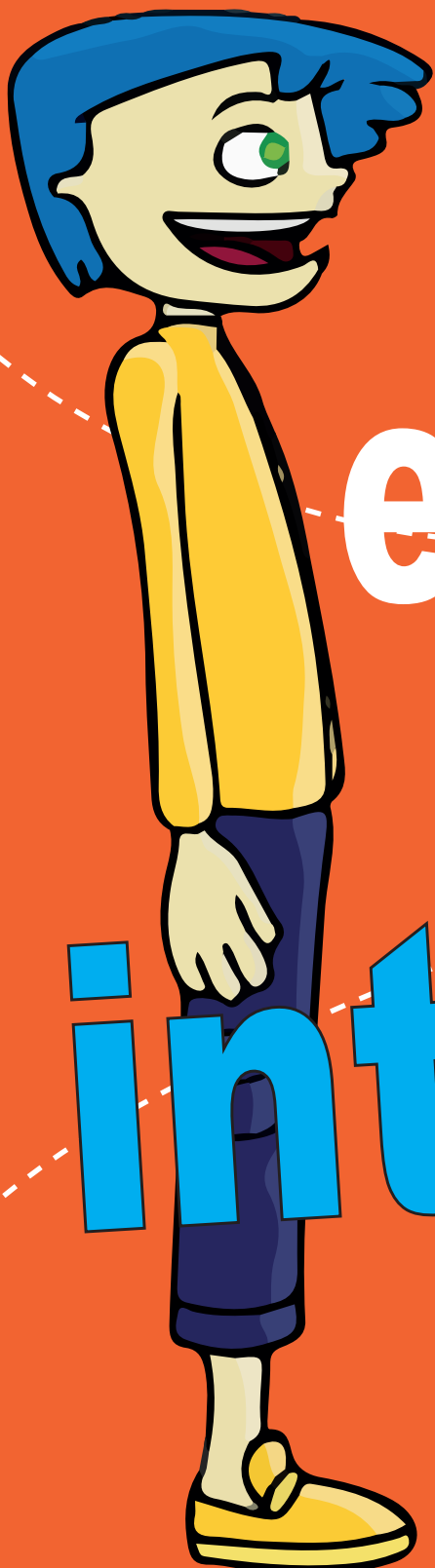


NO

GUÍA
para
JÓVENES



te

enredes

en

internet

FICHA 1

EL DATO PERSONAL

¿Jugamos? ¿Sabrías decir todos tus datos personales?

1. LOS MÁS FÁCILES SON LOS QUE TE IDENTIFICAN DIRECTAMENTE.

Tu nombre, tus apellidos, tu fotografía, tu domicilio, tu número de carnet de identidad o de pasaporte...

Cualquier información que hace posible que alguien pueda identificarte es uno de tus datos personales.

2. OTROS DICEN MÁS DE TI DE LO QUE IMAGINAS.

Tu correo electrónico, tu número de teléfono, las webs que visitas, las consultas que haces en los buscadores, los vídeos que consultas por internet, tus cuentas en redes sociales, tus mensajes, tus publicaciones, los comentarios que haces en un blog o un foro, tus «me gusta», el móvil que utilizas...

Todo lo que haces en internet deja un rastro, una huella digital que habla de ti.

¿Sabías que toda la información que dejas cuando te conectas forma lo que se llama tu identidad digital?

3. Y ADEMÁS...

Un lunar, una pequeña mancha en la piel, una cicatriz, la forma de tus manos o de cualquier parte de tu cuerpo, un objeto que utilizas como un anillo o un pendiente, tu ropa o incluso la foto de tu colegio o instituto pueden servir para que alguien te identifique.

4. TU INFORMACIÓN PERSONAL ES VALIOSA ¿CUIDAS DE TUS DATOS?

- 🕒 Tú decides quién puede tener tus datos.
- 🕒 Tú decides para qué pueden utilizarlos.
- 🕒 Te damos algunas pistas y trucos para cuidar de ellos.



Trucos para las trampas
de internet

1. LAS WEBS QUE ENGAÑAN

- ¿WWW.MOGOLLONDEJUEGOS.COM
O WWW.MOGOLONDEJUEGOS.COM?

Comprueba en tu navegador si realmente estás visitando la página que quieres. Mira en la barra de direcciones y decide dónde quieres ir.

