Consejo de la Unión Europea

Bruselas, 13 de febrero de 2026
(OR. en)

6361/26

FREMP 48
JAI 198
HYBRID 19
EDUC 47
JEUN 26
GENDER 13
TELECOM 67
CYBER 61
DISINFO 11
COPEN 43
AUDIO 20

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	11 de febrero de 2026
A:	D.ª Thérèse BLANCHET, secretaria general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2026) 71 final
Asunto:	COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES Plan de acción contra el ciberacoso «Más seguros en línea, más fuertes juntos»

Adjunto se remite a las delegaciones el documento COM(2026) 71 final.

Adj.: COM(2026) 71 final

COMISIÓN
EUROPEA

Estrasburgo, 10.2.2026
COM(2026) 71 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES

Plan de acción contra el ciberacoso

«Más seguros en línea, más fuertes juntos»

1. Introducción

«Estas empresas no son organizaciones benéficas. Sin embargo, los padres sufren a diario los riesgos y los daños del ciberacoso, del fomento de la autolesión, de los depredadores en línea y de los algoritmos adictivos. Nos corresponde a nosotros proteger a nuestra próxima generación».

Discurso de la presidenta Von der Leyen en el acto de alto nivel «Proteger a los niños en la era digital», 2025.

La transformación digital ha cambiado radicalmente la sociedad. Ofrece enormes oportunidades para que los niños y los jóvenes desarrollen sus capacidades y su creatividad. En la actualidad, el 97 % de los jóvenes de la UE utilizan Internet a diario y, en el caso de los jóvenes de entre 15 y 24 años, su principal fuente de información son las plataformas de redes sociales (65 %). Utilizan herramientas de inteligencia artificial, videojuegos, aplicaciones de mensajería y comunidades en línea.

Sin embargo, estas plataformas también conllevan riesgos, como la exposición a depredadores en línea, el fomento de la autolesión, los algoritmos adictivos, los retos peligrosos en línea y el ciberacoso.

Los derechos fundamentales, incluidos los derechos del niño, son esenciales para los valores de la UE y deben respetarse tanto en línea como fuera de línea. Los niños y los jóvenes tienen derecho a buscar información de forma segura, aprender, conectarse y convertirse en miembros comprometidos de la sociedad. Por lo tanto, las libertades y las posibilidades del mundo digital deben ir acompañadas de nuestra determinación de proteger a los niños y jóvenes y potenciar su participación. La promesa de la era digital no debe verse afectada por comportamientos que humillen, excluyan o perjudiquen.

El ciberacoso erosiona la confianza y daña la autoestima. Excluye a determinadas personas y limita su potencial. Dificulta alcanzar el objetivo compartido de una Europa dinámica, inclusiva y digital para nuestros niños y jóvenes.

Las redes sociales son el canal principal a través del cual los niños y adolescentes se exponen al ciberacoso, y cada vez hay más pruebas de que esta exposición a contenidos inadecuados en línea tiene efectos duraderos y perjudiciales. La UE ya cuenta con un marco jurídico y estratégico completo para proteger a los niños y potenciar su participación en Internet, con el Reglamento de Servicios Digitales como principal instrumento en este sentido.

Como se anunció en el discurso sobre el estado de la Unión de 2025, la presidenta Von der Leyen ha solicitado asesoramiento especializado sobre las restricciones de edad en las redes sociales en Europa a la luz de los riesgos en línea, y está previsto que reciba recomendaciones en el verano de 2026. Varios Estados miembros están estudiando la posibilidad de adoptar medidas para introducir una edad mínima de acceso a las redes sociales y requisitos para el consentimiento y el control parentales, lo que conlleva armonizar la edad mínima de acceso a las redes sociales con la del consentimiento digital, exigir la privacidad por defecto para los menores y establecer soluciones para la verificación anónima de la edad.

Un enfoque europeo coordinado con respecto a la edad mínima garantizaría la igualdad de protección de todos los niños europeos y evitaría la fragmentación jurídica en el mercado único digital. El panel de expertos allanará el camino hacia un enfoque europeo coordinado y, posiblemente, también en el ámbito legislativo con respecto a la edad mínima y una campaña de concienciación basada en datos contrastados, que permitirá a los padres tomar el control efectivo del acceso de sus hijos a los contenidos en línea.

El Comité Asesor Juvenil también ha compartido con la presidenta de la Comisión las perspectivas de los jóvenes sobre esta cuestión. La Comisión está llevando a cabo un proyecto piloto en los Estados miembros para la verificación de la edad que es fácil de usar, protege la privacidad y está estableciendo un «patrón de referencia» en lo relativo a la verificación de la edad en línea. El Parlamento Europeo ha instado a la armonización de la edad mínima digital en la UE de los dieciséis años para el acceso a las redes sociales, las plataformas de intercambio de vídeos y los asistentes virtuales, mientras se permite el acceso a los jóvenes de entre trece y dieciséis años con el consentimiento de los padres.

La Comisión también pondrá en marcha una investigación a escala de la UE para iniciar un debate basado en datos contrastados sobre el impacto de las redes sociales y la exposición excesiva a las pantallas en el bienestar y la salud mental de los jóvenes.

Mientras los niños tengan acceso a Internet, el ciberacoso seguirá siendo una amenaza importante que requiere una respuesta coordinada a escala nacional y de la UE. La responsabilidad de las plataformas en línea de garantizar la seguridad desde la etapa del diseño es primordial. La lucha contra el ciberacoso requiere la colaboración a todos los niveles de gobernanza, incluidas las autoridades de reglamentación y policiales, así como un enfoque que implique a toda la sociedad, con la participación de los padres, los profesionales, los educadores y los propios jóvenes.

Como se anunció en las orientaciones políticas de la Comisión para 2024-2029, la presente Comunicación establece un plan de acción específico para luchar firmemente contra la creciente tendencia a los comportamientos abusivos en línea. Se centra principalmente en los niños y los jóvenes, aunque también tiene en cuenta la mayor vulnerabilidad de determinados grupos. Sin embargo, muchas de las medidas propuestas ayudarán a hacer frente al ciberacoso en la población en general.

