

## teléfonos móviles, Internet y TV: lo que los padres deben saber

Esta guía les asesora para que usted y sus hijos/as puedan sacar el máximo partido a todos los servicios de comunicación, información y entretenimiento que proporciona Orange con total seguridad. También esperamos que les ayude a entender las nuevas tecnologías y los servicios asociados a las mismas.

Las nuevas tecnologías siguen evolucionando rápidamente y nada parece indicar que vaya a frenarse el ritmo al que se crean y se ponen a disposición de los usuarios nuevas prestaciones y servicios.

Así por ejemplo, en sólo diez años, los móviles han evolucionado desde una versión sin hilos del teléfono tradicional hasta un producto más parecido a un ordenador portátil o a un reproductor de música y televisión.

En el futuro inmediato, los móviles y las redes inalámbricas ofrecerán muchos otros servicios que en la actualidad sólo están disponibles en los ordenadores fijos.

El desafío para los padres es asegurarse de que sus hijos/as entienden perfectamente y están preparados para las posibilidades, tanto buenas como malas, que esta tecnología va a poner a su alcance.



## índice

4	introducción
6	contenido para adultos e Internet
10	chats/mensajería instantánea
14	blogs
18	servicios de localización
22	spam
26	intimidación y acoso por el móvil o correo electrónico
28	uso inapropiado de los teléfonos móviles – llamadas de emergencia falsas
30	robo y pérdida de teléfonos
34	delitos a través del correo electrónico
36	jóvenes, teléfonos móviles, tráfico y conducción
40	mensajes de vídeo/fotografías
42	teléfonos móviles y salud
46	televisión
48	glosario

## introducción

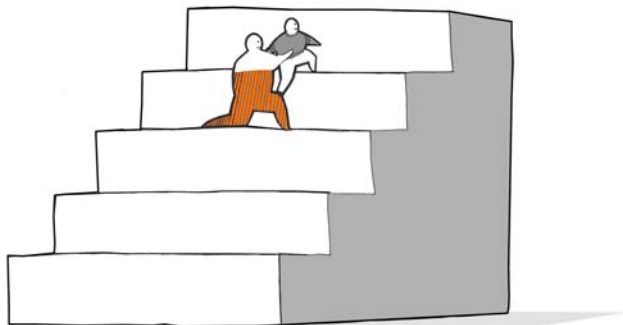
Si bien los móviles e Internet nos han aportado muchas ventajas, ciertos usos pueden ser antisociales o poco deseados. Estos usos van desde mantener una conversación en voz alta en un medio de transporte público hasta el envío de mensajes spam, el uso del teléfono para realizar bromas o timos y el acoso.

Asimismo, la aparición de Internet, espacio abierto a la publicación incontrolada de contenidos de todo tipo y de muy fácil acceso, ha hecho que los niños tengan a su alcance diversos tipos de material inapropiado, al que muchos adultos tampoco desean acceder. Además, al igual que en el mundo real, esta ventana abierta al ciberespacio, ha sido aprovechada en algunos casos para la captación y el engaño, sobre todo de menores.

A esto cabe añadir que los móviles, puesto que son objetos pequeños y deseados, se convierten a menudo en el objetivo de los ladrones.

Para ayudar a sus hijos/as a utilizar con toda seguridad los móviles e Internet, en esta guía le proporcionamos la información que necesita saber y le planteamos cuestiones que podrá tratar con ellos (véanse los recuadros de “recomendaciones” a lo largo de todo este documento).

También se ofrece información sobre a quién contactar para saber más sobre cualquiera de los temas presentados en esta guía.



### antes de utilizar un teléfono móvil y/o navegar por Internet

La información que encontrará en esta guía ha sido recopilada para que sus hijos/as saquen el máximo provecho de sus móviles e Internet. Pero antes de que naveguen y/o los utilicen por primera vez, debería tener en cuenta los siguientes puntos:

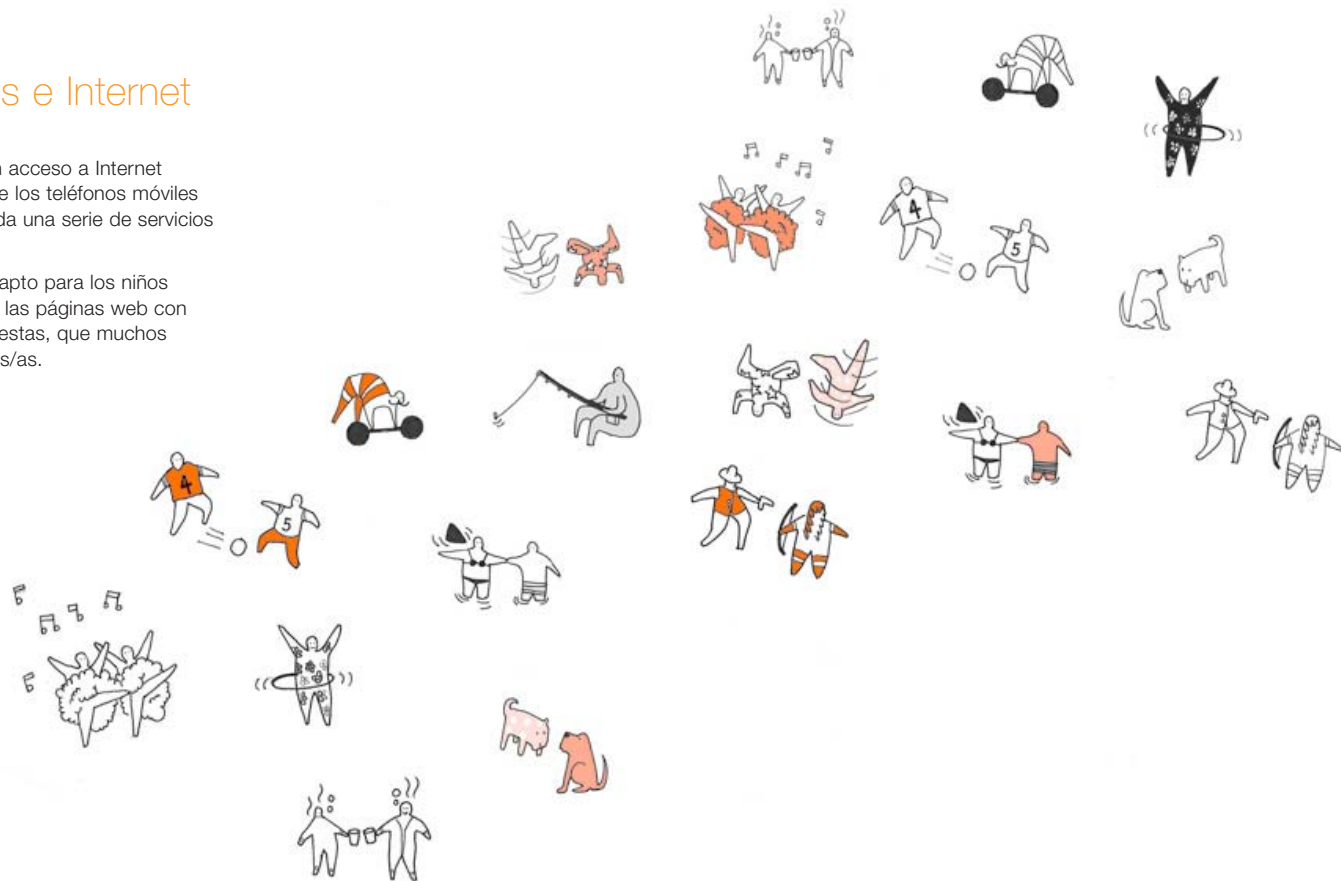
- déjeles claro cómo quiere que utilicen el teléfono e Internet.  
Hablar desde un primer momento del uso de los servicios de pago (como la música y los videoclips, o el tiempo pasado en Internet) puede evitar sorpresas desagradables al recibir la primera factura. Vigilar también el uso de sus tarjetas puede también no estar de más
- hable de todo lo relacionado con el contenido para adultos de una manera que haga que sus hijos/as se sientan cómodos para tratar de nuevo el tema si lo consideran necesario. Si bien es posible bloquear o evitar el acceso al material para adultos, nada le garantiza que sus amigos/as utilicen teléfonos u ordenadores en los que no se haya realizado este bloqueo
- advierta a sus hijos de la posibilidad de que las informaciones publicadas en Internet sean falsas, así como las identidades de las personas con las que puede tomar contacto
- probablemente tendrá que hablar más de una vez sobre la seguridad de los teléfonos móviles a medida que vayan apareciendo nuevos servicios y posibilidades
- en función de la edad de sus hijos/as, los consejos y reglas establecidas en la familia deberían evolucionar para reflejar el mayor nivel de confianza depositado en ellos
- es una buena idea compartir experiencias relacionadas con los nuevos servicios de comunicación con otros padres. Esto permite esclarecer algunos dilemas antes de que se conviertan en un problema para usted y sus hijos/as
- ubique el ordenador en un lugar “público” de la casa, de manera que sus hijos/as puedan contar con su supervisión con mayor facilidad
- es recomendable que los teléfonos móviles de sus hijos/as sean de contrato; de esa manera tendrán un registro de las llamadas realizadas, así como un control del consumo
- alerte a sus hijos para que no tomen en serio todo aquello de lo que puedan llegar a leer en Internet y, desconfíen y le informen de las personas que puedan llegar a conocer a través de la Red

