

Seguridad infantil en línea

PROTEGER Y EMPODERAR A LOS
MENORES EN UN MUNDO DIGITAL

INFORME DE LOS COPRESIDENTES DEL GRUPO ESPECIAL

SOBRE SEGURIDAD INFANTIL EN LÍNEA

Prof. Dr. Jörg M. Fegert y Dr.^a Maria Melchior



Prólogo

En marzo de 2026, la presidenta de la Comisión Europea, Ursula von der Leyen, encargó a dos consejeros especiales (Jörg M. Fegert y Maria Melchior) la copresidencia del Grupo Especial sobre Seguridad Infantil en Línea y posibles restricciones por edad en los medios sociales. Se encargó a los copresidentes que redactaran un informe sobre las conclusiones del Grupo y que asesoraran sobre el mejor enfoque para que Europa haga que el mundo digital sea más seguro para los niños.

El Grupo, anunciado por primera vez en el discurso sobre el estado de la Unión de 2025 por la presidenta de la Comisión, reunió a académicos de alto nivel, profesionales, representantes de jóvenes y padres y otros especialistas en diversos ámbitos de toda Europa para evaluar el impacto de los medios sociales en los menores.

«Y, en esta labor, nos guiaremos por la necesidad de empoderar a los padres y de construir una Europa más segura para nuestros hijos. **Porque, cuando se trata de la seguridad de nuestros hijos en el mundo digital, Europa cree en los padres, no en los beneficios.**»

Ursula von der Leyen, presidenta de la Comisión Europea

Discurso sobre el estado de la Unión de 2025

El Grupo Especial se reunió en tres ocasiones y contó con la participación de diversos especialistas en cada ocasión. La primera reunión del Grupo tuvo lugar el 5 de marzo de 2026 y examinó las pruebas científicas existentes sobre el impacto de los medios sociales y, más en general, del entorno digital, en los niños y adolescentes.

La segunda reunión tuvo lugar el 16 de abril de 2026 y debatió la legislación y las herramientas vigentes de la UE, así como los enfoques políticos nacionales para abordar la seguridad infantil en línea. En su tercera reunión, el 16 de junio de 2026, el Grupo se centró en los enfoques políticos nacionales y las posibles recomendaciones para proteger y empoderar a los niños y adolescentes en el mundo digital.

Los principales temas debatidos durante las reuniones fueron los siguientes:

- Los aspectos positivos y negativos de introducir restricciones específicas por edad para los medios sociales y otros servicios digitales;
- Enfoques adaptados para proteger y empoderar a los menores en función de sus grupos de edad, el contexto socioeconómico y los riesgos específicos de cada edad;

- La seguridad desde el diseño y por defecto y la responsabilidad de los proveedores de medios sociales y otros servicios digitales;
- Medidas educativas y de sensibilización para promover un uso responsable de internet entre niños y adolescentes, padres y cuidadores, profesores y educadores;
- Formas de apoyar a los padres y educadores y de capacitar a los niños y adolescentes para aprovechar las oportunidades del mundo digital.

El análisis y las recomendaciones del presente informe se basan en contribuciones cruciales de un grupo diverso de especialistas invitados a cada reunión del Grupo y en numerosas reuniones adicionales con representantes de los Estados miembros, en particular las organizadas por la Presidencia irlandesa del Consejo de la UE y Luxemburgo (reunión ministerial D9+), terceros países (incluidos Australia y Brasil), el Parlamento Europeo y sus diputados, especialmente del Intergrupo sobre los Derechos del Niño; la industria, la sociedad civil, los grupos de reflexión y otras organizaciones, como la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos y el Comité Europeo de Protección de Datos (CEPD).

Tras estas interacciones y sobre la base de las pruebas recopiladas, los copresidentes elaboraron sus recomendaciones. Si bien la responsabilidad de las recomendaciones recae exclusivamente en los copresidentes, su trabajo se debe en gran medida a las aportaciones de otros expertos de renombre, representantes de padres y jóvenes, y a los conocimientos especializados proporcionados por la Comisión Europea.

El informe tiene por objeto servir de base para futuras acciones que propondrán la Comisión Europea y los Estados miembros de la UE para reforzar la seguridad infantil en línea. Esta evaluación analítica independiente ofrece recomendaciones e inspiración a los niños y adolescentes, los padres y cuidadores, los profesores y educadores, los proveedores de medios sociales y otros servicios digitales sobre cómo proteger y empoderar mejor a los menores en línea.

Recuadro: Ámbito y terminología

La principal tarea, prescrita por la presidenta Von der Leyen, era que el Grupo Especial debatiera sobre la seguridad infantil en línea y las posibles restricciones por edad en los medios sociales. Si bien el ámbito del presente informe se ajusta a esta tarea, la evolución de los debates durante las reuniones del Grupo Especial y otros acontecimientos políticos (por ejemplo, el Llamamiento de los dirigentes del G7 sobre un espacio digital más seguro para los menores, de 17 de junio de 2026) subrayan la necesidad de que los copresidentes precisen la terminología utilizada en el presente informe.

Sin perjuicio de los actos jurídicos internacionales, de la UE o nacionales, a lo largo del presente informe se utilizan los siguientes términos y definiciones correspondientes:

- **Medios sociales y otros servicios digitales (abreviado, medios sociales+):** dentro del ámbito de aplicación del presente informe, los términos «medios sociales+» y «medios sociales y otros servicios digitales» se utilizan para definir de manera amplia los servicios que pueden estar disponibles para los menores y presentar características o contenido inapropiados para su edad o que entrañan riesgos (por ejemplo, características adictivas y perjudiciales, entre las que se incluyen el desplazamiento infinito por la pantalla, la reproducción automática, los algoritmos de recomendación y las notificaciones persistentes). Entre los proveedores de medios sociales y otros servicios digitales se encuentran las plataformas digitales que actúan como intermediarios de contenidos de terceros, como las redes sociales, y las tiendas de aplicaciones. También se incluyen los sistemas de IA que plantean riesgos para la seguridad y el desarrollo de los menores, incluidos los compañeros de IA, los videojuegos que exponen a los menores a prácticas comerciales perjudiciales o contactos peligrosos, y las plataformas de intercambio de vídeos que permiten un acceso inapropiado para la edad de los menores.
- **Menores, niños y adolescentes:** sin perjuicio del uso legalmente definido del término «niños» (por ejemplo, en la Convención de las Naciones Unidas sobre los Derechos del Niño), este informe aboga por la necesidad de un enfoque centrado en el desarrollo para proteger a los menores en línea, que aborde los riesgos y vulnerabilidades específicos a los que están expuestos a diferentes edades. A efectos de este análisis, los autores utilizan el término «menores» para referirse a todos los niños y adolescentes menores de 18 años (la mayoría de edad). El término «adolescentes» se aplica a todos los menores de 13 a 18 años. El término «niños» se refiere a todos los menores de 13 años. El presente informe utiliza el término «derechos del niño» para referirse a los derechos de todos los niños y adolescentes menores de 18 años, tal como se definen en los textos jurídicos. El término «seguridad infantil en línea», tal como se indica en el mandato del proceso del panel especial, se utiliza como término genérico para la protección y el empoderamiento de los menores en el mundo digital.

Prefacio. Crecer de forma segura en el mundo de los medios sociales+

El rápido avance de las tecnologías digitales ha cambiado radicalmente la forma en que los niños y adolescentes crecen e interactúan con sus iguales, padres, profesores y el mundo que los rodea. Al mismo tiempo, las actividades en el mundo fuera de línea siguen siendo cruciales para el aprendizaje, fomentando relaciones y experiencias significativas que conforman el desarrollo de los menores.

El mundo de los medios sociales+ ofrece muchas oportunidades para que los niños y adolescentes aprendan, establezcan conexiones, participen y sean creativos. Sin embargo, es necesario educar y capacitar a los menores para que aprovechen estas oportunidades y desarrollen todo su potencial.

A pesar de ello, **los espacios de los medios sociales+ también presentan una serie de riesgos** para el desarrollo saludable y el bienestar de los menores. Entre ellos se incluyen los riesgos de uso excesivo debido a características adictivas, la sustitución de actividades favorables al desarrollo, la exposición a contenidos perjudiciales y los contactos inapropiados en línea. Estos riesgos se ven amplificados por la aparición de nuevas tecnologías y requieren decisiones atrevidas, pero cuidadosas, para proteger a los niños y adolescentes en línea.

La adopción generalizada de los medios sociales y otros servicios digitales ha llevado a **los responsables políticos y los padres a una extrema preocupación por las amenazas a las que se enfrentan los niños y adolescentes en línea**. Si bien las restricciones por edad para el acceso a los medios sociales y otros servicios digitales han sido objeto de críticas, **pueden ser un paso preventivo necesario** hasta que se demuestre que los niños y adolescentes pueden acceder de modo seguro a los espacios de medios sociales+ o hasta que surjan alternativas seguras.

Las restricciones por edad no consisten en hacer que los padres y cuidadores o los propios niños y adolescentes sean los principales responsables de la seguridad de los menores en el mundo digital. Tampoco se trata de dejar que los proveedores se libren de esta responsabilidad. **Los proveedores de medios sociales y otros servicios digitales siguen siendo los principales responsables de la seguridad de los servicios que desarrollan y prestan.**

La carga de la prueba debe recaer en los proveedores, no en las autoridades reguladoras, los padres y los niños. **Hasta que demuestren que sus servicios son seguros desde el diseño, los proveedores de medios sociales y otros servicios digitales deben restringir el acceso a los menores de 13 años en la UE.** Además de las restricciones a escala de la UE, los Estados miembros pueden introducir otras restricciones preventivas por edad para los adolescentes mayores de 13 años.

