GUÍA
para
PADRES Y
PROFESORES

Guíales en internet

Ayúdales a construir su futuro

Los más pequeños manejan pantallas táctiles de forma natural y han crecido conociendo como parte de su entorno los dispositivos electrónicos e internet. Resulta casi imposible separar la convivencia del menor de la conexión con la Red. Su vida social ha pasado a tener un componente online en el que de forma casi instintiva sus datos personales son compartidos en red y la conciencia sobre la importancia de sus datos personales en ocasiones se acaba adquiriendo como resultado de una mala experiencia propia o de las personas próximas al menor. El niñ@ no es consciente de los riesgos a los que su actitud puede exponerle.

Esta guía sirve como complemento a la guía para jóvenes de la Agencia Española de Protección de Datos y pretende ofrecer a padres y educadores un texto orientador acerca de algunas consideraciones que pueden ser de utilidad en el buen uso de los datos personales, favoreciendo una convivencia saludable del menor con las nuevas tecnologías.

En la Agencia Española de Protección de Datos hemos diseñado una serie de elementos didácticos destinados a los menores pero, además, queremos facilitar una serie de reflexiones y recomendaciones que ayuden a los padres y profesores a comprender mejor estos riesgos y, así favorecer la tarea educacional en hábitos responsables para el adecuado uso de sus datos personales y los de terceros a través de cualquiera de los elementos electrónicos que tienen a su alcance.

Los datos personales del menor

FICHA 1

Ha llegado el momento de la adquisición de su primer móvil. Posiblemente sea una oportunidad para decidir juntos aquel que mejor se adecúa a su edad y al uso que se le pretende dar. El teléfono ofrece a los padres la gran ventaja de estar en contacto con el menor, pero también es la puerta de entrada de algunos riesgos para la seguridad y la privacidad de los datos personales del niñ@ e incluso de su propia integridad física y psicológica.

Es posible que ya manejara una tablet en casa, también es posible que jugara con el ordenador en tu presencia o incluso que navegara, pero el teléfono abre una nueva etapa en la convivencia del niñ@ con la Red. Es un dispositivo que siempre le acompañará, que almacenará sus datos e información personal a la que podrán acceder terceros y que irá acumulando datos de otras personas como amigos, profesores, familiares, etc. A esta situación hay que añadir que no siempre podrá contar con la supervisión de un adulto.

Hasta ahora los datos de navegación del niñ@ estaban asociados a la identidad de un adulto, ahora será el propio menor quien utilizará su dirección de correo electrónico y número de teléfono para identificarse en su terminal y acceder a determinados servicios[1]. Esta información puede identificarle y estar a disposición de terceros para diferentes fines, que pueden incluir, por ejemplo, el envío de publicidad personalizada. Por ello, tal vez, interese añadir la información del niñ@ en un fichero de exclusión[2] para el envío de comunicaciones comerciales, evitaremos en gran medida que personas desconocidas puedan dirigirse al menor para ofrecerle productos u ofertas a través de llamadas telefónicas o mensajes de cualquier tipo.

Cuando hablamos de los datos personales del niñ@ hay que tener en cuenta que no se trata únicamente de su nombre, apellidos, correo electrónico, número de teléfono, etc. Además, entre sus datos personales se encuentran también los que son recogidos por las cookies[3] de los sitios web por los que navega, la información de las búsquedas, el historial de navegación que genera, sus perfiles en las redes sociales, sus datos de ubicación, etc. En definitiva es el momento en el que su identidad digital empieza a perfilarse a la vez que desarrolla su personalidad.

Un dato personal es cualquier información que haga posible la identificación de una persona. A menudo internet proporciona una falsa sensación de anonimato y nula sensación de riesgo.

Por ejemplo, el envío de una parte desnuda de su cuerpo a un tercero les puede hacer pensar en la imposibilidad de que alguien descubra

1 La instalación de aplicaciones y el uso de servicios exige la existencia de una dirección de correo electrónico.

2 Los ficheros de exclusión para el envío de comunicaciones comerciales son listas de usuarios que han manifestado su derecho de oposición al envío de comunicaciones comerciales. La inclusión del usuario en estas listas es gratuita, como las Listas Robinson de Exclusión Publicitaria.