## contenido para adultos e Internet

### ¿qué es el “contenido para adultos”?

A través de Internet y de los teléfonos con acceso a Internet o navegación WAP (consulte el Glosario de los teléfonos móviles al final de la guía) es posible acceder a toda una serie de servicios e información destinada a adultos.

Está claro que no todo este material será apto para los niños e incluso para ciertos adultos, en especial las páginas web con contenido pornográfico, violento o de apuestas, que muchos padres considerarán nocivas para sus hijos/as.



### ¿de dónde procede el contenido para adultos?

Internet y los operadores de telefonía móvil ofrecen algunos servicios destinados a adultos como juegos, vídeos e imágenes que sólo se pueden ver si el usuario manifiesta que es mayor de edad.

### ¿el teléfono que he comprado me permite acceder a Internet?

En la actualidad, probablemente la respuesta es sí, sobre todo si el teléfono es de última generación.

### ¿cómo puedo bloquear el material para adultos?

Si le preocupa que su hijo/a pueda acceder a material para adultos con su teléfono, Orange puede bloquear el acceso a este tipo de servicios.

Activar y desactivar el bloqueo es sencillo. Para más información, llame al servicio de atención al cliente al 1414.

Si le preocupa el acceso a contenidos inapropiados de Internet, instale en su ordenador un programa de “control parental” o control de contenidos web.

Hay magníficas aplicaciones que realizan este servicio de filtrado, tan personalizado como se quiera. Orange ofrece a sus clientes la posibilidad de contratarlo por un precio reducido. Consulte en <http://seguridad.orange.es>

### más información

Si desea obtener más información sobre los filtros y sobre cómo controlamos la edad del cliente, puede llamar al servicio de atención al cliente de Orange al 1414.

### informar sobre contenido potencialmente ilegal en Internet

Si cree que ha encontrado imágenes ilegales en Internet, puede informar de ello a través del sitio web de INHOPE (la Asociación Internacional de Líneas Directas de Internet, por sus siglas en inglés) <http://www.inhope.org/en/index.html>

Además, en España existen otras direcciones a través de las cuales se pueden denunciar contenidos ilícitos:

[delitos.tecnológicos@policia.es](mailto:delitos.tecnológicos@policia.es)

[delitoinformativo@guardiacivil.es](mailto:delitoinformativo@guardiacivil.es)

<http://www.dmenor-mad.es/escribenos.php>

[contacto@protegeles.com](mailto:contacto@protegeles.com)

### recomendaciones

- recuerde a sus hijos/as que en Internet hay material desagradable, inapropiado e incluso ilícito
- anímeles a que le informen a usted o a un profesor en el que confíen si ven algo que les inquieta, ya sea en su propio teléfono y/u ordenador o en el de un amigo
- es posible que los niños no siempre utilicen el teléfono o el ordenador que les compró usted. Así pues, también sería bueno advertirles de que mirar cualquier tipo de material no “apto”, y sobre todo pagar por él, fomenta que se produzca más material de este tipo y que aumente el malestar y los problemas derivados de ello

## chats/mensajería instantánea

### ¿qué son?

Los chats son servicios en los que las personas intercambian mensajes casi en tiempo real.

Hay miles de ejemplos de chats en los que se habla de cualquier afición o interés. Algunos de los más conocidos aparecen en los sitios web de fans de estrellas del pop.

Los niños a menudo ven estos chats como lugares divertidos y poco peligrosos que pueden visitar para intercambiar experiencias e información. Algunos niños se reinventan a ellos mismos, lejos de la mirada crítica de los hermanos o de los compañeros del colegio.

Pero el hecho de que los niños utilicen estos chats ha llamado la atención de los pederastas, que pueden esconder su edad, su pasado y sus intenciones, y utilizar las conversaciones a través de la web para establecer relaciones impropias con los niños.

### ¿son los chats peligrosos?

Si bien los chats no son peligrosos en sí, pueden convertirse en un verdadero peligro si el niño que los utiliza responde de manera poco adecuada a comentarios o actividades expuestos en el sitio web.

El riesgo más importante que podría darse es que el niño se sienta tentado a concertar una cita con alguien a quien conoció en el chat. No todas las personas que participan en un chat son necesariamente lo que parecen ser.

Para evitar este riesgo, algunos chats están supervisados por moderadores.

En determinados chats se utilizan sofisticados paquetes de software para realizar esta función.

### ¿qué debería hacer?

Ningún filtro puede proteger totalmente a los usuarios de Internet de los actos de otros usuarios con intenciones delictivas o antisociales, ya se navegue desde un ordenador o desde el móvil. Siempre habrá personas que intentarán encontrar la manera de saltarse las protecciones existentes.

En este sentido, Internet y los chats podrían compararse a un espacio público real al aire libre. Al igual que en la vida real, la mejor protección en estos espacios virtuales es tomar las precauciones necesarias y entender los riesgos.

Teniendo esto presente, la mejor protección que puede ofrecer a su hijo/a será advertirle y prepararlo/a lo mejor posible.

### recomendaciones

A continuación aparecen algunas precauciones sencillas destinadas a los niños que pueden ayudarles a reducir significativamente los riesgos de encontrarse con alguien que no es quien pretende ser:

- no intentar encontrarse nunca en persona con alguien a quien se haya conocido en un chat, a menos que el menor vaya acompañado de un progenitor
- no facilitar datos personales
- evitar los chats que no disponen de moderador, a menos que se entre en ellos con la supervisión de los padres
- no compartir nunca secretos en un chat

### recomendaciones

- alertar sobre el peligro de abrir una webcam a un desconocido (una webcam es una videocámara que puede utilizarse en las conversaciones por chat para poner imágenes de cada uno de sus interlocutores y de sus entornos). Recomendar evitar también en lo posible el acceso a imágenes de webcams de personas que no sean conocidas y de confianza
- los niños deben confiar en sus instintos: si notan algo desagradable o extraño, deben abandonar el chat y avisar a sus padres o tutores
- no ir a ningún sitio web propuesto en el chat, ya que podría tener virus informáticos y/o material inapropiado

### más información

Mire la sección correspondiente a su país en este sitio web europeo  
<http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

o información organizada por temas aquí:

<http://www.saferinternet.org/ww/en/pub/insafe/safety.htm>

También puede encontrar más información en las siguientes webs:

<http://www.protegeles.com>

<http://www.ciberfamilias.com>

<http://www.aempi.com>

<http://www.asociacion-acpi.org>

<http://chaval.red.es/padres.html>



## blogs

En los últimos dos años se ha registrado un rápido aumento de los sitios web que permiten a los usuarios publicar su propia página personal o “perfil”. Son muy populares entre los niños y los adolescentes como un medio para auto expresarse y para establecer vínculos con amigos. A esta actividad se la conoce a menudo como “establecimiento de redes sociales online”.

