

Protección de menores

Al igual que todos tenemos una identidad en la vida real, tenemos también una identidad digital, formada por todo aquello que Internet sabe de nosotros. La identidad digital es como nuestra identidad real, pero en Internet.

Los menores también tienen una identidad digital, a veces incluso antes de haber utilizado Internet. La identidad digital está formada no sólo por lo que nosotros subimos a Internet, sino también por todo lo que otros publican sobre nosotros: familiares, amigos, colegios, asociaciones, etc.

Identidad digital

Hemos de ser conscientes y trasladar a los menores la perdurabilidad de la información en Internet. Es muy sencillo subir comentarios, fotografías o vídeos a Internet, especialmente desde la aparición de los dispositivos móviles, **pero no es tan fácil borrarlos**. Aunque ahora mismo sí podemos exigir a determinadas plataformas como Google que eliminen nuestra información personal.

Además, una vez que esa información está en Internet perdemos el control sobre ella y nunca sabemos cuándo ni hasta quién va a llegar. Por eso en el caso de los menores es todavía más importante ser selectivos a la hora de publicar cualquier tipo de información en una web o redes sociales.

Tengamos en cuenta que la foto más graciosa o el comentario más ingenioso puede no serlo dentro de unos años.

Las nuevas tecnologías tienen normas

Debemos transmitir a los menores que en el mundo de las nuevas tecnologías también hay normas. En Internet no podemos hacer lo que queramos y salir impunes, ni adultos, ni menores.

Es necesario transmitir a los menores la idea de que hay normas que se deben cumplir:

- Si no está bien insultar a un compañero en el patio del colegio, tampoco es correcto hacerlo en Internet o difundir el insulto de otro compañero. Esto en la vida real se llama acoso o bullying, y trasladado al mundo digital es ciberacoso o ciberbullying. Estamos hablando de lo mismo en diferentes contextos.
- Si no facilito datos personales a desconocidos por la calle, tampoco debo hacerlo en las redes sociales.
- Si alguien me incomoda en el colegio se lo contaría a mis padres o profesores y ellos me ayudarían a resolver el problema. Lo mismo debo hacer si esto ocurre a través de las nuevas tecnologías.

- Las redes sociales tienen edades legales a partir de las cuales puedo abrirme un perfil.
- Seguro que no me fiaría de una persona que no conozco porque podría engañarme, pues tampoco puedo hacerlo en la vida online porque es todavía más fácil que alguien se pueda hacer pasar por otra persona. De esta forma aparecen los casos de grooming: adultos que malintencionadamente se hacen pasar por menores con una finalidad sexual.

Los menores deben entender que el mundo real y las nuevas tecnologías NO son mundos tan lejanos y en ambos aplican reglas parecidas.

Establecer límites

Hoy en día existen dispositivos que no existían hace unos años. Muchos son especialmente utilizados por los menores, a menudo de manera intensiva, como los smartphones y tablets. Han pasado a formar parte de su día a día y, como cualquier otro objeto cotidiano, hay que enseñarles a usarlos correctamente y explicarles las consecuencias de un mal uso. Por ello, es necesario establecer unas pautas de uso que dependerán del contexto, la edad y la madurez del niño. Algunas de ellas son las siguientes:

- **Establecer horarios.** Los menores deben saber que hay horas para utilizar el WhatsApp, horas para jugar, para el estudio, el descanso, etc. En función de la edad, debemos establecer unas horas de uso de las nuevas tecnologías e incluso apagarlos el resto del tiempo.
- **Las zonas comunes.** Especialmente cuando se trata de ordenadores y de niños pequeños, es mejor que los utilicen en zonas comunes donde estén con toda la familia.
- **Instalación de aplicaciones.** No sólo los adultos, sino que los menores son también proclives a instalar todo tipo de aplicaciones en los dispositivos móviles, pero no son conscientes de los permisos que les otorgan ni del tipo de aplicación que están instalando.
Es conveniente que el menor instale nuevas aplicaciones de forma consensuada con los padres, valorando si es apropiada para la edad del niño.

