



Ciberseguridad en el entorno familiar

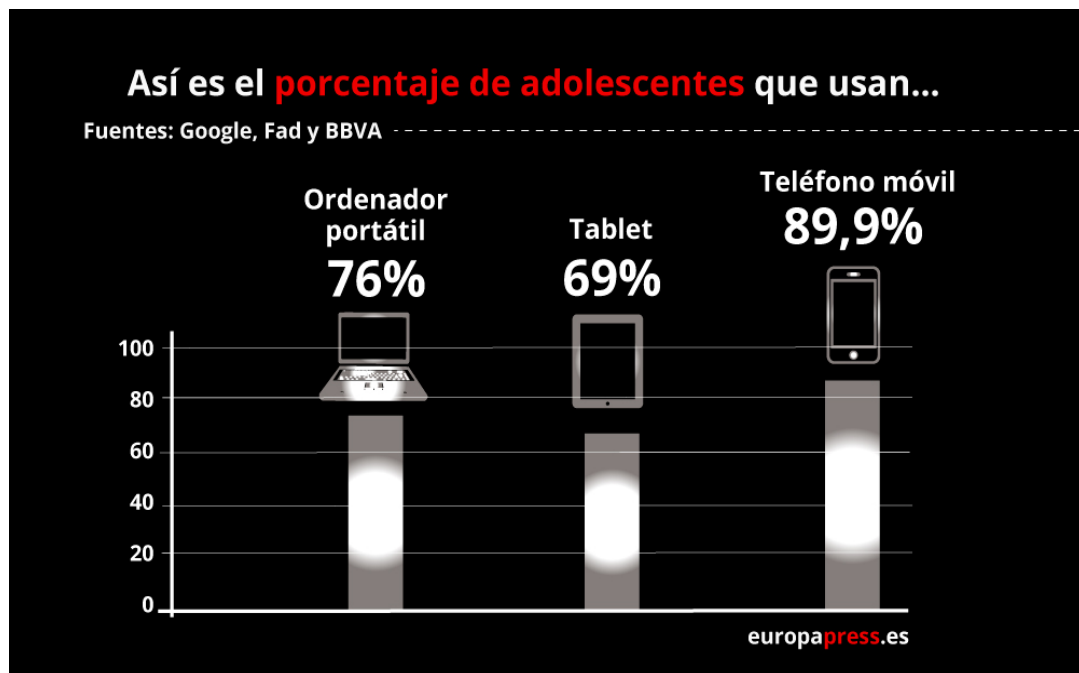
Índice

- **Introducción**
- **Definiciones**
- **Seguridad en casa**
- **Seguridad con los niños y adolescentes**
- **Enlaces de interés**

INTRODUCCIÓN

La pandemia Covid – 19 ha provocado un antes y un después en nuestras vidas, tanto en el ámbito laboral como en el personal

Esto es algo que también ha afectado a los menores y ha provocado el incremento en el uso de Internet y dispositivos electrónicos



- El **98%** de los menores usa Internet de forma habitual desde la pandemia

- 7 de cada 10 menores tienen teléfono móvil

Fuente: Observatorio de Tecnología y Sociedad (ONTSI)

- El **75,6%** de los adolescentes usa Internet para escuchar música
- Y el **48,8%** lo usa para mantener el contacto con amistades y personas que no ven de forma habitual

Fuente: Google, Fad y BBVA, www.epdata.es

INTRODUCCIÓN

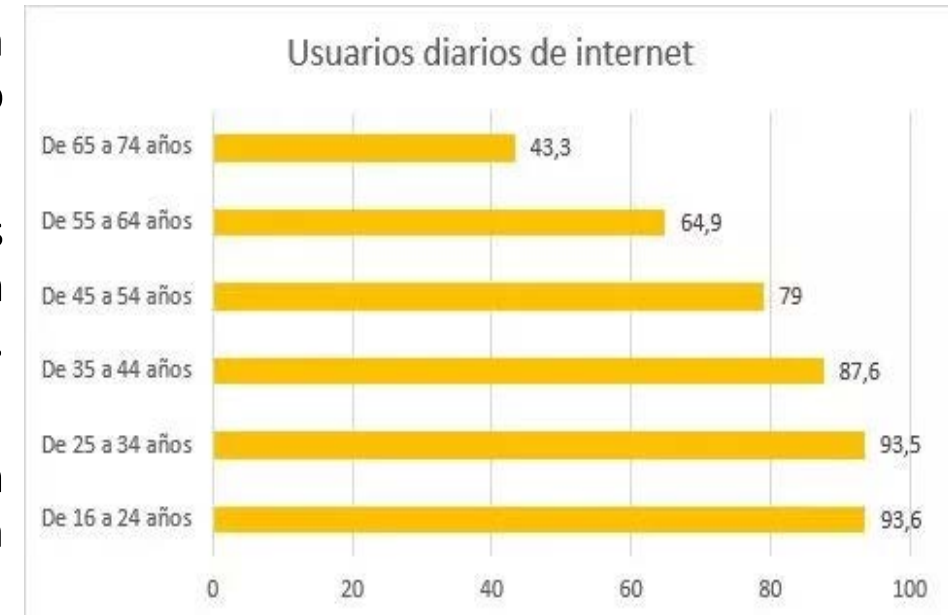
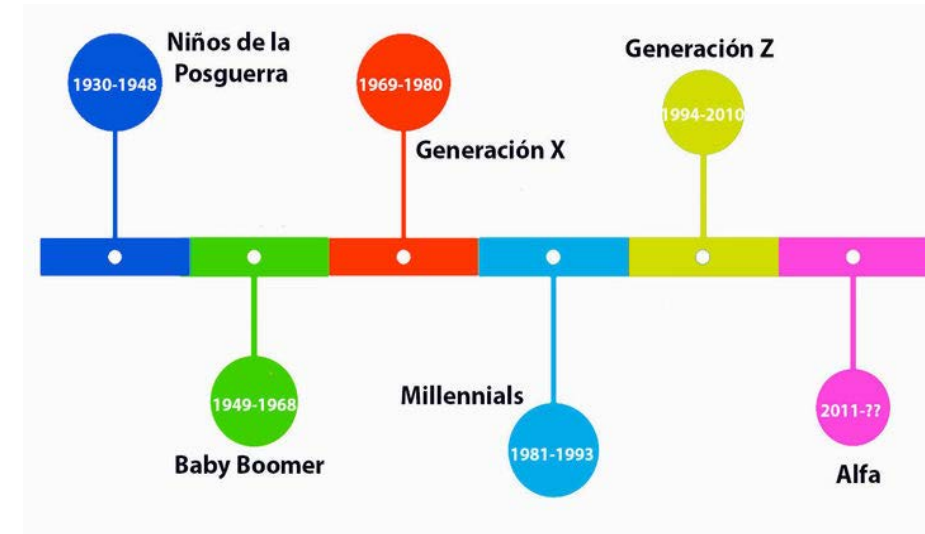
Baby Boomers: Se han adaptado, poco a poco a un entorno cada vez más digitalizado. Utilizan los dispositivos electrónicos para informarse sobre las últimas noticias, para organizar sus viajes, para buscar servicios y para ver productos y sus precios antes de decidirse a comprarlos, un acto que normalmente terminan haciendo de forma física

Generación X: Son los que más intensamente han vivido la transición entre lo analógico y lo digital. Fueron los primeros que crecieron con ordenadores, teléfonos móviles, nuevos formatos musicales y de vídeo, Internet, etc.