Las páginas web de redes sociales se utilizan normalmente para editar diarios en línea denominados “blogs”. Conocidos como weblog recopilan cronológicamente textos o artículos de uno o varios autores, apareciendo primero el más reciente, donde el autor conserva siempre la libertad de dejar publicado lo que crea pertinente. Habitualmente, en cada artículo, los lectores pueden escribir sus comentarios y el autor darles respuestas, de forma que es posible establecer un diálogo.

A menudo incluyen fotografías, listas de las cosas que le gustan o no a la persona que escribe, datos de contacto, enlaces a otros contenidos y, en definitiva, cualquier cosa que el usuario desee mostrar.

Para hacer que la experiencia sea aún más atractiva, algunas páginas ofrecen software que permite a los usuarios decorar su propia página personal con gráficos e imágenes gratuitas.

Ya existen espacios web de este tipo especialmente diseñados para los móviles y el acceso wap, sms y mms para actualizar y consultar blogs.

Se estima que en la actualidad hay al menos 30 millones de blogs en funcionamiento y se registra uno nuevo cada segundo.

### ¿debería preocuparme?

Los sitios web de este tipo disponen a menudo de unas directrices claras que los usuarios tienen que leer antes de registrarse. Pueden incluir “normas de la casa” sobre la edad de los usuarios y advertencias sobre lo que no se debe publicar, así como un dispositivo para informar de contenidos no deseados. Algunos disponen incluso de equipos de personas encargados de “eliminar” las publicaciones de menores de edad. No obstante, sigue habiendo puntos preocupantes en relación con estos sitios web, entre ellos:

#### ■ **visibilidad**

Los adolescentes, que representan un porcentaje elevado de los usuarios de estas páginas, no siempre son conscientes de que el material que colocan en ellas puede ser visto por cualquier persona en cualquier parte del mundo a través de un ordenador. Por esta razón, los comentarios, los datos personales y las fotografías o imágenes no son, en modo alguno, privados

#### ■ **supervisión**

Para asegurarse de que los niños utilicen dichos sitios web de manera razonable y con consideración, los padres deben saber qué servicios utilizan sus hijos/as y los nombres de usuario (alias) que usan. En la actualidad, la mayoría de los padres no sabe ninguna de estas dos cosas

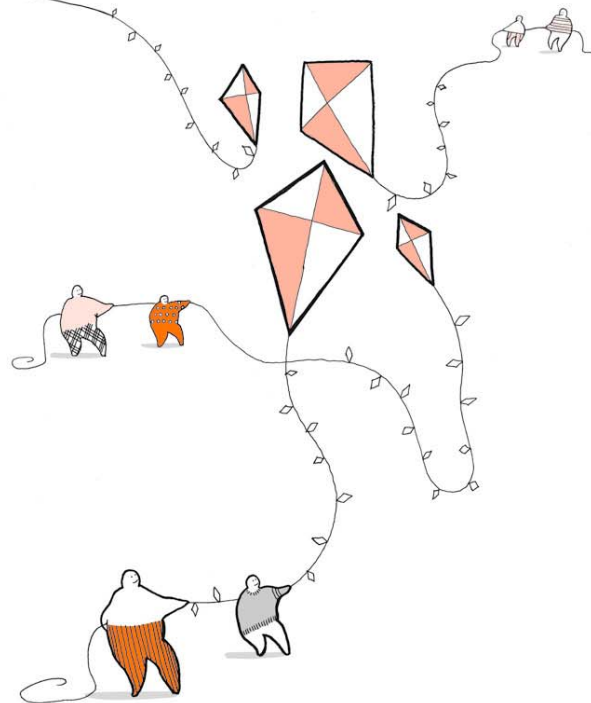
#### ■ **visitantes no deseados**

Estas páginas que tanto atraen a los adolescentes también son un reclamo para toda clase de gente que los padres preferirían que no tuvieran contacto con sus hijos/as. Entre estas personas pueden haber pederastas, personas dedicadas a la pornografía infantil, reclutadores de grupos extremistas y personas que fomentan comportamientos disfuncionales



## ¿qué puedo hacer?

- familiarícese con el funcionamiento de estos sitios web y, a continuación, llegue a un acuerdo con su hijo/a para que le permita comprobar periódicamente lo que publican en sus perfiles
- utilice cualquier error evidente como una oportunidad para aprender tanto usted como su hijo/a, en lugar de reaccionar de manera excesiva. Estas páginas web no van a desaparecer y su hijo/a tendrá que hacer frente a las complejidades de la actividad online el resto de su vida
- hable regularmente con su hijo/a sobre lo que hace en Internet para fomentar una actitud abierta. Generalmente, es más fácil para un niño esconder o borrar sus huellas que para un padre descubrirlas. Un diálogo abierto y sincero ayudará a reducir la necesidad de este tipo de acciones
- manténgase en contacto con los padres de los amigos de sus hijos/as. De esta manera, será más fácil y rápido hacer frente a los problemas que puedan surgir si se actúa de manera cooperativa



### recomendaciones

Algunas de las siguientes afirmaciones pueden ser válidas en la educación a sus hijos/as sobre el uso responsable de las redes sociales:

- recuerda que cualquier persona en cualquier parte del mundo puede ver lo que has escrito. Ten cuidado porque lo que dices puede tener un efecto mayor del que pensabas
- trata a los demás como te gustaría que te trataran a ti. Evita la difamación, la calumnia y la mentira
- no publiques nunca información personal, sobre todo cualquier dato que pueda dar pistas sobre dónde vives o qué lugares frecuentas
- recuerda que el “amigo de un amigo” podría no ser tu amigo

### recomendaciones

- no contestes a los mensajes de personas desconocidas
- informa a un adulto de cualquier cosa rara o molesta que veas
- informa de los ejemplos de intimidación a la propia página web, así como a tus padres
- evita la publicación automática de comentarios de visitantes de tu blog. En caso contrario, debes vigilar estos comentarios con cierta frecuencia y actuar de moderador, eliminando los que consideres inapropiados

## servicios de localización

### ¿qué son?

Los servicios de localización son un conjunto de servicios de valor añadido basados en la localización geográfica, más o menos precisa, de un dispositivo móvil, que requiere principalmente de una red de un operador móvil o de una red de satélites GPS.

Como ejemplos más representativos de los servicios de localización se pueden mencionar los siguientes:

- localización de personas que han dado su autorización para ser localizadas por sus empresas, amigos o familia
- localización de niños o adultos que tienen alguna discapacidad
- navegación durante la conducción
- seguimiento de rutas y desplazamientos de vehículos

Esta misma tecnología también proporciona servicios que muestran información dependiendo de dónde se encuentra el usuario. Algunos ejemplos serían los informes meteorológicos o información sobre promociones de establecimientos comerciales.

La posición/localización de una persona se establece por conexión radio entre su móvil y la antena más próxima. Incluso cuando no se está utilizando el móvil, si el aparato está encendido, sigue enviando regularmente señales para asegurarse de que ha establecido una comunicación con la antena más cercana.

La localización es más precisa si hay varias antenas en las cercanías, por lo que estos servicios funcionan mejor en las áreas urbanas.

Existe en la actualidad una clara tendencia a converger las capacidades de las redes de los operadores de telefonía móvil con la precisión ofrecida por la tecnología GPS.

### ¿quién solicita la información?

La solicitud de localización puede proceder del usuario, de otra persona o de una empresa.

### ¿debería preocuparme?

De los servicios de localización, quizás el más sensible en lo que afecta a los derechos esenciales de la persona, es aquel que permite que un tercero pueda conocer la posición geográfica de un usuario o de elementos de su propiedad/responsabilidad.

Cuando se solicita una localización, el usuario (la persona a la que se localiza) tiene que autorizar dicha solicitud.

También ocasionalmente deberían aparecer en el teléfono móvil mensajes que recuerden que el servicio de localización continúa activo.