Las restricciones preventivas por edad son medidas inmediatas para alcanzar el objetivo a largo plazo de garantizar que los espacios de los medios sociales+

sean seguros para los menores mediante la promoción del cambio cultural. Los primeros resultados de los países que han introducido prohibiciones generales por edad para acceder a los medios sociales muestran que la mayoría de los menores encuentran la manera de eludir estas políticas. Al mismo tiempo, algunos menores se han apartado de los medios sociales y otros servicios digitales de riesgo y ahora disponen de más tiempo para actividades fuera de línea (como el deporte y las interacciones sociales en persona). Esto demuestra que el cambio progresivo en torno a las normas de uso de los medios sociales+ por parte de los menores no solo es posible sino que debe reconocerse.

Sin embargo, todo cambio lleva tiempo. Por ejemplo, la evolución de las actitudes sociales con respecto a la prohibición legislativa del castigo corporal en la educación llevó más de una generación (en concreto, en Alemania y Suecia). La prohibición del castigo corporal aclaró las expectativas de los padres, cuidadores, profesores y educadores, y mejoró la participación de los transeúntes para garantizar una educación de los menores sin violencia. El éxito de esta medida se ha demostrado con las tendencias positivas y mediante una evaluación constante desde su introducción.

La eficacia de las restricciones por edad también requeriría un cambio de actitud social. La evaluación continua y el seguimiento a largo plazo pueden ayudar a los responsables políticos a comprender si los hábitos de los menores y sus padres, cuidadores y educadores cambiarán con el tiempo.

Al crecer en el mundo actual de los medios sociales+, los niños y adolescentes deben poder llevar una vida sana y satisfactoria y aprovechar las oportunidades que ofrecen los medios sociales y otros servicios digitales. **Los derechos de los niños son de aplicación tanto en el mundo digital como en el mundo real**, desde el derecho a estar seguros y protegidos de la explotación económica y la delincuencia en todas sus formas (en particular, la violencia sexual) hasta el derecho a acceder a la información, la educación y el ocio.

«Durante décadas hemos hecho que el mundo real sea más seguro para los niños y debemos hacer lo mismo en el mundo digital. Las oportunidades positivas que ofrece la tecnología no pueden ir en detrimento de su seguridad, salud o felicidad.»

Ursula von der Leyen, presidenta de la Comisión Europea

Los niños tienen derecho a crecer en un entorno seguro que favorezca su desarrollo, tanto en el mundo digital como en el mundo real. Si bien debe mantenerse el apoyo a los menores en el mundo real, también debemos reconocer que los entornos digitales se han convertido en una parte cada vez más importante de su vida cotidiana. Por esta razón debe garantizarse su protección por defecto en todos los medios sociales y otros servicios digitales.

Los derechos de los niños deben sustentar las medidas de seguridad infantil en línea. Las posibles restricciones por edad deben respetar plenamente los derechos de los menores y ser proporcionadas y equilibradas con el interés superior del menor. Los medios utilizados para lograrlo deben seguir el ritmo de los avances tecnológicos.

Si bien los proveedores de medios sociales y otros servicios digitales siguen siendo los principales responsables de la seguridad de sus servicios, especialmente en el caso de los menores, **es necesario un ecosistema de agentes para proteger y empoderar a los niños y adolescentes en el entorno de los medios sociales+**. Desde las autoridades reguladoras que deben adoptar las medidas necesarias, hasta los proveedores que ofrecen servicios seguros y adaptados a la edad, pasando por los padres, cuidadores, profesores y educadores, que desempeñan un papel clave a la hora de supervisar y orientar las actividades en línea de los menores. A medida que los menores maduran y los entornos de los medios sociales+ cambian rápidamente, **el éxito del ecosistema depende de las acciones interconectadas de todos los agentes** compartiendo el mismo objetivo: niños y adolescentes creciendo de forma segura en un mundo digital.

Gráfico 1: ecosistema para proteger y empoderar a los menores en línea



Aumento del impulso político para reforzar la seguridad infantil en línea

Durante los últimos meses se ha demostrado que la seguridad infantil en línea se está convirtiendo en una prioridad política en todo el mundo. La **introducción, aplicación y evaluación continua de un «retraso en el acceso a los medios sociales» por parte de Australia ha brindado enseñanzas clave al resto del mundo**. Otros países, como el Reino Unido y Canadá, han seguido su ejemplo con propuestas legislativas previstas, mientras que Indonesia ya ha adoptado una prohibición.

Un informe reciente sugiere que el 92 % de los europeos opina que reforzar la protección de los niños y adolescentes en el espacio digital debería ser una prioridad para la UEⁱ.

Los líderes europeos también han empezado a abordar la cuestión. La Declaración de Jutlandiaⁱⁱ de septiembre de 2025 y la Resolución del Parlamento Europeo en la que se pide una edad mínima digital armonizada a escala de la UEⁱⁱⁱ, la creación por la presidenta Von der Leyen del Grupo Especial sobre Seguridad Infantil en Línea, y las conclusiones recientes del Consejo Europeo^{iv}, son indicaciones claras de que existe un creciente ímpetu político por adoptar medidas concretas para abordar los riesgos cada vez mayores a los que se enfrentan los niños en el mundo digital.

En junio de 2026, por primera vez, el G7 —que incluye a Canadá, Francia, Alemania, Italia, Japón, el Reino Unido, los Estados Unidos y la Unión Europea— acordó al más alto nivel político principios comunes para proteger a los menores de los servicios digitales que plantean riesgos^v.

Además, **varios Estados miembros de la UE han comenzado a legislar con el fin de establecer una edad mínima para acceder a los medios sociales y otros servicios digitales** que puedan exponer a niños y adolescentes a posibles daños. Por ejemplo, Francia propone en la actualidad un límite de 15 años, sobre la base de una lista negra de servicios restringidos. Grecia prevé un límite de 15 años para los servicios de redes sociales en línea. Dinamarca está estudiando un límite para los menores de 16 años, con la opción de reducir la edad con el consentimiento de los padres. Suecia plantea un límite basado en el año en que el menor cumple 15 años, con varios tipos de servicios exentos. Muchos otros, desde Portugal y España hasta Alemania y Polonia, están estudiando la posibilidad de legislar sobre este tema.

En este contexto, la fragmentación del mercado único europeo de servicios digitales constituye un riesgo real. En vista de ello, muchos Estados miembros piden que la cuestión se aborde a escala de la UE. Debe reconocerse que los Estados miembros tienen contextos culturales y nacionales diferentes en lo que respecta a la educación, la alfabetización digital y la protección de los menores. La fragmentación podría hacer que los menores disfrutasen de diferentes niveles de protección en toda la UE. Esto conllevaría además complejidades de orden práctico para las autoridades reguladoras en relación con la aplicación de las normas y unos costes derivados del

cumplimiento más elevados para los proveedores. Todo ello podría tener repercusiones en el desarrollo de medios sociales y otros servicios digitales más seguros, así como en la eficacia de la legislación en materia de seguridad en línea.

La UE ya ha tomado medidas específicas para proteger a los menores. Las recientes decisiones adoptadas por la Comisión Europea solo han puesto de relieve con pruebas concretas la necesidad de abordar las amenazas a las que se enfrentan los niños y adolescentes en línea. Constituyen ejemplos claros las conclusiones preliminares contra Meta y TikTok por el supuesto incumplimiento de las estrictas normas de protección de los menores en línea exigidas en virtud del Reglamento de Servicios Digitales y por no proporcionar mecanismos de fácil acceso que permitan señalar contenidos de abuso sexual infantil. Además, las recientes decisiones históricas de los órganos jurisdiccionales estadounidenses han marcado un punto de inflexión significativo en el debate sobre la responsabilidad de las plataformas.

Breve historia de la protección de los menores en línea

Los esfuerzos por proteger a los niños y adolescentes en línea son tan antiguos como internet y tienen su origen en un momento anterior a los medios sociales, los teléfonos inteligentes y la IA. Las bases de las normas actuales para proteger a los menores en línea se establecieron en la década de 1990 y principios de la década de 2000, con leyes diseñadas para permitir que los servicios y las empresas operen e intercambien información a través de las fronteras. Aunque estas normas no se concibieron con el único fin de proteger a los niños y adolescentes en línea, establecieron muchos de los principios que siguen sustentando la legislación vigente en tres ámbitos.

En primer lugar, la regulación de los medios de comunicación y los servicios digitales en el mercado interior introdujo normas comunes para los servicios de televisión en toda Europa, incluidas salvaguardias contra los contenidos que pudieran ser perjudiciales para los menores. El primer marco armonizado para los servicios en línea o «servicios de la sociedad de la información» (en virtud de la Directiva sobre el comercio electrónico) también apoyó el desarrollo de servicios transfronterizos en línea dentro de la UE.

El segundo ámbito son las normas de protección de datos y privacidad, empezando por las normas comunes de la Directiva sobre protección de datos de 1995 para la recogida y el uso de información personal en todos los Estados miembros.

En tercer y último lugar, la protección de los consumidores. Las normas comunes de la UE abordan las prácticas comerciales engañosas y agresivas. Dichas normas reconocen que los consumidores vulnerables necesitan protección adicional, un principio importante en el entorno digital. Esto incluye los casos en que los niños y adolescentes están expuestos a prácticas comerciales que pueden afectarles de manera diferente a los adultos.

