

“CONDUCTAS DE RIESGO ONLINE Y CIBERDELINCUENCIA”



Jose Torres
Experto en Investigación de la Ciberdelincuencia

<https://es.wikihow.com/convencer-a-tus-padres-para-que-te-den-un-tel%C3%A9fono-inteligente>

YA ESTÁ EN CASA... ¿Y AHORA QUÉ?





Riesgos



Calendario

Conocer y cambiar nuestras citas, fechas, reuniones y rutinas.



Contactos

Acceder a nuestra lista de contactos y ver la lista de cuentas de servicios.



Cámara Micrófono

Realizar grabaciones de video, audio o tomar fotografías.



Memoria

Acceder o modificar cualquier archivo o dato almacenado.



Mensajes De texto

Acceder, modificar, o enviar mensajes SMS.



Sensores Del cuerpo

Conocer datos sensibles sobre nuestra salud y actividad física.



Teléfono

Acceder al histórico de llamadas y funcionalidades del teléfono.



Ubicación

Conocer nuestra ubicación en tiempo real.



Otros permisos

Que debemos revisar por no estar exentos de riesgos.

Suplantación de identidad



Robo de datos personales y confidenciales



Publicidad dirigida



Ataques de ingeniería social y phishing



Riesgo para la seguridad física



Envío de spam, fraudes y malware



Pérdida de privacidad



Extorsión/sextorsión



Suscripción a servicios premium



Difusión de datos sobre el estado de salud



Administradores del dispositivo: control total del dispositivo



Antivirus y cleaners



¿Necesitas una herramienta que detecte y elimine virus y otras amenazas en tiempo real? Lo que buscas es una herramienta antivirus. Si sospechas que tu dispositivo ya está infectado, entonces, lo que necesitas es un *cleaner*.

Analizadores de URL y archivos



Para comprobar si un archivo que recibes es malicioso o una página web es fraudulenta, esta herramienta es lo que buscas. Detecta rápidamente cualquier tipo de amenaza antes de que te afecte, así evitarás muchos problemas.

Doble factor de autenticación



Si quieres dotar de mayor seguridad a tus cuentas de usuario para que tú y solo tú puedas acceder a ellas, esta es la herramienta que necesitas. Además de la contraseña, necesitarás un código que sólo tú recibirás a través del teléfono móvil.

Gestores de contraseñas



Herramienta muy útil para que puedas almacenar todas tus contraseñas robustas y cifradas de tal forma que sólo tengas que memorizar una, la que te da acceso al resto de contraseñas guardadas.