### recomendaciones

- asegúrese de que sus hijos/as entienden por qué nunca tienen que decir "sí" a un extraño o a alguien en quien no confían y que intenta encontrarlos mediante un servicio de localización. Asegúrese también de que entiendan por qué esto es importante
- explíqueles que deberían consultarlo con usted antes de aceptar cualquier tipo de servicio que les ofrezcan por teléfono

### las regulaciones que rigen

#### el uso de datos privados son:

En la Unión Europea está regido por la Directiva 2002/58/EC del Parlamento Europeo y del Consejo de 12 de julio de 2002

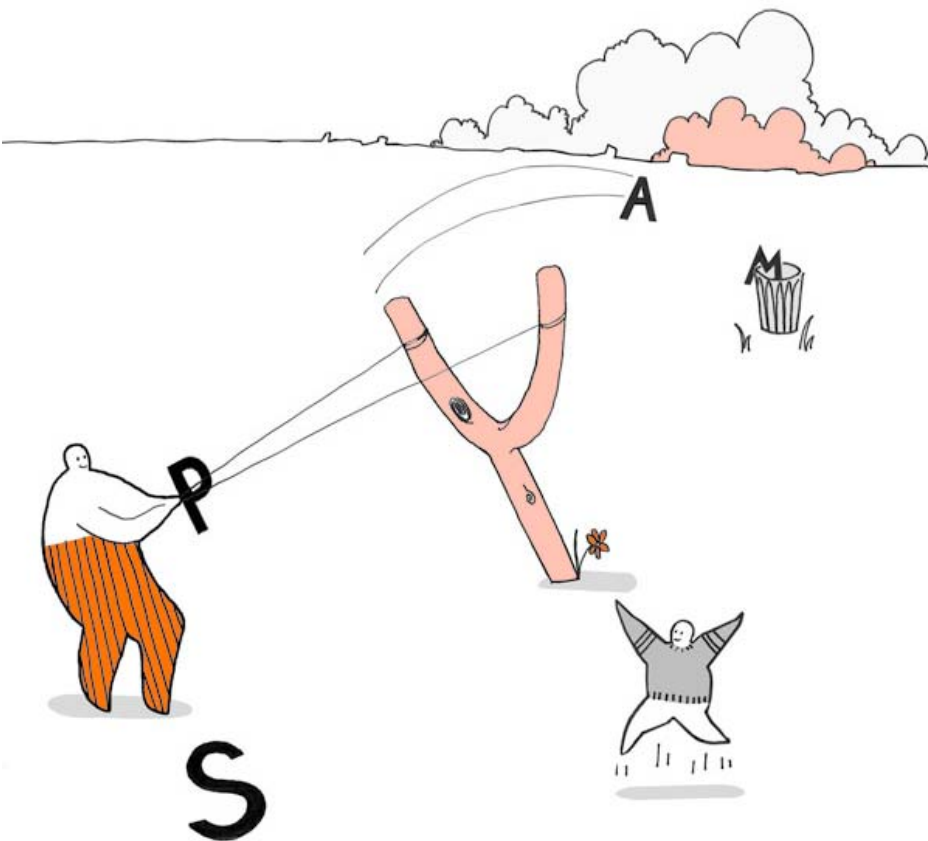
[http://eur-lex.europa.eu/LexUriServ/site/es/oj/2002/l\\_201/l\\_20120020731es00370047.pdf](http://eur-lex.europa.eu/LexUriServ/site/es/oj/2002/l_201/l_20120020731es00370047.pdf)

#### la legislación española es:

- ley Orgánica 15/1999 de 13 de Diciembre de 1999, de protección de datos de carácter personal
- real Decreto 994/1999, de 11 de junio, Reglamento de medidas de seguridad de los ficheros automatizados
- ley 32/2003 de 3 de noviembre, General de Telecomunicaciones
- real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios
- ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y Comercio Electrónico

### más información

Si sospecha que se está utilizando un servicio de localización de manera inadecuada, llame al Servicio de atención al cliente de Orange al 1414.



## spam

### ¿qué son los mensajes no deseados o “spam”?

El “spam” es un mensaje de marketing no deseado que usted no ha solicitado ni al que se ha suscrito de manera voluntaria. Algunos ejemplos de “spam” son los mensajes que le informan de que ha ganado un “regalo misterioso”, que “le gusta a alguien” o que le piden que llame a un número de pago.

Los mensajes no deseados son en realidad una nueva versión de los “mensajes basura” o de las llamadas telefónicas comerciales que se reciben en casa, generalmente de personas o empresas a las que no conocemos.

Los niños pueden ser muy sensibles a estos mensajes, ya que no siempre entienden el coste de los servicios que se ofrecen o lo que implican.

### ¿cómo funcionan los mensajes “spam”?

El spam puede llegar a través del teléfono móvil o a través del correo electrónico. También pueden crearse listas de teléfonos móviles y direcciones de correo electrónico de forma ilegal que luego se venden a empresas como “listados de marketing”. En tales casos, se envía el mismo texto a millones de clientes, por lo que usted o su hijo/a no habrán sido identificados individualmente.

El problema afecta a todas las redes de telefonía móvil y proveedores de correo electrónico, no sólo a Orange. Orange no proporciona los números de teléfono o direcciones de correo de sus clientes a otras empresas.

La vía principal para el spam es sin embargo todavía el correo electrónico. Las cuentas de correo pueden captarse de Internet, de programas de chats y del propio uso del correo. Y el peligro es el mismo que en el spam de teléfonos móviles: muchas veces son puertas abiertas al fraude y al engaño.

### cancelación de servicios

- si recibe mensajes de texto de un número con código corto para un servicio al que se ha suscrito pero que ya no desea recibir, basta con enviar la palabra “baja” al remitente del mensaje
- si no tiene sus datos de contacto, llame al Servicio de atención al cliente de Orange al 1414, que podrá ayudarle a encontrar los datos de contacto del suministrador del servicio
- si recibe en su correo boletines periódicos no deseados, busque en el texto de los boletines las instrucciones para darse de baja (deben estar incluidas)

Para cancelar los Mensajes de Marketing Orange, llame directamente al Servicio de atención al cliente de Orange al 1414.

### **cómo evitar el “spam”**

- lea atentamente los términos y condiciones de uso que aparecen en los formularios antes de proporcionar su número de teléfono o dirección de correo electrónico
- cuando rellene formularios en Internet o en papel, deberá marcar o quitar la marca de las casillas de autorización para declarar que no desea recibir mensajes comerciales. Y si utiliza su teléfono para dar estos detalles, deje claro a su interlocutor cuáles son sus preferencias en relación con su teléfono móvil o dirección de correo electrónico
- no se registre nunca en páginas web que prometan retirar su nombre de las listas de mensajes “spam”. Aunque estas páginas pueden ser legítimas, a veces lo que hacen es recopilar números de teléfonos móviles o direcciones de correo electrónico
- utilice filtros antispam para su correo. Muchos antivirus los incluyen. Orange ofrece a sus usuarios de Internet la posibilidad de incluir un servicio de antispam. Para más información llame directamente al Servicio de atención al cliente de Orange al 1414

### **más información en**

<http://www.spamhaus.org/>

### **recomendaciones**

- explique los riesgos de contestar a los mensajes “spam” o de llamar al número que aparece en el mensaje, ya que el precio de la llamada podría ser muy elevado
- pida a su hijo/a que le pregunte antes de aceptar ofertas hechas por teléfono
- explique a su hijo/a que si responde a un mensaje “spam”, es mejor reconocer el error lo antes posible, ya que así podrá contactar directamente con la empresa para detener el servicio antes de que la factura se suba por las nubes
- transmita a su hijo/a la desconfianza ante todo correo no solicitado en el que se pidan datos personales o claves de identificación

# intimidación y acoso por el móvil o correo electrónico

## ¿qué es?

La gran familiaridad que tienen algunos niños con los servicios de móvil les ha permitido desarrollar maneras de utilizar el móvil para intimidar y acosar a otros niños.

Por ejemplo, pueden:

- dejar mensajes de voz con amenazas
- enviar mensajes de texto con amenazas
- distribuir fotografías hechas con las cámaras de los móviles

## ¿cuáles son las señales que pueden indicarme que esto le está ocurriendo a mi hijo/a?

La intimidación por teléfono puede formar parte de una estrategia más compleja de intimidación y es extremadamente molesta porque pueden verse afectados hasta en su propio hogar.

La intimidación puede causar sentimientos de vergüenza, desprecio y desesperanza, y los niños a menudo se niegan a hablar de ello porque piensan que deberían ser capaces de afrontarlo solos. Algunas señales que podrían

indicar que existe un problema son los cambios de humor repentinos e infundados, los cortes y moratones para los que no se da una explicación, un comportamiento demasiado tranquilo o recluso poco usual para el niño/a o intentos persistentes de evitar ir a la escuela con el pretexto de “no sentirse bien”, por ejemplo.

