exposición a riesgos y facilitar el acompañamiento familiar. Entre ellas se encuentran la limitación de contactos y comunicaciones no deseadas, la gestión de permisos y tiempos de uso, los mecanismos de supervisión de actividad, las alertas ante comportamientos potencialmente problemáticos, los filtros de contenidos, las restricciones de acceso a determinados servicios o funcionalidades, y las configuraciones adaptadas a la edad de los usuarios.

Asimismo, varias organizaciones han incorporado medidas orientadas a reforzar la privacidad y la protección de datos de los menores, incluyendo configuraciones privadas por defecto, limitación de la compartición de información personal, mecanismos de consentimiento y herramientas que facilitan a familias y usuarios la gestión de los datos personales.

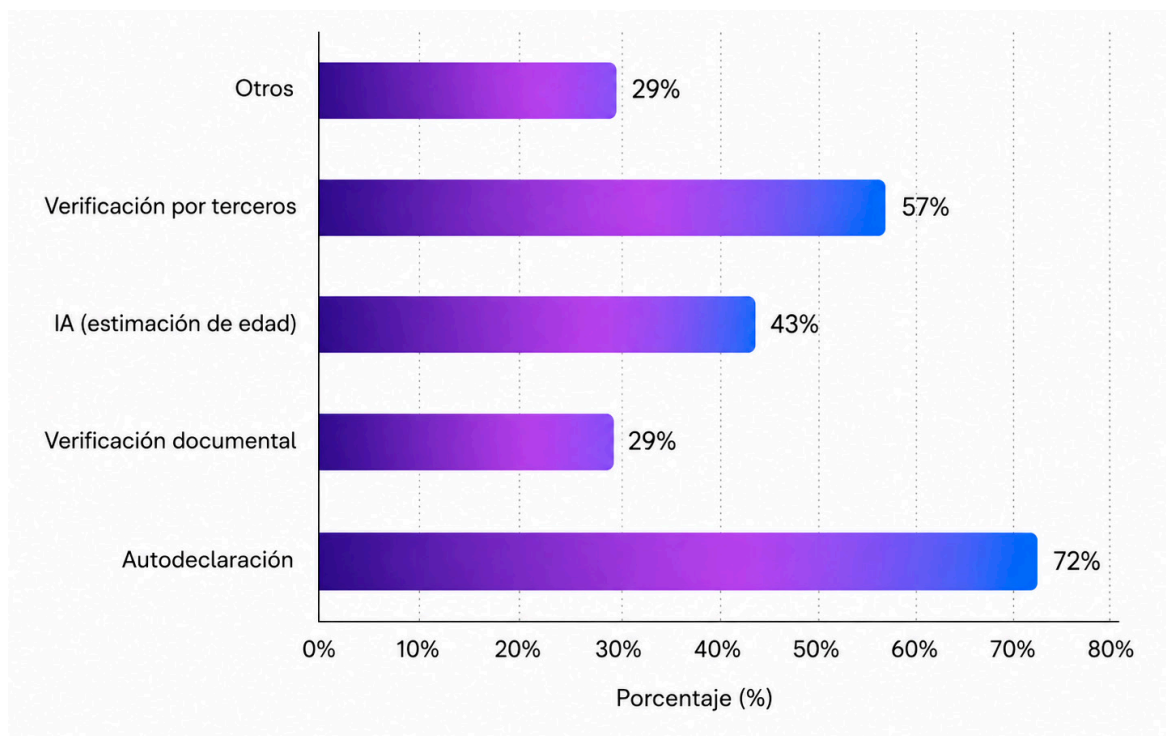
Para la gestión de éstas, existe de que estén preconfiguradas, sobre los que es posible realizarlo de forma manual.

Nivel de automatización en la moderación de contenidos



En el ámbito de los contenidos y las interacciones, las soluciones desplegadas incluyen sistemas de detección y moderación, procedimientos de reporte accesibles para los usuarios, herramientas para bloquear o denunciar comportamientos inapropiados y mecanismos destinados a limitar la difusión de contenidos potencialmente perjudiciales.