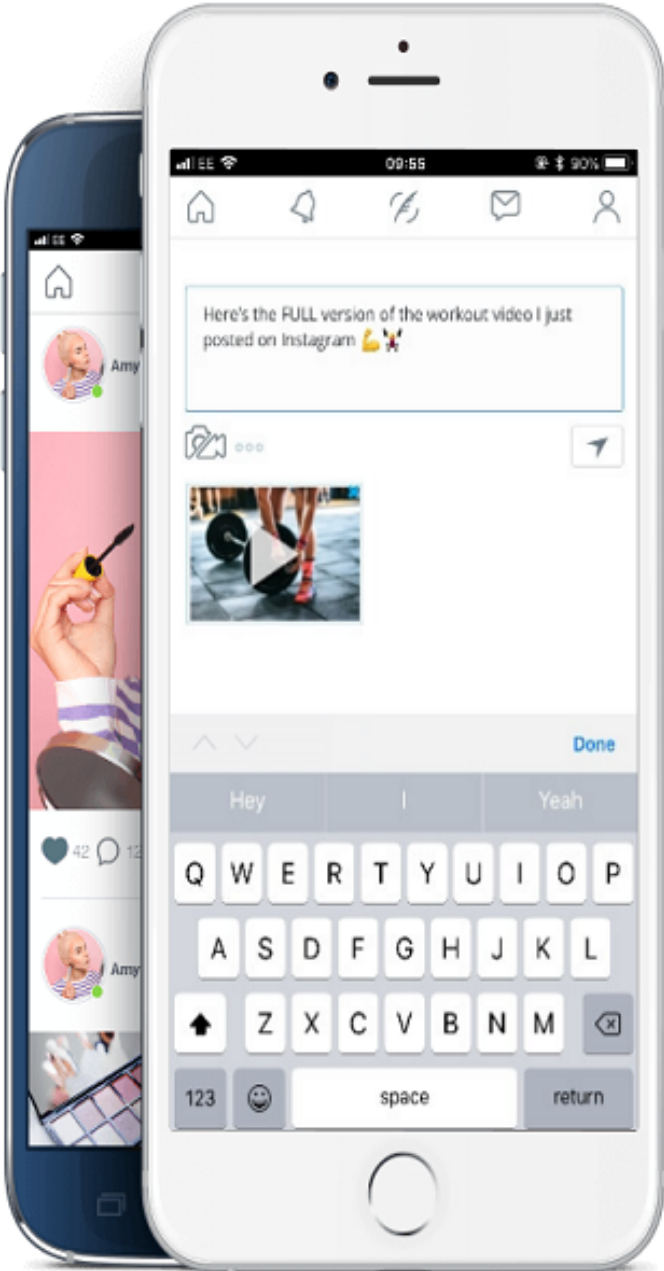


**Seguridad
en redes wifi:**

MENSAJERÍA INSTANTÁNEA MÓVIL



EL NUEVO INSTAGRAM CON CONTENIDO DE PAGO





¡Regístrate para ganar dinero e interactuar con tus fans!

 REGISTRARSE/INICIAR SESIÓN CON TWITTER

 REGÍSTRASE/LOGIN CON GOOGLE

0

Correo electrónico

Contraseña

[¿Olvidó su contraseña?](#)

INICIAR SESIÓN

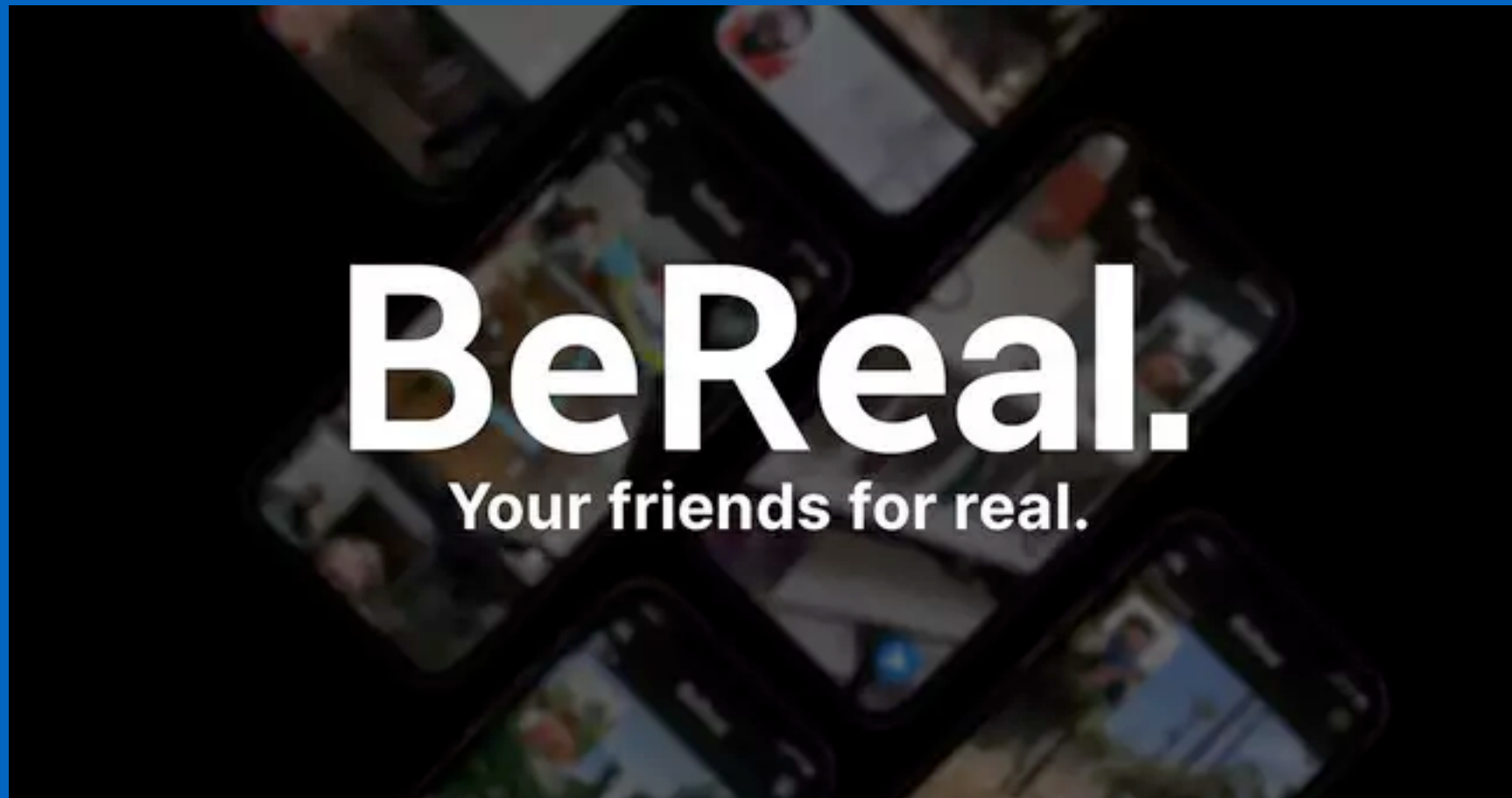
Don't have an account yet?