La Comisión utilizará todas las herramientas a su disposición para complementar el Reglamento de Servicios Digitales, de manera que las plataformas digitales asuman su plena responsabilidad en la detección y la lucha contra el ciberacoso. Ayudará a todos los Estados miembros a adoptar las mejores prácticas disponibles en la UE, a fin de maximizar la eficacia de la lucha contra el ciberacoso. Asimismo, se esforzará en hacer llegar la información a todos los sectores de la sociedad y concienciará sobre qué es el ciberacoso, cómo puede prevenirse y cómo ayudar a las víctimas.

Con este plan de acción, la Comisión invita a los Estados miembros, las autoridades regionales y locales, las plataformas digitales, la sociedad civil, las instituciones educativas, las familias y los propios niños y jóvenes a que se comprometan a aunar esfuerzos para que el espacio digital sea seguro, respetuoso, inclusivo y colaborativo. La Comisión propone que la Unión se mantenga unida por el bienestar mental y la dignidad de todos los niños y jóvenes.

2. El ciberacoso es el problema

El ciberacoso afecta a los niños en todas partes: el 18,3 % de los niños de todo el mundo ha sufrido ciberacoso a través de mensajería instantánea, publicaciones en redes sociales, correos electrónicos o mensajes de texto. El ciberacoso no solo se produce por escrito, sino también a través de contenidos audiovisuales como imágenes o vídeos compartidos en línea.

En Europea, alrededor de uno de cada seis niños de entre once y quince años afirma haber sido víctima de ciberacoso y alrededor de uno de cada ocho admite haber ciberacosado a otros. Entre 2018 y 2022, el número de adolescentes víctimas de ciberacoso aumentó en un 25 % en el caso de los niños y casi en la misma proporción en el de las niñas. En los últimos cinco años, el ciberacoso ha sido sistemáticamente la principal razón de contacto con las líneas de ayuda de los Centros de Seguridad en Internet.

Los 6 343 encuestados de entre 12 y 17 años consultados para este plan de acción informaron de una exposición generalizada al ciberacoso: 1 de cada 4 niños y adolescentes de entre 12 y 17 años han sufrido ciberacoso y más de 1 de cada 3 lo han presenciado.

2.1 ¿Qué es el ciberacoso?

Las tecnologías digitales han ampliado las oportunidades de conexión, pero también han intensificado los riesgos en línea, como la exclusión social, los delitos de odio, el acoso, la humillación y el abuso, que pueden traspasar los límites físicos y tener lugar las veinticuatro horas del día.

A efectos del presente plan de acción, la Comisión tiene la intención de promover **una interpretación común del ciberacoso**:

> El ciberacoso se refiere a **comportamientos llevados a cabo a través de las tecnologías digitales, con la intención o el efecto principal de humillar, excluir socialmente, abusar, acosar o perjudicar repetida o continuamente a niños o jóvenes**.

La repetición se considera una característica clave del acoso y el ciberacoso. Se refiere a los efectos continuados en la víctima, que también puede temer que un acontecimiento puntual pueda compartirse en numerosas ocasiones en línea, lo que ampliaría el trauma y daría lugar a una revictimización aunque no haya participación directa del autor.

El desequilibrio de poder es fundamental en el acoso, pero puede manifestarse de manera diferente en línea. En el acoso tradicional, el desequilibrio de poder se deriva normalmente de la fuerza física, el estatus social o las normas de grupo. En el ciberacoso, también se deriva de niveles desiguales de influencia digital, capacidades digitales, acceso a la tecnología o control sobre los contenidos.

El ciberacoso es cada vez más difícil de hacer frente, ya que puede producirse en dispositivos privados en cualquier momento, en cualquier lugar y sin la presencia física del autor. Además, también se produce en canales no disponibles para el público.

Las formas más comunes de ciberacoso incluyen comentarios crueles o hirientes, la difusión de rumores en línea o el intercambio de publicaciones embarazosas o humillantes.

El anonimato, el amplio alcance y la posibilidad de enviar mensajes privados a las personas en cualquier momento amplifican los daños del acoso tradicional. Además, los entornos digitales fomentan la desconexión moral, la reducción de la empatía y la desinhibición en línea, lo que facilita la agresión en la red.

Los contenidos nocivos pueden permanecer en línea indefinidamente. Se puede acceder a ellos y volver a compartirlos una y otra vez, o hacerlos virales, lo que amplifica el daño, provoca una revictimización e impide que la víctima se recupere. Estos factores deben tenerse en cuenta a la hora de prestar un apoyo eficaz. Internet amplía el público potencial, lo que permite una agresión continuada entre espacios físicos y en línea, o viceversa.

El rápido desarrollo digital en curso implica que los entornos y las herramientas utilizados para infligir daño están cambiando continuamente. Para garantizar la flexibilidad, deben utilizarse las últimas tecnologías para detectarlo y abordarlo.

En particular, si bien la inteligencia artificial (en lo sucesivo, la «IA») puede ayudar a detectar el ciberacoso, la creciente adopción de la IA, en particular la IA generativa (GenAI), y su integración en aplicaciones y servicios en línea aumenta los riesgos y herramientas de ciberacoso o incluso crea otros nuevos. Por ejemplo, las ultrafalsificaciones han ido en aumento, lo que ha incrementado cada vez más los abusos sexualmente explícitos y ultrafalsos dirigidos mayoritariamente contra mujeres y niñas, también en casos de ciberacoso, y que han pasado de constituir comportamientos nocivos a infracciones penales en lo relativo a la creación de imágenes que constituyen abuso sexual de menores o ciberviolencia de género. Esto introduce una dimensión adicional del daño que no solo perjudica a la reputación, sino que, al igual que otros comportamientos de ciberacoso, también podría dar lugar a traumas psicológicos, lo que subraya la urgencia de supervisar y abordar estos riesgos emergentes a escala de la UE.

El ciberacoso y los delitos de odio pueden concurrir cuando el ciberacoso está motivado por el odio o incita a la violencia y al odio y se dirige contra personas con determinadas características protegidas. La Decisión marco 2008/913/JAI obliga a los Estados miembros a tipificar como delito la incitación pública a la violencia o al odio cuando se dirija contra un grupo de personas o un miembro del grupo, caracterizado por la raza, el color, la religión, la ascendencia o el origen nacional o étnico. También exige a los Estados miembros que prevean sanciones adicionales para los delitos cometidos por motivos racistas o xenófobos.