Si tiene alguna sospecha de que su hijo/a puede ser víctima de intimidación, es vital que aborde el tema con los profesores lo antes posible.

Si es necesario, también se puede tratar específicamente cualquier problema relacionado con el móvil de su hijo/a. Estas son las principales opciones:

- llamar al Servicio de atención al cliente de Orange 1414
- hacer los trámites para cambiar el número de teléfono

Si lo desea, podemos proporcionar información pertinente a la policía. No obstante, de conformidad con la ley de protección de datos, no podemos suministrarle directamente información sobre la persona que realiza la llamada.



## recomendaciones

Antes de que sus hijos/as se pongan a utilizar el móvil, es bueno darles los siguientes consejos:

- nunca des información sobre ti a menos que conozcas a la persona que llama
- deja que la persona que llama se identifique, sobre todo si no aparece su número
- si recibes una llamada de un número que te causa problemas, no respondas: desvía las llamadas al contestador sin responder
- no menciones ningún dato de contacto alternativo en el mensaje del contestador
- ten mucho cuidado sobre a quién das tu número de teléfono y pide a las personas a las que se lo hayas dado que no se lo proporcionen a otras
- desactiva la función Bluetooth™ de tu teléfono si los mensajes no deseados los recibiste por Bluetooth™

Díales que si no saben de quién es un mensaje de texto, no lo contesten (podría haber sido enviado a un número equivocado o a un número marcado al azar), y que si reciben un mensaje molesto, deberían:

- enseñárselo a un miembro de la familia o a un profesor en el que confíen
- guardar el mensaje como prueba
- anotar el número del remitente o los datos de origen que aparecen al final del mensaje

Por último, explique a sus hijos/as que puede hacerse un rastreo de todos los mensajes de texto y de las llamadas, y que las actitudes intimidantes de este tipo nunca son aceptables y pueden causar un verdadero sufrimiento.

## más información

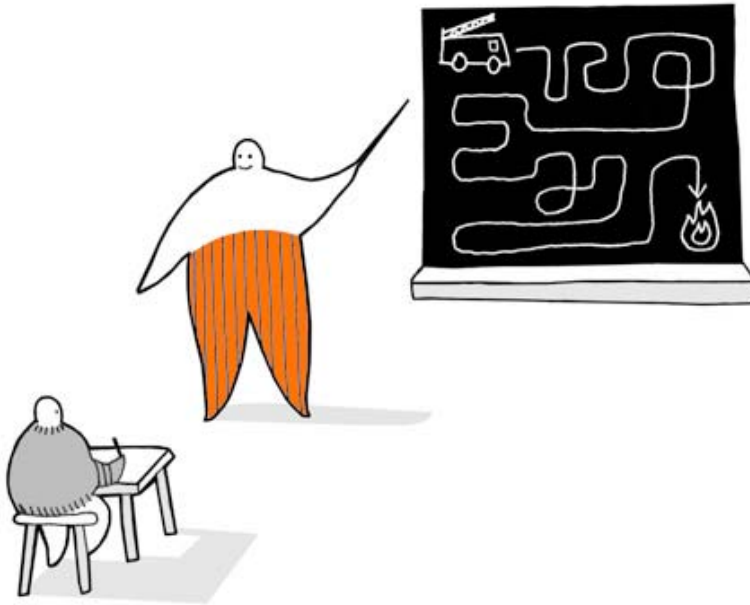
Los siguientes sitios web contienen información sobre el tema del acoso en general:

- <http://www.protegeles.com/acosoescolar.asp>
- <http://www.acosoescolar.info/index.htm>
- <http://www.cyberbully.org/docs/cbcteducator.pdf>

## uso inapropiado de los teléfonos móviles – llamadas de emergencia falsas

Una de las formas de uso inapropiado de los teléfonos móviles más extendida y peligrosa es la realización de llamadas de emergencia falsas.

Las falsas alarmas no sólo hacen perder el tiempo a los servicios de emergencia, sino que si una unidad se desplaza debido a una falsa alarma, no podrá atender una emergencia real. En otras palabras, no se trata de una simple broma, sino que estas llamadas pueden poner realmente en peligro la vida de otras personas.



### recomendaciones

- cuando se le da un móvil a un niño asegúrese de que antes de que empiece a utilizarlo entienda que hacer bromas con él es peligroso e irresponsable
- dígame que este comportamiento tiene consecuencias tanto para él/ella como para las personas que podrían estar en peligro. Hacer una falsa llamada al 112 puede llegar a considerarse una infracción y la persona que la realiza puede ser sancionada
- también hay que tener cuidado cuando los teléfonos están en el bolso o en el bolsillo, ya que están diseñados para poder llamar al 112 incluso si el teclado está bloqueado
- pueden identificarse todas las llamadas realizadas al 112

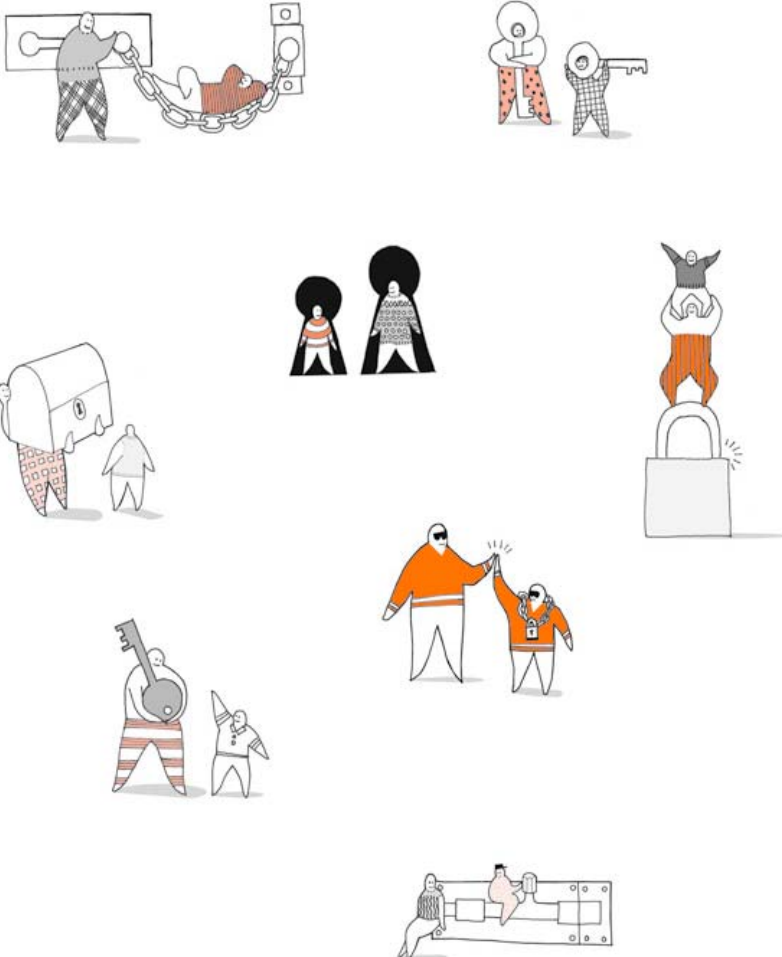
## robo y pérdida de teléfonos

A medida que el número de personas que adquieren móviles ha aumentado, los teléfonos se han ido convirtiendo en “accesorios de moda”, especialmente entre los jóvenes. Si a esto se añade que su valor es relativamente elevado, que son pequeños y que es fácil revenderlos, no es de extrañar que los ladrones estén cada vez más interesados en ellos.

Es una buena idea hacer los trámites necesarios para que no se pueda volver a utilizar el teléfono en caso de robo.

En caso de robo o pérdida del móvil, es importante llamar al Servicio de atención al cliente de Orange al 1414 lo antes posible. Orange bloqueará la tarjeta SIM e inmovilizará el terminal asociado al número IMEI siempre y cuando se presente la conveniente denuncia, en la que el afectado deberá facilitar su número IMEI.

