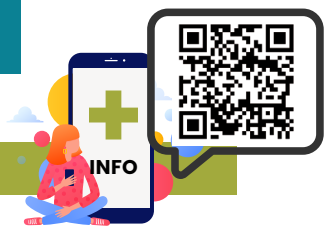
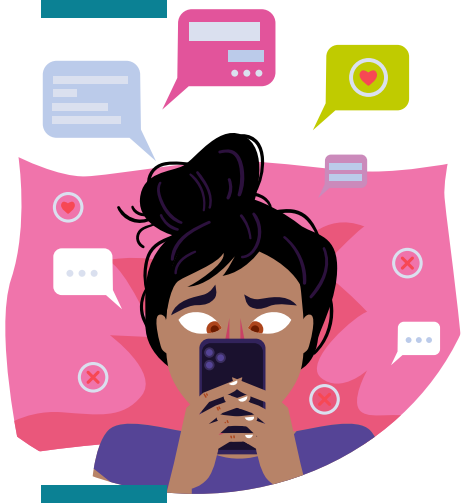
Conectados y Seguros

Riesgos y recomendaciones en el uso de dispositivos electrónicos por menores

NO CLAMES, RECLAMA!



1. Riesgos para la salud y neurodesarrollo



✓ **Diseño adictivo:** Las redes sociales están diseñadas para fomentar un uso frecuente o prolongado, que pude causar problemas de visión, trastornos del sueño y reducción de la atención. En este entorno, los menores están expuestos a **contenidos peligrosos**, inapropiados para su desarrollo psicológico y emocional e incluso ilícitos.

RECOMENDACIONES

- Educa sobre riesgos y fomenta el diálogo familiar.
- Desarrolla el pensamiento crítico y la responsabilidad digital.
- Reflexiona sobre tus propios hábitos con los dispositivos electrónicos.
- Usa controles parentales de manera abierta y consensuada.

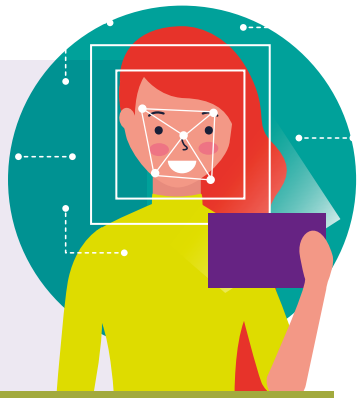
2. Riesgos para la privacidad y protección de datos personales

✓ **Robo o suplantación de identidad:** Recibir mensajes engañosos que solicitan información personal o permitir el acceso a sus cuentas.

✓ **Explotación de datos para personalizar contenido:** Los algoritmos pueden identificar vulnerabilidades, como complejos físicos o trastornos alimenticios, y mostrar contenido que puede dañar su salud mental y emocional.

✓ **Difusión** de imágenes o videos personales, reales o *deepfakes*, compartidos sin consentimiento, que exponen a los menores al acoso o *bullying*.

✓ **Publicidad dirigida a menores:** A pesar de estar prohibidos los anuncios personalizados a menores, la actividad en línea los expone constantemente a publicidad que muchas veces no está claramente identificada.



RECOMENDACIONES

- Contraseñas seguras y autenticación de doble factor.
- Configura cuentas privadas y pon atención a las aplicaciones.
- Vigila activamente y usa versiones infantiles de aplicaciones.
- Infórmate sobre cómo se retienen y usan los datos personales.
- Reflexiona sobre la creación de la huella digital desde una edad temprana.

3. Riesgos Técnicos y de Seguridad

✓ ***Malware:*** *Software* malicioso que roba información o daña dispositivos.

✓ ***Phishing:*** Correos o mensajes falsos que buscan revelar información sensible, como contraseñas, datos bancarios o robo de cuentas de servicios online.

RECOMENDACIONES

- Descarga desde fuentes oficiales y verifica los enlaces.
- Actualiza regularmente los sistemas operativos y apps.
- Evita conexiones Wi-Fi públicas.
- Realiza copias de seguridad regulares.

MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030

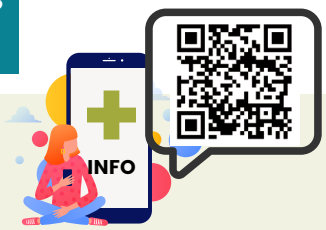
CECU

El presente proyecto ha sido subvencionado por el Ministerio de Derechos Sociales, Consumo y Agenda 2030, siendo su contenido responsabilidad exclusiva de CECU. 2024

Conectados y Seguros

Guía rápida sobre cómo proteger los datos y los derechos en línea de los menores

NO CLAMES, RECLAMA!



1 ¿Qué hacer frente al contenido inapropiado o ilícito recomendado a menores a través de Internet?

Denuncia el contenido que consideres ilegal o contrario a las condiciones generales del servicio. Lo puedes hacer:

- ✓ A través de las plataformas, que están obligadas por la DSA (Ley de Servicios Digitales) a disponer de mecanismos de denuncia internos: Instagram, TikTok, Snapchat, X.
- ✓ Además, **frente a incumplimientos a la DSA**, puedes:
  - Acudir a un sistema de resolución extrajudicial de litigios
  - Reclamar ante el Coordinador de Servicios Digitales (CNMC).
  - Reclamar una compensación por los daños sufridos por incumplimiento de la normativa.
  - Ser representado por una asociación e iniciar acciones colectivas.

2 ¿Qué hacer frente a un caso de robo o suplantación de identidad, ciberacoso o grooming?

- ✓ Las plataformas disponen de recursos en caso de:
  - Ciberacoso: TikTok, Instagram, Facebook, X
  - Suplantación de identidad: TikTok, Instagram, Facebook, X
  - Contenido inapropiado/ilegal: Instagram, TikTok, X
- ✓ Además, puedes acudir a la
  - **Vía penal:** Puedes denunciar ante las Fuerzas y Cuerpos de Seguridad de Estado: Guardia Civil o Dirección General de la Policía; o ante los tribunales de justicia por delitos como, por ejemplo, suplantación de identidad o *grooming*, distribución de contenidos que promuevan autolesiones o contenidos sexuales, ciberacoso, etc.
    - Utiliza la Línea de Ayuda del INCIBE, donde obtendrás información y ayuda en cuestiones de ciberseguridad y asesoramiento legal.
  - **Vía civil:** Puedes interponer una demanda en reclamación de una indemnización por los daños y perjuicios sufridos, tanto económicos como psicológicos.
  - **Vía administrativa.** Puede dirigirte a:
    - La **AEPD** si afecta al derecho a protección de datos personales. Utiliza el Canal prioritario de la AEPD para casos de difusión de contenido sexual o violento.
    - La **CNMC**, en caso de incumplimiento de la DSA, por ejemplo, inacción de una plataforma frente a una denuncia de contenido ilegal.

3 ¿Qué hacer si exponen información personal de un menor sin consentimiento, por ejemplo, si generan y comparten una deepfake o explotan sus datos personales?

- ✓ Denuncia ante la propia plataforma. Recursos: Facebook, Instagram, TikTok, Twitter, YouTube y buscadores Google y Bing.
- ✓ Si no se resuelve tu solicitud, reclama ante la AEPD. Modelos de reclamaciones aquí. Acude al Canal Prioritario, si procede.
- ✓ Si consideras que estás siendo víctima de un delito, como ciberacoso, puedes denunciar ante las FFCCSS o iniciar acciones judiciales.

4 ¿Qué hacer si un ataque malware o de phishing afecta a los datos personales de un menor?

- ✓ Denuncia al Grupo de Delitos Telemáticos de la Guardia Civil o a la Brigada Central de Investigaciones Tecnológica de la Policía.
- ✓ Utiliza la Línea de Ayuda del INCIBE.
- ✓ Informa a la plataforma ante una posible de brecha de datos personales.

MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030

CECU

El presente proyecto ha sido subvencionado por el Ministerio de Derechos Sociales, Consumo y Agenda 2030, siendo su contenido responsabilidad exclusiva de CECU. 2024