El ciberacoso puede concurrir con el abuso sexual de menores en el sentido de la Directiva 93/2011 relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil.

La Directiva 2024/1385 sobre la lucha contra la violencia contra las mujeres y la violencia doméstica exige a los Estados miembros que garanticen que la incitación a la violencia o al odio por medios cibernéticos por razón de género sea punible como delito. También tipifica como delitos otros casos de ciberviolencia que a menudo se producen en el contexto del ciberacoso: la difusión no consentida de material íntimo o manipulado, el ciberacecho y el

ciberacoso. La Directiva también incluye disposiciones para permitir la rápida eliminación del material ilegal de ciberviolencia.

2.2 Grupos en riesgo de ciberacoso

El ciberacoso es frecuente entre los **niños y adolescentes en edad escolar**, especialmente a medida que aumenta su actividad en línea.

Las niñas y las mujeres jóvenes están expuestas al acoso sexista y misógino y se ven afectadas de forma desproporcionada, por ejemplo, por la difusión no consentida de imágenes íntimas y las ultrafalsificaciones sexualmente explícitas.

Los **grupos vulnerables** están expuestos de manera desproporcionada al ciberacoso, ya que este puede dirigirse a una persona por su supuesta pertenencia a dichos grupos.

Los niños de los hogares de renta baja están más expuestos al ciberacoso que sus compañeros.

Los niños y jóvenes con discapacidad experimentan niveles más altos de victimización en línea, incluida la violencia sexual y de género. Algunos incluso se retiran de los espacios digitales debido a abusos constantes.

Las minorías étnicas y religiosas, los migrantes y los refugiados se enfrentan a elevados riesgos de acoso racista o discriminatorio. Por ejemplo, la población gitana y otras minorías raciales o étnicas están especialmente expuestas al acoso en línea y a la incitación al odio vinculados a la exclusión sistémica y el noventa por ciento de los europeos judíos declararon haber sufrido antisemitismo en línea en el último año.

Entre las **personas LGBTIQ+**, el sesenta y tres por ciento se ha enfrentado a menudo a contenidos violentos en línea contra la comunidad LGBTIQ+. Además, el once por ciento informó de que alguien publicó comentarios ofensivos o amenazantes sobre ellos en Internet el año pasado y dos tercios han sido ridiculizados o han sufrido acoso cuando estaban en la escuela.

Las medidas presentadas en este plan de acción contribuirán a abordar el ciberacoso para todas las víctimas. Las consideraciones de igualdad expuestas con anterioridad se tendrán en cuenta en la ejecución de las medidas para mejorar su eficacia.

2.3 Los efectos del ciberacoso

Las consecuencias del ciberacoso pueden ser graves y duraderas, tanto para las personas afectadas como para la sociedad en general. A corto plazo, el ciberacoso puede ser un primer paso hacia delitos o abusos más graves, incluido el abuso sexual.

Las víctimas de ciberacoso presentan un mayor riesgo de sufrir ansiedad, depresión, soledad, autolesiones y comportamientos suicidas y son más propensas a tener problemas de conducta, como comportamientos de adaptación nocivos. Además, quienes sufren ciberacoso pueden cometer ciberacoso, aunque solo se trate de un intento de dejar de ser la víctima. Todo esto requiere una respuesta cuidadosa y adaptada a la infancia.

El ciberacoso también puede afectar al rendimiento académico, el bienestar de los estudiantes y el entorno escolar, lo que puede tener consecuencias a largo plazo en la vida laboral y educativa de los estudiantes, así como para su bienestar general y satisfacción con la vida.

Por lo tanto, las consecuencias en niños y jóvenes pueden tener un gran alcance para la sociedad, exacerbando las desigualdades existentes.

3. El camino a seguir

Es necesaria una respuesta al ciberacoso más sólida y coordinada por parte de la UE que refuerce las actividades de prevención y alfabetización digital y mejore y simplifique la presentación de denuncias y el apoyo a las víctimas en toda la Unión. Queremos una Europa en la que todos los niños y jóvenes puedan crecer libres de ciberacoso, con su dignidad protegida y que tengan la posibilidad de prosperar en un mundo digital que respete los valores europeos. A tal efecto, el presente plan de acción se basa en tres pilares interrelacionados: un enfoque coordinado de la UE; la prevención y la concienciación; y la presentación de denuncias y el apoyo.

Este llamamiento a la acción cuenta con el apoyo de la opinión pública: más de nueve de cada diez europeos consideran que urge que las autoridades públicas tomen medidas para proteger a los niños del ciberacoso. La consulta pública que secundó este plan mostró un firme apoyo a los programas de alfabetización digital y creación de empatía en las escuelas y en la formación del profesorado, así como a unas herramientas de denuncia y servicios de apoyo a las víctimas mejorados.

3.1 Pilar I: Un enfoque coordinado de la UE en materia de protección

La Comisión hará pleno uso de los instrumentos políticos y jurídicos existentes y determinará oportunidades para luchar contra el ciberacoso como parte de futuras iniciativas. Además, **se invita a los Estados miembros a traducir los objetivos comunes en medidas nacionales eficaces y a construir un ecosistema integrado y que funcione correctamente para hacer frente al ciberacoso**.

El Reglamento de Servicios Digitales continúa siendo clave en los esfuerzos por asegurar su correcta aplicación, ya que requiere a los prestadores de plataformas en línea accesibles a los menores que garanticen un elevado nivel de privacidad, seguridad y protección de los menores en sus servicios.

Además, las directrices del Reglamento de Servicios Digitales sobre la protección en línea de los menores establecen las medidas que los prestadores de plataformas en línea deben adoptar para cumplir dicha obligación, incluidas las medidas adecuadas para reducir el riesgo de exposición de los menores a contenidos nocivos, como el diseño de sistemas de recomendación en el interés superior de los menores, o a comportamientos nocivos, incluidos los riesgos relacionados con el contacto derivados de interacciones con otros usuarios. Para proteger a las víctimas de ciberacoso, exigen además medidas de control y capacitación de los usuarios, mecanismos de denuncia y herramientas de reclamación adaptados a los menores, así como moderación de contenidos en las lenguas oficiales del Estado miembro en el que se presta el

servicio. El Reglamento de Servicios Digitales también exige a los prestadores de plataformas en línea que establezcan mecanismos de fácil acceso y manejo que permitan a todos los usuarios, incluidos los menores, denunciar contenidos ilícitos, por ejemplo, determinadas formas de incitación al odio o material de abuso sexual de menores. En función de la legislación nacional aplicable, determinadas formas de ciberacoso también pueden ser ilegales. Los prestadores deben tomar decisiones rápidas tras la recepción de dichas denuncias.