Sistemas de verificación de edad. ¿Qué tecnologías utiliza?



Hay un creciente interés por las tecnologías de verificación y garantía de edad, consideradas una de las herramientas con mayor potencial para adaptar la experiencia digital al nivel de madurez de los usuarios, si bien las empresas subrayan la importancia de desarrollar soluciones eficaces, interoperables y respetuosas con los principios de privacidad y protección de datos.

Estas medidas se complementan con mecanismos de detección y respuesta ante comportamientos potencialmente perjudiciales, así como con procedimientos internos de gestión de incidencias, revisión de riesgos y mejora continua.

Muchas de estas soluciones se encuentran ya operativas y forman parte habitual de los servicios digitales utilizados por millones de usuarios, lo que pone de manifiesto el papel activo que desempeña el sector en la protección de los menores y en el desarrollo de entornos digitales más seguros.



4.3

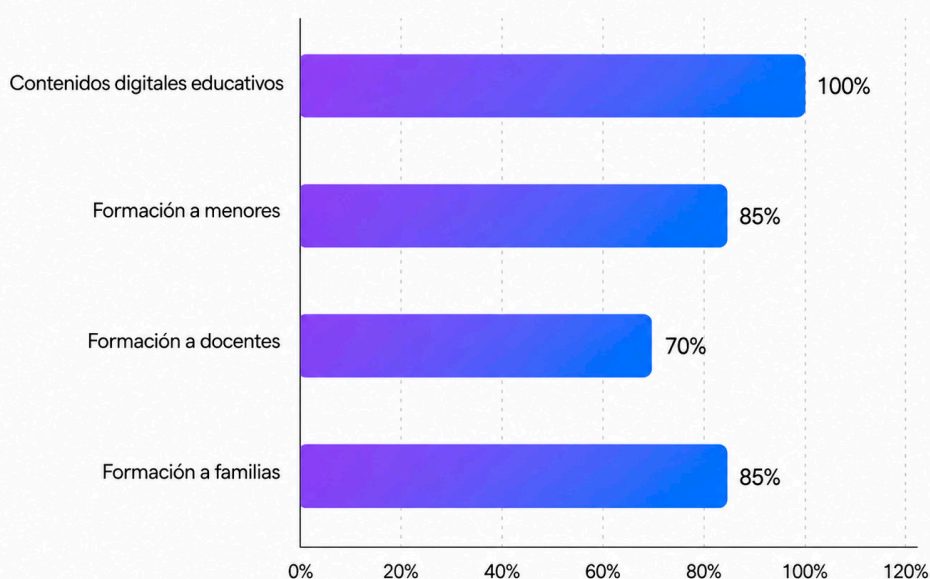
EDUCACIÓN Y SENSIBILIZACIÓN

Se pone de manifiesto que la protección de los menores en los entornos digitales no puede apoyarse exclusivamente en herramientas tecnológicas o medidas regulatorias. La mayoría de las empresas participantes coincide en señalar que la educación, la alfabetización digital y el acompañamiento constituyen elementos esenciales para promover experiencias digitales seguras y positivas.

Esta conclusión se encuentra alineada con los resultados de los estudios analizados en los apartados anteriores. En ellos se destaca la importancia del entorno familiar, la adquisición de competencias digitales y el desarrollo del pensamiento crítico como factores fundamentales para afrontar los riesgos asociados al uso de la tecnología.

En este contexto, las empresas desarrollan un amplio conjunto de iniciativas orientadas a reforzar las capacidades de los distintos actores que participan en el ecosistema digital de los menores. Estas actuaciones se dirigen no sólo a niños, niñas y adolescentes, sino también a familias, docentes y otros profesionales que desempeñan un papel relevante en su educación y acompañamiento.