[Regístrate en OnlyFans.com](#)



©2020 OnlyFans · [Blog](#) · [Twitter](#) Preguntas frecuentes · [Términos](#) · [Privacidad](#) · [Contacto](#) · [Cómo funciona](#) · [USC 2257](#) · [Blog](#)  Spanish 

“BE.REAL, LA RED SOCIAL IMPREVISIBLE”



“BE-REAL, ¿QUE DATOS GUARDA DEL USUARI@?”



¿Cuándo publicar?

Todo el mundo recibe una notificación al mismo tiempo, todos los días a una hora aleatoria.



Todo es cuestión de tiempo

Tienes 2 minutos para abrir BeReal y hacer una foto de lo que estés haciendo.



No es solo una foto

Cuando haces un BeReal, se hace una foto de la cámara frontal y trasera.



Todo el mundo juega a lo mismo

Solo puedes ver lo que están haciendo tus amigos si publicas a tiempo.

BeReal.
01:50

Una vez al día, en algún momento aleatorio, tendrás 2 minutos para hacer y compartir tu BeReal.

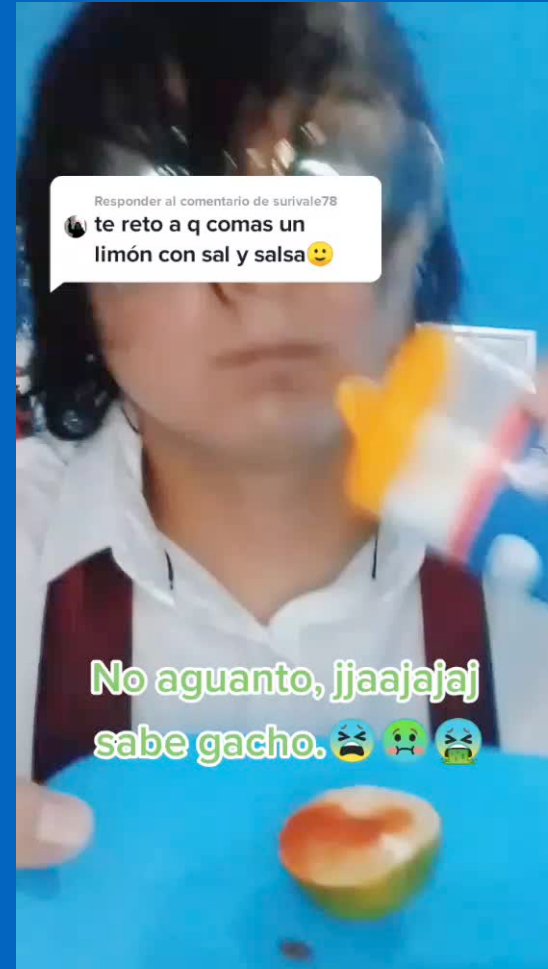
“TIK TOK”, LOS PELIGROS DE ESTA APP QUE ESTA DE MODA



“TIK TOK”, LOS PELIGROS DE LOS RETOS VIRALES

- ALGUNOS EJEMPLOS:

- * CORONA CHALLENGE
- * DESAFIO DE LA LIMA DE DIENTES
- * RETO DE LA SAL
- * BRIGHT EYE CHALLENGE
- * RETO DEL ENCHUFE
- * ROMPECRANEOS
- * ETC.