Este plan de acción servirá de base para la próxima revisión y actualización de las directrices del Reglamento de Servicios Digitales sobre la protección en línea de los menores. En particular, las directrices podrían ayudar a los prestadores de plataformas en línea a diseñar herramientas de denuncia más eficientes, por ejemplo, en lo que respecta a su visibilidad, accesibilidad técnica y régimen lingüístico, y a utilizar tecnologías eficaces para prevenir la exposición al ciberacoso. Las directrices también podrían ayudar a los prestadores a diseñar medidas adecuadas para responder a las denuncias de los menores, por ejemplo, ayudando a los usuarios a almacenar información que pueda servir de prueba.

La Ley de Servicios Digitales también prevé la posibilidad de contar con «alertadores fiables», entidades expertas cuyas notificaciones deben priorizarse. Estas disposiciones pueden utilizarse para hacer frente al ciberacoso, al tiempo que involucran a los alertadores fiables en la lucha contra la difusión de contenido ilícito de ciberacoso. La Comisión publicará directrices sobre alertadores fiables que ayudarán a aclarar su papel en la lucha contra el contenido ilícito, incluido el ciberacoso ilegal. Estas directrices también ayudarán a aclarar las obligaciones de los prestadores de plataformas en línea en lo que respecta a las notificaciones enviadas por alertadores fiables.

El ciberacoso también puede producirse a través de contenidos audiovisuales en línea. La Directiva de servicios de comunicación audiovisual establece requisitos generales para proteger a los menores, en particular en línea, de los contenidos nocivos que puedan perjudicar su desarrollo físico, mental o moral, lo que incluye el contenido que se considera ciberacoso. La Directiva de servicios de comunicación audiovisual exige a las plataformas de distribución de vídeos que adopten las medidas adecuadas para evitar que los menores accedan a contenidos nocivos mediante la inclusión de normas sobre contenidos audiovisuales en los términos y condiciones o mediante sistemas de control parental y clasificación de contenidos. Además, los Estados miembros tienen la obligación de proteger la dignidad humana al aplicar la Directiva de servicios de comunicación audiovisual. La evaluación y revisión en curso de la Directiva valorarán la eficacia con la que las plataformas de distribución de vídeos han aplicado estas normas y si es necesario seguir trabajando para proteger a los menores de los contenidos nocivos en línea, también en relación con el ciberacoso, y en consonancia con el Reglamento de Servicios Digitales.

El Reglamento de Inteligencia Artificial prohíbe los sistemas de IA que manipulen o engañen a las personas aprovechando las vulnerabilidades vinculadas a su edad, con el fin de alterar su comportamiento y causar así un perjuicio considerable. Estas prohibiciones pueden prevenir el ciberacoso. La Comisión adoptó directrices sobre las prácticas de inteligencia artificial prohibidas para facilitar una aplicación coherente y eficaz en toda la Unión. El Reglamento de Inteligencia Artificial también establece requisitos de transparencia, incluida la obligación de

informar a los usuarios cuando interactúen con un sistema de IA y de etiquetar claramente el contenido generado o manipulado por IA, como las ultrafalsificaciones, para evitar el engaño.

Además, estas políticas deben complementarse con la recopilación de datos sobre el ciberacoso, que actualmente es incoherente y obstaculiza una comprensión íntegra de las tendencias en todos los Estados miembros. En respuesta a la petición formulada en la consulta pública, la Comisión facilitará una recogida de datos coherentes y comparables sobre el ciberacoso en toda la UE, por ejemplo, proporcionando orientaciones como un marco e indicadores comunes de recogida de datos y la puesta en marcha de encuestas a nivel de la UE a través de la plataforma *Better Internet for Kids* [«Una internet mejor para los niños» (en lo sucesivo, BIK)] en cooperación con otros mecanismos de participación infantil y juvenil. Se proporcionarán recursos adecuados para que la red de Centros de Seguridad en Internet pueda asumir estas tareas adicionales y garantizar la continuidad a largo plazo de esta labor.

La Comisión:

1. dará más importancia a la lucha contra el ciberacoso en la **revisión de las directrices del Reglamento de Servicios Digitales sobre la protección de los menores**, en particular en lo que respecta a las medidas para seguir previniendo la exposición a contenidos nocivos y mejorar los sistemas de denuncia de las plataformas en línea, prevista para **2026**;

2. **adoptará las directrices del Reglamento de Servicios Digitales sobre alertadores fiables** para aclarar su papel en la lucha contra los contenidos ilícitos, incluido el contenido ilícito de ciberacoso, **para el segundo trimestre de 2026**;

3. evaluará formas de abordar el ciberacoso en las plataformas de intercambio de vídeos en la **evaluación en curso de la Directiva de servicios de comunicación audiovisual y su revisión, para el tercer trimestre de 2026**;

4. **contribuirá a la aplicación efectiva de las disposiciones del Reglamento de Inteligencia Artificial sobre prácticas de inteligencia artificial prohibidas**, también cuando se utilicen para el ciberacoso, mediante la coordinación en el seno del Consejo de IA y las orientaciones facilitadas con las directrices de la Comisión sobre prácticas de inteligencia artificial prohibidas, **para el tercer trimestre de 2026**;

5. **facilitará la aplicación efectiva de las obligaciones de transparencia del Reglamento de Inteligencia Artificial, en particular mediante un código de prácticas sobre el marcado y el etiquetado de los contenidos generados por IA**, cuyo objetivo es apoyar el cumplimiento de las obligaciones de transparencia del Reglamento de Inteligencia Artificial relacionadas con el marcado y el etiquetado de los contenidos generados por IA, también cuando se utilicen para el ciberacoso, **para el tercer trimestre de 2026.**

Se solicita a los Estados miembros que:

1. establezcan **planes nacionales integrales contra el acoso, incluidos planes contra el ciberacoso**, con el respaldo de la Red de la UE para los Derechos del Niño en

consonancia con la Comunicación y la Recomendación de la Comisión sobre sistemas integrados de protección de la infancia;

2. utilicen la interpretación común del ciberacoso propuesta por el presente plan de acción para recopilar **datos coherentes y comparables sobre el ciberacoso**, facilitados por el apoyo de la Comisión a través de la red de Centros de Seguridad en Internet y la plataforma BIK, y trabajen conjuntamente para establecer normas comunes contra el ciberacoso en toda la UE.