Tipología de acciones

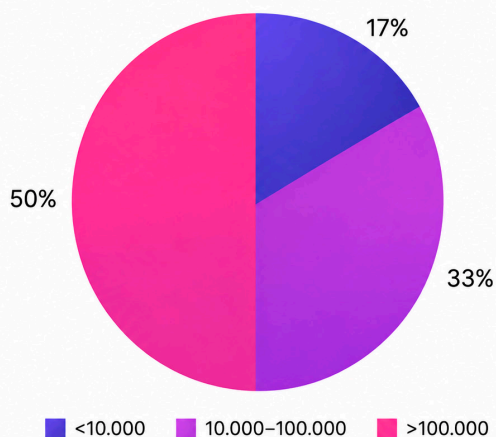


Entre las iniciativas identificadas destacan:

- **Programas de educación digital dirigidos a menores.**
- **Recursos formativos para familias y cuidadores.**
- **Materiales educativos para centros escolares.**
- **Campañas de sensibilización sobre seguridad en Internet.**
- **Actividades relacionadas con privacidad y protección de datos.**
- **Formación en ciberseguridad y gestión de riesgos.**
- **Programas para fomentar el pensamiento crítico y la alfabetización mediática.**
- **Iniciativas para promover el uso responsable y equilibrado de la tecnología.**



Alcance (estimación anual de personas participantes)



Además, se observa una visión compartida por gran parte del sector: la capacitación de los menores debe orientarse no sólo a evitar riesgos, sino también a potenciar un uso positivo de la tecnología. En este sentido, la educación digital se concibe como una herramienta para desarrollar competencias, fomentar la creatividad, favorecer la participación responsable y preparar a los jóvenes para desenvolverse en una sociedad crecientemente digitalizada.

También pone de manifiesto la relevancia del acompañamiento familiar. Aunque las empresas reconocen que existen herramientas técnicas de protección cada vez más avanzadas, consideran que su eficacia aumenta significativamente cuando van acompañadas de diálogo, mediación y participación por parte de las familias. Esta conclusión resulta especialmente relevante si se tiene en cuenta que los estudios analizados muestran una elevada preocupación de los progenitores por los riesgos digitales, mientras que el nivel de utilización efectiva de algunas herramientas de protección continúa siendo limitado.

Otro aspecto destacado por las empresas es la necesidad de reforzar la formación de los propios adultos. La rápida evolución tecnológica, la aparición constante de nuevos servicios digitales y la creciente sofisticación de las plataformas hacen necesario que familias y docentes dispongan de conocimientos actualizados que les permitan comprender mejor los entornos utilizados por los menores y ejercer una labor de acompañamiento más eficaz.

Asimismo, se identifica una creciente demanda de iniciativas colaborativas entre sector tecnológico, administraciones públicas, centros educativos y organizaciones sociales para impulsar programas coordinados de educación digital. Las empresas consideran que los retos asociados a la protección de los menores requieren un enfoque compartido que combine innovación tecnológica, formación, sensibilización y apoyo continuado a los usuarios.

En conjunto, hay un amplio consenso en torno a la idea de que la educación digital constituye uno de los pilares fundamentales de la protección de los menores en línea. Las herramientas tecnológicas pueden contribuir significativamente a reducir riesgos, pero su efectividad depende en gran medida de que los usuarios dispongan de los conocimientos, habilidades y criterios necesarios para utilizarlas adecuadamente. Por ello, la alfabetización digital y el acompañamiento continuado deben considerarse elementos estratégicos para garantizar un entorno digital más seguro, inclusivo y beneficioso para niños, niñas y adolescentes.



4.4

BUENAS PRÁCTICAS IDENTIFICADAS

Las empresas han desarrollado enfoques cada vez más integrales para abordar la protección de los menores en los entornos digitales. Más allá del cumplimiento normativo, muchas organizaciones han incorporado la seguridad y el bienestar de los usuarios menores de edad como un elemento transversal en el diseño, desarrollo y operación de sus productos y servicios.

El análisis de las respuestas permite identificar una serie de buenas prácticas comunes que reflejan un elevado grado de madurez del sector y una evolución hacia modelos preventivos basados en la combinación de tecnología, educación y colaboración.

Un modelo basado en tecnología, educación y acompañamiento

Las empresas no entienden la protección de los menores como una cuestión exclusivamente tecnológica. Por el contrario, existe un amplio consenso en que las soluciones más eficaces son aquellas que combinan herramientas técnicas con iniciativas de educación, sensibilización y acompañamiento.