A medida que las tecnologías digitales se integraron profundamente en la vida cotidiana, la UE ha seguido actualizando estos marcos jurídicos para responder a los

nuevos retos. El Reglamento General de Protección de Datos (RGPD) introdujo protecciones específicas para salvaguardar los datos personales y el consentimiento de los niños en línea. La Directiva de Servicios de Comunicación Audiovisual se amplió para abarcar nuevas formas de contenidos audiovisuales y plataformas de intercambio de vídeos. Por último, el Reglamento de Servicios Digitales estableció normas para los servicios intermediarios en línea, también con el fin específico de proteger a los menores.

Esta evolución refleja una tendencia más amplia: las tecnologías digitales ya no encajan claramente en una única categoría reglamentaria o jurídica. Los medios sociales y otros servicios digitales combinan elementos de los medios de comunicación, la comunicación en general, el comercio y el tratamiento de datos, a menudo dentro de la misma plataforma. En consecuencia, para ser eficaz, la protección de los menores en línea debe abordarse desde un enfoque global y basarse en instrumentos en diversos ámbitos del Derecho de la Unión, como la regulación de las plataformas, la protección de datos, la protección de los consumidores y la regulación de los medios audiovisuales.

Con el rápido desarrollo y despliegue de la IA, se están superponiendo los riesgos para los menores en línea. Esto va acompañado de la evolución continua de los medios sociales y otros servicios digitales para captar y mantener la participación de los usuarios en la «economía de la atención» actual. La necesidad de que las autoridades reguladoras intervengan para reforzar la protección de los menores y capacitarlos para navegar por el mundo de los medios sociales+ de forma segura es mayor que nunca.

Las pruebas sobre los riesgos y oportunidades a los que se enfrentan los menores en línea

El rápido cambio tecnológico ha traído consigo oportunidades extraordinarias para que los niños intercambien puntos de vista con sus iguales, expresen su creatividad y accedan al conocimiento y al apoyo. Sin embargo, los niños no son adultos y el entorno de los medios sociales+ los expone a diversos riesgos para su salud física y mental y su desarrollo a diferentes edades. Los factores socioeconómicos e individuales, como el origen familiar y el género, así como el diseño de los medios sociales y otros servicios digitales, también pueden influir de forma decisiva.

Es fundamental disponer de pruebas sólidas sobre la relación entre los riesgos y los daños y los medios sociales y otros servicios digitales para fundamentar las medidas adecuadas para proteger y empoderar a los menores en línea. Las características, funcionalidades o formatos específicos utilizados en los medios sociales+ pueden ser perjudiciales en distinta medida, dependiendo de las circunstancias sociales y personales de un niño o adolescente. Los menores pertenecientes a grupos raciales, étnicos y religiosos minoritarios, los miembros de la comunidad LGBTIQ +, los que tienen necesidades educativas especiales o problemas

de salud mental preexistentes pueden ser especialmente vulnerables a los perjuicios derivados de las actividades en línea. Por supuesto, esta vulnerabilidad se ve amplificada por los medios sociales y otros servicios digitales con contenidos o diseños perjudiciales, manipuladores o adictivos. A medida que estas características evolucionan, también deben hacerlo la investigación y la recopilación de pruebas.

Los riesgos para la salud física y mental que plantean los medios sociales y otros servicios digitales para los menores son amplios. En términos de salud física, un tiempo excesivo frente a la pantalla sustituye al juego al aire libre y al deporte y puede afectar a la salud, el estado físico y el sueño de los niños. El uso de medios sociales+ y dispositivos a una edad temprana desplaza la exploración práctica y las interacciones sociales presenciales. Esto puede afectar al desarrollo socioemocional y a la susceptibilidad a los problemas de salud mental. El uso prolongado de dispositivos también puede provocar problemas, como problemas musculoesqueléticos y fatiga ocular digital.

Los riesgos para la salud mental que plantea el uso de los medios sociales y otros servicios digitales para los niños son significativos. Los riesgos del entorno de los medios sociales+ que perjudican directamente la salud mental de los niños se entrecruzan con su potencial para exacerbar los problemas de salud mental preexistentes, como la depresión y la ansiedad. También en este caso, los factores sociales e individuales determinan la exposición de los niños y adolescentes a los riesgos.

En general, el elevado uso de los medios sociales y otros servicios digitales entre niños y adolescentes se asocia a problemas de sueño y concentración, así como a un aumento de las tasas de depresión y ansiedad. Las características de diseño adictivo amplifican estos efectos al fomentar la comprobación compulsiva, el «miedo a perderse algo» (FOMO) y una mayor comparación social. Esto puede erosionar la autoestima de los menores y aumentar su estrés. Los sistemas de amplificación algorítmica y de recomendación tienen el potencial de mejorar la desinformación y la incitación al odio. Estos efectos causan graves daños, en particular, a los grupos vulnerables en línea.

Los riesgos de exposición de los menores a contenidos delictivos e ilícitos en línea son considerables. Tanto los adultos como los menores explotan deliberadamente los medios sociales y otros servicios digitales, incluidas las plataformas de juegos, para interactuar con niños y adolescentes. Los riesgos incluyen la exposición al abuso sexual de menores (material), la captación de menores, el ciberacoso, la radicalización y la incitación a cometer actos ilegales, violentos o terroristas. El uso generalizado de herramientas de IA plantea graves amenazas para los niños y adolescentes derivadas de la producción de contenidos falsos de abuso sexual de menores (por ejemplo, las ultrafalsificaciones). Estos usos indebidos tienen efectos drásticos en el desarrollo de los menores, su salud mental y física y, en los casos más graves, pueden costarles la vida.

Los proveedores de medios sociales y otros servicios digitales siguen siendo los principales responsables de mantener la seguridad de los menores cuando utilicen sus servicios. Además, los padres y cuidadores desempeñan un papel importante a la hora de supervisar el tiempo en línea de los niños y adolescentes y de orientar a los menores a la hora de abordar juntos los riesgos a los que se enfrentan en los entornos de los medios sociales+. Garantizar actividades no digitales e interacciones en persona adecuadas es crucial a todas las edades.

A pesar de los múltiples daños potenciales, **el mundo de los medios sociales+ ofrece muchas oportunidades a los niños y adolescentes.** Cuando los menores están capacitados para interactuar de forma segura en línea y tienen capacidades digitales sólidas, el uso de los medios sociales y otros servicios digitales puede favorecer el bienestar, la conexión social, proporcionar redes de apoyo entre iguales, oportunidades para la autoexpresión, el compromiso cívico y el aprendizaje independiente. Las iniciativas específicas en materia de capacidades digitales — como la estrategia «Una Internet mejor para los niños» de la UE, los Centro de Seguridad en Internet y la integración de la alfabetización mediática en los planes de estudio nacionales de educación y formación— han demostrado su capacidad para mejorar el pensamiento crítico, la resiliencia frente a la desinformación y la capacidad de los menores para desenvolverse de forma segura en línea.

Las redes sociales y otros servicios digitales «seguros desde el diseño» podrían contribuir al empoderamiento y la participación en línea de niños y adolescentes apoyando la adquisición de capacidades digitales y la alfabetización mediática. La educación digital adaptada a la edad impartida por los centros educativos con el apoyo de padres y cuidadores también podría equipar a los menores para aprovechar las oportunidades del mundo digital y gestionar los posibles riesgos y daños.

La necesidad de abordar los riesgos específicos de cada edad

A medida que los niños crecen y se hacen más independientes, disminuye la capacidad de los padres para supervisar sus actividades en internet y aumenta el papel de la influencia de los compañeros. Durante la adolescencia, a medida que llegan a la mayoría de edad, los menores son cada vez más autónomos en el uso de internet y más capaces de comprender y abordar los riesgos a los que están expuestos en internet. Naturalmente, a los 3 años no se tienen las mismas necesidades que a los 16, lo que pone de relieve la **importancia de que el enfoque en materia de seguridad infantil en internet sea sensible a la fase del desarrollo, como el que se aplica en el presente informe, diferenciando entre distintos grupos de edad:**

Los menores de 3 años sufren principalmente riesgos relacionales y «tecnointerferencias»¹ como usuarios pasivos en internet. Los riesgos se derivan en

¹ La interrupción de la interacción entre padres e hijos por la tecnología.

gran medida del hecho de que los cuidadores sustituyen la interacción directa por pantallas para «calmar» o distraer a los niños pequeños. Esto puede afectar a la capacidad de atención de los niños, la adquisición del lenguaje y el desarrollo socioemocional.

Entre los 3 y los 5 años, los niños se inician como usuarios independientes con supervisión y son cada vez más vulnerables a los riesgos presentes en los entornos en línea derivados de una mayor exposición a las pantallas. Los medios sociales y otros servicios digitales que están optimizados para generar gratificación inmediata, recompensas repetitivas y continua estimulación externa no se ajustan en absoluto a las capacidades aún en desarrollo de los niños y pueden perjudicar su desarrollo a largo plazo.

Entre los 6 y los 9 años, el uso de los medios sociales y otros servicios digitales por parte de los niños se expande significativamente. La validación externa procedente del entorno digital (como los «likes», las puntuaciones o las clasificaciones) interfieren con una autoestima incipiente, sustentada en las competencias que los niños van adquiriendo en el mundo real. Esto les puede agravar la ansiedad al comparar su rendimiento con los compañeros, aumentando así su vulnerabilidad al ciberacoso, la incitación al odio y el acoso por parte de compañeros.