3 Cookies: o «galletas» son ficheros que utilizan los sitios web en los que se almacena información de la sesión (usuario y contraseña) que se utiliza para acceder a un portal (correo electrónico, red social, etc.), también son ficheros que utilizan los sitios web por los que navegamos con el fin de almacenar información acerca de nuestras preferencias de navegación para adecuar la publicidad de estos sitios webs a nuestros hábitos de navegación.

IDENTIDAD DIGITAL

su identidad. Sin embargo, en ocasiones, es tan fácil de descubrir su identidad como abrir en un ordenador las propiedades de la imagen y leer los metadatos[4]. También puede ocurrir que una marca en la piel (la forma del bronceado, un lunar, una cicatriz, etc.) que inicialmente no era perceptible aparece al ampliar la imagen y haga posible su identificación, o puede ocurrir que posteriormente, incluso años después, un determinado comentario del menor en una red social permita su identificación.

Es fundamental hablar con nuestros hijos o alumnos para concienciarles de la importancia de sus datos personales y de los del resto de personas con las que intercambian información. Una adecuada convivencia digital redundará en lo que podríamos denominar «salud digital», evitando problemas que puedan repercutir en su normal desarrollo.

«El paso por internet deja un rastro fácil de seguir»

4 Metadatos: muchos archivos digitales contienen información adicional a su contenido. Información relativa al terminal telefónico o cámara fotográfica utilizada, identidad de la persona que ha creado el archivo, fecha de captura, ubicación, etc.

Privacidad y seguridad: trucos para las trampas de internet

FICHA 2

Cada vez son más frecuentes los intentos de engañar a los usuarios de internet mediante la utilización de webs que suplantan la identidad de sitios conocidos como bancos, redes sociales, webs de comercio electrónico, etc.

El engaño a veces se basa en la similitud tipográfica del nombre del sitio real al que se suplanta. En la guía para jóvenes se ha utilizado el ejemplo «www.mogollondejuegos.com» como supuesto nombre real de un sitio web frente al de nombre«www.mogolondejuegos.com», un supuesto sitio web que intenta engañar al menor, un pequeño error al teclear la dirección le llevaría a un sitio web con una posible identidad falsa.

Es necesario hacer entender al niñ@ la necesidad de verificar la dirección de internet en el navegador, especialmente cuando se va a introducir su nombre de usuario y contraseña o cuando intenta registrarse en una web con sus datos personales.

Otra vía frecuente para este engaño son los correos electrónicos o la mensajería instantánea[5]. Es frecuente la realización de campañas de «phishing»[6] en las que se remiten masivas oleadas de mensajes electrónicos que le invitan a enviar, actualizar o revisar sus códigos de usuario, contraseña o sus datos personales, y que contienen enlaces a sitios web fraudulentos o ficheros que al abrir dañan el dispositivo o el ordenador.

Conviene que el niñ@ entienda esta situación para no poner en riesgo sus datos personales. En algunos casos los mensajes contienen un archivo adjunto que al abrirlo ocasiona el bloqueo del ordenador o del dispositivo. En la Guía para Jóvenes nos referimos a esta situación como el robo o el secuestro de las carpetas porque la información que contenga el dispositivo o el ordenador dejará de ser accesible. Además, el pago de la cantidad reclamada por el delincuente no garantiza el desbloqueo del ordenador o dispositivo.

Determinadas descargas de programas o apps pueden poner en riesgo los datos personales del menor, por lo que es preciso concienciarle para evitar la instalación de programas o apps de origen desconocido. Suele ser habitual la descarga de contenido multimedia o programas informáticos que por su nombre crean en el niñ@ la expectativa de disponer de determinados contenidos que en última instancia pueden resultar inapropiados.

Es indispensable disponer de un antivirus tanto en el ordenador como en el resto de dispositivos, ya que el antivirus realiza un análisis de los programas, apps y archivos que se cargan en el ordenador y en los dispositivos del menor. Sin olvidar que los antivirus no realizan un análisis del contenido temático, por ejemplo, de las webs que visita el menor por lo que no ofrecen

5 Mensajería instantánea: cualquier herramienta, app, o aplicación informática que permite el envío de mensajes en tiempo real como por ejemplo: WhatssApp, Hangouts, Line, etc. En este apartado se incluyen los medios de mensajería de las redes sociales que permiten el «chat» o diálogo en tiempo real entre varios usuarios.