En este sentido, las organizaciones señalan que la protección efectiva requiere actuar simultáneamente sobre varios niveles:

- Diseño seguro de productos y servicios.
- Herramientas de protección y control accesibles.
- Capacitación de menores y familias.
- Información clara para los usuarios.
- Colaboración con administraciones, centros educativos y organizaciones sociales.

Este enfoque coincide con la evidencia reflejada en los estudios analizados previamente, donde la educación digital y la mediación familiar aparecen como factores de protección tan relevantes como las propias herramientas tecnológicas.

Medidas preventivas incorporadas en los productos y servicios

Las empresas están incorporando cada vez más medidas preventivas destinadas a anticipar riesgos antes de que se produzcan situaciones perjudiciales.

Entre las actuaciones identificadas destacan:

- Configuraciones seguras activadas por defecto para usuarios menores de edad.
- Sistemas de detección y mitigación temprana de riesgos.
- Restricciones automáticas sobre determinadas funcionalidades.
- Herramientas de control y supervisión para familias.
- Sistemas de notificación y alerta ante comportamientos potencialmente problemáticos.
- Mecanismos reforzados de privacidad y protección de datos.
- Procedimientos de reporte y actuación frente a contenidos o conductas inapropiadas.

Frente a modelos reactivos centrados exclusivamente en la gestión de incidentes, las empresas muestran una apuesta creciente por prevenir la exposición al riesgo desde el diseño de los propios servicios.

Buenas prácticas de educación y sensibilización

Otro de los ámbitos donde se identifican actuaciones relevantes es el de la formación y la sensibilización.

Las empresas tecnológicas desarrollan iniciativas dirigidas a diferentes colectivos:

- Programas educativos para menores.
- Talleres y recursos para familias.
- Materiales didácticos para centros educativos.
- Guías de buenas prácticas en Internet.
- Campañas de concienciación sobre privacidad, ciberseguridad y uso responsable.
- Actividades de promoción del pensamiento crítico y la alfabetización mediática.

Estas iniciativas buscan proporcionar a los usuarios conocimientos y capacidades que les permitan tomar decisiones informadas, identificar riesgos y desenvolverse con autonomía en los entornos digitales.

Casos prácticos y experiencias de colaboración

También se pone de relieve la existencia de experiencias de colaboración entre empresas tecnológicas, administraciones públicas, entidades sociales y centros educativos.

Estas iniciativas incluyen:

- Participación en campañas de sensibilización dirigidas a familias y menores.
- Colaboración en programas de educación y ciudadanía digitales.
- Desarrollo conjunto de materiales educativos y recursos divulgativos.
- Cooperación con organismos especializados en protección de menores.
- Participación en grupos de trabajo, foros sectoriales y espacios de intercambio de buenas prácticas.

Los retos asociados al bienestar digital de los menores difícilmente pueden ser abordados por un único actor y que la colaboración constituye un mecanismo esencial para maximizar el impacto de las medidas de protección.

De la reacción a la prevención

La principal tendencia identificada es la evolución desde enfoques reactivos hacia modelos preventivos e integrales.

Las empresas consideran que la protección efectiva no debe limitarse a actuar cuando el riesgo ya se ha materializado, sino que debe centrarse en reducir la probabilidad de que dichos riesgos lleguen a producirse. Para ello, combinan herramientas tecnológicas, diseño seguro, educación digital, acompañamiento familiar y colaboración institucional.