Entre los 10 y los 12 años, el acceso de los niños a los espacios de los medios sociales+ se convierte en un requisito previo esencial para la participación social. A esta edad, los niños se encuentran en una etapa en la que convergen del modo más crítico las vulnerabilidades de su desarrollo y la amplificación generada por las plataformas. Los sistemas de recomendación algorítmica intensifican la comparación social, la exposición a contenidos nocivos o ilícitos (como el abuso sexual de menores, la propaganda extremista y la desinformación) y a patrones de diseño adictivos que aumentan los síntomas de la depresión y la ansiedad. Estudios prospectivos recientes sugieren que la adquisición de un teléfono inteligente por primera vez a los 12 años (en lugar de a los 13) puede estar relacionada con un mayor riesgo de depresión y otros problemas de salud mental al cabo de un año^{vi}. Este ejemplo pone de relieve que, en general, los niños menores de 13 años son especialmente vulnerables.

Entre los 13 y 15 los años, los adolescentes pasan del uso de los medios sociales y otros servicios digitales bajo supervisión al uso autónomo progresivo. A esta edad, las formas tradicionales de supervisión por parte de cuidadores y educadores escolares resultan cada vez más ineficaces. Los riesgos proceden cada vez más de las estructuras de los medios sociales y otros servicios digitales, más que del comportamiento individual por sí solo. Un reto clave reside en abordar los sistemas algorítmicos que estructuran la exposición e influyen en el comportamiento y funcionan con una transparencia limitada.

La transición a la autonomía es una parte normal del crecimiento en el mundo actual de internet, al igual que en el mundo real. Por lo tanto, la cuestión no es cómo frenar

la transición de los adolescentes a la autonomía, sino cómo limitar su exposición a peligros durante una fase de su desarrollo en la que la vulnerabilidad es máxima. Una protección eficaz requiere un enfoque multinivel diferenciado por fases del desarrollo que combine la regulación de los medios sociales y otros servicios digitales, las intervenciones educativas y el apoyo a la autorregulación y al uso crítico de los medios de comunicación.

Por último, **entre los 16 y los 18 años**, los adolescentes se encuentran en una fase en la que se desarrollan tanto la consolidación de la identidad como la autonomía. La evolución de las capacidades de los adolescentes les capacita mejor para comprender y gestionar los riesgos a los que se enfrentan en internet. Sin embargo, el desarrollo neurobiológico dista mucho de haberse completado y los riesgos de adicción, ansiedad y problemas de salud mental se ven exacerbados por el uso de los medios sociales y otros servicios digitales. Los adolescentes a esta edad deben adquirir las capacidades necesarias (por ejemplo, de pensamiento crítico y de evaluación) para navegar con éxito y seguridad por el mundo digital y aprovechar todo su potencial.

Seis principios rectores para proteger y empoderar a los menores en internet

La presencia tanto de riesgos como de oportunidades para los niños y adolescentes en el entorno de los medios sociales+ requiere un marco político global que proteja y empodere a los menores en internet. Los siguientes **Seis Principios Rectores elaborados por los copresidentes orientaron el trabajo del Grupo Especial** y se reflejan en la estructura del presente informe. Las medidas deben basarse en pruebas y análisis sólidos de los retos y oportunidades a los que se enfrentan los niños en internet. La aplicación y evaluación efectivas son fundamentales para lograr los resultados.

- **Principio 1: Enfoque por fases del desarrollo (véase el capítulo 1)**

Garantizar unas normas adecuadas a cada edad y orientaciones diferenciadas por edades. El desarrollo por etapas de niños y adolescentes exige el diseño y el despliegue de medidas de protección que aborden los riesgos a los que se enfrentan a edades específicas. Cuando sea posible, estas medidas deberían tener en cuenta las circunstancias personales y sociales de los niños, las cuales pueden agravar su exposición al riesgo.

- **Principio 2: Igualdad y diversidad (véase el capítulo 2)**

Reconocer que edades y grupos socioeconómicos diferentes implican una desigualdad en los riesgos y la exposición a los peligros de internet. El género, la sexualidad, el origen racial, étnico y religioso, las necesidades educativas especiales y los problemas de salud mental preexistentes determinan la vulnerabilidad de los menores a los peligros de internet. Estos factores también influyen en los recursos y

capacidades que los padres y cuidadores tienen para apoyar a los niños y adolescentes en su camino hacia la autonomía.

- **Principio 3: Protección de los menores (véase el capítulo 3)**

Los niños y adolescentes deben poder utilizar espacios seguros en los medios sociales+. En el diseño de los medios sociales y otros servicios digitales debería incorporarse la protección de los menores contra los contenidos nocivos, las características adictivas, la negligencia digital² y los delitos en línea (por ejemplo, el abuso sexual). Debería ser fácil que los menores puedan denunciar cualquier contenido o elemento nocivo. Debería darse prioridad a estas denuncias y los proveedores deberían retirar rápidamente los contenidos o elementos nocivos.

- **Principio 4: Responsabilidad de los servicios digitales y derechos de los consumidores (véase el capítulo 3)**

Los proveedores de medios sociales y otros servicios digitales deben asumir la responsabilidad primaria de garantizar que los espacios en línea sean seguros para que los menores accedan a ellos y los utilicen. Incentivar la adopción de medidas de seguridad en los servicios digitales ya en la fase del diseño y aplicar rápidamente una regulación sobre los contenidos. La carga de la prueba de que las características de sus servicios no son perjudiciales debe recaer sobre los proveedores de medios sociales y otros servicios digitales, antes de que puedan acceder a niños y adolescentes.

- **Principio 5: Empoderamiento y educación en medios de comunicación (véase el capítulo 4)**

Capacitar a padres y cuidadores, profesores y educadores para apoyar la transición gradual de los niños y adolescentes hacia un uso de internet seguro y autónomo. Ofrecer suficientes oportunidades (por ejemplo, formación en alfabetización digital y mediática) y una infraestructura adecuada para que los padres puedan reflexionar sobre sus propias actividades y orientar las interacciones en internet de los menores. Las medidas deben adaptarse a las funciones de los cuidadores y educadores, que evolucionan a medida que los niños y adolescentes maduran.

- **Principio 6: Derechos y participación de los niños (véase el capítulo 4)**

Salvaguardar el derecho de los niños a la participación, la interacción y la creación conjunta seguras, tanto en internet como en el mundo real. Los derechos del niño, tal como se entienden en los marcos internacionales pertinentes,³ deben sustentar

² La omisión reiterada por parte de un cuidador de sus deberes de atención, capacidad de respuesta, supervisión o protección adecuadas del desarrollo de un menor debido a que las tecnologías digitales interfieren con las funciones asistenciales esenciales, las sustituyen o las disminuyen.

³ En particular, la Convención de las Naciones Unidas sobre los Derechos del Niño y las Observaciones generales del Comité de los Derechos del Niño, la Carta de los Derechos Fundamentales de la Unión Europea y la Estrategia de la UE sobre los Derechos del Niño.

siempre las medidas de protección de la infancia. Las restricciones de edad deben respetar los derechos del niño en internet, ser proporcionadas, limitadas en el tiempo y equilibradas con el interés superior del niño. Esto también pone de relieve la necesidad de invertir en actividades al margen de internet para menores de todas las edades y de promoverlas.

Consejeros especiales del presidente y copresidentes del Grupo Especial sobre Seguridad Infantil en Línea

Prof. Dr. Jörg M. Fegert

Dra. Maria Melchior



Prof. Dr. Jörg M. Fegert

Director médico del
Departamento de Psiquiatría,
Psicosomática y Psicoterapia
infantojuvenil del Hospital
Universitario de Ulm



Dra. Maria Melchior

Directora de investigación del
Instituto Nacional de Salud e
Investigación Médica de
Francia (INSERM)

SEIS PRINCIPIOS RECTORES

para proteger y empoderar a los menores en internet

SEGURIDAD INFANTIL EN INTERNET

ANÁLISIS DE LA SITUACIÓN

ENFOQUE POR FASES DEL DESARROLLO

Asegurar una regulación adecuada a la edad y orientaciones diferenciadas

IGUALDAD Y DIVERSIDAD

Reconocer que los diferentes grupos están expuestos a riesgos y peligros digitales distintos

PROTECCIÓN DE LOS MENORES

Proteger contra los contenidos nocivos, el diseño adictivo, el abandono digital y los delitos (p.ej., abuso sexual, acoso)

RESPONSABILIDAD DE LOS SERVICIOS DIGITALES Y DERECHOS DE LOS CONSUMIDORES

Incorporar la seguridad y la regulación del contenido desde el diseño

EMPODERAMIENTO Y EDUCACIÓN EN MEDIOS DE COMUNICACIÓN

Posibilitar que padres y cuidadores ayuden a los menores a usar responsablemente las habilidades digitales y la alfabetización mediática

DERECHOS Y PARTICIPACIÓN DE LOS NIÑOS

Salvaguardar el derecho a la participación y la cocreación en internet con seguridad