Generación Y (Millennials): Son nativos digitales, no conciben una vida sin el uso de tecnología y utilizan Internet en su día a día para todo, tanto en el entorno laboral como en el entorno personal.

Generación Z (Centennials): Son creativos y proactivos. Utilizan varias plataformas al mismo tiempo, comparten continuamente contenidos en redes sociales, pasan horas y horas visualizando tutoriales y vídeos. Internet es fundamental en su vida.

Generación Alpha: Representa a los niños nacidos a partir del 2010. Han nacido con los dispositivos móviles y son capaces de interactuar con estas plataformas mucho antes de aprender a hablar



INTRODUCCIÓN

¿Cómo actúa cada generación y que amenazas pueden impactarles?



Son los que mas se preocupan por su seguridad digital, dado a su adaptación a las nuevas tecnologías y son conscientes de que tienen que protegerse.

Las amenazas que más sufren son:

- Robos de identidad
- Estafas bancarias
- Vishing



Son mas propensos a adoptar mejores prácticas de seguridad, aunque son los que optan por pagar un rescate por recuperar su información.

Las amenazas que más sufren son:

- Suplantación de identidad en redes
- Sexting



Se preocupan por su seguridad digital y toman medidas para protegerse.

Las amenazas que más sufren son:

- Phishing
- Smishing
- Ransomware



Es mucho mas relajada y menos responsables a la adopción de mejores prácticas de seguridad.

Las mayores amenazas que más sufren son:

- Cyberbulling
- Grooming

DEFINICIONES

Malware:

Diferentes formas de software dañino. Una vez que entra en el dispositivo puede causar todo tipo de daños, desde tomar el control del dispositivo y monitorear las acciones y pulsaciones del teclado, hasta enviar todo tipo de datos confidenciales al atacante

Ciberbullying o ciberacoso:

Es un acoso psicológico usando las tecnologías como Internet, móviles, videojuegos, etc. Es decir, cuando se atormenta, amenaza, hostiga, humilla o molesta a menores usando estos medios

Phishing:

Se conoce como suplantación de identidad. Para combatir este tipo de ataques es esencial comprender la importancia de verificar los remitentes de correo electrónico y tanto los archivos adjuntos como los enlaces

Ransomware:

Es un tipo de malware que provoca el bloqueo de un dispositivo desde una ubicación remota y cifrar nuestros archivos quitando el control de toda la información y datos almacenados. Se pide un rescate y se suele pedir en bitcoins para que nos devuelvan el control sobre los datos

DEFINICIONES

Grooming:

Un adulto se pone en contacto con un niñ@ o adolescente con el fin de ganarse su confianza para luego involucrarle en una actividad sexual

Retos virales:

Realizar algo extremo, arriesgado o doloroso sin mucho sentido que se hacen populares en Internet y que muchos adolescentes copian para subir su propia versión e invitando a todos sus contactos a hacer el reto, llegando así a un número mayor de personas

Troll:

Persona que publica mensajes instigadores incitando al odio y con el único fin de crear polémica. Siempre ocultan su identidad y actúan en redes sociales

Stalkear:

Hace referencia a la acción de revisar o cotillear a otra persona a través de las redes sociales. Consiste en observar el perfil y publicaciones y/o fotos de una persona para averiguar información sobre ella y su vida

Nomofobia:

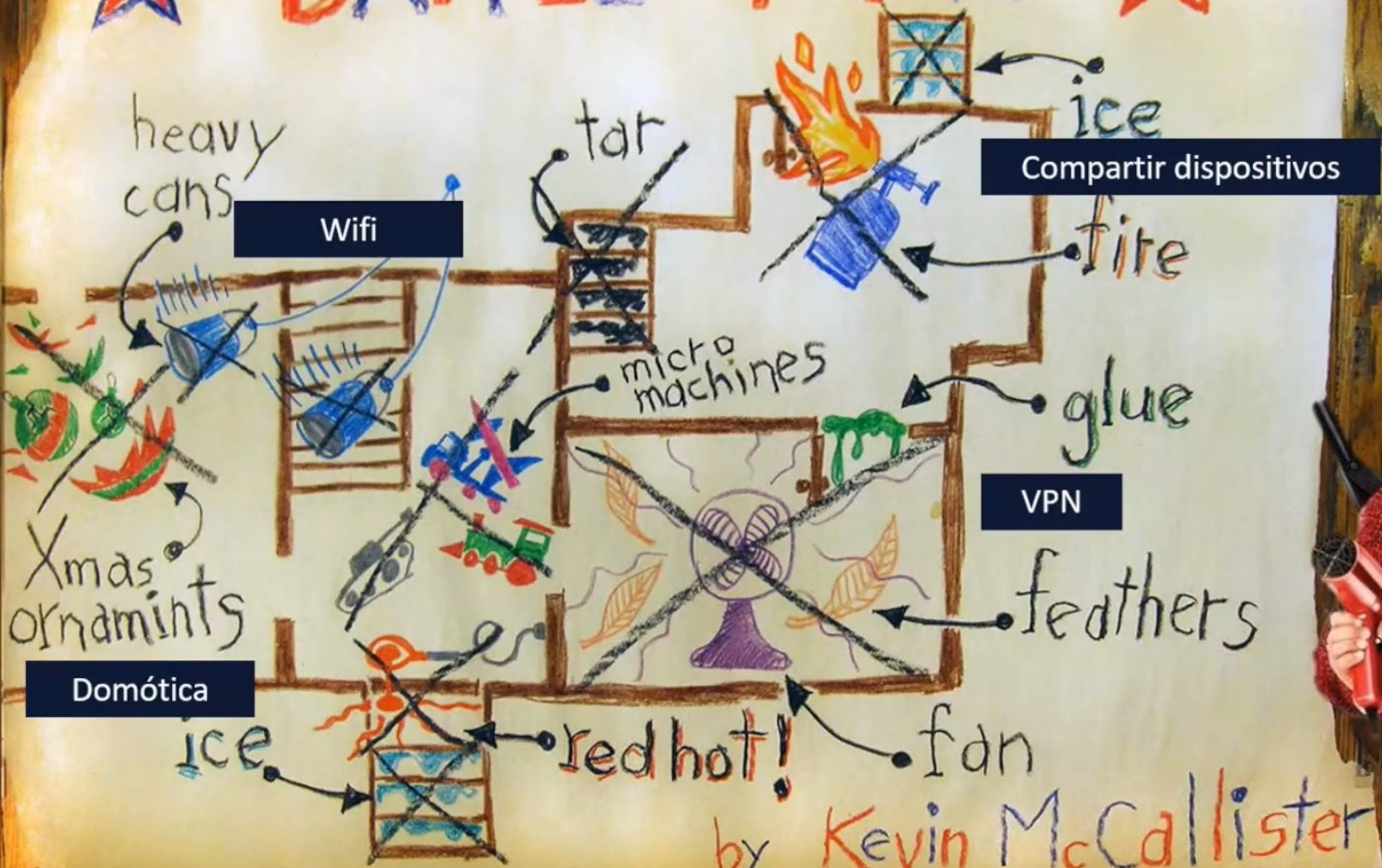
Miedo irracional a estar sin teléfono móvil o a estar desconectados de la red. Es una dependencia a las nuevas tecnologías y más en concreto al móvil.