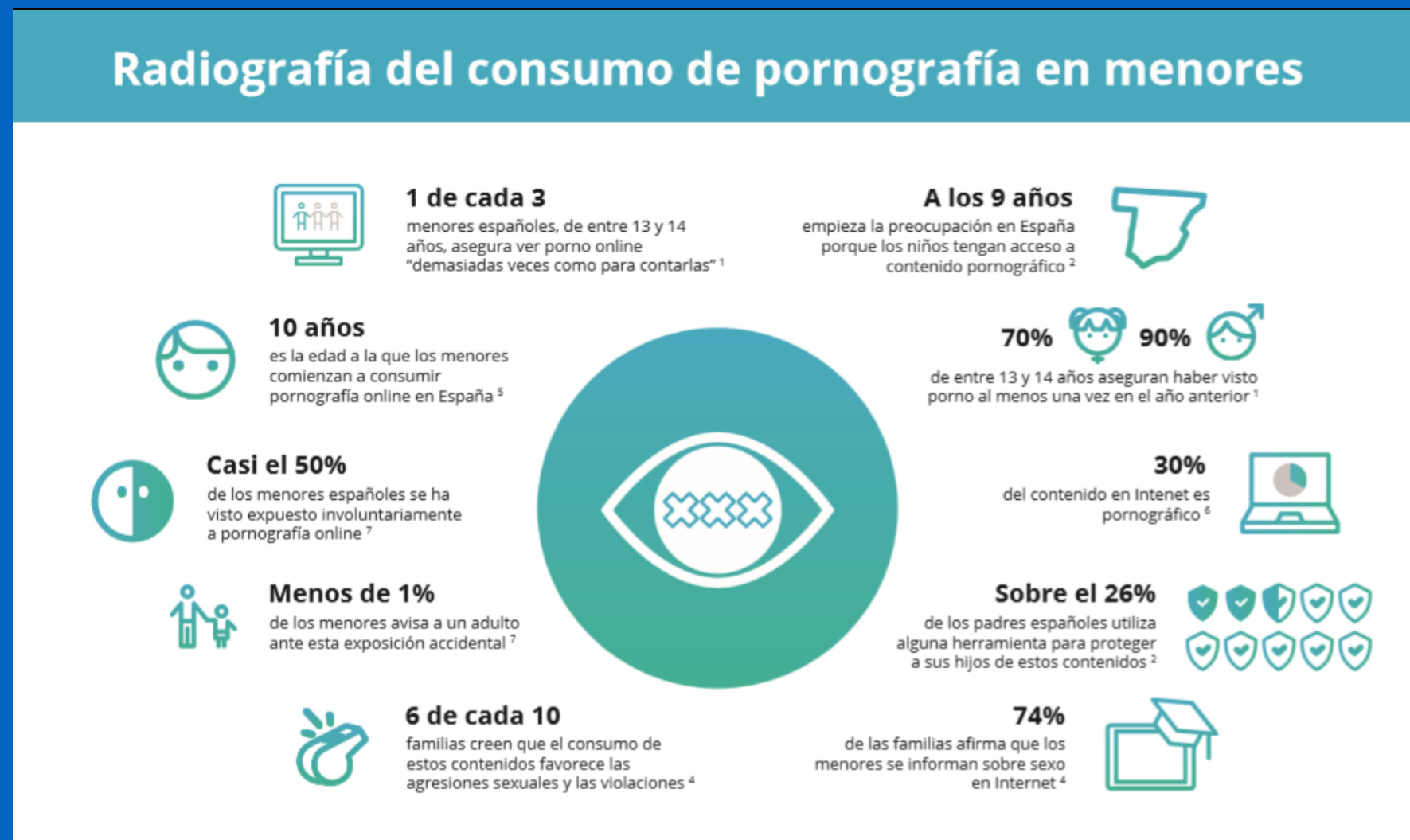
CONSECUENCIAS NEGATIVAS DE RECURRIR AL PORNO COMO SUSTITUTO DE LA EDUCACION SEXUAL