MEDIDAS

EVALUACIÓN

Recomendaciones clave para proteger y empoderar a los menores en internet

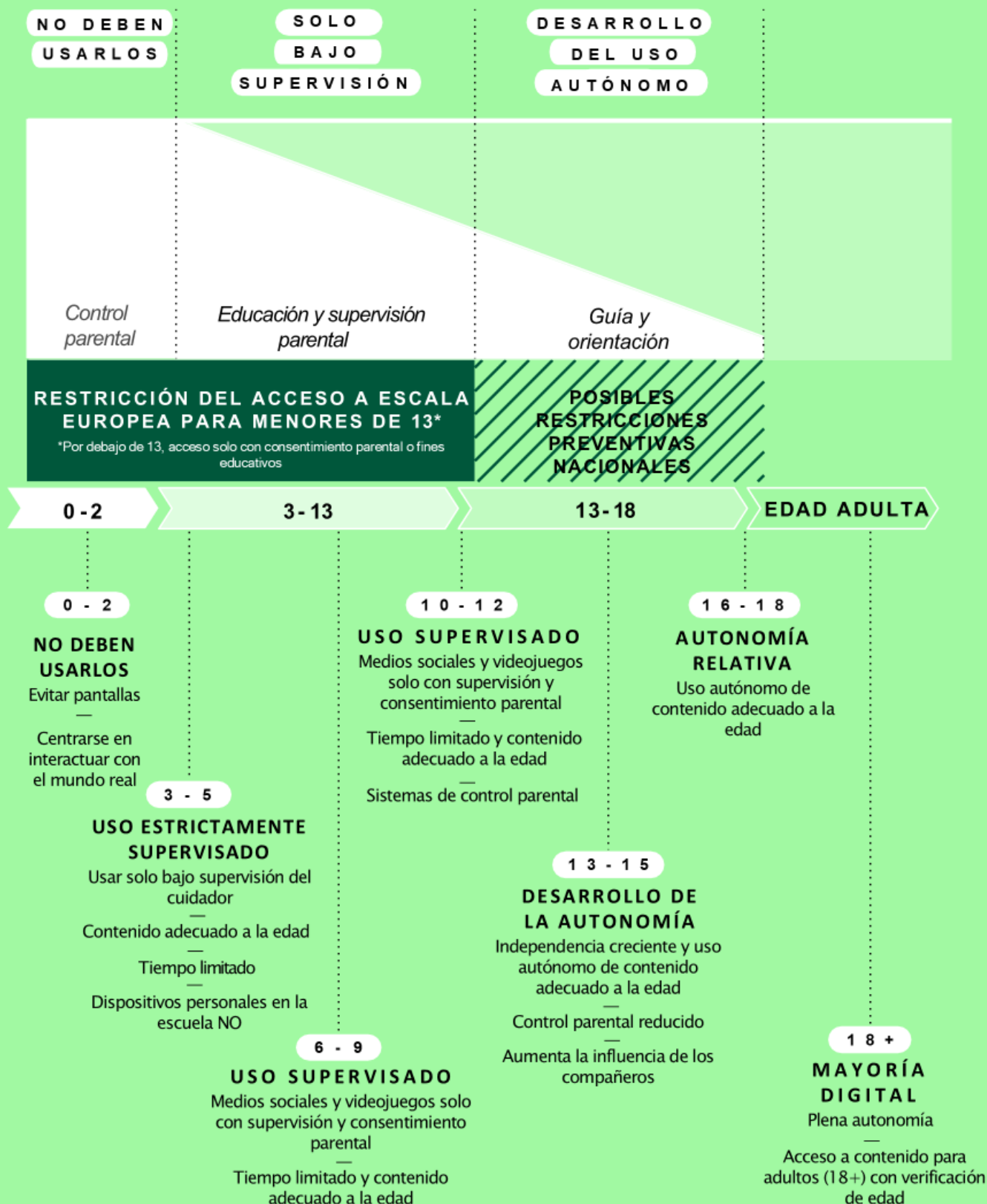
El objetivo general de las recomendaciones del presente informe, basado en un enfoque sensible a las fases del desarrollo y que refleja los seis principios rectores, es equilibrar la necesidad de proteger a niños y adolescentes en internet con su derecho a participar y aprovechar las oportunidades del mundo de los medios sociales.

Recomendaciones sobre el uso adecuado a la edad de los medios sociales y otros servicios digitales

- 1. De 0 a 2 años Evitar las pantallas y los medios sociales+.** Evitar en gran medida la exposición a pantallas durante la primera infancia no significa una prohibición total. De hecho, reconoce las necesidades de desarrollo de los niños en cuanto al apego, el desarrollo sensorial y la adquisición temprana del lenguaje. Los padres y cuidadores deben dar prioridad a las interacciones presenciales y ser conscientes de su propio uso de los dispositivos digitales para ofrecer un modelo positivo y evitar la «tecnointerferencia». Este enfoque está en consonancia con las recomendaciones de la Organización Mundial de la Salud para evitar alteraciones en el desarrollo neurobiológico y cognitivo de los niños y en la formación de vínculos emocionales, así como problemas físicos (por ejemplo, que afecten a la visión).
- 2. De 3 a 12 años: Uso supervisado de medios sociales+ y dispositivos adecuados a la edad.** No debe permitirse a los niños el uso no supervisado de dispositivos con acceso a internet. Los centros educativos deben acondicionar instalaciones para el uso supervisado y limitado de dispositivos con fines educativos, fomentando la alfabetización digital y mediática, la resiliencia emocional y la reflexión crítica sobre los riesgos. Los padres y cuidadores deben supervisar y apoyar gradualmente la autonomía digital con medios sociales y otros servicios digitales adecuados a la edad. También deben conversar regularmente con los niños sobre los posibles beneficios y riesgos de las interacciones de los menores en internet. Tanto los cuidadores como los educadores deben seguir animando a los niños de esta edad a participar en actividades al margen de internet.
- 3. De 13 a 18 años: Evolución del uso autónomo de los medios sociales+ adecuados a la edad.** De 13 a 18 años, los adolescentes solo deberían tener acceso a medios sociales y a otros servicios digitales adecuados a su edad y «seguros por defecto» que hayan introducido activamente funciones de seguridad clave (por ejemplo, límites al *scroll* infinito y a los sistemas de recomendación). Hasta que se desarrollen estos medios sociales y otros servicios digitales «seguros por defecto», el control y la supervisión parental individual adecuada a la edad siguen siendo esenciales. Podría considerarse la adopción de medidas

preventivas adicionales por parte de las autoridades reguladoras. A medida que los adolescentes mayores de 16 años avanzan hacia una mayor autonomía digital, persisten los riesgos relacionados con la exposición a contenidos nocivos en internet. Los padres y cuidadores deben seguir conversando con los menores sobre sus experiencias en internet. Los adolescentes deberían tener un acceso privilegiado a los servicios de ayuda y a los sistemas de reclamaciones, y al mismo tiempo beneficiarse de redes de ayuda entre compañeros que promuevan el uso responsable de los medios sociales y otros servicios digitales.

Edades adecuadas para que los menores usen los medios sociales+



Recomendaciones para proteger a los niños y adolescentes en internet

- **Proponer una restricción del acceso a los medios sociales y otros servicios digitales armonizada a escala de la UE para los menores de 13 años.**

Una restricción del acceso a los medios sociales y otros servicios digitales armonizada a escala de la UE para los menores de 13 años. Una restricción armonizada del acceso facilitaría la aplicación de mecanismos de control de la edad proporcionados y respetuosos de los derechos, e impulsaría los requisitos de seguridad desde el diseño para los proveedores de medios sociales y otros servicios digitales. Los menores de 13 años deben tener un acceso de duración limitada a entornos de medios sociales+ adecuados a su edad, únicamente con autorización y supervisión parental o en contextos educativos. A partir de los 13 años, el uso que hacen los adolescentes de los medios sociales y otros servicios digitales adecuados a su edad y seguros debe poder evolucionar hacia la autonomía.

Unas normas armonizadas a escala de la UE sobre una edad mínima de 13 años contribuirían al correcto funcionamiento del mercado único al garantizar un marco único de cumplimiento para los proveedores. Las normas armonizadas facilitarían la aplicación y la supervisión por parte de las autoridades reguladoras, tanto a escala nacional como de la UE. También garantizarían un mismo nivel de protección para todos los menores en internet en toda la UE, independientemente de los contextos socioeconómicos, culturales y nacionales.

- **Introducir sistemas eficaces de control de la edad para aumentar la seguridad ya desde el diseño y enfoques adecuados a la edad para proteger y empoderar a los menores en internet.**

Los métodos de control de la edad —tanto la verificación como la estimación— deben ser proporcionados y respetar unos requisitos mínimos, en particular en lo que respecta a los derechos fundamentales de los usuarios, incluidos los derechos de los menores y las garantías conexas. Cualquier método empleado para comprobar la edad debe respetar las normas más estrictas en materia de privacidad y protección de datos, y no debe implicar el tratamiento de los documentos de identidad ni de los datos biométricos con el fin de estimar la edad. Deben implantarse normas técnicas, como la «prueba de conocimiento cero», a fin de garantizar que ni la plataforma encargada de evaluar la edad ni el proveedor de verificación de la edad reciban información alguna que permita rastrear o identificar al usuario.

Los métodos de control de la edad deben determinar con precisión la edad o los grupos de edad requeridos, y ser fáciles y fiables en la práctica, en condiciones

reales. Los métodos deben ser sólidos para evitar su elusión y las amenazas a la ciberseguridad, inclusivos (y no discriminatorios) y estar disponibles por igual para todas las personas que necesiten utilizarlos. Los proveedores de medios sociales y otros servicios digitales deben cumplir su obligación de evitar que los menores se vean expuestos a servicios de riesgo y que haya usuarios que se hagan pasar por niños y adolescentes.