6 Phishing: envío de mensajes electrónicos con enlaces que conducen a sitios web que suplantan la identidad digital de sitios webs habituales (bancos, redes sociales, correo electrónico, etc.) para el usuario con el fin de robar claves de acceso a cuentas bancarias, datos personales o bloquear el ordenador o dispositivo electrónico reclamando dinero a cambio de una contraseña para el desbloqueo del mismo. Algunas de estas campañas utilizan direcciones de correo electrónico aparentemente reales como por ejemplo «**envios@correos.es**» o «**policia@policia.es**».

«¿www.mogollondejuegos.com o www.mogolondejuegos.com? Enséñales a verificar los direcciones de internet»

protección frente a contenidos inadecuados.

Si se desea controlar el acceso del menor a determinados contenidos es necesario disponer de un programa para el control parental que permita controles y opciones sobre el uso del dispositivo por parte del menor, como impedir el acceso a contenido inapropiado[7], limitar el tiempo de uso del terminal o de los juegos, evitar el uso de determinado vocabulario, restringir los resultados de las búsquedas en internet o conocer los sitios que ha visitado, limitar el acceso de aplicaciones a los datos personales del menor, conocer la ubicación del niñ@, etc. En cualquier caso, si se decide usar este tipo de herramientas, habría que considerar la posibilidad de llegar a acuerdos con el menor de forma que sea consciente de que se ha instalado una herramienta de este tipo y los motivos por los que es necesaria.

La Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad pone a su disposición abundante información y herramientas gratuitas que podrían ser útiles para garantizar la seguridad de los dispositivos electrónicos en general.

En la Guía para Jóvenes se recomienda no utilizar ninguna wifi sin clave: un canal wifi que no disponga de clave envía nuestros datos (incluyendo nombre de usuario y contraseña) sin ningún cifrado ni protección y los hace accesibles a cualquier persona con ciertos conocimientos informáticos.

Con relación a las «galletas» o «cookies», que se mencionan en la Guía para Jóvenes, es ya habitual que al entrar en una web se nos informe acerca del uso de cookies que guardan nuestra información personal. Sería interesante ayudar al menor a entender que la finalidad de esta información es la publicidad y explicarle la forma de eliminar las las cookies[8].

7 Contenido pornográfico, webs de compras, suicidio, anorexia, etc. conocido también como «internet tóxico».

8 En el navegador del ordenador (Google Chrome, Internet Explorer, Mozilla) el menú para eliminar los datos de navegación se obtiene a través de los menús del propio navegador o con la combinación del teclado «Mayús + Ctrl + Supr». En smartphones y tabletas se accede a través de las opciones de configuración de privacidad.

Protección de datos personales. (Seguridad, derechos.

FICHA 3

En este apartado de la Guía para Jóvenes se facilitan al menor unas nociones sobre sus derechos[9], que siempre podrá ejercer cuando se registra en un sitio web, junto a algunas recomendaciones que debe tener en cuenta.

El menor de catorce años debe de contar con el consentimiento de sus padres o tutores legales para registrarse y, a su vez, la información que se le puede pedir debe ser proporcional a la finalidad o uso que se pretende. Para el caso de un registro web no sería proporcional que le pidan al menor datos de su entorno familiar salvo que se solicite con el fin de otorgar el consentimiento[10] de padres o tutores.

Es muy probable que al menor le cueste decidir su nombre de usuario: puede que le guste un nombre que permita a sus amigos reconocerle fácil y rápidamente. Como es probable que ese nombre ya haya sido utilizado, la solución suele ser que el menor añada a continuación su edad o su fecha de nacimiento para poder utilizar el nombre que haya elegido. El nombre de usuario es un identificador personal que no debe de facilitar a extraños información acerca de la fecha de nacimiento o de la edad del usuario. Se evitará encarecidamente que se pueda obtener información partiendo de su nombre de usuario, ya que esta información del niñ@ puede funcionar como reclamo para actividades como el acoso o la pederastia.