Uso de la webcam

Prácticamente todos los dispositivos hoy en día tienen webcam: smartphones, tablets, ordenadores y portátiles. Una webcam es una herramienta muy útil pero siempre debe usarse siendo consciente de sus riesgos.

Los menores deben saber que lo que se muestra a través de una webcam puede ser falso, por ejemplo un vídeo grabado previamente, y que todo lo que ellos muestren puede ser grabado por la otra persona y luego subido a Internet.

Además existe software malintencionado capaz de acceder a la webcam y grabar, por lo que deben taparla siempre que no esté siendo utilizada.

Establecer un clima de confianza

Establecer un clima de confianza es primordial para que los menores puedan confiar en los adultos si tienen algún problema. No podemos estar constantemente vigilándoles, eso no es bueno para ellos ni para nosotros. Es por ello que debemos ir a su lado, observar y mostrar confianza en lo que ellos hacen.

Como son nativos digitales, las nuevas tecnologías, las redes sociales o la mensajería instantánea son para ellos herramientas naturales, son parte de su vida.

Sin embargo, esto genera una falsa sensación de seguridad en el menor que le lleva a adoptar comportamientos de riesgo. Debe comprender que los problemas de Internet son muy similares a los del mundo real, donde los adultos estamos más informados y sabemos cómo ayudarles. De esa forma no dudarán en solicitar nuestra ayuda cuando tengan un problema en Internet, al igual que harían en la vida real.

Debemos crear un clima de confianza. Confiar en los menores y facilitar que ellos confíen en nosotros.

Medidas de seguridad

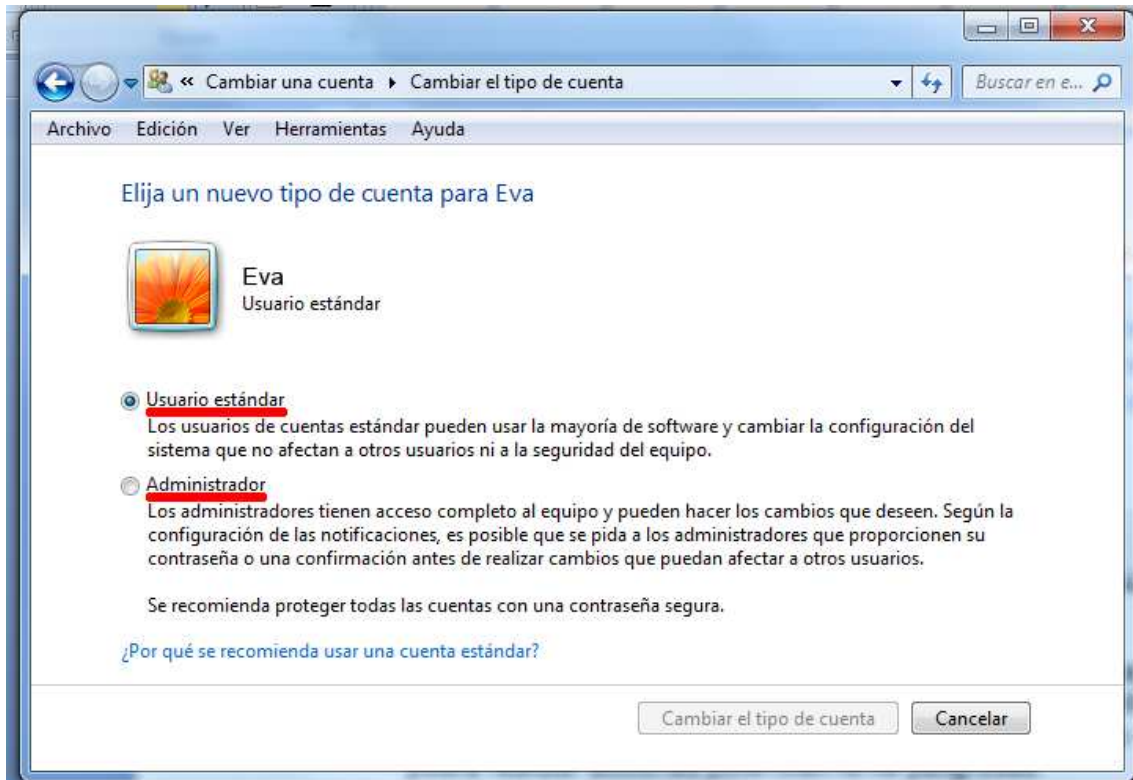
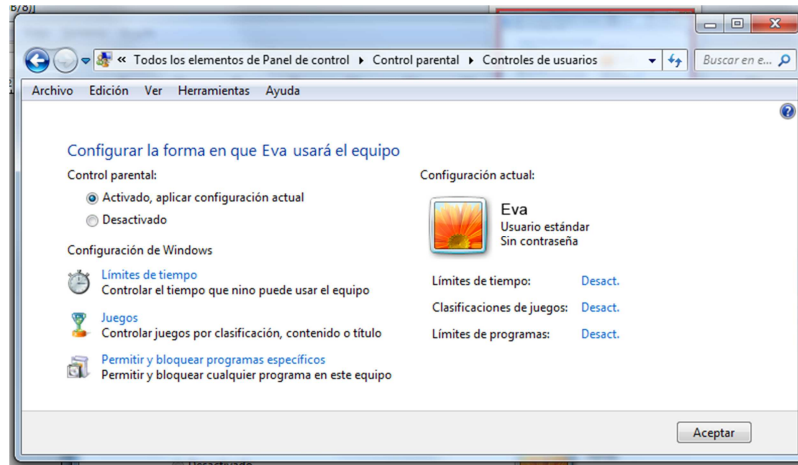
Existen algunas medidas básicas que podemos aplicar para garantizar su seguridad y un buen uso del equipo sin que sean demasiado invasivas:

- **Proteger sus ordenadores y dispositivos.** Para que no tengan problemas con sus equipos debemos mantenerlos actualizados y sin virus.
- **Ayudarles a configurar sus perfiles en redes sociales.** No les dejemos solos. Si van a registrarse en una red social podemos aprovechar para registrarnos nosotros también y entre todos consensuar las mejores opciones de la configuración de la privacidad.
- **Instalar un control parental.** Existen buenos programas para limitar las acciones que el menor puede realizar en el dispositivo que utilice: ordenador, portátil, smartphone... Además los principales sistemas operativos y navegadores de Internet incorporan opciones para garantizar la seguridad del menor en el acceso a contenidos.

Por supuesto, todo ello debe hacerse siempre respetando la intimidad del menor.

Estas herramientas deben ser usadas con el objetivo de proteger al menor, no como mecanismos de espionaje. Por ello, si se va a instalar en el dispositivo del menor, se recomienda mantener una conversación con él para explicarle la medida que se va a tomar y cuáles son los motivos.

- **Utilizar una cuenta sin privilegios de administrador.** Una cuenta de administrador permite que el usuario instale programas, deshabilite protecciones, active dispositivos como la webcam, etc. Si el menor tiene una cuenta sin privilegios, no podrá realizar acciones potencialmente peligrosas.



Además de estas medidas técnicas, lo más importante es formarles y explicarles las amenazas que existen en Internet, qué cosas no deben hacer y el porqué. La solución no es prohibir sino educar.

Podemos poner rejas a las ventanas de nuestra casa, pero si no le enseñamos qué es una ventana y por qué no debe saltar por ella, lo más probable es que lo haga en casa de un amigo.

Consejos finales

Las nuevas tecnologías no son una amenaza para los menores. Son una necesidad, una herramienta y una oportunidad. Sin embargo, debemos guiarlos en sus primeros pasos por ese mundo para evitar que tengan problemas.

- Conozcamos el concepto de identidad digital y expliquémoslo a los menores.
- Seamos muy selectivos a la hora de publicar nueva información o imágenes de menores en la red.
- Establezcamos límites en el uso de los dispositivos.
- Creemos un clima de confianza con los menores.
- Es necesario formarnos y formarles en el uso de las nuevas tecnologías.
- Aprovechemos las ventajas de la tecnología para protegerlos: controles parentales, cuentas sin privilegios, etc.
- No les dejemos solos en esta nueva aventura.