Algunos hackers aprovechan nuestros despistes para crear webs casi iguales a las que utilizas habitualmente pero con contenido que puede dañar tus dispositivos (tu tablet, tu móvil, tu ordenador) o para robarte tu cuenta o tus datos personales.

Antes de escribir tu nombre de usuario y contraseña asegúrate de que has entrado en la web correcta. Para ello, revisa la barra de direcciones.

2. WEBS CON DEMASIADAS
COOKIES.

Las cookies o galletas guardan información sobre ti: dicen qué páginas has visitado, qué te gusta, qué sueles hacer y mucho más.

- 🕒 Para borrarlas busca la opción en el menú del navegador. Si estás en tu ordenador pulsa las teclas may+ctrl+supr.
- 🕒 En tu móvil, revisa los ajustes de privacidad.

3. WIFI GRATIS Y SIN CLAVE.

Desconfía de las redes wifi gratis o sin clave. No son seguras, otra persona puede ver lo que haces, las contraseñas que utilizas o incluso pueden entrar en tus dispositivos y robarte tu

información personal.

Comprueba que la wifi de tu casa tiene contraseña, evitarás que accedan invitados no deseados.

4. LOS VIRUS QUE ESTROPEAN TU
ORDENADOR TAMBIÉN LO HACEN
CON TU TABLET Y TU MÓVIL.

Utiliza un antivirus en tus dispositivos.

5. LOS SECUESTRADORES DE TUS
CARPETAS.

- 🕒 Cuando navegues por internet puede que al abrir una imagen, pinchar un enlace o descargar un programa, se te instalen archivos que pueden bloquear tu dispositivo y hacer ilegibles tus ficheros.
- 🕒 No abras mensajes de desconocidos. No abras ficheros o enlaces a sitios webs que aparezcan en estos mensajes.
- 🕒 Haz una copia de tus fotos, vídeos, documentos, etc.

6. LAS DESCARGAS GRATIS.

Descarga aplicaciones sólo de sitios de confianza.

FICHA 3

PROTECCIÓN DE DATOS PERSONALES (SEGURIDAD, DERECHOS, POLÍTICA DE PRIVACIDAD)

Trucos para apuntarme y borrar-me de una web

1. DOY TODA LA INFORMACIÓN QUE PIDAN: RELLENO MIS DATOS, LOS DE MIS PADRES, HERMANOS, AMIGOS, PROFESORES, LOS DE MI COLEGIO... ¿ESTÁS SEGUR@?

Nunca des información de tu familia o de otras personas. Desconfía de las webs que te piden demasiada información.

Evita que tu usuario o tu *login* tengan tu nombre, fecha de nacimiento o edad.

2. TUS CLAVES SECRETAS.

- Ⓢ No utilices como contraseñas palabras que se puedan asociar fácilmente a ti, como el nombre de tu mascota, el nombre de tu calle, tu fecha de nacimiento...
- Ⓢ Utiliza contraseñas de un mínimo de 8 caracteres y mezcla mayúsculas, minúsculas, caracteres especiales (@ # *) y números.
- Ⓢ Evita utilizar palabras que vengan en los diccionarios.
- Ⓢ Nunca des a otra persona tus claves y utiliza siempre el botón de salir o cerrar sesión. Así evitas que alguien robe tu sesión, tu cuenta o tus datos personales.

3. ¡EN ESTE SITIO WEB SOMOS MUY GUAYS, SIEMPRE DE BUEN ROLLO!

Si es «guay» tienen que decirte quiénes son, para qué van a utilizar tus datos y cómo puedes borrarlos.

Esto es lo que se llama la «política de privacidad».

Todos los sitios web que utilicen tus datos personales deben tener una política de privacidad.

4. CUANDO TE DICEN QUE NO PUEDEN BORRARTE DE UNA WEB.

¡Es falso!

Cuando te apuntas a una web das tus datos y tú decides cuándo borrarlos. Tienes derecho a decidir sobre tus datos.

5. LAS FOTOS O VÍDEOS DONDE APAREZCO Y OTRAS COSAS QUE HABLAN DE MÍ.

Piensa bien si quieres compartir una imagen o vídeo con los demás.

Si lo haces, fíjate en quién puede verlo.

6. PARA QUITAR LAS FOTOS Y VÍDEOS DONDE APAREZCO Y OTRAS COSAS QUE HABLAN DE MÍ.

Dirígete, en primer lugar, a quien subió esa información y dile que quieres que la borre.