Actividades llevadas a cabo por los menores relacionadas con la sexualidad en la red:

Visualización de contenidos sexuales

Recepción de mensajes con contenido sexual, mas del 35% afirma haber recibido este tipo de mensajes en el último año (Whatsapp, Facebook, Instagram, Twitter, etc).

Publicación y envío dirigido de mensajes con contenido sexual. El 33% manifiesta enviar este tipo de mensajes



¿QUE ES EL CIBERACOSO?



Insultar en redes sociales puede salir muy caro

4 abril 2011 - 6:00 - Autor: [Alejandro Touriño](#)



Compartir

564



Twittear

332



+1

0



Si tenías en mente utilizar una red social para desatar tu ira, quizás deberías pensártelo dos veces antes de hacerlo. Que se lo digan sino a las dos jóvenes, tristes protagonistas de estos hechos, cuya “broma” les ha salido muy cara.

Y es que el **Juzgado de Instrucción nº 4 de Segovia**, por medio de Sentencia nº 8/2011, de 21 de febrero, **ha condenado a dos jóvenes al pago de 18.284,22 euros** como autoras de una falta continuada de vejaciones a consecuencia de los insultos vertidos por éstas desde un perfil falso en la red social Tuenti, creado previamente por ellas.

La situación es la siguiente. Según resultó acreditado en el procedimiento penal instado frente a ellas, las dos jóvenes se pusieron de acuerdo para crear en Tuenti un perfil falso a nombre de una tercera persona -una compañera de instituto-, haciéndose pasar por ella y utilizando el perfil ficticio para verter comentarios que ridiculizaban a la propia víctima y a sus compañeras de instituto, llamándolas entre otras lindezas, “payasas creídas” o “niñatas que parecen travestidas”.

QUÉ HACER SI PUBLICAN EN INTERNET CONTENIDO ÍNTIMO SIN MI CONSENTIMIENTO

1) Identifica que tipo de agresión estás viviendo.



2) Guarda toda la evidencia como pruebas: ss, links, urls de la publicación, etc.



3) Denuncia el contenido de la red social donde se esté publicando.



4) Crea elementos de auto seguridad digital, como cambiar contraseñas, verificación en dos pasos, privacidad en tus publicaciones, etc.

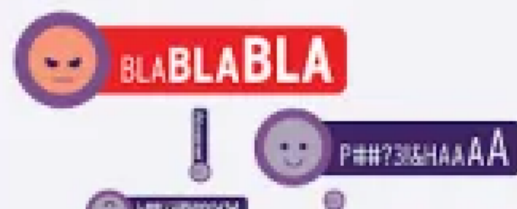


5) Elimina de tus redes a "amigos" que no conozcas, de ahí podría venir un agresor.



6) No sigas el chantaje de tu agresor, intenta no intimidarte con sus amenazas.

7) No interactúes en la publicación, cuentas o grupos en los que te intenten acosar. Hacerlo podría provocar que se viralice.



8) Antes de acudir con las autoridades, delimita si te sientes segura de hacerlo y busca apoyo de una amiga o persona de tu máxima confianza.

9) Por último, denuncia ante un ministerio o policía cibernética.