Otra de las recomendaciones que se hacen al menor trata de la elección de sus claves, que siempre deberían ser de más de ocho caracteres incluyendo mayúsculas minúsculas y caracteres especiales. Se puede recomendar al niñ@ que utilice recursos nemotécnicos para recordar la contraseña usando, por ejemplo, parte de una canción que le guste o de un texto que recuerde y que sobre el mismo haga variaciones de carácter tipográfico.

Se recomienda también al menor no elegir palabras que ya existan en un diccionario, pues suele ocurrir que los delincuentes utilizan bases de datos de diccionarios para acceder a cuentas de otros usuarios y obtener sus datos personales o la cuenta o la identidad digital del niñ@.

En ningún caso se deben utilizar contraseñas del entorno del menor, por ejemplo, el nombre de la mascota, la marca o modelo del vehículo de la madre o del padre, el barrio donde se vive, el equipo de fútbol en el que juega el niñ@, etc.

También es importante que el menor conozca que siempre debe utilizar el botón de «cerrar sesión» o «salir». Cerrar el navegador no siempre equivale a cerrar sesión, y puede permitir que otro usuario abra el navegador y tenga acceso a su información personal o utilice la identidad digital del menor.

Antes de proceder al registro de los datos personales del menor se recomienda leer la política de privacidad[11] de la página web. En la política de privacidad nos deben informar sobre la fina-

9 Derechos ARCO: derecho de acceso: a solicitar y obtener información de nuestros datos de carácter personal sometidos a tratamiento, derecho a rectificarlos, derecho a cancelarlos y derecho a oponernos a su tratamiento.

10 En cualquier caso la información ofrecida al menor deberá expresarse en un lenguaje que le sea fácilmente comprensible.

11 La política de privacidad describe como se recoge, guarda y utiliza la información que facilitamos a través de los diferentes servicios, redes sociales o páginas webs que visitamos. Es importante que el niño entienda qué información se recoge y cómo se utiliza ya que el acceso a este sitio implica la aceptación de esas condiciones.

política de privacidad): trucos para apuntarme y borrarme en un sitio web

lidad de los datos que aportamos, la identidad del responsable de tratar los datos y la forma de ejercer los derechos de acceso, rectificación, cancelación y oposición (ARCO).

Para el ejercicio de los derechos del menor de 14 años en relación con sus datos personales, los padres o tutores legales deberán solicitarlo ante el responsable del fichero o del tratamiento de datos personales, acreditando su condición de madre, padre o tutor legal.

La información para ejercer estos derechos debe aparecer dentro de la política de privacidad de cualquier sitio web que utilice datos personales de sus usuarios. Si no fuera así, siempre se puede consultar el Registro General de Protección de Datos en la web de la Agencia Española de Protección de Datos donde se encuentra a disposición de los interesados la información relativa a los titulares de ficheros de datos personales ante quienes ejercer los derechos de acceso, rectificación, cancelación y oposición. Finalmente, si los derechos del menor no fueran atendidos, los padres o tutores legales pueden solicitar la Tutela del Derecho ante la Agencia Española de Protección de Datos, que instará al responsable del fichero para que atienda los derechos del menor.

También es posible que el niñ@ ejerza sus derechos frente a los buscadores de internet, solicitando la cancelación de los resultados de búsqueda en los que aparezca. Es lo que se denomina «derecho al olvido», derecho que puede ser ejercido por cualquier persona afectada y, en el caso de menores de 14 años, siempre a través de sus padres o tutores legales.

Acoso y convivencia en la red: trucos para evitar malos rollos

FICHA 4

En este apartado intentamos dar al joven la noción de respeto y convivencia en la Red. La convivencia digital no se distingue de la convivencia de la vida real y el niñ@ debe ser consciente de que sus palabras o sus hechos pueden ofender o dañar a otras personas y que en ningún caso en la Red se debe de hacer algo que no se haría en la vida real. Detalles como evitar escribir mensajes en mayúsculas[12] o evitar palabras malsonantes, que no se utilizarían en presencia del interlocutor, pueden ayudar a mantener un clima de convivencia entre los menores.