Si no te hace caso, pídeselo al responsable de la web. Si tampoco la quita, habla con tus padres o con alguien de confianza. Podéis recurrir a la Agencia Española de Protección de Datos para que os ayude a borrarla.

Trucos para evitar
malos rollos**1. ALGUIEN QUE NO CONOCES
QUIERE CONTACTAR CONTIGO.**

- ☉ Cuando un desconocido te pide tu número de teléfono o te escribe un mensaje, ignóralo.
- ☉ Nunca facilites tu teléfono, tu nombre, o cualquier información tuya a un desconocido y menos aún una fotografía tuya o de alguna parte de tu cuerpo.

2. ESCRIBIR Y GRITAR.

- ☉ Cuando escribes mensajes en mayúsculas alguien puede entender que le gritas.

3. RESPETA A LOS DEMÁS.

- ☉ No hagas en internet algo que no harías en la vida real.
- ☉ Evita gestos o conductas que puedan ofender a otras personas.

4. CUANDO NO TE DEJAN EN PAZ.

Si recibes mensajes o comentarios que te molestan, si recibes incluso durante la noche toques o mensajes en tu teléfono o tablet, si alguien te molesta aunque sea con número oculto...

Se llama acoso. No lo permitas. Cuéntalo. No tengas miedo. Pide ayuda a tus padres o a alguien de tu confianza.

5. NO ACOSES A OTRAS PERSONAS.

- ☉ No participes en el acoso de otras personas y, si conoces algún caso, cuéntaselo a tus padres o a alguien de tu confianza.
- ☉ No utilices datos personales de otras personas para acosar.
- ☉ No reenvíes mensajes, fotos o vídeos humillantes o pensados para dañar a otra persona. Además podrías estar cometiendo un delito.



FICHA 5

REDES SOCIALES

Con los amig@s
en la red

1. SI TODO LO PONES EN LA RED SOCIAL.

- ☉ Elige a tus amig@s de la red social entre las personas que conoces.
- ☉ Rechaza solicitudes de amistad de desconocidos.
- ☉ No cuentes cosas de otras personas.
- ☉ Revisa la configuración o los ajustes de tu cuenta en la red social y decide quién puede ver tus cosas ([Facebook](#), [Twitter](#), [Instagram](#), [Youtube](#), [Tuenti](#), [Google+](#)). Visita nuestros [vídeos](#).
- ☉ Piensa antes de publicar algo si lo que dices o pones en tu perfil puede molestar a otras personas.
- ☉ Te aconsejamos que lo que publicas sólo puedan verlo tus amig@s.
- ☉ No compartas tu ubicación, la información de dónde te encuentras ([Facebook](#), [Twitter](#), [Instagram](#), [Youtube](#), [Tuenti](#), [Google+](#)) podría ser conocida por extraños.

2. SI SUBES A LA RED SOCIAL INFORMACIÓN DE OTRAS PERSONAS.

- ☉ Si vas a publicar fotos o vídeos en los que aparecen otras personas, asegúrate de que no les va a molestar.
- ☉ No etiquetes.

3. LOS AMIG@s DE MIS AMIG@s EN LAS REDES.

- ☉ Los amig@s de tus amig@s también pueden llegar a ver lo que compartes.
- ☉ Evita compartir con otras personas lo que tus amig@s comparten contigo.

4. BLOGS Y FOROS.

- ☉ No facilites información que permita que desconocidos te puedan localizar o identificar. Podrías tener problemas.
- ☉ Utiliza siempre un pseudónimo y nunca digas tu nombre real o el nombre real de tus amig@s.
- ☉ No publiques tu domicilio, tu colegio o instituto, tu correo, tu número de teléfono y, en general, tus datos personales o los de otras personas.



1. REENVÍO TODO LO QUE RECIBO.

- ☉ Muchos mensajes contienen datos personales de otras personas.
- ☉ Consulta antes con quien te envía un mensaje para saber si lo puedes pasar a otra persona.
- ☉ Cuando escribas un mensaje o mandes fotos o vídeos, piensa que las personas a las que se lo envías siempre pueden reenviarlos a otras personas.
- ☉ Nunca reenvíes imágenes y vídeos que puedan molestar a otras personas. Puedes causar muchos problemas y a veces estarás cometiendo un delito.
- ☉ No participes en las cadenas de mensajes.