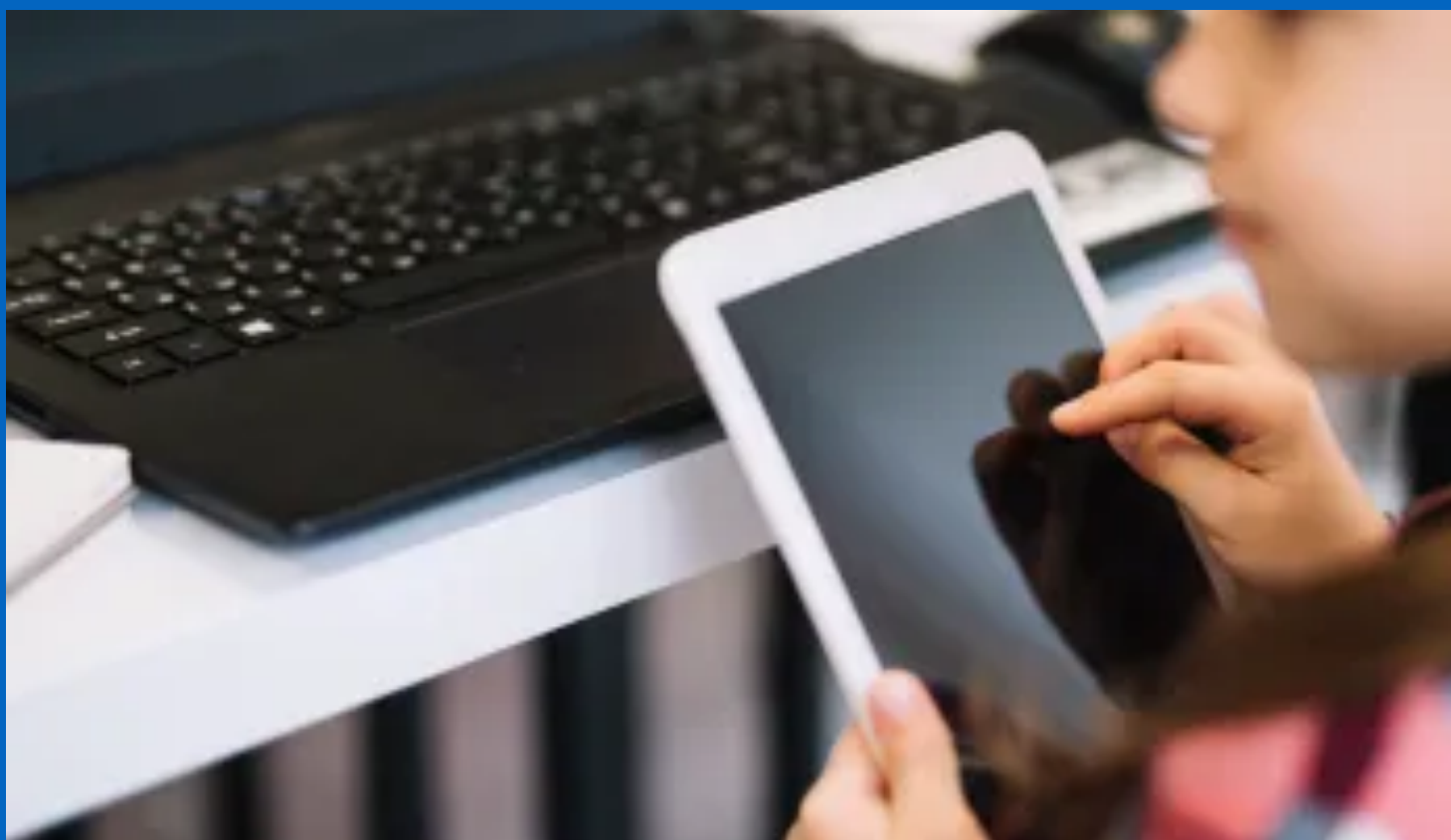
GEOLOCALIZACION



RESPONSABILIDADES Y OBLIGACIONES EN LA UTILIZACION DE DISPOSITIVOS MOVILES EN LA ENSEÑANZA



RESPONSABILIDADES EN MATERIA DE PROTECCION DE DATOS

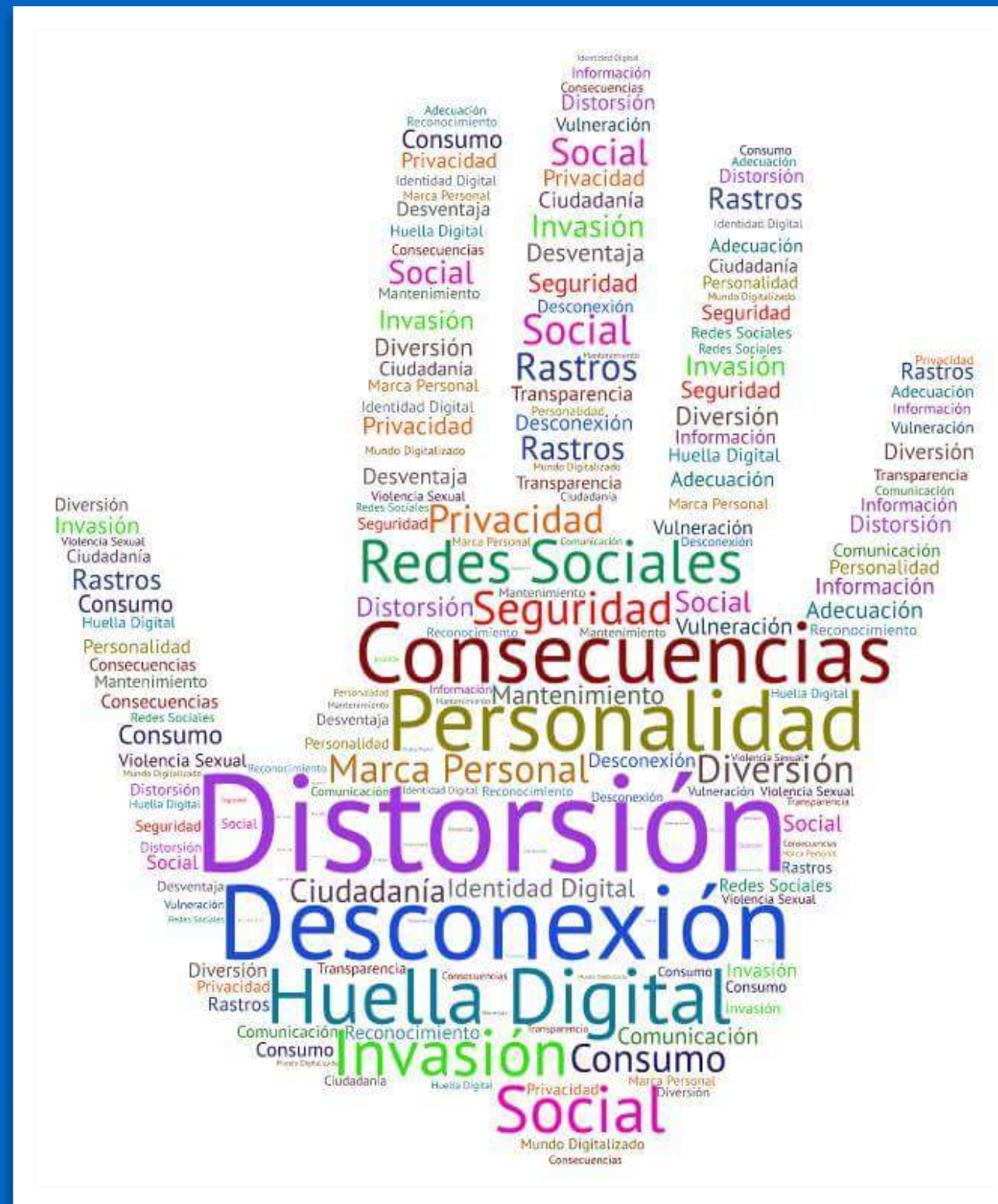


USO DEL TELEFONO MOVIEL EN LOS CENTROS DOCENTES



RIESGOS DE LOS DERECHOS Y LIBERTADES DE LOS ALUMNOS

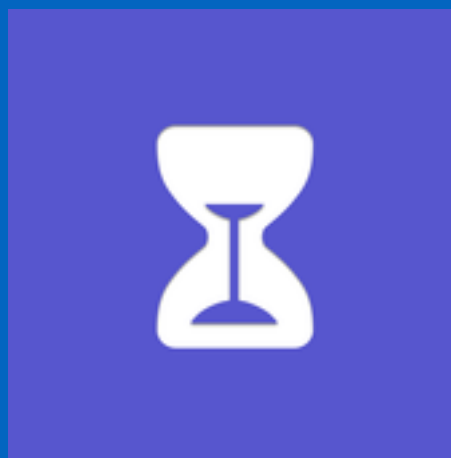




SISTEMAS DE CONTROL PARENTAL



DISPOSITIVOS DE LA FIRMA “APPLE”



movistar 12:37 76 %

Cancelar

Tiempo de uso

Consulta información sobre el tiempo de uso y define límites para las apps que quieras gestionar.