3.2 Pilar II: Prevención y concienciación

La mejor manera de luchar contra el ciberacoso es actuar antes de que se produzcan incidentes. La prevención del ciberacoso requiere prácticas digitales saludables desde una edad temprana, lo que se traduce en dotar a los niños, jóvenes y adultos de las capacidades y la confianza necesarias para reconocer los riesgos en línea y hablar sobre ellos. Asimismo, es importante hacer frente a las conductas subyacentes que pueden dar lugar a comportamientos dañinos en línea.

Para ser eficaces, las iniciativas de prevención deben implicar a los testigos, los compañeros, los acosadores, los padres, los cuidadores, los educadores y a la comunidad escolar en general, con el apoyo de todos los agentes pertinentes, en particular las organizaciones de la sociedad civil. El 62 % de los encuestados en la consulta pública estuvo a favor de ello, ya que subrayaron la necesidad de garantizar la formación profesional de los educadores, los cuerpos y fuerzas de seguridad y los trabajadores sociales.

Las iniciativas de prevención y concienciación también deben tener lugar en entornos de aprendizaje informal y no formal, como centros juveniles, clubes deportivos y entornos comunitarios, en los que los niños y los jóvenes pasan gran parte de su tiempo. Estas iniciativas también deben integrar la prevención y la lucha contra cualquier forma de discriminación, en consonancia con las estrategias de igualdad de la UE.

La educación digital y la alfabetización digital son cada vez más necesarias para navegar por el mundo en línea de forma segura y responsable. Informar a los niños y los jóvenes sobre la importancia de ser respetuosos y responsables en entornos digitales puede reducir los casos de daños intencionados o involuntarios. Se trata también de una medida preventiva prevista en la Directiva sobre la lucha contra la violencia contra las mujeres y la violencia doméstica.

Los niños y los jóvenes, incluidos aquellos con necesidades especiales, con discapacidad o en situaciones vulnerables, deben participar activamente en el diseño y la realización de actividades de concienciación que sean inclusivas y accesibles y potencien su participación, así como romper el silencio en torno al ciberacoso.

La Comisión pondrá a disposición una serie de herramientas de prevención y concienciación a escala de la UE, desarrolladas en colaboración con niños y jóvenes, padres, educadores, profesionales de la salud mental y los Estados miembros, así como con organizaciones de la sociedad civil.

Como parte del Plan de Acción de Educación Digital (2021-2027), la Comisión actualizará sus directrices para profesores y educadores sobre la lucha contra la desinformación y la promoción de la alfabetización digital a través de la educación y la formación. Además, como se anunció en la Comunicación sobre el Escudo Europeo de la Democracia, las actualizaciones reflejarán la evolución de la IA y las redes sociales e incluirán material didáctico y actividades sobre el ciberacoso y prestarán atención a la inclusión y la diversidad. La Comisión elaborará además un marco de competencias en materia de ciudadanía de la UE junto con directrices para reforzar la educación cívica en la escuela.

Además, la alfabetización digital, la prevención del ciberacoso y el bienestar digital serán ámbitos de interés en la hoja de ruta de 2030 sobre el futuro de la educación y las competencias en el ámbito digital. La hoja de ruta de 2030 tendrá por objeto garantizar que los jóvenes reciban apoyo para desarrollar hábitos saludables en línea e información sobre el uso responsable de los dispositivos digitales tanto dentro como fuera del aula.

Este trabajo sobre alfabetización digital se basa en iniciativas que la Comisión está llevando a cabo a través del programa Erasmus+ y el Cuerpo Europeo de Solidaridad, la Plataforma Europea de Educación Escolar y eTwinning. En el contexto de la Plataforma Europea de Educación Escolar, la Comisión facilitará una visibilidad más amplia y permanente de todos los materiales útiles para las escuelas en materia de acoso, incluido el ciberacoso. A partir de la convocatoria de Erasmus+ de 2026, se reforzarán las prioridades del bienestar en los centros escolares para ofrecer una mejor asistencia, supervisión y promoción a los proyectos que luchen contra el acoso y ciberacoso.

La red de la UE para la prevención del abuso sexual de menores ayudará a promover la educación y la concienciación de los menores en relación con el abuso sexual de menores, y contemplará iniciativas destinadas a evitar que los casos de ciberacoso se conviertan en comportamientos delictivos (por ejemplo, la difusión de material de abuso sexual de menores). Además, la prevención del ciberacoso se tendrá en cuenta en el próximo plan de acción de la UE para la protección de los menores contra la delincuencia. El plan de acción tratará de ofrecer una respuesta integral y coherente a los diversos riesgos a los que se enfrentan los menores en relación con la delincuencia, tanto en línea como fuera de línea.

La plataforma BIK y su red de Centros de Seguridad en Internet proporcionan herramientas de apoyo a los niños, los padres, los educadores y los profesionales a escala nacional y de la UE. Estos recursos se ampliarán aún más para reforzar las competencias, llegar a más partes interesadas y responder a los nuevos retos del ciberacoso.

Dado que las escuelas desempeñan un papel clave en la prevención del ciberacoso, se llevarán a cabo actividades de concienciación con el apoyo de los Centros de Seguridad en Internet y la plataforma BIK, empezando por la campaña anual «de vuelta a la escuela» al inicio de cada nuevo curso escolar, a fin de dotar a profesores y niños de materiales de formación, herramientas e información sobre cómo prevenir y denunciar el ciberacoso.

Los recursos y la formación sobre ciberacoso para la educación no formal e informal estarán disponibles a través de plataformas europeas. Entre ellos figuran el Portal Europeo de la Juventud, la ventanilla única para concienciar y promover oportunidades para los jóvenes, y la

Plataforma Europea de Educación Escolar, el punto de encuentro para la comunidad educativa escolar y la Zona de Aprendizaje, que proporciona a profesores y profesionales de la educación recursos y herramientas sobre iniciativas de la UE.

