

## Nota informativa

### Día de Internet Segura: CEC-España reclama entornos digitales seguros y responsables para la infancia y la adolescencia

Con motivo del Día de Internet Segura, el Centro Europeo del Consumidor en España (CEC-España) advierte del impacto de las redes sociales en la salud mental de niños y adolescentes y reclama mayor protección, alfabetización digital y supervisión de las plataformas online.

Madrid, 10 de febrero de 2026 – El Día de Internet Segura ([Safer Internet Day](#)) se celebra anualmente el segundo día de la segunda semana del segundo mes del año. Es un evento promovido con el apoyo de la Comisión Europea, cuyo objetivo es concienciar acerca de la seguridad en Internet, promoviendo un uso seguro y positivo de las tecnologías digitales, especialmente entre la infancia y la adolescencia.

La edición de este año se celebra el 10 de febrero bajo el lema “**Seguridad digital para educar en tiempos de inteligencia artificial**”, centrado en promover el uso seguro y positivo de las tecnologías digitales entre las personas menores y su entorno inmediato, fomentando sus capacidades digitales y ayudándoles a mostrar respeto, y desarrollar capacidad crítica y creatividad, en consonancia con los principios digitales europeos.

Este año, con motivo de la celebración del Día de Internet Segura, el Centro Europeo del Consumidor en España quiere poner de manifiesto que las redes sociales son a menudo la principal causa del ciberacoso y, en términos más generales, de los problemas de salud mental entre los jóvenes que pueden derivar en síntomas de depresión o riesgo suicida, de ahí la importancia de ofrecer a los menores una protección adecuada. Según el informe de Unicef, [Infancia, Adolescencia y Bienestar Digital](#) del pasado mes de noviembre, el 5,7% de los niños y adolescentes presenta un uso problemático de las redes sociales que interfiere en su vida cotidiana y se asocia a síntomas de ansiedad, peor calidad de vida o una mayor exposición a situación de acoso. Por este motivo, países como Australia, Francia, Portugal o recientemente España, ya están trabajando para prohibir su uso entre niños y adolescentes.

Igualmente, el Centro Europeo señala que los problemas de seguridad online no tienen su origen en los jóvenes, sino en los aspectos estructurales como el diseño y navegación de las plataformas online basadas en algoritmos que maximizan la atención de los usuarios; la falta de sistemas seguros y efectivos de verificación de edad que impidan que los menores puedan acceder a contenidos inadecuados; así como la facilidad para difundir contenidos nocivos. De esta forma, CEC-España apunta que hay que seguir trabajando para transformar el entorno en línea en un espacio más seguro, inclusivo y estimulante.

Del mismo modo, deberían adoptarse las medidas necesarias para garantizar el desarrollo de una tecnología ética y responsable que garantice que los más jóvenes también puedan beneficiarse de los aspectos positivos del nuevo entorno digital como el desarrollo de las relaciones sociales y la identidad, la creatividad, o el acceso a la información. Por este motivo, el reto debería pasar también por crear entornos digitales adecuados para cada edad e impulsar nuevos espacios para la educación y la orientación.