- Informes semanales**
Consulta un informe semanal con información sobre el tiempo de uso.
- Tiempo de inactividad y límites de uso de apps**
Define un tiempo para estar apartado de la pantalla y pon límites de tiempo para las categorías que quieras gestionar.
- Restricciones de contenido y privacidad**
Restringe los ajustes de contenido explícito, de compras y

Continuar

movistar 13:06 70 %

< Ajustes **Tiempo de uso**

TIEMPO DE USO hoy 13:06

iPhone de Sandra

21min

Redes sociales
2min

- Tiempo de inactividad**
Define un horario de descanso.
- Límites de uso de apps**
Define límites de tiempo de uso.
- Siempre permitido**
Elige las apps sin restricciones.
- Contenido y privacidad**
Bloquea contenido inadecuado.

Usar código para “Tiempo de uso”

Usa un código para asegurar la configuración de “Tiempo de Uso” y para poder aumentar el tiempo

movistar 12:46 74 %

Cancelar **Seleccionar apps** Añadir

CATEGORÍAS

- ☒ **Todas las apps y categorías**
- ☐ **Redes sociales**
Instagram, WhatsApp y 14 más
- ☐ **Juegos**
GnG, Pictionary y 8 más
- ☐ **Entretenimiento**
YouTube, Shazam y 10 más
- ☐ **Creatividad**
Layout, Prisma y 17 más
- ☐ **Productividad**
Dropbox, e-park y 35 más
- ☐ **Formación**
Duolingo
- ☐ **Lectura y consulta**
Mapas, Tiempo y 18 más
- ☐ **Salud y forma física**
Nike Run Club, SitUps y 11 más

DISPOSITIVOS “ANDROID”



20:18 [íconos] 75 %

← Ajustes del padre, madre o tutor

Para Elena

- ▶ Controles de Google Play
- 🔒 Filtros de Google Chrome
- 🔒 Filtros de la Búsqueda de Google
- ▶ Filtros de YouTube
- 📱 Aplicaciones de Android
- 📍 Ubicación
- 👤 Información de la cuenta
- 👤 Supervisión de cuenta
- ⋮ Más

Revisa las prácticas de privacidad de la cuenta de Elena. [AVISO DE PRIVACIDAD](#)

20:18 [íconos] 75 %

← Google Play

Gestiona el contenido que Elena puede explorar, comprar o descargar en Google Play.

Autorizaciones de compras y descargas

📁 Requerir aprobación para
Todo el contenido

Restricciones de contenido

Elige qué contenido puede explorar Elena en Google Play. Seguirá necesitando tu aprobación para comprar o descargar contenido, a menos que provenga de tu colección familiar.

🤖 **Aplicaciones y juegos**
Permitir todo el contenido (incluido el que no tenga clasificación)

🎬 **Películas**
Permitir todo el contenido (incluido el que no tenga clasificación)

📖 **Libros**
Permitir todo

🎧 **Música**
Permitir todo

20:18 [íconos] 75 %

← Chrome

Puedes permitir que Elena visite todos los sitios web o solo algunos cuando inicie sesión en Chrome. Elena también puede solicitar permiso para visitar sitios web bloqueados. [Más información](#)

☐ Permitir todos los sitios web

☒ **Intentar bloquear sitios web para adultos**

Ningún filtro es perfecto, pero este debería ocultar los sitios web con contenidos violentos y sexualmente explícitos. [Más información](#)

GESTIONAR SITIOS WEB

☐ Permitir solo determinados sitios web

Aprueba las solicitudes de Elena y elabora tu propia lista personalizada.

GESTIONAR SITIOS WEB

Para gestionar los permisos de sitios web y otras opciones avanzadas, utiliza el [panel de control de Chrome](#).

MUCHAS GRACIAS



José E. Torres Meira
Experto en investigación de la ciberdelincuencia