- **Ampliar y armonizar las normas sobre las características clave de seguridad en el diseño de las redes sociales y otros servicios digitales.**

Los medios sociales y otros servicios digitales debería incorporar salvaguardias claras de seguridad desde el diseño y adecuadas a la edad (por ejemplo, posibles límites al *scroll* infinito, a la reproducción automática, a las notificaciones automáticas y a los motores de recomendación personalizados problemáticos). Para hacer frente al diseño que genera adicción, los patrones oscuros, el contacto no solicitado y las espirales de contenido, los ajustes predeterminados de protección deberían ser parte integrante de los medios sociales y otros servicios digitales. La ampliación y armonización de las normas sobre los elementos clave de seguridad garantizaría la seguridad y la uniformidad en todo el entorno de las redes sociales+. Debido al rápido desarrollo de la tecnología, cualquier norma sobre características clave de seguridad debería ser adaptable para poder abordar en permanencia nuevas características nocivas de diseño.

- **Trasladar la carga de la prueba de que sus productos y servicios son seguros para los menores a los medios sociales y otros proveedores de servicios digitales.**

Deberían aplicarse restricciones específicas de edad hasta que los proveedores de medios sociales y otros servicios digitales introduzcan elementos clave de diseño de seguridad que protejan a los niños y adolescentes. Hasta que los proveedores no demuestren haber incorporado elementos seguros y adecuados a la edad, cumpliendo así las medidas nacionales y de la UE, no deberían tener acceso a los menores. Cuando exista una versión «segura por defecto», los elementos inadecuados para la edad (elementos para adultos) solo deberían activarse tras unos controles de la edad eficaces.

- **Reforzar las capacidades de ejecución y evaluación.**

Habida cuenta de las múltiples normas que se aplican actualmente a la seguridad infantil en internet (el Reglamento de Servicios Digitales, el Reglamento General de Protección de Datos, el Reglamento de Inteligencia Artificial, etc.), las autoridades de control deberían intensificar la cooperación y el intercambio de información entre los marcos jurídicos. Esto es fundamental para evitar incoherencias y garantizar un entorno jurídico coherente, predecible y eficaz

basado en la protección de los derechos fundamentales. La Comisión Europea debería explorar mecanismos que permitan una cooperación fluida entre las autoridades de supervisión para aprovechar las estructuras de ejecución existentes. Además, es necesario valorar si se necesitan recursos adicionales y reestructuración para las autoridades reguladoras responsables de la aplicación y la evaluación. Deberían considerarse actuaciones para reforzar el papel de la sociedad civil en la ejecución y su contribución a la capacidad de ejecución, también a través de las estructuras existentes. La ejecución debería ser complementaria y evitar actuaciones contradictorias.

- **Adoptar rápidamente medidas para garantizar que los proveedores de medios sociales y otros servicios digitales tengan obligaciones claras para prevenir, detectar, denunciar y bloquear el abuso sexual de menores en internet, también en las comunicaciones interpersonales.**

Debería colmarse rápidamente la laguna en materia de seguridad infantil que existe actualmente debido a la expiración del Reglamento provisional por el que se establecen normas para prevenir y combatir el abuso sexual de menores. Los colegisladores de la UE deberían adoptar rápidamente la propuesta de Reglamento para el largo plazo destinado a prevenir y combatir el abuso sexual de menores. Más del 80 % de las investigaciones de abuso sexual de menores parten de denuncias presentadas por los proveedores de medios sociales y otros servicios digitales. A menudo, los menores tienen demasiado miedo a denunciar abusos. Detectar material de abuso sexual de menores, también en las comunicaciones interpersonales, es a menudo la única manera de detenerlo.

- **Los Estados miembros pueden introducir restricciones preventivas adicionales de acceso a los medios sociales y otros servicios digitales a partir de los 13 años.**

Las restricciones prudenciales adicionales de acceso deben ser complementarias a la restricción de acceso a los medios sociales y otros servicios digitales a escala de la UE contemplada en el punto 13. Los adolescentes solo pueden tener acceso a un entorno de medios sociales+ que sea seguro, tanto en contenidos como en las características de diseño, adecuado a la edad y diseñado teniendo en cuenta sus derechos y necesidades. Los Estados miembros tienen diversos contextos históricos y nacionales diversos y pueden preferir fijar un umbral de edad superior a los 13 años. Todas las restricciones nacionales de acceso prudenciales adicionales deberían estar sujetas a una evaluación continua y, en su caso, reevaluarse, una vez que los medios sociales y otros servicios digitales sean seguros por defecto para niños y adolescentes.

- **Reforzar la aplicación de las normas sobre el acceso de los investigadores a los datos y su control.**

El acto delegado de julio de 2025 relativo al artículo 40 del Reglamento Delegado de Servicios Digitales ha abierto, en principio, una nueva vía para que los investigadores autorizados accedan a los datos de las plataformas en línea. Estos datos pueden utilizarse para llevar a cabo investigaciones que contribuyan a la detección, identificación y comprensión de los riesgos sistémicos, así como a la evaluación de las medidas de mitigación de riesgos que promueven la seguridad infantil en internet.

Que esta vía cumpla su cometido depende del cumplimiento por parte de los proveedores de medios sociales y otros servicios digitales y de la aplicación efectiva por parte de las autoridades reguladoras. También se basa en la extensión de los servicios cubiertos y en la calidad y continuidad de los datos facilitados. La Comisión debería evaluar el funcionamiento operativo de los requisitos del acceso a datos y el escrutinio del artículo 40 tras la experiencia inicial de los investigadores al amparo del acto delegado. Esto es fundamental para garantizar que las plataformas en línea hagan un seguimiento de las solicitudes de acceso a los datos con fines de cumplimiento, evaluación de riesgos e investigación.

Las obligaciones de acceso a los datos no solo son un elemento clave del conjunto de instrumentos de transparencia del Reglamento de Servicios Digitales, sino que también forman parte de las responsabilidades más amplias de mitigación de riesgos de los proveedores de medios sociales y otros servicios digitales. También debe alentarse a las plataformas más pequeñas a que permitan a los investigadores acceder a los datos, teniendo en cuenta los riesgos que estas plataformas plantean para los menores y el papel del escrutinio independiente a la hora de abordar estos riesgos. El uso de los principios rectores FAIR⁴ para la gestión y administración de datos científicos debe ser la norma en la aplicación del artículo 40.

Recomendaciones para empoderar a los niños y adolescentes en línea

- **Ampliar las oportunidades seguras para que los menores participen activamente en la configuración del entorno de los medios sociales y otros servicios digitales.**

⁴ Los principios rectores FAIR para la gestión y administración de datos científicos se introdujeron en 2016 en una publicación de la revista *Scientific Data*. Los principios tienen por objeto mejorar la infraestructura de apoyo a la reutilización de datos académicos mediante el refuerzo de la capacidad de las máquinas y de las personas para encontrar y utilizar datos. Véase: Wilkinson, M.D., et al. (2016). [The FAIR Guiding Principles for scientific data management and stewardship](#) (Los principios rectores FAIR para la gestión y administración de datos científicos). Datos científicos, 3.

Los niños y adolescentes deben tener oportunidades significativas para configurar activamente la legislación, las políticas y las iniciativas educativas que promuevan la seguridad y el empoderamiento de los niños en línea. Debe ampliarse el uso de las herramientas de participación infantil y juvenil para fundamentar este trabajo. Más concretamente, debe incluirse a los niños en el diseño conjunto de las políticas de seguridad, los programas de formación, las evaluaciones y las directrices. Las medidas deben ser objeto de un seguimiento y una evaluación continuos para valorar su impacto en la seguridad y los derechos de los niños.

Los procesos de participación deben garantizar que los niños reciban información clara, comprendan cómo se utilizarán sus contribuciones y reciban comentarios sobre los resultados. Deben realizarse esfuerzos especiales para incluir a los niños de grupos desfavorecidos, marginados y vulnerables. Todas las actividades de participación que impliquen a niños deben ir acompañadas de medidas de salvaguardia adecuadas.

- **Reforzar los mecanismos de denuncia y los derechos de los consumidores para niños y adolescentes.**

Los proveedores de medios sociales y otros servicios digitales deben dar prioridad a los informes y quejas de niños y adolescentes en los procedimientos de moderación de contenidos. Deben reforzarse las obligaciones de los proveedores en virtud de los marcos existentes para financiar adecuadamente las líneas telefónicas de ayuda y los mecanismos de reclamación. Estos mecanismos deben ser adecuados para la edad, fáciles de usar, accesibles, respetuosos de la privacidad y eficaces.

- **Integrar acciones de educación y alfabetización digitales para menores, padres y cuidadores, profesores y educadores.**

La educación y la alfabetización digitales deben integrarse en todos los niveles educativos como una competencia básica clave para los menores, los padres y los profesores. El bienestar digital debe integrarse en la educación digital para todos.

La educación debe permitir a los niños y adolescentes evaluar de forma crítica la información y las fuentes en línea y reconocer las técnicas de manipulación, como la desinformación, las falsedades profundas y la publicidad personalizada. También debe lograr que los menores, los padres y los profesores comprendan cómo se crean y comparten los contenidos digitales y cómo los algoritmos configuran lo que los usuarios ven y experimentan en el mundo de los medios sociales y otros servicios digitales.