Existe un procedimiento acordado entre los operadores móviles españoles y el Ministerio de Industria, Turismo y Comercio para que los IMEIs correspondientes a terminales robados se introduzcan en una base de datos nacional y se impida el uso de estos terminales en cualquier red española.



### ¿qué es un número IMEI?

Es un número de identificación único para cada teléfono y puede averiguarse marcando \*#06# en el teclado. También aparece en la caja del teléfono móvil.

Cuando se avisa del robo de un móvil, saber este número ayudará a garantizar que los operadores podrán desactivar el teléfono de todas las redes. La policía también podrá utilizarlo para probar que un teléfono ha sido robado.

### recomendaciones

Para los niños y los adolescentes, el mayor riesgo de robo viene de otros jóvenes. La mejor manera de reducir el riesgo es:

- evitar mostrar el nuevo teléfono, excepto a las personas allegadas o a amigos de confianza
- evitar llamar en lugares públicos y muy visibles: es mejor hacer la llamada de manera discreta. Un alto porcentaje de robos de móviles se produce cuando la víctima está hablando
- anota en varios sitios seguros los datos de su móvil (código PIN de acceso a la SIM, número IMEI, marca y modelo del terminal...)

# delitos a través del correo electrónico

## phishing

Phishing es un término utilizado en informática con el cual se denomina el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria.

El estafador, mejor conocido como phisher se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Dado el creciente número de denuncias de incidentes relacionados con el phishing se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica, campañas para prevenir a los usuarios y con la aplicación de medidas técnicas a los programas.

La mayoría de los métodos de phishing utilizan alguna forma técnica de engaño en el diseño para mostrar que un enlace en un correo electrónico parezca una copia de la organización por la cual se hace pasar.

URLs mal escritas o el uso de subdominios son trucos comúnmente usados por phishers, como el ejemplo en esta URL, <http://www.nombredetubanco.com.eje.mplo.com/>. Otro ejemplo para disfrazar enlaces es el de utilizar direcciones que contengan el carácter arroba: @, para posteriormente preguntar el nombre de usuario y contraseña.

Por ejemplo, el enlace <http://www.google.com@members.tripod.com/> puede engañar a un observador casual a creer que el enlace va a abrir en la página de [www.google.com](http://www.google.com), cuando realmente el enlace envía al navegador a la página de [members.tripod.com](http://members.tripod.com) (y al intentar entrar con el nombre de usuario de [www.google.com](http://www.google.com), si no existe tal usuario, la página abrirá normalmente).

Varios programas de software anti-phishing están disponibles. La mayoría de estos programas trabajan identificando contenidos phishing en sitios web y correos electrónicos.

El software anti-phishing puede integrarse con los navegadores web y clientes de correo electrónico como una barra de herramientas que muestra el dominio real del sitio visitado. Los filtros de spam también ayudan a proteger a los usuarios de los phishers, ya que reducen el número de correos electrónicos relacionados con el phishing que un usuario puede recibir.

Muchas organizaciones han introducido la característica denominada preguntas de desafío, en la que se pregunta información que sólo debe ser conocida por el usuario y la organización. Las páginas de internet también han añadido herramientas de verificación que permite a los usuarios ver imágenes secretas que los usuarios seleccionan por adelantado; si estas imágenes no aparecen, entonces el sitio no es legítimo.

Muchas compañías ofrecen a bancos y otras entidades que sufren de ataques de phishing, monitorización continua, analizando y utilizando medios legales para cerrar páginas con contenido phishing.

El Anti-Phishing Working Group, industria y asociación que aplica la ley contra las prácticas de phishing, ha sugerido que las técnicas convencionales de phishing podrían ser obsoletas en un futuro a medida que la gente se oriente sobre los métodos de ingeniería social utilizadas por los phishers.

## spoofing

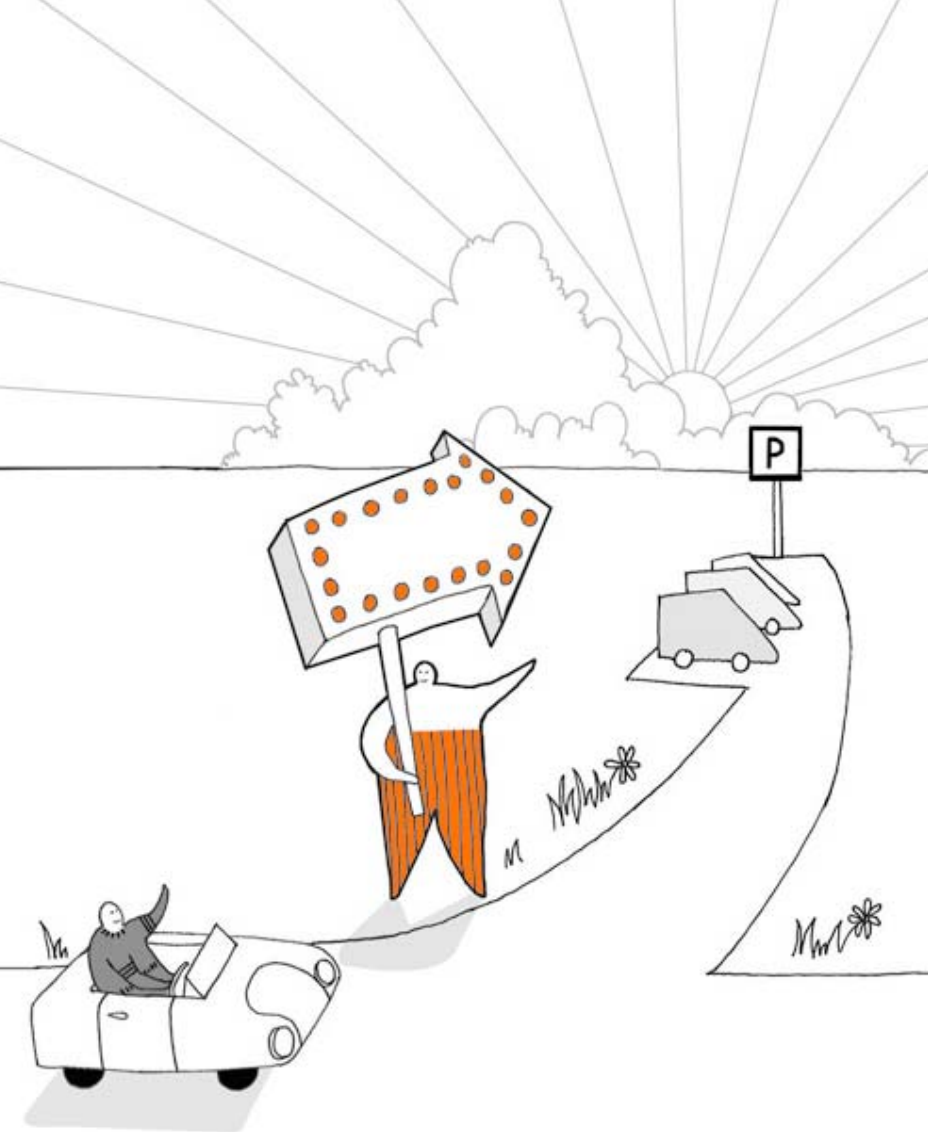
Spoofing, en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Existen diferentes tipos de spoofing dependiendo de la tecnología a la que nos refiramos, como el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

## pharming

Pharming es la explotación de una vulnerabilidad en el software de los equipos de los usuarios, que permite a un atacante redireccionar un nombre de dominio (domain name) a otra máquina distinta.

De esta forma un usuario que introduzca un determinado nombre de dominio, que haya sido redireccionado, en su explorador de internet, accederá a la página web que el atacante haya especificado para ese nombre de dominio.



## jóvenes, teléfonos móviles, tráfico y conducción

### conducción

La Dirección General de Tráfico prohíbe utilizar los teléfonos móviles o cualquier otro medio de sistema de comunicación mientras se conduce, salvo que el desarrollo de la comunicación tenga lugar sin emplear las manos, cascos, auriculares o instrumentos similares.