Eventos como la Semana Europea de la Juventud y la Semana Europea del Deporte facilitan la participación en diversos temas, incluida la lucha contra el ciberacoso. El grupo del método abierto de coordinación sobre la lucha contra la incitación al odio en el deporte, creado en el contexto del plan de trabajo de la UE para el deporte, está trabajando en recomendaciones para los Estados miembros y las partes interesadas para el entorno deportivo en general, incluido en línea. Su informe está previsto para finales de 2026 e incluirá recomendaciones para luchar contra el ciberacoso.

La Comisión:

6. **abordará el ciberacoso** en la **actualización de las directrices para profesores y educadores sobre la lucha contra la desinformación y la promoción de la alfabetización digital** a través de la educación y la formación, **para el segundo trimestre de 2026**;

7. **reforzará la educación cívica en las escuelas** a través de un marco y unas directrices de competencias de la UE en materia de ciudadanía, **en 2027**;

8. **reforzará** las competencias digitales, **la prevención del ciberacoso** y el bienestar digital a través de **la hoja de ruta de 2030 sobre el futuro de la educación y las competencias digitales**, **para el tercer trimestre de 2026**;

9. contribuirá a la **prevención del ciberacoso** en el próximo **plan de acción de la UE para la protección de los niños contra la delincuencia**, **para el tercer trimestre de 2026**;

10. **ampliará los recursos de ciberacoso y la formación** para las escuelas y para la educación no formal e informal, accesibles para las personas con discapacidad, a través de la plataforma BIK, los Centros de Seguridad en Internet, el Portal Europeo de la Juventud y la Plataforma Europea de Educación Escolar, **a partir del segundo trimestre de 2026**;

11. dará apoyo al grupo del método abierto de coordinación sobre la lucha contra la incitación al odio en el deporte en su trabajo sobre **recomendaciones para luchar contra el ciberacoso en el entorno deportivo**: informe previsto para el **cuarto trimestre de 2026**.

Se solicita a los Estados miembros que:

3. refuercen la prevención y la detección temprana del ciberacoso con **directrices claras y formación para las partes interesadas**, como educadores, cuidadores y profesionales que trabajan con niños en diferentes ámbitos (por ejemplo, la salud, el deporte, la justicia y las fuerzas y cuerpos de seguridad);

4. **refuercen la participación de los niños** en el diseño de políticas y la aplicación de medidas para el bienestar infantil.

3.3 Pilar III: Denuncias y apoyo integral

Las víctimas de ciberacoso deben disponer de canales claros, fiables y accesibles para denunciar abusos y obtener ayuda, incluido para el ciberacoso por mensaje privado. Para ser eficaces, las iniciativas de apoyo deben ir más allá de ayudar únicamente a las víctimas de ciberacoso para llegar también a los testigos, los compañeros, los acosadores, los padres, los cuidadores, los educadores y a la comunidad escolar en general.

La Comisión promoverá posibilidades de presentación de denuncias coherentes a nivel de la UE y el apoyo a las víctimas. Las denuncias deben dar lugar rápidamente a un apoyo multidisciplinar, tanto en línea como fuera de línea. Deben implicar a todas las autoridades pertinentes a todos los niveles, a los agentes privados, a las organizaciones de la sociedad civil, así como a los padres, los cuidadores, los niños y los propios jóvenes.

Sobre la base de la información recabada a través de varias consultas específicas, **la Comisión apoyará el uso de una aplicación de seguridad en línea en todos los Estados miembros**, sobre la base de modelos nacionales de prácticas eficaces, como la aplicación francesa «3018 app». La aplicación será una herramienta segura, fácil de usar y confidencial que permitirá que los niños y jóvenes:

i. **denuncien fácilmente el ciberacoso** a **una línea de ayuda**,

ii. **almacenen y transmitan pruebas de forma segura** de conformidad con los marcos jurídicos nacionales, y

iii. reciban **asistencia personalizada a través de remisiones coordinadas** a, por ejemplo, los cuerpos de seguridad y a los servicios educativos y de protección de menores.

La Comisión ayudará a los Estados miembros, cuando sea necesario y pertinente, a:

i. **adaptar la aplicación al contexto y las necesidades nacionales** (por ejemplo, traducción, imagen de marca, conexión a los servicios nacionales pertinentes de apoyo y plataformas para la presentación de denuncias), proporcionar características como la presentación segura de denuncias, la conservación de pruebas en consonancia con la legislación nacional y la confidencialidad garantizada;

ii. **garantizar la interoperabilidad** con las infraestructuras y los sistemas de apoyo existentes, y

iii. **contribuir a la promoción** de la adopción de la aplicación entre los Estados miembros, los usuarios y las plataformas en línea.

Las plataformas en línea seguirán siendo responsables de establecer mecanismos de denuncia eficaces, lo que puede equivaler a la adopción de una de las medidas establecidas para garantizar el cumplimiento de las obligaciones del Reglamento de Servicios Digitales en materia de protección de menores. Como complemento de estas iniciativas, la aplicación se pondrá a disposición de las plataformas en línea para su integración en sus herramientas de denuncia y apoyo al usuario, en particular a través de interfaces de programación de aplicaciones («API»), lo que hará que la notificación y la respuesta sean eficientes y eficaces desde el punto de vista de los recursos.

El éxito de la aplicación depende del apoyo y seguimiento por parte de las autoridades nacionales. Los Estados miembros desempeñarán un papel importante a la hora de garantizar que las denuncias a través de la aplicación estén respaldadas por un apoyo coordinado fuera de línea (por ejemplo, apoyo jurídico, social, psicológico y educativo), así como a la hora de comunicar los beneficios de la aplicación. La aplicación tendrá por objeto crear sinergias con mecanismos de denuncia bien establecidos en los Estados miembros para denunciar material de abuso sexual de menores y violencia contra las mujeres en línea, así como líneas de ayuda de la UE, nacionales e internacionales, en particular líneas de ayuda a la infancia (116 111) y líneas directas para casos de niños desaparecidos (116 000).

La Comisión adoptará la próxima estrategia de la UE sobre los derechos de las víctimas en 2026 para complementar las normas de la UE con medidas no legislativas. La Estrategia promoverá estructuras de apoyo específico (por ejemplo, exámenes médicos, emocionales y psicológicos) y servicios de protección para las víctimas menores de edad, incluidas las de delitos en línea. Estos servicios también protegerán a las víctimas del ciberacoso en los Estados miembros en los que tales actos estén tipificados como delito en el Derecho nacional.