La seguridad en casa



BATTLE PLAN



by Kevin McCallister



IoT – Internet of Things

En 2021, se han analizado en España más de 4 millones de dispositivos IoT.

Lo que implica que cada vez convivimos con más aparatos que están comunicándose.

El Internet de las cosas (IoT) aporta una enorme comodidad en el hogar.

El uso de dispositivos inteligentes con conexión a Internet te permite tener el café a punto cuando te levantas e incluso poner el horno en funcionamiento para encontrarte la cena caliente al regresas a casa. Puedes controlar la temperatura y la calidad del aire, cerrar las puertas e incluso vigilar la casa desde el teléfono móvil



IoT – Internet of Things

INTERNET

Una Roomba grabó a una mujer en el baño y las imágenes terminaron en Facebook

Fue en 2020, como parte del desarrollo de nuevas Roomba. No obstante, de alguna forma, las imágenes salieron a la luz.

por Hipertextual (Redacción)
20 de diciembre de 2022



¡La Roomba espía!

No es ficción, es un artículo dónde se cuenta la historia de uno de estos dispositivos de limpieza inteligente producida por iRobot que, en función de desarrollo y entrenamiento de Inteligencia Artificial (AI), terminó tomando fotos íntimas que pasaron del robot al Scale AI y luego en las redes sociales.

No es un caso de hackeo, sino más bien un error en el algoritmo empleado en el electrodoméstico (un error humano) y posteriormente si un caso que está siendo investigado para determinar quién filtró las fotos desde Scale AI hacia las redes sociales

IoT – Internet of Things

RIESGOS



- **Problemas de privacidad:** Recogen gran cantidad de datos, que se envían a proveedores, y en ocasiones los comparten o los venden a terceros.
- **Amenazas de seguridad y malware:** Al estar conectados a Internet pueden ser atacados.
- **Robos:** Los dispositivos IoT guardan gran cantidad de datos que pueden suponer un riesgo, ya se sea contraseñas, datos de tarjetas de crédito o incluso nuestros movimientos.
- **Secuestro de dispositivos:** Un actor malicioso puede hacerse con el control del dispositivo y pedir, por ejemplo, un rescate por ello.
- **Problemas de cumplimiento:** Los dispositivos IoT suelen estar configurados para cumplir órdenes de personas autorizadas, pero es fácil realizar un ataque de suplantación

IoT – Internet of Things

¿Cómo me protejo?



- Mantener los dispositivos y el software actualizado.
- Cambiar las contraseñas por defecto, utilizando contraseñas robustas.
- Cambiar la configuración por defecto, deshabilitando las funciones que no sean necesarias, y dotando de toda la seguridad posible.
- Usar un método de cifrado WIFI seguro, para mantener las comunicaciones seguras.
- Activar la autenticación multifactor cuando sea posible

Configuración segura en redes wifi

Lo primero que haremos será ir a nuestro navegador web e introducir 192.168.1.1 y nos llevará a la pantalla de acceso de nuestro router. La imagen que se muestra puede cambiar dependiendo de la compañía con la que se tenga contratado

Por favor, introduce tu usuario y contraseña para continuar

Introduce tu contraseña de administración del Router.
Tu contraseña por defecto es la clave Wi-Fi indicada en la etiqueta de la parte inferior del Router.



Para simplificar la protección de seguridad puedes:

1. Guardar tu contraseña utilizando tu navegador de Internet.
2. Cambiar la contraseña por un valor personal dentro de la interfaz de usuario en la página "configuración avanzada" pestaña "administración".

Acceso

Contraseña

Introducimos los datos que nos solicitan. Normalmente, esta información la podemos encontrar en la parte trasera de nuestro router o en su manual de instrucciones.

En caso de que no lo tengas, siempre tienes la opción de introducir el usuario y contraseña genéricos (admin/admin, admin/1234...)

Recuerda que esta contraseña viene por defecto y debes cambiarla para aumentar la seguridad de acceso a tu router

Configuración segura en redes wifi

Una vez accedamos, debemos fijarnos en el menú de navegación de nuestro router y dirigirnos a la pestaña donde se encuentre los datos del Wi-Fi

mi red local **Wi-Fi** mis archivos mi teléfono información y diagnóstico configuración avanzada

Estado de Wi-Fi Wi-Fi activado desactivar

nombre del Wi-Fi (SSID)

clave Wi-Fi

banda Wi-Fi de 2.4 GHz Wi-Fi de 5 GHz

canal canal actual: 11 escanear canal actual: 108 escanear

Planificación Wi-Fi [definir programación horaria del Wi-Fi](#)

cancelar guardar

Una vez llegado a este panel, solo debemos cambiar el nombre de nuestra wifi por el que queramos poner. Por ejemplo “Miwifi” y poner una contraseña robusta y que podamos recordar.

Nuestro router también tiene la posibilidad de activar una Wifi para invitados, así si recibes visitas y necesitan usar el wifi no se conectarán directamente a tu misma wifi.