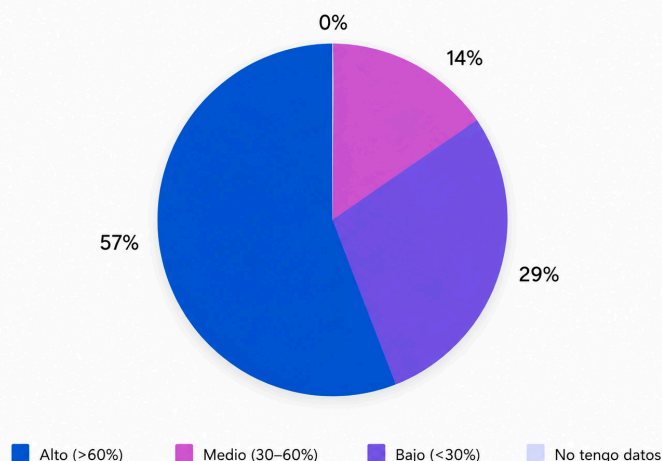
En conjunto, se pone de manifiesto que existe un ecosistema de iniciativas, herramientas y buenas prácticas ya desplegadas por el sector tecnológico que contribuyen activamente a la protección de los menores. La evidencia recopilada refleja que la combinación de innovación tecnológica, educación digital y cooperación entre actores constituye actualmente uno de los enfoques más sólidos para afrontar los desafíos que plantea la participación de niños, niñas y adolescentes en la sociedad digital.



4.5

BRECHAS Y RETOS IDENTIFICADOS

Nivel de uso estimado por usuarios/familias



Pese al elevado nivel de desarrollo de las soluciones existentes, se identifican algunos desafíos pendientes.

El primero de ellos es la diferencia entre la disponibilidad de herramientas y su utilización efectiva por parte de los usuarios. Esta conclusión coincide con los resultados obtenidos por ONTSI y UNICEF, que muestran que muchas familias desconocen determinadas funcionalidades o no las utilizan de forma regular, a pesar de manifestar una elevada preocupación por la seguridad digital de los menores¹ y ².

Un segundo reto identificado es la necesidad de mejorar la medición del impacto de las medidas desplegadas. Aunque existe una amplia variedad de herramientas e iniciativas, las empresas señalan la conveniencia de disponer de indicadores y metodologías más homogéneas que permitan evaluar su eficacia y conocer mejor qué actuaciones generan mejores resultados.

Por último, se pone de manifiesto la necesidad de seguir reforzando la adopción de buenas prácticas y el acompañamiento de los usuarios. La rápida evolución de los servicios digitales, la aparición de nuevas tecnologías y la diversidad de situaciones familiares requieren mantener un esfuerzo continuado en materia de sensibilización, formación y colaboración.

En conjunto, la evidencia refleja que el sector tecnológico dispone de un elevado grado de madurez y de un conjunto amplio de herramientas para contribuir a la protección de los menores. No obstante, los resultados también muestran que la eficacia de estas soluciones depende de su utilización efectiva y de la capacidad de combinar tecnología, educación y corresponsabilidad para responder a los desafíos del entorno digital.

05



CORRESPONSABILIDAD EN LA PROTECCIÓN DE LOS MENORES



5.1

LA PROTECCIÓN DE LOS MENORES COMO RESPONSABILIDAD COMPARTIDA

La evidencia analizada en los capítulos anteriores muestra que los riesgos identificados en el entorno digital no responden a una única causa ni pueden ser abordados eficazmente por un único actor. Factores tecnológicos, educativos, familiares, sociales y de bienestar interactúan entre sí y requieren respuestas coordinadas.

Los estudios de ponen de manifiesto la importancia del acompañamiento familiar, el desarrollo de competencias digitales, la existencia de herramientas tecnológicas de protección y la necesidad de generar entornos digitales seguros. Del mismo modo, los testimonios recopilados de las empresas tecnológicas asociadas a AMETIC evidencian que las organizaciones han desarrollado un amplio conjunto de soluciones, mecanismos de protección y programas educativos orientados a reforzar la se-

guridad y el bienestar de los menores. No obstante, persisten retos significativos relacionados con el conocimiento, la adopción y el uso efectivo de estas herramientas por parte de familias y usuarios. Esta situación pone de manifiesto la necesidad de reforzar los esfuerzos de sensibilización, formación y acompañamiento, así como de continuar mejorando y evaluando las soluciones disponibles para maximizar su impacto real en la protección de los menores.

En consecuencia, la protección de la infancia en entornos digitales debe abordarse desde un modelo de corresponsabilidad que implique de forma coordinada a administraciones públicas, sector tecnológico, familias, sistema educativo y sociedad civil.