También intentamos dar al menor la noción de acoso, que puede resultar un término abstracto que conviene concretarlo de alguna manera con algunos ejemplos específicos, como el hecho de recibir constantes llamadas o mensajes a cualquier hora. Si el niñ@ no es capaz de identificar una situación de acoso podría verse involucrado en ella por el simple desconocimiento y verse envuelto en un posible delito.

Otra medida preventiva es la concienciación del menor para que ignore mensajes de personas desconocidas, mensajes de correo electrónico, mensajería instantánea, redes sociales, buzón de voz o de cualquier otra índole. El menor nunca debe enviar fotografías a un desconocido porque podría dar información de su edad, vivienda, entorno social o sobre su ubicación.

Finalmente, además de ayudar al menor a identificar una situación de acoso, se le recomienda que evite acosar a otras personas. El menor debe ser consciente del uso respetuoso de los datos personales de los demás y no utilizarlos para ofender o ridiculizar a otros.

12 En los mensajes electrónicos las mayúsculas pueden ser entendidas como gritos por la persona a la que se dirige el mensaje.

FICHA 5

Redes sociales: con los amigos en la red

El objetivo de este apartado es proporcionar algunas pautas encaminadas a facilitar la convivencia y el buen uso de los datos personales del joven y de los de sus amigos y conocidos.

En primer lugar es conveniente que el menor entienda que el término «amigos» en las redes sociales no es lo mismo que en la vida real, donde la amistad se forja compartiendo experiencias. En las redes sociales un simple clic se utiliza para designar a un«amigo». En algunas redes se utiliza el término «seguidor[13]» para designar a las personas con las que compartes contenidos en la red. La semántica utilizada en las redes sociales puede crear cierta confusión en el niñ@.

Una vez que el menor se registra en una red social, deberemos ayudarle a revisar su configuración de privacidad, evitando que sus publicaciones puedan ser visibles por todo el mundo o indexadas por los buscadores. Un detalle que se debe tener en cuenta es evitar en todo momento facilitar las opciones de ubicación que posibiliten a terceros identificar el lugar donde se encuentra el menor.

Es recomendable compartir con el niñ@ sus primeras publicaciones para que vea cómo ven los demás lo que publica. Mostrando al menor el resultado de sus publicaciones, etiquetados y comentarios puede entender que no gusten o molesten.

La información personal que el menor comparte con sus amigos podría, a su vez, ser vista por los amigos de sus amigos. El menor no debe compartir la información personal que sus amigos comparten con él, antes debería considerar si esto podría molestarles.

Si el menor utiliza blogs o foros es importante proteger su identidad con un alias o pseudónimo y evitar cualquier información que permita que sea identificado o que proporcione pistas acerca de su edad.

13 Redes Sociales como por ejemplo Twitter o Instagram utilizan el término «seguir», en otros casos, como por ejemplo Facebook, se utiliza el término «amigos» o «mejores amigos» y, en ocasiones, se utiliza la palabra «seguir» para designar a las personas de entre sus «amigos» cuyas publicaciones tiene interés en seguir.

FICHA 6

Mensajería instantánea: mensajes sin parar

Los mensajes que intercambiamos contienen información personal nuestra o de otras personas. En este apartado intentamos que el niñ@ sea consciente de esta situación proporcionándole algunas recomendaciones para evitar el mal uso de la mensajería o la información personal que se intercambia en los mensajes.

El smartphone o la tablet facilitan el envío o reenvío de cualquier información de forma intuitiva, lo que puede empujar al menor al reenvío de mensajes que podrían ofender a otras personas, como podría ser el caso de imágenes o vídeos que pudieran resultar ofensivos para otro menor o formar parte de una cadena de acoso.

En el correo electrónico es importante hacerle ver la conveniencia de utilizar la opción de envío con copia oculta, evitando que un mensaje que vaya dirigido a múltiples personas revele las direcciones de correo de todos los destinatarios: las direcciones de correo electrónico son un dato personal que puede aportar información de otra persona (trabajo, colegio, etc.) por lo que antes de enviar un correo electrónico a múltiples destinatarios el menor deberá ser capaz de entender esta situación.