Wi-Fi de invitados 2.4 GHz + 5 GHz

estado El Wi-Fi de invitados está activado desactivar

Nombre (SSID)

temporizador ☒ permanente ☐ 1h ☐ 2h ☐ 4h ☐ 24h ☐ 48h

clave Wi-Fi

modo de seguridad

Uso del ordenador

RECOMENDACIONES

- No utilizar contraseñas no robustas
- No instalar software de fuentes no seguras
- Realizar backups de la información.
- No conectar a wifis abiertas, públicas o no protegidas.
- Si se utiliza la nube para el almacenamiento de datos, utilizar herramientas de cifrado.
- No prestar el equipo a personas que no sean de nuestra plena confianza
- Mantener separados los entornos personales y laborales.
- No pinchar nunca en enlaces en los que no sepamos quién nos lo remite o que nos metan prisa para realizar algo.
- Nunca facilitar datos personales de ningún tipo.
- Utilizar siempre webs oficiales



Seguridad con los niños y adolescentes

Seguro que a tu hij@ le previenes de lo que le puede ocurrir en su día a día en la calle, la seguridad en Internet también se basa en educación y es sencillamente, trasladar tus consejos a internet:

- **No hables con extraños por la calle.** No chatees, ni agregues a personas que no conozcas, aunque su foto de perfil sea la de un niño/a.
- **No aceptes regalos de desconocidos.** No aceptes invitaciones de personas que no conoces y menos, si te ofrecen algo a cambio.
- **No digas dónde vives a nadie que no sea de confianza.** No des información sensible: dirección de casa, móvil, email, datos bancarios en tu muro ni por chat a nadie, nunca sabes quién está detrás. Puede ocurrir que te los pidan tus propios amigos a los que han usurpado su identidad



Seguridad con los niños y adolescentes

- **No vayas solo por la calle.** En este caso, es importante la ubicación del ordenador en casa o que no se aíslen con el móvil. Éste debe estar en una zona transitada para poder “echar un ojo” de vez en cuando.
- **No se puede ir desnud@ por la calle.** No envíes fotos y/o vídeos comprometidas a nadie, ni subas fotografías que te dieran vergüenza que vieran otras personas. Pueden ser usadas por personas que no conoces y que acceden de forma ilegal a ellas.
- **Si te pasó algo, llámame corriendo, sea lo que sea, yo te ayudaré aunque no me hayas obedecido.** Si te amenazan o te cohiben en al red, no dudes en contármelo, podré ayudarte.



Seguridad con los niños y adolescentes

Ciberbullying

Según un estudio de la ONG Bullying Sin Fronteras, 7 de cada 10 niños en España sufre acoso escolar. Así mismo, a raíz de la pandemia, el ciberacoso ha aumentado

- Ayudar a los niños a gestionar el problema.
- Hacerle ver a los niños que no deben responder a las provocaciones, ya que es una ventaja para quienes acosan. Lo más importante en estos casos es mantener la calma y no actuar de forma impulsiva.
- Actuar sin entender el contexto puede agravar los problemas.
- Evitar frecuentar lugares dónde se sufre ciberbullying, como redes sociales o comunidades online y, en casos extremos, incluso cambiar de perfil o número de teléfono

Multa histórica a un menor por amenazar a otra con publicar fotos íntimas

El joven, de dieciséis años, presionaba a su víctima, de trece, con la publicación de las imágenes que le mandaba si no continuaba haciéndolo

La AEPD ha multado a un menor con 5.000 euros por el hecho de tratar, registrar y conservar imágenes íntimas de una menor con el fin de seguir chantajeándola.



Seguridad con los niños y adolescentes

Cyberbullying

- **Eliminar cualquier aplicación sospechosa** de los dispositivos digitales utilizados, cambiar las claves de acceso a los servicios online, depurar la lista de contactos y reconfigurar las opciones de privacidad de las redes sociales y apps para hacerlas más restrictivas.
- Guardar las **pruebas de acoso**, tratar de conocer la identidad de los autores, comunicarles que lo que hacen molesta y pedirles sin confrontaciones que dejen de hacerlo.
- Hacer ver a quienes acosan que sus actos **están perseguidos por la ley** y emprender acciones legales.



Seguridad con los niños y adolescentes

14 AÑOS			
13 AÑOS			
			
2-8 AÑOS			



Aunque cada plataforma establece una edad mínima para registrarse en la misma, en España, el acceso a las redes sociales se encuentra regulado en el art. 13 del Real Decreto 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD y también deriva ahora de la LOPDGDD

Seguridad con los niños y adolescentes

Control Parental

1. Cómo configurar en Google la búsqueda segura para niños:

Para controlar que tu hijo no se encuentre nada raro haciendo una búsqueda en Google, únicamente accede a esta url: <https://www.google.com/preferences> y activa el control parental:

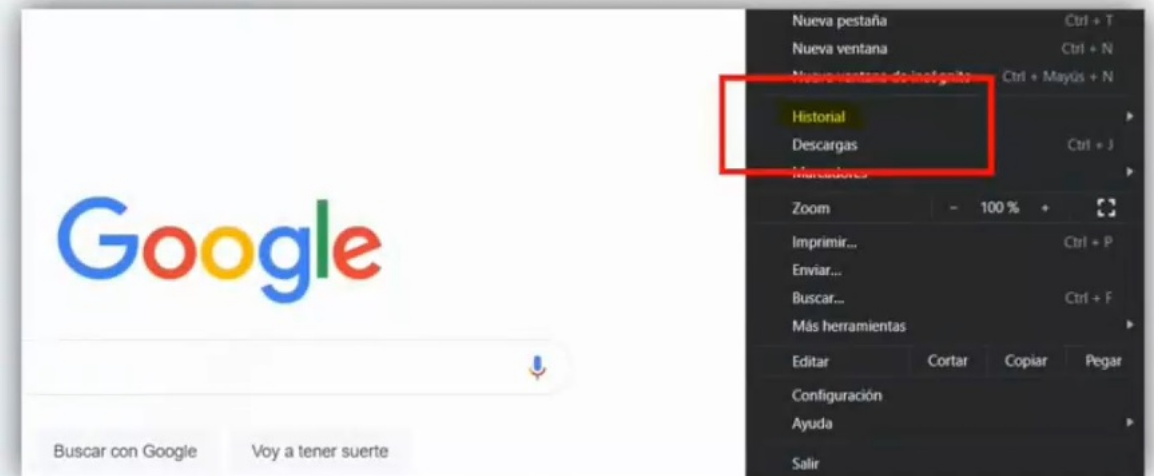
Filtros Búsqueda Segura

Si activas Búsqueda Segura, se ocultará el contenido explícito de carácter sexual, como la pornografía. Recuerda que el administrador de tu dispositivo o de tu red puede haber activado las preferencias de Búsqueda Segura. Si no puedes desactivarlas, avisa al administrador del dispositivo o de la red.

☒ Activar Búsqueda Segura [Más información](#)

2. Consultar historial de búsquedas

Si quieres revisar las **búsquedas que realiza tu hijo/a** en Google, puedes hacerlo. Con esta ruta podrás ver las páginas por las que navega tu hijo/a y ver si está consultando alguna que no debería.