Si no dispone de un kit de manos libres, es mejor apartarse a un lado, parar en un lugar seguro y apagar el motor antes de hacer o recibir una llamada. Aunque este consejo va dirigido a todos los conductores, está especialmente dirigido a los conductores noveles. Además, aunque se disponga de un kit de manos libres, sigue siendo más seguro salir fuera de la calzada antes de hacer o recibir una llamada. Escribir o leer mensajes de texto mientras se conduce, además de estar prohibido, es extremadamente peligroso.

### reproductores de música

Los teléfonos móviles pueden causar distracción y por ello se debe evitar mandar o recibir textos, llamar o utilizar el móvil de cualquier otra manera al cruzar una calle o sortear el tráfico.

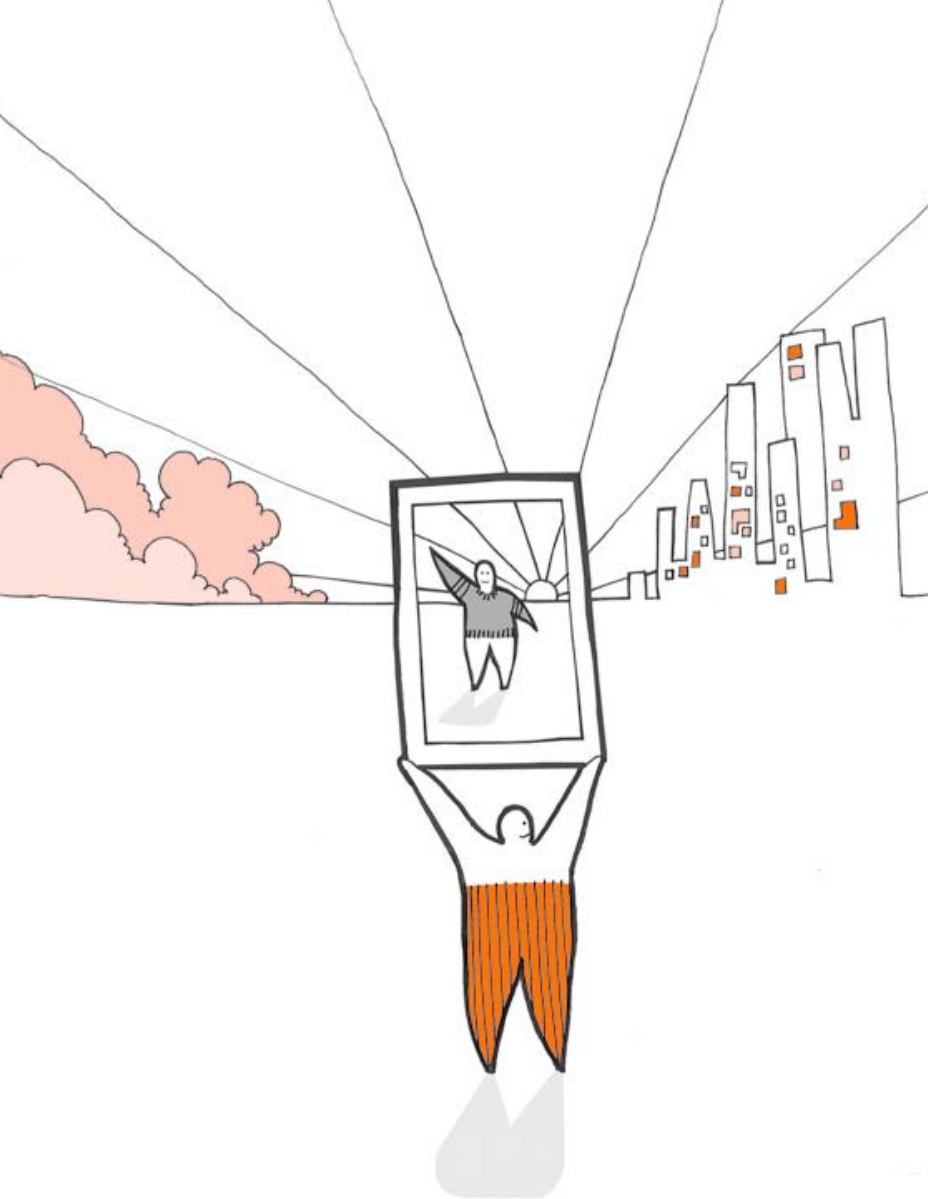
Esto es especialmente importante ahora que muchos móviles disponen de reproductores de música incorporados, que tienen un gran poder de atracción para los niños y los adolescentes. Es importante que se les recuerde que deben tener mucho cuidado a la hora de cruzar una calle o de utilizar bicicletas o motos mientras escuchan música. En estas situaciones, el hecho de no oír el tráfico los hace mucho más vulnerables a cualquier accidente.



### recomendaciones

Los siguientes consejos van dirigidos a todos los adultos, pero especialmente a los conductores noveles:

- no utilizar nunca un móvil cuando se conduce, si no se dispone de un kit de manos libres
- incluso si se usa un dispositivo de manos libres, es más seguro decir a la persona que llama que estamos conduciendo y que la llamaremos más tarde (cuando hayamos llegado al destino o hayamos salido de la carretera, el coche esté parado y el motor apagado)
- no vaya en bicicleta ni en moto mientras escucha música a un volumen tan alto que le impida oír el tráfico
- no cruce la calle mientras escucha música o utiliza otras funciones de su teléfono móvil



## mensajes de vídeo/fotografías

Una de las funciones más populares entre los usuarios de móviles e Internet, sobre todo entre los niños, es la de hacer, guardar y mandar fotografías realizadas con la cámara de los teléfonos.

Sin embargo, el uso correcto de estas cámaras y los contenidos de las mismas requieren una mezcla de cuidado y sentido común.

### recomendaciones

Ante el uso que sus hijos/as puedan realizar de las cámaras de los teléfonos, es bueno darles los siguientes consejos:

- no mandes nunca fotografías que podrían avergonzar o comprometer a otras personas: esto es especialmente importante en relación con las fotografías hechas a otros niños. Lo mejor es tratar a los demás como te gustaría que te trataran a ti
- enviar tu foto a los chats no es una buena idea y puede ser peligroso
- enviar imágenes desagradables o indecentes a otras personas podría constituir un delito en ciertas situaciones
- todo el mundo debe respetar las restricciones de uso de las cámaras de los móviles en ciertos lugares como las piscinas, las escuelas o algunos gimnasios
- mantente alerta con las personas, sobre todo los adultos desconocidos, que te hacen fotos a ti o a tus amigos
- si te envían una imagen de una agresión a otra persona, guarda la imagen y enséñasela enseguida a tu padre o tu madre, a un profesor o a un adulto en el que confíes

## teléfonos móviles y salud

En los últimos cincuenta años la sociedad ha dado un fuerte impulso tecnológico y poco a poco nos hemos acostumbrado a la electricidad, a la radio, a la televisión, a los microondas, mandos a distancia y, en definitiva, a toda una serie de dispositivos basados en los campos electromagnéticos, que en estos momentos, forman parte esencial de nuestra vida.

Uno de los últimos dispositivos de este tipo en aparecer en nuestras vidas y convertirse rápidamente en imprescindible son los teléfonos móviles. Esta evolución tan rápida en el uso de los móviles en tan pocos años ha despertado en la sociedad cierta inquietud sobre sus posibles efectos en la salud.

### ¿qué efectos tienen los teléfonos móviles en la salud?

La Organización Mundial de la Salud al igual que muchos Ministerios de Sanidad de distintos países, el español entre ellos, han estudiado y analizado toda la información existente y sus conclusiones son similares "todas las revisiones de expertos sobre los efectos que tiene sobre la salud la exposición a campos de radiofrecuencia han llegado a la misma conclusión: No se han establecido consecuencias nocivas para la salud debido a la exposición a campos de radiofrecuencia a niveles inferiores a las directrices internacionales sobre límites de exposición" (Organización Mundial de la Salud, julio de 2005)  
[http://www.who.int/peh-emf/meetings/ottawa\\_june05/en/index4.html](http://www.who.int/peh-emf/meetings/ottawa_june05/en/index4.html)

Los límites incorporan factores de seguridad amplios para proteger a los trabajadores e incluso más amplios para proteger al público general. Son límites de seguridad protectores y se basan en todas las pruebas científicas disponibles.