En virtud del Reglamento General de Protección de Datos, el derecho a la supresión de los datos personales es especialmente pertinente cuando el interesado ha dado su consentimiento como niño y puede que no haya sido plenamente consciente de los riesgos existentes, también en el contexto del ciberacoso. La Comisión seguirá dando apoyo a las autoridades de protección de datos en el diseño de herramientas centradas en la infancia para proteger los datos de las redes sociales, prevenir el robo de datos o cuentas y permitir el ejercicio de sus derechos.

La Comisión:

12. **apoyará la adopción en todos los Estados miembros de una aplicación de seguridad en línea accesible** para denunciar fácilmente el ciberacoso, adaptada a los contextos nacionales, en sinergia con los mecanismos de denuncia existentes, incluidas las líneas telefónicas de ayuda y las líneas directas, de manera que se fomente el apoyo multidisciplinar en línea y fuera de línea, **a partir del tercer trimestre de 2026**;

13. incluirá a las víctimas menores de edad y la victimización en línea, que puede incluir el ciberacoso, en la próxima **estrategia de la UE sobre los derechos de las víctimas, en 2026**.

Se solicita a los Estados miembros que:

5. analicen su contexto nacional con vistas a poner a disposición una **aplicación nacional de seguridad en línea** con apoyo personalizado y, sobre la base de los modelos de prácticas nacionales existentes que hayan prosperado, **adapten dicho modelo al entorno nacional**, incluida, por ejemplo, la traducción, la imagen de marca, la conexión a los servicios nacionales pertinentes de apoyo y las plataformas para la presentación de denuncias, garantizando al mismo tiempo características básicas como la presentación de denuncias segura, la conservación de pruebas con arreglo al Derecho nacional y la confidencialidad garantizada;

6. garanticen que la presentación de denuncias a través de la aplicación nacional de seguridad en línea se integre en **un ecosistema holístico y que funcione correctamente para el apoyo y la gestión de casos**, incluido el apoyo coordinado fuera de línea (por ejemplo, servicios de apoyo jurídico, policial, social, psicológico y educativo);

7. **pongan la aplicación a disposición de las plataformas en línea para su integración en sus herramientas de denuncia y apoyo al usuario**, en particular a través de interfaces de programación de aplicaciones («API»), lo que hará que la presentación de denuncias y la respuesta sean eficientes y eficaces desde el punto de vista de los recursos;

8. **promuevan la adopción y el uso generalizados de la aplicación nacional de seguridad por parte de todas las partes interesadas pertinentes;**

9. **promuevan herramientas desarrolladas por las autoridades de protección de datos** en sus lenguas nacionales para que los menores se protejan de los riesgos en línea, como el ciberacoso, el robo de datos o cuentas, los intentos de estafa y el chantaje sexual.

4. Divulgación internacional y cooperación multilateral

La UE aspira a salvaguardar el bienestar y los derechos de los niños dentro de sus fronteras, pero también contribuye significativamente a fomentar un entorno digital más seguro e inclusivo en todo el mundo. El Día por una Internet más Segura es ahora una campaña mundial en la que se pide a las partes interesadas que adopten conjuntamente medidas para hacer de internet un lugar más seguro y mejor para todos, especialmente para niños y jóvenes, de manera que se conciencie sobre los principales retos en línea y las preocupaciones y tendencias emergentes.

Proteger a los menores en línea y potenciar su participación en internet es una prioridad mundial. Esto se refleja en la Estrategia Digital Internacional de la UE. La red cofinanciada por la UE de líneas directas en los Estados miembros para hacer frente a la difusión de material

de abuso sexual de menores en línea forma parte de la red INHOPE, con cincuenta y siete líneas directas que operan actualmente en todo el mundo.

La Comisión seguirá colaborando con reguladores afines en materia de seguridad en línea, incluida la prevención y la lucha contra el ciberacoso, en el marco de acuerdos administrativos (por ejemplo, actualmente con Ofcom en el Reino Unido y la comisaria de eSafety en Australia) y asociaciones digitales (por ejemplo, con Canadá, Singapur e India).

La UE promoverá una cooperación contra el ciberacoso en los foros internacionales, en consonancia con el Pacto Digital Global. Las organizaciones de las Naciones Unidas han desarrollado orientaciones y herramientas que pueden utilizarse como buenas prácticas y puntos de referencia, en particular de UNICEF (sitio web y API de código abierto), la Unión Internacional de Telecomunicaciones (directrices sobre protección infantil en línea), así como de la Representante Especial del Secretario General de las Naciones Unidas sobre la Violencia contra los Niños. La UE secunda el acercamiento de la Unesco a los reguladores para aplicar las directrices de la Unesco sobre la gobernanza de las plataformas en línea.

La UE financia programas específicos de concienciación y apoyo a la protección de los menores en países no pertenecientes a la UE, en particular en los países candidatos y vecinos, tanto en línea como fuera de línea, a través del instrumento IVCDCI - Europa Global. La UE también contribuye a la armonización con las normas de la UE en el marco del proceso de adhesión de los países candidatos y países candidatos potenciales y promueve la seguridad en línea de los niños y jóvenes de los países vecinos mediante el intercambio de conocimientos y mejores prácticas a través del programa del Centro de Seguridad en Internet+.

5. Próximas etapas

La Comisión supervisará la aplicación de los tres pilares del plan de acción, en estrecha colaboración con los Estados miembros, los Centros de Seguridad en Internet y otras partes interesadas. Los avances, los retos y las buenas prácticas serán objeto de seguimiento a través de las herramientas existentes, como el mapa anual de políticas relativas a la plataforma BIK, los informes de los Centros de Seguridad en Internet y los intercambios periódicos a través de foros de expertos, de forma que se garantice un seguimiento transparente y participativo.

La Comisión trabajará con los Estados miembros para integrar los marcos de seguimiento en las estrategias o políticas nacionales sobre el ciberacoso, evaluando la aplicación, la accesibilidad, la inclusividad y la adaptabilidad a contextos digitales en evolución, con la participación de los niños y los jóvenes. Las conclusiones se compartirán a escala de la UE para contribuir al aprendizaje mutuo y la armonización de las políticas, lo que servirá de base para las actualizaciones de las iniciativas en el marco de BIK+ y el Reglamento de Servicios Digitales.