La educación estructurada en materia de seguridad en línea debe desarrollar capacidades prácticas para proteger los datos personales, gestionar los ajustes

de privacidad, mantener identidades digitales seguras e identificar los riesgos en los medios sociales, los mensajes y los entornos de juego en particular. Estas capacidades deben desarrollarse progresivamente, empezando por los hábitos básicos de seguridad y avanzando hacia una comprensión más compleja de las huellas digitales, el consentimiento y los riesgos de las plataformas. El uso saludable de pantallas debe abordarse mediante orientaciones sobre el equilibrio, la gestión de la atención y el reconocimiento de patrones de uso excesivos o nocivos.

- **Crear más oportunidades e infraestructuras adecuadas para apoyar las actividades fuera de línea.**

Los Estados miembros y las autoridades locales deben mantener y ampliar el acceso a deportes, artes, clubes juveniles, bibliotecas y espacios comunitarios asequibles para fomentar una participación saludable en el mundo real y crear alternativas atractivas al uso excesivo de pantallas entre los menores. Esto debe incluir la inversión en entornos seguros, inclusivos y adaptados a la edad en los que los menores puedan conectar, aprender, jugar y establecer relaciones positivas dentro de sus comunidades.

- **Promover la creación conjunta de directrices para los padres.**

Junto con las asociaciones de padres, la UE y los Estados miembros deben promover el desarrollo de directrices para padres. Las directrices podrían proporcionar asesoramiento claro y accesible para capacitar a los padres y cuidadores a la hora de apoyar el uso seguro, responsable y positivo de los menores con los entornos de los medios sociales y otros servicios digitales. Las directrices deben proporcionar asesoramiento práctico sobre ámbitos clave, como la seguridad y la privacidad en línea, el bienestar digital, el uso ético y responsable y el acceso al apoyo.

- **Garantizar una financiación pública suficiente y normas comunes para las organizaciones de la sociedad civil y el asesoramiento entre iguales.**

La UE y los Estados miembros deben velar por que los Centros de Seguridad en internet y organizaciones comparables de la sociedad civil sigan recibiendo recursos financieros suficientes y su trabajo se base en normas comunes elaboradas por expertos. Esto es vital para mantener y seguir desarrollando sus actividades, incluidos los servicios de sensibilización, formación y apoyo. La financiación pública es crucial para garantizar la independencia y la cohesión.

La financiación también debe apoyar un mayor desarrollo del asesoramiento entre iguales, las líneas de ayuda, las líneas directas, los recursos educativos, las

campañas de sensibilización y las actividades de desarrollo de capacidades. Deben destinarse inversiones adicionales para aumentar la visibilidad, la accesibilidad y el alcance de estos instrumentos, también entre los menores vulnerables, y para apoyar iniciativas que promuevan entornos más seguros en los medios sociales y otros servicios digitales.

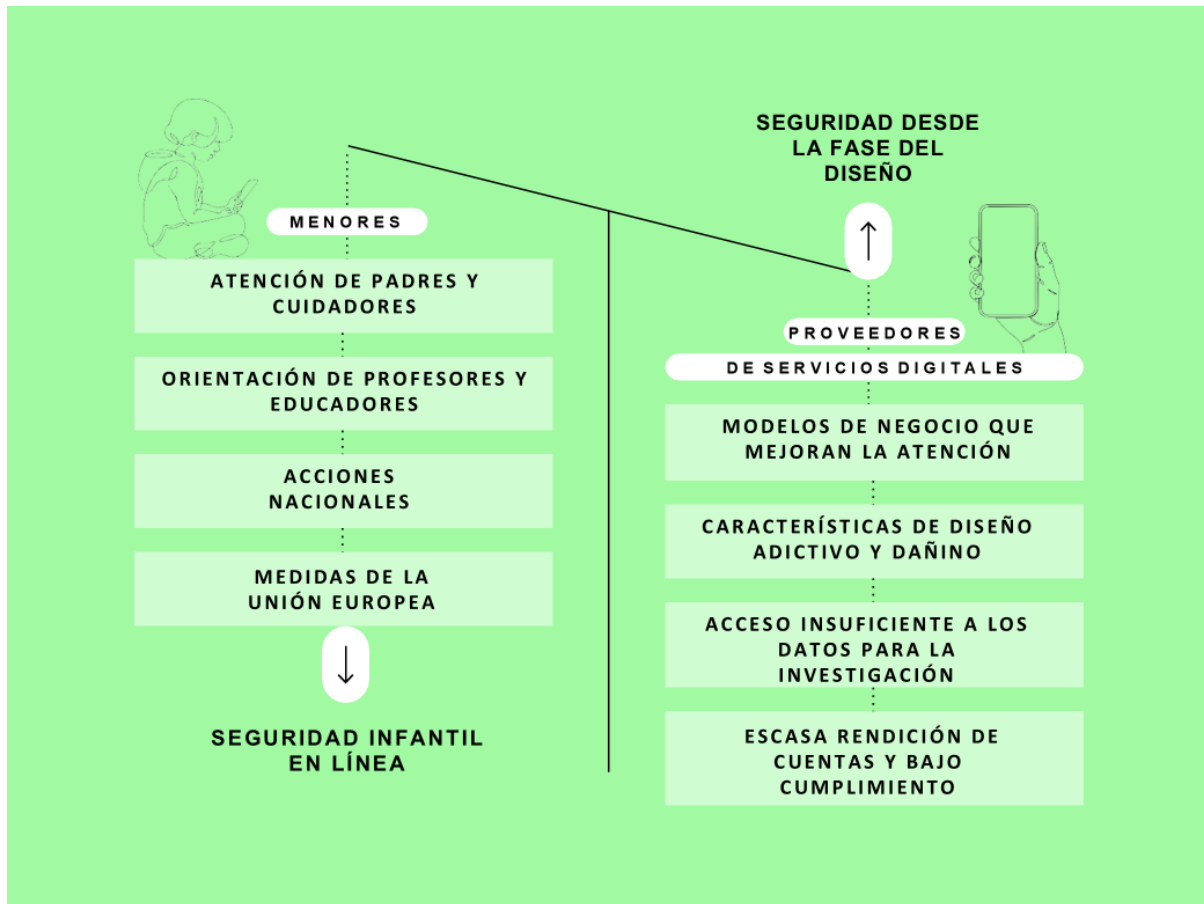
- **Poner a disposición financiación a largo plazo para la investigación longitudinal europea a gran escala y seguir apoyando los ensayos aleatorios de control.**

Ejemplos como el North American Adolescent Brain Cognitive Development (ABCD) Study [«Estudio sobre el desarrollo cognitivo cerebral en adolescentes de América del Norte» (ABCD, por sus siglas en inglés)]⁵ podrían inspirar la investigación longitudinal europea a gran escala relacionada con la seguridad infantil en línea. La disponibilidad de pruebas longitudinales europeas a gran escala (que abarquen un período de diez años o más) es importante para apoyar un enfoque neurobiológico y de desarrollo de la seguridad infantil en línea. Esto ayudaría a abordar las lagunas en las conclusiones en gran medida correlativas en el contexto europeo relacionadas con el impacto del uso de las redes sociales y otros servicios digitales en el desarrollo de los menores adolescentes, su salud física y mental y su exposición a daños por su actividad en línea.

Los ensayos aleatorios de control también son fundamentales para reforzar la base empírica de las políticas. La financiación de la investigación debe apoyar explícitamente los enfoques de desarrollo y psicopatología que investigan la susceptibilidad de los menores a los riesgos en línea, influidos por factores sociales e individuales en la infancia y la adolescencia.

⁵El estudio ABCD antes citado es el mayor estudio a largo plazo sobre el desarrollo cerebral y la salud infantil en los Estados Unidos. El estudio sigue la evolución del comportamiento de más de 11 000 niños de entre 9 y 10 años a través de la adolescencia hasta la edad adulta. Los datos recopilados permitirán la creación de normas de referencia para el desarrollo cerebral de los adolescentes y examinarán las influencias del sexo, el género, el sueño, la actividad física y el tiempo de visualización en el desarrollo de los adolescentes. Sus conclusiones también ayudarán a comprender el desarrollo de los problemas de salud mental durante la adolescencia y su relación con el abuso de sustancias.

Gráfico 2: Equilibrar el ecosistema: seguridad desde la fase del diseño en los entornos de los medios sociales y otros servicios digitales



Seguridad en línea

CONSEJOS PARA NIÑOS Y ADOLESCENTES



Conoce tus derechos: recuerda que tienes derecho a estar seguro y a ser respetado en línea.



Se amable con los demás en línea: las redes sociales y los juegos deben ser una experiencia positiva para todos. Trata a otras personas con el respeto con el que le gustaría que te trataran a ti.



Piensa antes de publicar: las fotos, los vídeos y los comentarios pueden permanecer en línea para siempre. Comparte ahora solo lo que no te disgustaría que otros pudieran ver años después.



Protege tus datos personales: no compartas en línea datos privados tales como tu nombre completo, dirección, centro escolar, número de teléfono, contraseñas o localización en directo.



Recuerda que la IA es una herramienta, no una persona real: la IA puede cometer errores y crear información falsa, imágenes falsas, vídeos, voces y mensajes.



Comprueba antes de confiar o compartir: no todo en línea es cierto. Cuestiona siempre la información, especialmente las historias, vídeos o mensajes sorprendentes, y comprueba las fuentes fiables antes de compartirlas.



Reconoce el peligro: detente y piensa en peticiones extrañas de «amigos de amigos», ofertas «demasiado buenas para ser verdaderas» o mensajes que intentan presionarte para que tomes una decisión.