### ¿cuáles son las directrices sobre límites de exposición?

En España los límites y restricciones de exposición, siguiendo los criterios internacionales y europeos, vienen establecidos en el Real Decreto 1066/2001, de 28 de septiembre, por el que se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitarias frente a emisiones radioeléctricas.

Todos los teléfonos vendidos por Orange cumplen con los límites de exposición de esta normativa.

### ¿qué teléfono móvil tiene los límites de emisión más bajos?

Los niveles de magnitud de emisión de los teléfonos móviles vienen determinadas por el Índice de Absorción Específica (SAR –siglas en inglés). El límite en España es de 2 vatios/kilogramo (W/kg) de media sobre diez gramos de tejido corporal (cabeza y tronco).

La mayor parte de los fabricantes indican estos niveles en la documentación del teléfono móvil o en sus páginas web.

Podrá encontrar información sobre el SAR de cada teléfono en la página web del foro de fabricantes de móviles:  
<http://www.mmfa.org/public/index.cfm?lang=es>

Cuanto menor es el índice SAR menor es la energía emitida por el teléfono móvil.

## recomendaciones

- díga a sus hijos/as que reduzcan la duración de las llamadas
- aníme a sus hijos a enviar mensajes de texto en lugar de realizar llamadas

Encontrará mucha información sobre los teléfonos móviles y la salud en la página web de Orange.

[http://acercadeorange.orange.es/responsabilidad\\_corporativa](http://acercadeorange.orange.es/responsabilidad_corporativa)

Ministerio de Sanidad y Consumo:

<http://www.msc.es/ciudadanos/salud/AmbLaboral/medioAmbiente/home.htm>

Ministerio de Industria, Turismo y Comercio:

<http://www.mityc.es/nivelesexposicion>

Colegio Oficial de Ingenieros de Telecomunicaciones:

<http://www.coit.es/web/servicios/tecnologia/emision/index.html>

La Comisión Internacional sobre protección contra la radiación no ionizante (ICNIRP)

<http://www.icnirp.de/index.html>

EU EMF net

<http://www.jrc.cec.eu.int/emf-net/>

La Organización Mundial de la Salud:

[http://www.who.int/topics/radiation\\_non\\_ionizing/es/](http://www.who.int/topics/radiation_non_ionizing/es/)

## televisión

Orange TV tiene dos cuentas de usuario claramente diferenciadas: la cuenta familiar y la cuenta parental.

El objetivo de la distinción entre estas dos cuentas es otorgar al usuario un mayor control y seguridad sobre las acciones que puede realizar disponiendo de un acceso seguro al acceso de contenidos adulto.

El usuario sabrá en todo momento cuando está en la cuenta parental de una forma muy sencilla ya que aparecerá el logo en la parte superior derecha de su pantalla.



Además existen dos códigos de seguridad para acceder a los contenidos adulto: PIN y Código Adulto.

A continuación se detalla brevemente qué es y para qué sirven las diferentes cuentas y códigos del servicio Orange TV.

Al acceder por primera vez al servicio, el usuario deberá configurar el código adulto. Este código se le solicitará cada vez que desee acceder a un contenido restringido a adultos, de esta forma podrá controlar el acceso a ese tipo de contenidos de sus hijos y familiares.

En el apartado "control parental" tendrá la opción de restringir entre varias categorías en las que están clasificados todos los contenidos que se emiten: películas, series, vídeos, etc.

Los niveles de restricción disponibles actualmente son los siguientes: todos los públicos, menores de 7 años, menores de 13 años y menores de 18 años.

Una vez definido este control, sólo los contenidos autorizados estarán accesibles (tráiler, emisión, película, etc) en el catálogo de Videoclub. Para acceder a los servicios no autorizados deberá introducir el PIN y si además se trata de un contenido adulto también se le solicitará el Código Adulto.

	qué es	para qué sirve
cuenta familiar	Cuenta a la que tiene acceso toda la familia que permite acceder a todos servicios y funcionalidades generales	<ul style="list-style-type: none"><li>■ acceder a los canales de tv</li><li>■ comprar un vídeo</li><li>■ ver un vídeo</li><li>■ ver la lista de compras, etc...</li></ul>
cuenta parental	Cuenta de acceso restringido mediante el PIN que permite la configuración del servicio y la gestión del saldo	<ul style="list-style-type: none"><li>■ recargar la cuenta</li><li>■ distribuir el saldo</li><li>■ modificar el código adulto</li><li>■ definir el control parental</li></ul>
* PIN	Código de 4 dígitos definido por Orange y no modificable por el usuario	<ul style="list-style-type: none"><li>■ acceder a la cuenta parental</li></ul>
código adulto**	Código de 4 dígitos que por defecto está definido como 0000, y puede ser modificable por el usuario	<ul style="list-style-type: none"><li>■ acceder a contenidos adulto</li><li>■ acceder a contenidos restringidos por el control parental</li></ul>

### recomendaciones

A continuación aparecen algunas precauciones sencillas que pueden ayudarles a reducir significativamente el riesgo de que los niños accedan a contenidos inadecuados a su edad

- evitar marcar el PIN y el Código adulto en presencia del niño
- si escribe los códigos, evitar dejarlos al alcance del niño
- no dejar que el niño alquile o acceda a ningún contenido en ausencia de su progenitor
- asegúrese de que el contenido que el niño está visionando es el adecuado a su edad
- explique los riesgos de ver emisiones no adecuadas a su edad

## glosario

Hay muchas expresiones relacionadas con las nuevas tecnologías y a medida que éstas avanzan surgen muchas más. A continuación encontrará una lista de las expresiones más comunes:

### **blog**

Weblog – diario en línea o artículos personales.

### **Bluetooth**

Es un sistema de comunicación inalámbrica entre dispositivos. Muchos teléfonos móviles y accesorios manos libres disponen de Bluetooth, lo que les permite comunicarse entre ellos cuando no están excesivamente alejados.

### **flaming**

El término en inglés que se utiliza cuando se es maleducado o “incendiario” en una conversación en la Web.

### **fondo de pantalla**

Es la imagen que aparece detrás de las diversas listas de opciones de un teléfono. Algunos vienen incluidos en el teléfono y son gratuitos, pero la mayoría tienen un coste por descarga.

### **infrarrojo**

Es otra forma de transmitir de forma inalámbrica datos a corta distancia entre dispositivos móviles. Es una alternativa al Bluetooth, pero con el inconveniente de que los dispositivos tienen que estar a muy poca distancia y enfrentados entre sí.

### **MMS**

Son las siglas en inglés de Multimedia Messaging Service (Servicio de Mensajería Multimedia). Permite enviar y recibir fotografías, vídeos y archivos de audio a través del teléfono móvil.

### **salvapantallas**

Es una imagen animada que aparece cuando el móvil está encendido, pero no se está utilizando. Algunos vienen incluidos en el teléfono y son gratuitos, pero la mayoría tienen un coste por descarga.

### **SMS**

Son las siglas en inglés de Short Message System (Servicio de Mensajes Cortos), es decir, los mensajes de texto.

### **tarjeta SIM**

Son las siglas en inglés de Subscriber Identity Module (módulo de identidad del abonado). Es el chip extraíble que se encuentra dentro del teléfono móvil y que contiene información como el número de teléfono del usuario, la agenda y otros datos relativos al abonado.

### **thread**

Conversación online en un chat.

### **tonos de llamada**

El anticuado tono de llamada de los teléfonos ha sido sustituido en los móviles por toda una gama de sonidos que incluyen hasta canciones reales. Algunos vienen incluidos en los teléfonos y son gratuitos, pero la mayoría tienen un coste por descarga.

### **WAP**

Son las siglas en inglés de Wireless Application Protocol (Protocolo de Aplicación Inalámbrica). Permite a los usuarios acceder a sencillas páginas de información basadas en texto e imágenes y a otros servicios de Internet.

### **3G**

Es la abreviación de “tercera generación” y es el equivalente móvil de la “banda ancha”. Es un estándar técnico común en el sector de la telefonía móvil que permite la transferencia de datos a gran velocidad. Esta alta velocidad de transmisión de datos permite beneficiarse de nuevos servicios como el vídeo, el acceso a Internet y los servicios interactivos.