#### Recomendaciones para crear una Internet Segura:

- **Alfabetización.** Basada en prácticas reales para fomentar el uso responsable de la tecnología, desarrollar el pensamiento crítico y la autonomía digital. La iniciación de los menores en el entorno digital debería realizarse de forma gradual apoyándoles para que participen en el mundo digital de forma acompañada y tutelada. Igualmente, los entornos online deben estar adaptados a la edad del usuario y que los menores vayan asumiendo de forma progresiva responsabilidades. Esta alfabetización contribuiría a capacitar a los jóvenes para explorar el mundo digital con perspicacia y conocimiento. Para ello, las intervenciones deben ser sensibles al género, adecuadas a la edad, y universales apoyando igualmente a niños que presenten una alta vulnerabilidad, así como a los que se encuentran en situación de riesgo.
- **Regulación y supervisión de las plataformas.** Las plataformas deben garantizar espacios digitales seguros para los niños y los jóvenes. Igualmente, deben garantizar los derechos fundamentales, la libertad de expresión, así como el derecho a recibir una información transparente, honesta y veraz.
- **Acompañamiento de padres y educadores.** Tanto padres como educadores deberían recibir directrices claras, herramientas prácticas y recursos adecuados para ayudar a los menores a aprender a navegar en el entorno digital de forma responsable, ética y saludable; así como para fomentar el diálogo intergeneracional. De esta forma, se garantizaría que los adultos estén bien preparados para guiar y apoyar a los más jóvenes.
- **Canales de información seguros y accesibles.** Garantizar canales para que los usuarios -especialmente los menores y personas vulnerables- puedan denunciar agresiones online o contenidos inapropiados. Es importante también fomentar una cultura de confianza dentro de las escuelas, las familias y las redes de padres para que los menores no tengan miedo a denunciar.

## Recomendaciones para navegar seguros por Internet

- **Actualiza los equipos y el software.**
- **Verifica y actualiza los *plugins* y extensiones.**
- **Gestiona la seguridad y privacidad del navegador.**
- **No guardes las contraseñas en el navegador si te da la opción de recordar la contraseña.**
- **Elimina las cookies de sesión.**
- **Cifra las comunicaciones** utilizando protocolos en los que las comunicaciones van cifradas, por ejemplo, siempre que puedas utiliza HTTPS.
- **Verifica que los sitios por los que navegas son fiables.** Teclea la URL (con HTTPS://) y abre la información (**certificado**) en el candado en la barra de navegación. Comprueba que el certificado está vigente, y que estás en el sitio correcto verificado por una empresa de confianza.
- **Activa la autenticación de dos factores para reforzar la protección de las cuentas online.**

## ¿Cómo protege la Ley de Servicios Digitales a los menores en el entorno online?

Su objetivo es crear un entorno en línea seguro y fiable de forma que garantice que las plataformas en línea de muy gran tamaño, como Instagram, Snapchat, TikTok y YouTube, protejan los derechos de los usuarios y eviten la difusión de contenidos prohibidos o inapropiados. Igualmente obliga a las redes sociales, por ejemplo, a ser más transparentes sobre los algoritmos de recomendación, a eliminar rápidamente los contenidos nocivos y a disponer de procedimientos de reclamación uniformes en toda Europa. De esta forma, las redes sociales deben garantizar que los menores no estén expuestos a contenidos inadecuados, que sus datos y su privacidad estén protegidos, que no reciban publicidad personalizada, o que la información sea clara y no engañosa. Otro objeto de esta ley es garantizar que los contenidos en línea sean adecuados para la edad y los intereses de los niños y niñas. Por lo tanto, las plataformas en línea están obligadas a identificar los riesgos en una fase temprana y a adoptar las medidas adecuadas.

Las plataformas deben ofrecer funciones de notificación de fácil acceso, por ejemplo, a través de un botón de notificación claramente visible. Las plataformas están obligadas a responder con prontitud y proporcionar comentarios a los usuarios. Si una plataforma no responde lo suficientemente rápido o si el contenido es particularmente peligroso, los llamados alertadores de confianza (trusted flaggers) pueden ofrecer soporte.

En España, la [CNMC actúa como Coordinador de Servicios Digitales](#), supervisando que los prestadores de servicios cumplan sus obligaciones y protejan los derechos de los usuarios, especialmente de los menores. En ningún caso, la CNMC es competente para moderar o retirar contenidos, para actuar como órgano de apelación de las decisiones de los proveedores de servicios en línea, o para dirimir los litigios entre diferentes partes o diferentes usuarios. Para reclamar, la Ley de Servicios Digitales prevé estas dos vías:

1. **Mecanismo Interno de Reclamaciones del Proveedor**
2. **Resolución Extrajudicial**

>> Listado [de Órganos de resolución de litigios certificados por los Coordinadores de Servicios Digitales.](#)