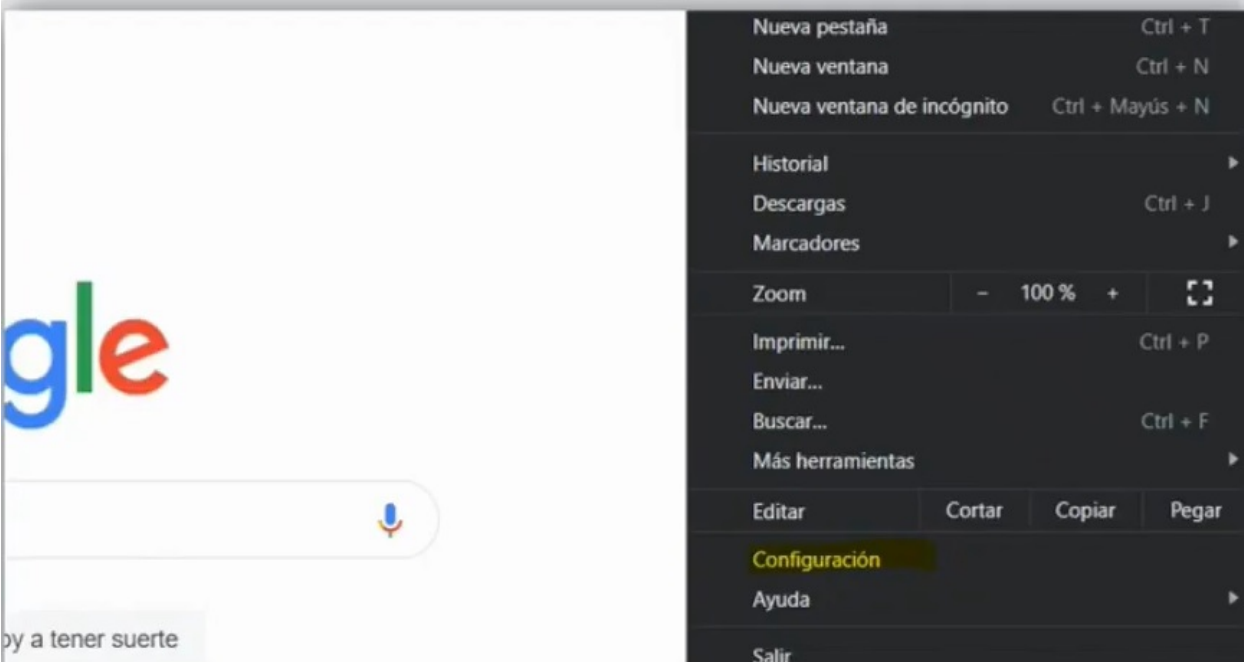
Seguridad con los niños y adolescentes

Control Parental

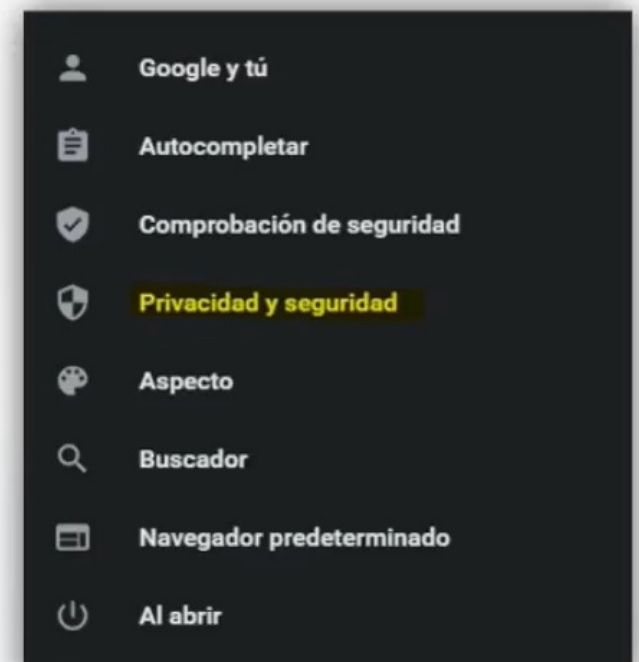
3. Bloquear páginas concretas

Si has visto alguna página que te preocupa, en Google es posible bloquear páginas concretas

Paso 1: Desplegamos y vamos a configuración



Paso 2: Abrimos Privacidad y seguridad

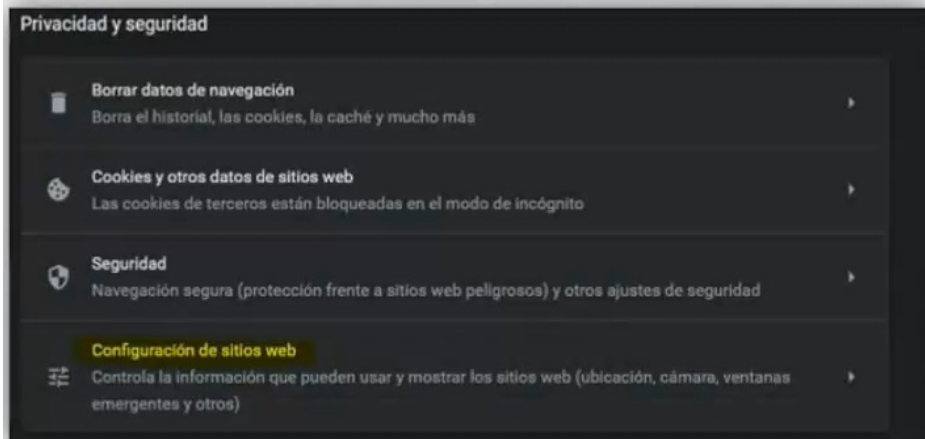


Seguridad con los niños y adolescentes

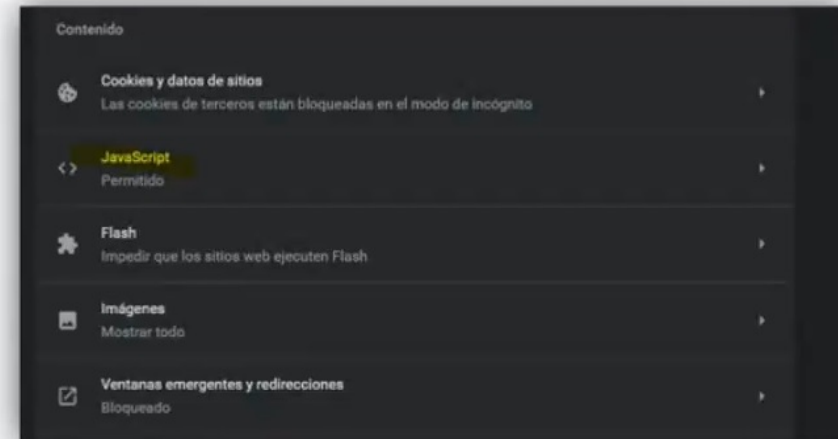
Control Parental

3. Bloquear páginas concretas

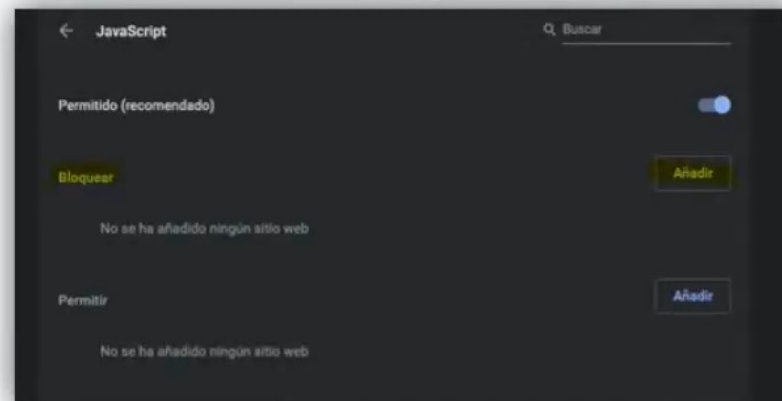
Paso 3: Abrimos Configuración de sitios web