No aceptes fotos o peticiones de chat de extraños: si dudas de la edad o identidad de alguien, pide a un adulto que compruebe quién es (o diles que «tu padre/madre está cerca de ti» y fíjate en su reacción).



Utiliza parámetros de privacidad y seguridad: mantén tus cuentas privadas, utiliza contraseñas seguras y utiliza elementos de seguridad adicionales siempre que sea posible.



No compartas imágenes privadas: nunca compartas fotos o vídeos íntimos, aunque alguien te presione (especialmente si eres menor de 18 años). Una vez compartidas, quedan fuera de tu control.



Bloquea, denuncia y guarda pruebas: si alguien en línea te está acosando, estafando, amenazando o haciendo que te sientas incómodo, denuncia y bloquea y conserva las capturas de pantalla o mensajes.



Comparte con un adulto en el que confías los casos en que sientes que algo está mal: no estás haciendo una tontería y no te va a provocar ningún problema pedir ayuda.



Ayuda a hacer de internet un lugar más seguro: aprende cómo funcionan las aplicaciones, los juegos, los sitios web, los algoritmos y la IA, y ayuda a otros a mantenerse seguros.



Utiliza tu voz: participa y configura el futuro del mundo digital.

Abuso en línea: ¡obtén ayuda, denuncia! La ayuda está disponible a través de equipos siempre atentos y expertos en la red de Centros de Seguridad en Internet en toda Europa. Ningún problema es demasiado grande o demasiado pequeño.



Seguridad en línea

CONSEJOS PARA PADRES Y CUIDADORES



Ayude a su hijo a crear hábitos de pantalla saludables: limite el tiempo de uso de la pantalla, desde la ausencia total de pantalla para niños de entre 0 y 2 años hasta límites de tiempo adecuados a la edad para niños de hasta 10 a 12 años, bajo su supervisión. En el caso de los adolescentes de 13 a 18 años, deben seguir debatiéndose los límites del tiempo de uso de pantallas, de modo que dispongan de tiempo suficiente para estudiar y reunirse con amigos de forma real.



Compruebe que las aplicaciones y los juegos están adaptados a la edad del menor.



En el caso de los niños más pequeños (hasta 12 años), **las consolas y los dispositivos solo deben utilizarse en presencia de un adulto.**



No permita los dispositivos en el cuarto de baño, en el dormitorio o a la hora de comer.



Preste atención al **tono de sus conversaciones** en línea y durante los juegos. Busque señales de alerta.



Pase tiempo juntos en línea: pida a su hijo que vea con usted su contenido favorito.



No critique «sus cosas»: ayude a su hijo a desarrollar su propio juicio (también obtendrá una idea de lo que sugiere su algoritmo).



Anime a su hijo a hablar con usted si le preocupa algo en línea; convénzale de que su intención es ayudarle, no culparlo, castigarlo o arrebatárle el dispositivo.



Continúe las conversaciones sobre la seguridad en línea a medida que su hijo crece, incluso cuando tiene entre 16 y 18 años y más años.



Evite la sobreexposición de los hijos: piense cuidadosamente antes de compartir fotos o vídeos de sus hijos o adolescentes en línea. Los extraños y la IA pueden utilizar esa información de muchas maneras.



Sea un ejemplo: no esté pegado a su dispositivo cuando sus hijos estén a su alrededor. Présteles la atención que merecen y no pierda momentos y conversaciones importantes con su hijo.



Lista de todas las recomendaciones de los copresidentes por capítulo

Capítulo 1: Un enfoque de desarrollo de la seguridad infantil en línea

1. Diseñar y desplegar medidas en línea de protección de la infancia adaptadas a la edad
2. Garantizar espacios en línea seguros para los menores
3. Empoderar a los menores y sus círculos de apoyo
4. (De 0 a 2 años) — Aumentar la concienciación de los cuidadores sobre la importancia para el desarrollo de la interacción directa y humana, desde la primera infancia
5. (De 0 a 2 años) — Evitar el uso de las redes sociales y otros servicios digitales y garantizar una exposición mínima a las pantallas, en particular para los menores de 3 años
6. (De 0 a 2 años) — Limitar la difusión de datos de niños a través de perfiles de redes sociales
7. (De 3 a 12 años) — Garantizar un uso estructurado y supervisado para niños en línea
8. (De 3 a 12 años) — Ofrecer a los niños y a sus círculos de apoyo una educación digital y de bienestar de calidad
9. (De 13 a 18 años) — Garantizar la evolución del uso autónomo de los adolescentes en línea

Capítulo 2: Pruebas sobre los riesgos a los que se enfrentan los menores en línea

10. Basarse en pruebas en ámbitos poco estudiados para reforzar la elaboración de políticas basadas en datos contrastados
11. Los medios sociales y otros servicios digitales deben implicar activamente a expertos académicos independientes en el diseño de estrategias y herramientas de mitigación de riesgos
12. Se han de poner a disposición financiación a largo plazo para la investigación longitudinal europea a gran escala y seguir apoyando los ensayos aleatorios de control
13. Invertir en infraestructuras de investigación europeas seguras y compartidas para permitir un acceso seguro a los datos de los menores

14. Reforzar la aplicación de las normas sobre el acceso de los investigadores a los datos y su control

Capítulo 3: Protección de los menores en un entorno de medios sociales y otros servicios digitales en rápida evolución

15. Proponer una restricción armonizada del acceso a los medios sociales y otros servicios digitales a escala de la UE para los menores de 13 años
16. Introducir sistemas eficaces de garantía de la edad para comprobar la edad y respaldar la seguridad desde el diseño y enfoques adecuados a la edad para proteger y empoderar a los menores en línea
17. Ampliar y armonizar las normas sobre las características clave de seguridad en el diseño de las redes sociales y otros servicios digitales
18. Trasladar la carga de la prueba a los proveedores de medios sociales y otros servicios digitales para demostrar que sus productos y servicios son seguros para los menores
19. Reforzar las capacidades de ejecución y evaluación
20. Adoptar rápidamente medidas para garantizar que los proveedores de medios sociales y otros de servicios digitales tengan obligaciones claras para prevenir, detectar, denunciar y bloquear el abuso sexual de menores en línea, también en las comunicaciones interpersonales
21. Los Estados miembros pueden introducir restricciones preventivas adicionales de acceso a las redes sociales y otros servicios digitales a partir de los 13 años
22. Reforzar las políticas de protección de los consumidores para proteger a los menores en línea
23. Supervisar y evaluar continuamente el impacto de las medidas que se están aplicando
24. Al tratar los datos de los menores en virtud del RGPD, las redes sociales y otros servicios digitales deben garantizar que el interés superior del menor sea una consideración primordial
25. Garantizar la aplicación efectiva de la Directiva sobre responsabilidad por los daños causados por productos defectuosos

Capítulo 4: Capacitar a los menores para navegar con seguridad por el mundo digital

26. Ampliar las oportunidades seguras para que los menores participen activamente en la configuración del entorno de los medios sociales y otros servicios digitales

27. Reforzar los mecanismos de denuncia y los derechos de los consumidores para niños y adolescentes
28. Financiar y promover la creación y el uso de redes sociales y otros servicios digitales basados en valores de la UE en los que los menores puedan interactuar de forma segura entre sí
29. Integrar acciones de educación y alfabetización digitales para menores, padres y cuidadores, profesores y educadores
30. Crear más oportunidades e infraestructuras adecuadas para apoyar las actividades fuera de línea
31. Promover la creación conjunta de directrices para los padres
32. Garantizar que los padres y los cuidadores cuenten con el apoyo continuo de herramientas de control y supervisión de última generación y actualizadas
33. Garantizar una financiación pública suficiente y normas comunes para las organizaciones de la sociedad civil y el asesoramiento entre iguales
34. Permitir que el sistema sanitario diagnostique y trate las adicciones y otros trastornos de salud mental relacionados con el uso de las redes sociales y otros servicios digitales
35. Apoyar la formación del profesorado para incluir la alfabetización digital y mediática e implicar a los padres
36. Promover la alfabetización en materia de IA como parte integrante de la educación digital
37. Las escuelas deben ofrecer oportunidades estructuradas para mejorar la salud mental y el bienestar digital
38. Las respuestas educativas deben prestar especial atención a los grupos vulnerables
39. Invertir en infraestructuras digitales educativas seguras, preventivas, sólidas y fiables

Notas finales — Prefacio

ⁱ Comisión Europea (2026). [Década digital, informe del Eurobarómetro, febrero — marzo de 2026](#).

ⁱⁱ Presidencia danesa del Consejo de la Unión Europea (2026). [La Declaración de Jutlandia: Construyendo un mundo digital más seguro para los niños](#).

ⁱⁱⁱ Parlamento Europeo (2025). [Protección de los menores en línea — Resolución del Parlamento Europeo, de 26 de noviembre de 2025, sobre la protección de los menores en línea \(2025/2060\(INI\)\)](#).

^{iv} Consejo Europeo (2026). [Conclusiones del Consejo Europeo](#), 19 de marzo de 2026.

^v G7 (2026). [Llamamiento de los dirigentes sobre un espacio digital más seguro para los menores](#).

^{vi} Hospital Infantil de Filadelfia (2026). [Age Limits Alone Won't Fix Smartphone Risks, Suggests Children's Hospital of Philadelphia Study](#). (Los límites de edad por sí solos no evitan los riesgos de los teléfonos inteligentes, sugiere el estudio del Hospital Infantil de Filadelfia). Consultado el 12 de julio de 2026.