Administraciones públicas

- Impulso de marcos regulatorios coherentes y proporcionados.
- Promoción de campañas de sensibilización y educación digital.
- Coordinación de iniciativas públicas y privadas.
- Desarrollo de sistemas de evaluación y seguimiento.

Sistema educativo

- Integración de la competencia digital en el proceso educativo.
- Formación en ciudadanía digital.
- Desarrollo de pensamiento crítico y alfabetización mediática.
- Detección temprana de situaciones de riesgo.

Familias

- Acompañamiento activo y diálogo permanente.
- Uso de herramientas de supervisión cuando resulte necesario.
- Promoción de hábitos digitales saludables.
- Participación en procesos de formación y alfabetización digital.

Industria tecnológica

- Diseño de productos y servicios seguros.
- Desarrollo continuo de herramientas de protección.
- Innovación en mecanismos de verificación de edad, privacidad y seguridad.
- Colaboración con administraciones, educadores y familias.

Sociedad civil y entidades especializadas

- Impulso de marcos regulatorios coherentes y proporcionados.
- Promoción de campañas de sensibilización y educación digital.
- Coordinación de iniciativas públicas y privadas.
- Desarrollo de sistemas de evaluación y seguimiento.



5.2

PRINCIPIOS PARA UNA ACTUACIÓN EFECTIVA

La acción conjunta de todos los actores debería sustentarse en una serie de principios compartidos:

- **Interés superior del menor.**
- **Protección compatible con el ejercicio de derechos.**
- **Proporcionalidad de las medidas.**
- **Innovación y seguridad como elementos complementarios.**
- **Decisiones basadas en evidencia.**
- **Transparencia y rendición de cuentas.**
- **Evaluación continua del impacto de las medidas adoptadas.**
- **Colaboración público-privada.**



06

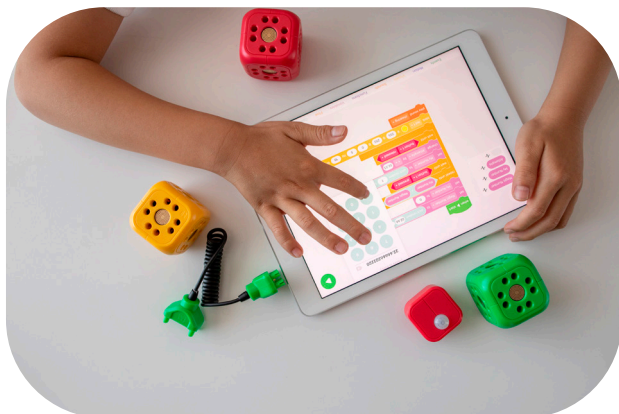


RECOMENDACIONES



6.1

IMPULSAR UN MODELO INTEGRAL BASADO EN LA CORRESPONSABILIDAD



La protección efectiva de los menores requiere la actuación coordinada de administraciones públicas, sector tecnológico, familias, centros educativos y sociedad civil.

Las políticas públicas deberían fomentar mecanismos permanentes de colaboración e intercambio de buenas prácticas entre todos los actores implicados.

Promover políticas públicas que combinen protección, innovación y capacitación digital, priorizando medidas basadas en evidencia y evaluaciones de impacto, y evitando enfoques exclusivamente prohibitivos o centrados en un único actor del ecosistema digital.



6.2

REFORZAR LA EDUCACIÓN Y ALFABETIZACIÓN DIGITAL



La educación digital debe constituir una política estructural y continuada.

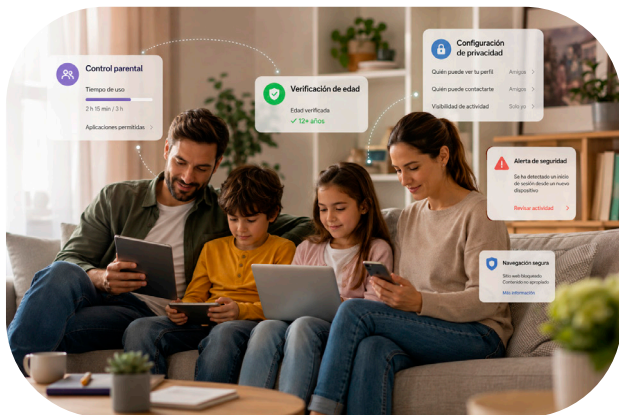
Se recomienda:

- Incorporar contenidos de ciudadanía digital en todas las etapas educativas.
- Reforzar la formación de docentes.
- Impulsar programas específicos para familias.
- Promover el pensamiento crítico y la alfabetización mediática.
- Incluir el uso responsable de la IA y otras tecnologías emergentes.