Paso 4: Abrimos JavaScript

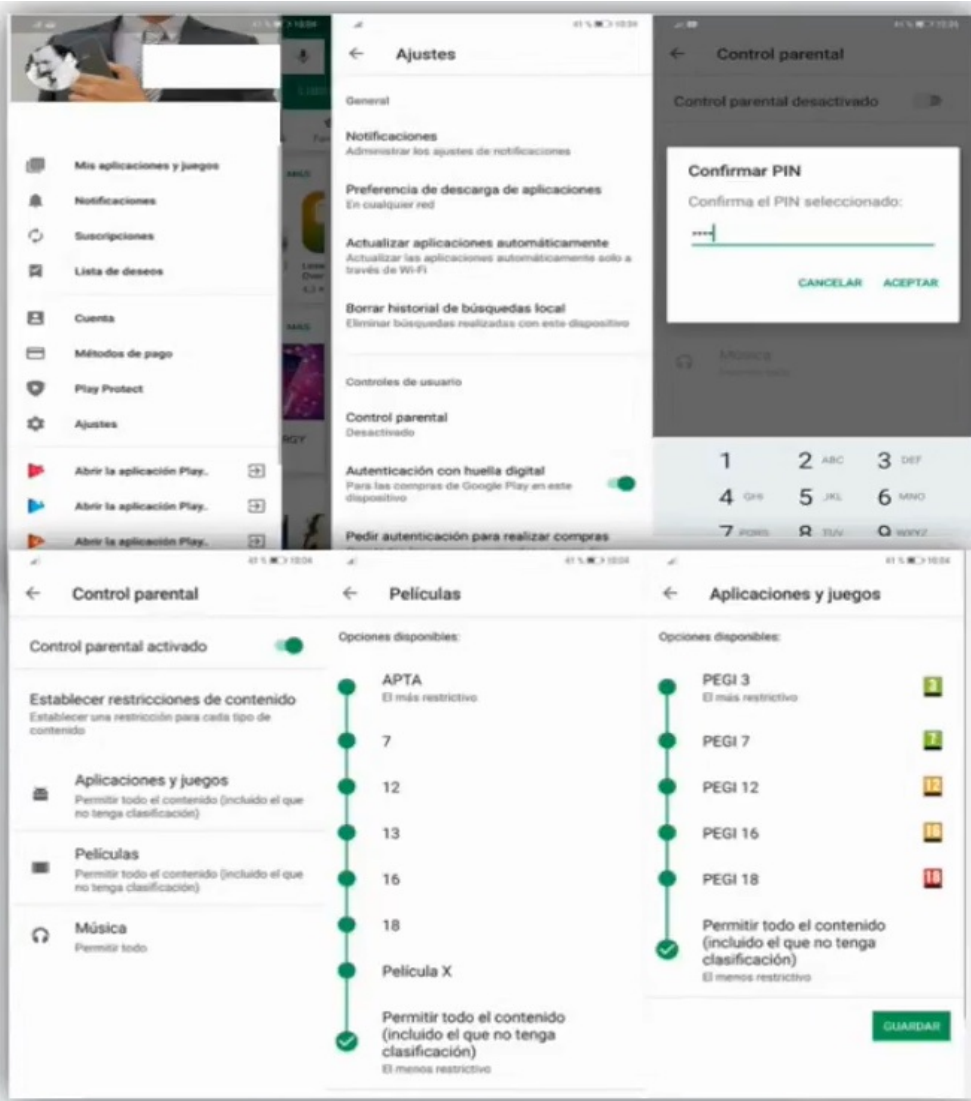


Paso 5: Añadimos las páginas que queremos bloquear



Seguridad con los niños y adolescentes

Control Parental - Android



Para activar esta función debemos ir a la tienda de aplicaciones y tras abrir el menú lateral pulsamos en Ajustes. Ahí veremos una sección llamada Control Parental y al entrar nos pedirá que activemos la opción de control parental.

Para hacerlo debemos usar un PIN que es el que pedirá al intentar descargar un elemento que no coincida con los filtros elegidos.

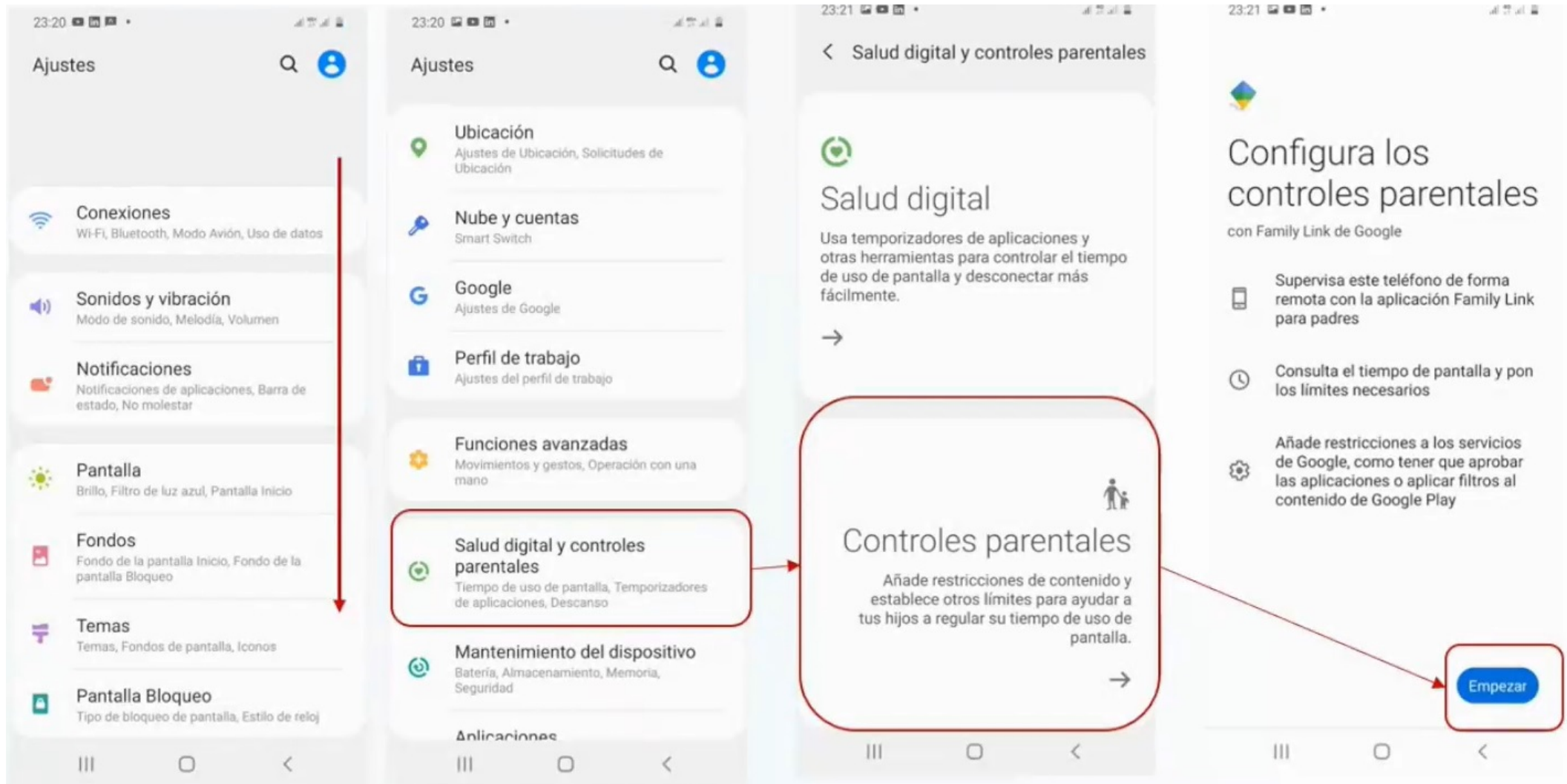
La Google Play Store usa parámetros bastante genéricos en el caso de aplicaciones y vídeos:

- **Juegos y aplicaciones** → Se puede restringir la descarga desde PEGI 3 a PEGI 18.
- **Películas** → Se puede escoger películas para todos los públicos, para mayores de 13, 16 o 18 y películas pornográficas.
- **Música** → Solo se puede restringir o no la música que está marcada como explícita por su vocabulario o expresiones.

Además hay una opción que pide autenticación para realizar compras, algo muy adecuado para no llevarnos sorpresas en las facturas ya que sirve tanto para el contenido de pago como para el gratuito

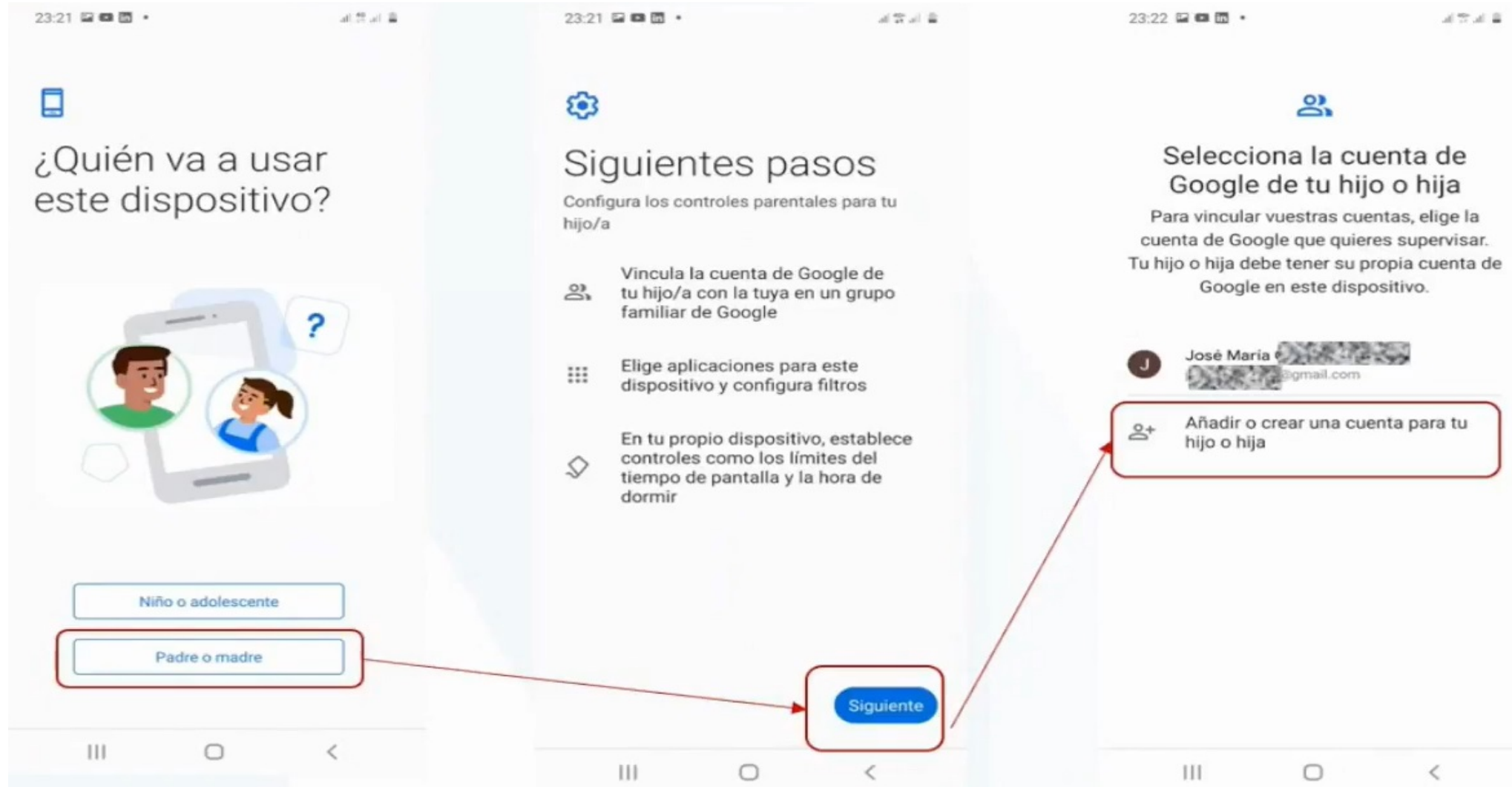
Seguridad con los niños y adolescentes

Control Parental - Android



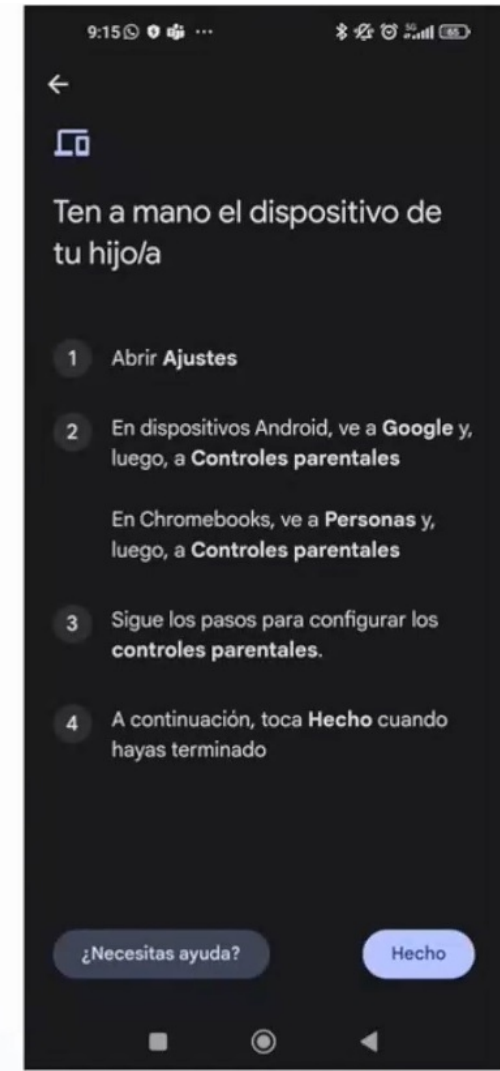
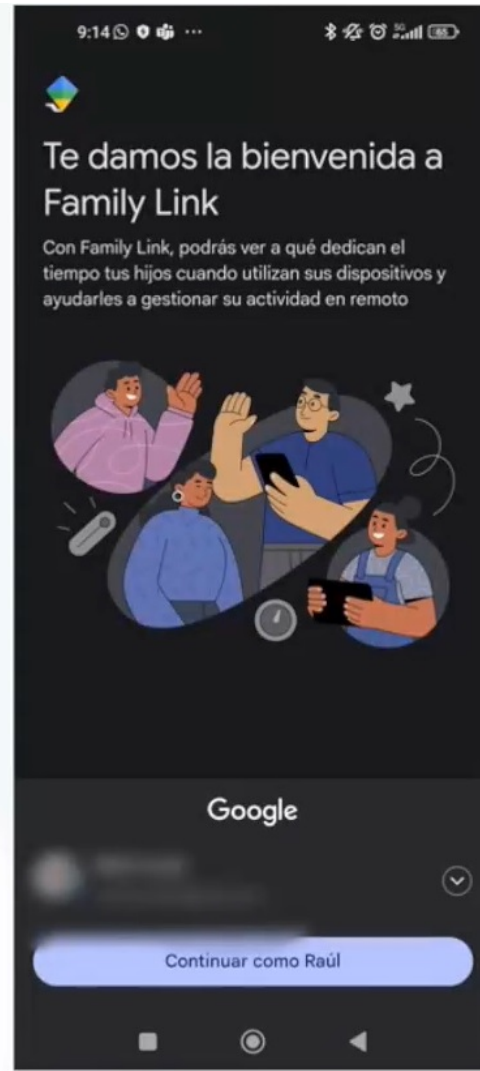
Seguridad con los niños y adolescentes

Control Parental - Android



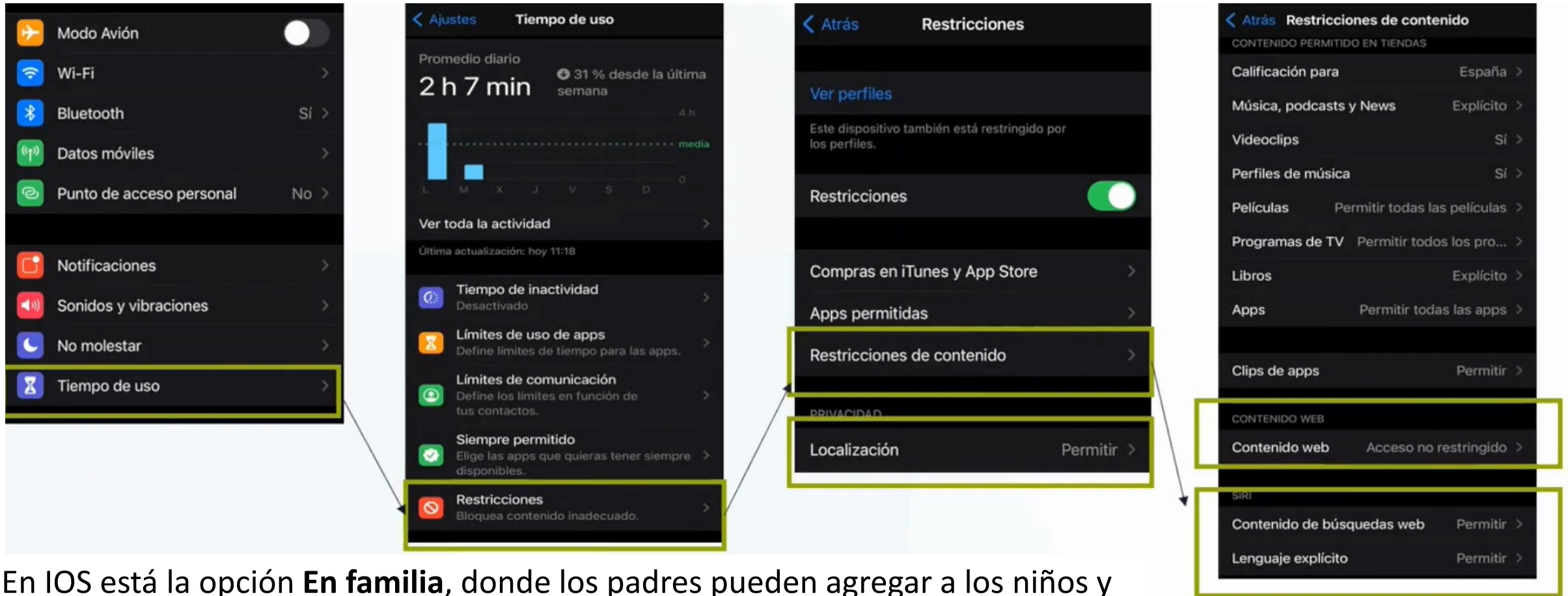
Seguridad con los niños y adolescentes

Control Parental - Android



Seguridad con los niños y adolescentes

Control Parental - iOS



En IOS está la opción **En familia**, donde los padres pueden agregar a los niños y realizar estas opciones para cada uno de los dispositivos

Enlaces de interés

Webs con recursos:

<https://www.is4k.es>

<https://www.osi.es/es>

Enlaces con ampliación de información:

Sistemas de control parental https://files.incibe.es/is4k/is4k_guía_controles_parentales.pdf

Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía

https://www.policía.es/es/tupolicia_conocenos_infantil_portada.php

Tipos de Groomers <https://diarionorte.com/182065-peligro-en-las-redes-detectan-4-formas-de-groomers>

Fases del acoso virtual <https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo>

Estudios:

Fundación Anar <https://www.anar.org/descarga-el-estudio-anar-sobre-abuso-sexual-en-la-infancia-y-adolescencia-según-los-afectados-y-su-evolución-en-España-2008-2019/>