En las redes sociales, debe distinguir entre publicar un mensaje que sea visible a todos sus amigos de la red social o utilizar la opción de mensaje privado que solamente sea visible para su destinatario. Habitualmente los comentarios en las redes sociales son públicos y si no se desea que sea visible públicamente es preciso recurrir a un mensaje privado[14].

Las aplicaciones de mensajería instantánea y mensajes multimedia (MMS) pueden permitir la posibilidad de descargar automáticamente el contenido multimedia o descargarlo a petición del usuario. Una buena medida para limitar el acceso del menor a posibles contenidos no deseados o software malicioso podría ser configurar la aplicación para que vídeos y fotografías no se descarguen sin el control del usuario.

La inclusión forzada del menor en un grupo de intercambio de mensajes puede hacer que se sienta acosado. Por este motivo debemos concienciarle para que no permanezca en un grupo del que no desea formar parte y que debe respetar la decisión de otra persona que no desee pertenecer a un determinado grupo.

14 Mensaje Privado: a veces se representa con su acrónimo MP.

FICHA 7

Ajustes de privacidad: trucos para la tablet, móvil y ordenador

La mayor parte de los fabricantes de dispositivos móviles incluyen una cuota de espacio para el almacenamiento de archivos en la nube. Este espacio suele venir configurado por defecto, de forma que fotografías, archivos y copias de seguridad se suben directamente a la nube.

En este apartado intentamos que el menor sea consciente de esta circunstancia y de que existe la posibilidad de no guardar información en la nube si no lo desea. También puede ocurrir que el espacio de almacenamiento en la nube pudiera ser accesible a otras personas. Por ello es importante leer las condiciones de uso y de acceso a la información del menor en la nube con el fin de determinar quién podría tener acceso a sus cosas. Si se optara por no utilizar la nube se recomienda que se guarde una copia del contenido de la tablet o móvil en otro soporte (ordenador, pendrive, disco duro).

Otra de las cuestiones importantes de este apartado son las opciones de los terminales móviles que permiten a un tercero realizar un seguimiento del menor como la interfaz wifi, bluetooth y GPS. Se recomienda que cuando no los utilice procure desconectarlos.

Finalmente, en esta sección prevenimos al menor acerca de la posibilidad de que un virus permita que otra persona pueda observarle a través de la cámara de su ordenador, recomendándole que procure utilizar una pegatina sobre el objetivo de la cámara cuando no la necesite. Se debe evitar disponer de una webcam siempre en disposición de captar el espacio en el que se encuentra el niñ@. El mismo riesgo puede existir con las cámaras del smartphone o la tablet.

FICHA 8

Sexting y adicción: bloquea y desconecta

Comprobar si ha llegado un mensaje en las redes sociales, en el correo electrónico o en cualquier aplicación de mensajería electrónica puede ocasionar adicción.

En algunos casos esta situación tiene repercusión sobre el descanso del niñ@ y en consecuencia sobre su rendimiento y desarrollo como persona. Si fuera necesario, se recomienda en primer lugar que exista un diálogo entre padres, tutores, profesores y el niñ@ con el fin de ayudarle a ser consciente de la situación. El diálogo es una herramienta fundamental para, por una parte, racionalizar el uso de los dispositivos y, por otra, si fuera necesario, acordar horarios y formas de uso.

El sexting[15] no es ajeno a los menores. En algunos casos se utiliza el teléfono móvil para capturar imágenes parciales del cuerpo, suyas o de otras personas, para lanzar una cadena de reenvíos desafiando a los demás a averiguar la identidad de la persona que aparece en la imagen o bien como una forma de acoso. El sexting es un delito. El menor debe ser conocedor de este extremo con el fin de no participar en ningún juego de este tipo y de advertir a sus padres, profesores o personas de su confianza acerca de esta situación.

«El sexting es un delito. El menor debe ser conocedor de este extremo»

15 Visita nuestra **Ficha Didáctica** sobre «Suplantación de Identidad, Ciberbullying, Grooming, Sexting».

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.tudecideseninternet.es

www.agpd.es

canaljoven@agpd.es

901 23 31 44

616 172 204 (Whatsapp)

Calle de Jorge Juan, 6
28001, Madrid