6.3

FAVORECER LA ADOPCIÓN EFECTIVA DE HERRAMIENTAS DE PROTECCIÓN



Los estudios muestran que existe una brecha entre la disponibilidad de soluciones y su utilización efectiva.

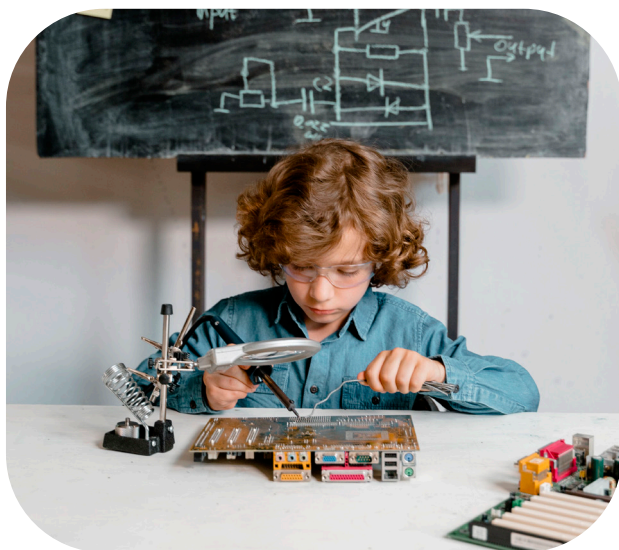
Por ello se recomienda:

- Incrementar el conocimiento sobre las herramientas disponibles.
- Mejorar la usabilidad de las soluciones.
- Facilitar la configuración de controles y medidas de protección.
- Desarrollar campañas de información dirigidas a familias y educadores.



6.4

IMPULSAR LA INNOVACIÓN PARA LA PROTECCIÓN DE MENORES



Se recomienda apoyar el desarrollo de:

- Sistemas de verificación y garantía de edad.
- Herramientas avanzadas de control parental.
- Soluciones de moderación y gestión de riesgos.
- Tecnologías de protección de privacidad.
- Sistemas de detección temprana de comportamientos de riesgo.

Todo ello respetando los principios de privacidad, seguridad y proporcionalidad.



6.5

PROMOVER UNA REGULACIÓN ARMONIZADA Y BASADA EN EVIDENCIA



Las medidas regulatorias deben:

- Basarse en riesgos identificados y evidencia contrastada.
- Evaluar su impacto antes de su adopción.
- Mantener coherencia con el marco europeo.
- Evitar fragmentaciones regulatorias que reduzcan la eficacia de las medidas.
- Combinar protección e innovación.

07

CONCLUSIONES

La evidencia analizada a lo largo de este documento pone de manifiesto que la tecnología forma parte de la vida cotidiana de niños, niñas y adolescentes y constituye un elemento cada vez más relevante en sus procesos de aprendizaje, socialización, participación y desarrollo personal. Los estudios revisados confirman una realidad caracterizada por una elevada conectividad, un acceso cada vez más temprano a los dispositivos digitales y una creciente integración de los entornos digitales en la experiencia vital de los menores.

Asimismo, los resultados muestran que la tecnología genera importantes oportunidades para el acceso al conocimiento, el desarrollo de competencias digitales, la creatividad, la comunicación y la inclusión social. Al mismo tiempo, plantea desafíos relacionados con la seguridad, la privacidad, la exposición a contenidos inadecuados, la interacción con desconocidos, el bienestar emocional y otros riesgos asociados al uso intensivo o inadecuado de determinados servicios digitales.