La Comisión hará balance de este plan de acción en 2029, en particular mediante consultas con niños y jóvenes.

6. Conclusiones

> *«Queremos un espacio en línea seguro para los niños, los jóvenes y la próxima generación, pero todavía no lo tenemos. Lo que tenemos son algunos problemas y no son problemas que solo afecten a esta generación. Por eso, necesitamos ayuda de la Unión para hacer que nuestros espacios en línea sean seguros. Hay que empezar por algo y hay que empezar ahora. Por el futuro».*
>
> Una cita de niños que son parte de la Plataforma de Participación Infantil de la UE.

Los niños y los jóvenes se ponen en contacto con nosotros pidiendo ayuda para que los espacios en línea sean seguros para ellos, sus compañeros y las generaciones futuras. Debemos estar a la altura del reto en toda nuestra Unión, ya que proteger a nuestros niños y jóvenes y potenciar su participación en Internet no deben depender de un código postal.

Sobre la base de un conjunto sólido de medidas jurídicas y políticas de la UE contra los daños en línea y de las contribuciones de una amplia gama de partes interesadas, este plan de acción contribuirá a construir un entorno digital seguro e inclusivo para los niños y los jóvenes en Europa que les permita potenciar su participación en la red. Complementará e inspirará las iniciativas en curso de la UE sobre una Internet más segura, la responsabilidad de las plataformas, las competencias y la educación digitales, la capacitación de los niños y los jóvenes, la recogida de datos y la cooperación internacional.

La Comisión invita al Parlamento Europeo y al Consejo a que aprueben el presente plan de acción y colaboren en su aplicación. La Comisión pide al Comité de las Regiones y al Comité Económico y Social Europeo que promuevan el diálogo con las autoridades locales y regionales, los interlocutores económicos y sociales, y la sociedad civil.

ANEXO: Acciones clave y calendario previsto

Pilar I: Enfoque coordinado de la UE en materia de protección

La Comisión:	
reforzará la atención prestada a la lucha contra el ciberacoso en la revisión de las **directrices del Reglamento de Servicios Digitales sobre la protección de los menores**;	2026
adoptará las directrices del Reglamento de Servicios Digitales sobre alertadores fiables para aclarar su papel en la lucha contra los contenidos ilícitos, incluido el contenido ilícito de ciberacoso;	para el 2T 2026
evaluará formas de abordar el ciberacoso en las plataformas de intercambio de vídeos en la **evaluación en curso de la Directiva de servicios de comunicación audiovisual** y su revisión;	para el 3T 2026
apoyará la **aplicación efectiva de las disposiciones del Reglamento de Inteligencia Artificial sobre prácticas de IA prohibidas**, en particular cuando se utilizan para el ciberacoso;	a partir del 3T 2026
facilitará la **aplicación efectiva de las obligaciones de transparencia de la Ley de Inteligencia Artificial relacionadas con el marcado y el etiquetado de los contenidos generados por IA**, incluidos los que pueden utilizarse indebidamente para el ciberacoso.	a partir del 3T 2026

Se solicita a los Estados miembros que:
establezcan **planes nacionales integrales contra el acoso, incluidos planes contra el ciberacoso**, en particular con el respaldo de la Red de la UE para los Derechos del Niño;
recopilen datos coherentes y comparables sobre el ciberacoso facilitados por la red de Centros de Seguridad en Internet y la plataforma BIK.

Pilar II: Prevención y concienciación

La Comisión:	
abordará el ciberacoso en la **actualización de las directrices para profesores y educadores sobre la lucha contra la desinformación y la promoción de la alfabetización digital**;	para el 2T 2026
reforzará la educación cívica en las escuelas a través de un marco y unas directrices de competencias de la UE en materia de ciudadanía;	2027

reforzará las competencias digitales, la prevención del ciberacoso y el bienestar digital a través de **la hoja de ruta de 2030 sobre el futuro de la educación y las competencias digitales**;	para el 3T 2026
contribuirá a la prevención del ciberacoso en el próximo **plan de acción de la UE para la protección de los niños contra la delincuencia**;	para el 3T 2026
ampliará **los recursos de ciberacoso y la formación** para las escuelas y para la educación no formal e informal, accesibles para las personas con discapacidad, a través de la plataforma BIK, los Centros de Seguridad en Internet y el Portal Europeo de la Juventud;	a partir del 2T 2026
dará apoyo al grupo del método abierto de coordinación sobre la lucha contra la incitación al odio en el deporte en su trabajo sobre **recomendaciones para luchar contra el ciberacoso en el entorno deportivo**.	a más tardar en el 4T 2026

Se solicita a los Estados miembros que:
refuercen la prevención y la detección temprana del ciberacoso con **directrices claras y formación para las partes interesadas**, como educadores, cuidadores y profesionales que trabajan con niños en diferentes ámbitos;
refuercen la participación de los niños en el diseño de políticas y la aplicación de medidas para el bienestar infantil.

Pilar III: Denuncias y apoyo completo

La Comisión:	
apoyará la adopción de **una aplicación de seguridad en línea accesible** en todos los Estados miembros;	a partir del 3T 2026
incluirá a las víctimas menores de edad y la victimización en línea, que puede incluir el ciberacoso, en la **estrategia de la UE sobre los derechos de las víctimas**.	2026

Se solicita a los Estados miembros que:

analicen su contexto nacional con vistas a poner a disposición **una aplicación nacional de seguridad en línea** y, sobre la base de los modelos de prácticas nacionales existentes que hayan prosperado, adapten dicho modelo al entorno nacional;
garanticen que la presentación de denuncias a través de la aplicación nacional de seguridad en línea se integre en un **ecosistema holístico y que funcione correctamente**;
pongan la aplicación a disposición de las plataformas en línea para su integración en sus herramientas de denuncia y apoyo al usuario;
promuevan la aplicación nacional de seguridad en línea entre las partes interesadas pertinentes;
promuevan herramientas desarrolladas por las autoridades de protección de datos en sus lenguas nacionales para que los menores se protejan de los riesgos en línea, como el ciberacoso