2. SI ENVÍAS UN CORREO A MUCHAS PERSONAS.

- ☉ Utiliza la opción de tu correo con copia oculta (cco).
- ☉ Evitarás que todos vean la dirección de correo de los demás.
- ☉ Algunas personas no quieren que se facilite su correo a otros. Es un dato suyo y ellos deciden. Respeta sus deseos.

3. MENSAJES Y COMENTARIOS EN REDES SOCIALES.

- ☉ Si haces un comentario o publicas un mensaje en una red social piensa si quieres que todo el mundo pueda verlo o prefieres enviar un mensaje privado.

- ☉ Si crees que a la otra persona le puede molestar que el mensaje o comentario sea visible utiliza la opción del mensaje privado.
- ☉ No reveles tus datos personales o los de otras personas en mensajes y comentarios que no sean privados.

4. DESCARGAS AUTOMÁTICAS.

- ☉ Algunos virus llegan a tu móvil o tablet dentro de vídeos y pueden robar tus datos personales.
- ☉ Revisa los ajustes para mensajes multimedia (MMS) y apps de mensajes (Whatsapp, Snapchat, Telegram...) para evitar que los vídeos se descarguen automáticamente.
- ☉ Evitarás recibir contenido multimedia de desconocidos que puede dañar tu tablet o móvil.
- ☉ También ahorrarás megas de tu contrato del móvil.

5. GRUPOS.

- ☉ Si te incluyen en un grupo y no te interesa, bórrate.
- ☉ No vuelvas a incluir en un grupo a alguien que se ha borrado salvo que te lo pida él.
- ☉ El número de teléfono o el usuario de otras personas son datos personales que no puedes utilizar si ellos no lo desean. Cuenta con ellos antes de incluirlos en un grupo o una lista para el envío de mensajes.

FICHA 7

AJUSTES DE PRIVACIDAD

Trucos para el tablet, móvil y ordenador

1. ¿ESTÁS EN LAS NUBES?

- ☉ Tu móvil y tu tablet almacenan mucha información tuya, de tus amig@s y de tu familia.
- ☉ Decide si te interesa guardar tus cosas en la nube o si prefieres tenerlas en tu dispositivo móvil.
- ☉ Si utilizas la nube, comprueba quién tiene acceso a tus cosas.

2. GPS, WIFI Y BLUETOOTH EN TU TABLET O MÓVIL.

- ☉ Apaga tu GPS, wifi y Bluetooth cuando no los necesites.
- ☉ Evitarás que otras personas puedan saber dónde estás.
- ☉ Además la batería te durará más tiempo.

3. PARA QUE NO TE VEAN.

- ☉ Un hacker puede observarte a través de la cámara de tu dispositivo sin que lo sepas.
- ☉ Utiliza una pegatina y tapa tu cámara cuando no la utilices.



1. DESNUD@S POR LA RED.

- ☉ No te hagas o hagas a otros fotos comprometidas.
- ☉ No envíes fotos de nadie desnudo. Podría llegar a ser un delito.
- ☉ Bloquea al remitente para que no te envíe este tipo de imágenes y evitar que te acose.
- ☉ Enviar o reenviar imágenes comprometidas puede ser acoso. No lo permitas. Pide ayuda a tus padres o a alguien de tu confianza.

2. NO DUERMO, NO ESTUDIO, NO PUEDO DEJAR DE MIRAR MENSAJES...

- ☉ Tú controlas tu móvil, tu tablet, tu ordenador. No permitas que él te controle a ti.
- ☉ No permitas que nadie te acose con mensajes constantes.

3. DESCONECTA.

- ☉ Cuando duermes no necesitas estar conectad@.
- ☉ Apaga tu tablet, tu móvil o tu ordenador cuando descansas.

4. CONSULTA CON TUS PADRES, PROFESORES O CON ALGUIEN DE TU CONFIANZA.

- ☉ Cuando tengas dudas.
- ☉ Cuando te sientas acosado.
- ☉ Cuando creas que se está acosando a otra persona.



AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



www.tudecideseninternet.es

www.agpd.es

Calle de Jorge Juan, 6
28001, Madrid

Llámanos

901 23 31 44

Whatsapp

616 17 22 04

Escríbenos

canaljoven@agpd.es