A partir de la evidencia disponible, este documento propone un modelo de actuación basado en tres pilares complementarios: **tecnología, educación y corresponsabilidad**.

La tecnología constituye una parte esencial de la solución, tanto por las oportunidades que ofrece como por el amplio conjunto de herramientas y mecanismos de protección que el sector ha desarrollado en los últimos años. Las empresas tecnológicas asociadas a AMETIC han incorporado medidas de seguridad y privacidad desde el diseño, herramientas de control y supervisión, mecanismos de moderación y soluciones orientadas a la protección de los menores. No obstante, también se identifican





retos relacionados con la adopción efectiva de estas medidas y la necesidad de continuar mejorando su alcance e impacto.

La educación digital es igualmente, un elemento central. Los estudios analizados y las propias empresas coinciden en señalar que el desarrollo del pensamiento crítico, la alfabetización digital, la formación de familias y docentes y la promoción de hábitos digitales saludables constituyen factores fundamentales para reforzar la seguridad y el bienestar de los menores en línea.

Por último, la corresponsabilidad emerge como el marco más adecuado para afrontar un fenómeno complejo que no puede atribuirse exclusivamente a un único actor. La protección efectiva de los menores requiere la participación coordinada de administraciones públicas, familias, centros educativos, organizaciones sociales y sector tecnológico, cada uno desde sus respectivas competencias y capacidades.

Entre los principales retos de futuro destacan la adaptación a la rápida evolución tecnológica, la generalización de tecnologías emergentes como la inteligencia artificial, la mejora de los mecanismos de verificación de edad, el fortalecimiento de las competencias digitales de menores y adultos, el incremento de la utilización efectiva de las herramientas de protección disponibles y una mejor evaluación del impacto real de las medidas adoptadas.

La complejidad de estos desafíos exige avanzar hacia modelos de actuación basados en el conocimiento, la evidencia y la colaboración. Las respuestas exclusivamente centradas en la restricción o en la atribución de responsabilidades a un único actor difícilmente podrán ofrecer soluciones eficaces y sostenibles a largo plazo. Por el contrario, la combinación de innovación tecnológica, educación digital, acompañamiento familiar y colaboración institucional ofrece mayores posibilidades de construir entornos digitales más seguros y beneficiosos para los menores.

En definitiva, la protección de la infancia en la era digital constituye una responsabilidad compartida que requiere el compromiso de todos los agentes implicados. El reto no consiste en excluir a los menores del entorno digital, sino en garantizar que puedan desarrollarse en él de forma segura, responsable y acorde con su grado de madurez, aprovechando plenamente las oportunidades que la tecnología puede ofrecer para su bienestar, aprendizaje e inclusión social.

FUENTES Y REFERENCIAS

Estudios e informes de referencia

1 ONTSI – Observatorio Nacional de Tecnología y Sociedad y Red.es (2025). Uso de las tecnologías por niños, niñas y adolescentes en España.

2 UNICEF España, USC, Consejo Colegios de Ingeniería Informática y Red.es (2025). Infancia, adolescencia y bienestar digital. Una aproximación desde el bienestar integral.

3 Google & Livity (2025). The Future Report Spain 2025. Google Safety Engineering Center, 2025

4 Fundación Fad Juventud y Amazon (2026). Consumo online en familias con hijos e hijas adolescentes.

5 Encuesta sectorial AMETIC sobre protección de menores en entornos digitales (2025).

Reglamento (UE) 2022/2065 de Servicios Digitales (Digital Services Act – DSA).

Reglamento (UE) 2024/1689 de Inteligencia Artificial (AI Act).

Reglamento eIDAS 2.0 y desarrollos relacionados con identidad digital y verificación de edad.

Reglamento General de Protección de Datos (RGPD).

Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.

Otras referencias

Agencia Española de Protección de Datos (AEPD). Guías, recomendaciones y recursos sobre menores y privacidad en Internet.

Comisión Europea. Documentación sobre protección de menores, ciudadanía digital, DSA y verificación de edad.

OCDE, UNESCO y otros organismos internacionales. Informes y recomendaciones sobre bienestar digital, alfabetización mediática y competencias digitales.

