La seguridad de nuestros hijos en Internet

Pablo Pérez San-José
Instituto Nacional de Tecnologías de la Comunicación (INTECO)
pablo.perez@inteco.es

Los niños y niñas españoles nacen y crecen en un entorno tecnológico, que además está en constante cambio, por lo que su aproximación a las tecnologías de la información y comunicación (TIC) es muy diferente a la de sus padres y madres. Los adultos *utilizamos* Internet, es decir, nos aproximamos a la Red buscando una utilidad puntual (leer las noticias en un periódico digital, una transacción económica, enviar un mensaje). En cambio los niños y adolescentes *viven* en Internet, lo hacen todo allí: juegan, hablan con sus amigos, estudian, buscan información para el colegio, cuelgan sus fotos, etc. Es una realidad: Internet es ya una parte inseparable de sus vidas.

La familiaridad y habilidad con las que nuestros hijos e hijas se desenvuelven en Internet, participando en la Red de forma activa, hace que aprovechen al máximo sus posibilidades de comunicación y socialización. Así, son indudables las ventajas que la tecnología les aporta: oportunidades de desarrollo personal, social y cultural. Algunas de ellas son:

- El acceso ilimitado a información multimedia, herramientas de aprendizaje colaborativo, posibilidades de apertura, socialización y conocimiento de otras personas y culturas. Todo esto, aplicado al ámbito educativo, aporta enormes beneficios en la adquisición de conocimiento.

- El establecimiento de nuevas maneras de relacionarse, como el teléfono móvil, Internet o los videojuegos que contribuyen a crear en los más pequeños la sensación de autonomía y reafirmación.

- La posibilidad de una participación activa en la sociedad, a través de las herramientas que permiten a nuestros hijos e hijas compartir opiniones y contenidos con otros.

- Sin embargo, tan importante como conocer las indudables ventajas y enormes posibilidades que las nuevas tecnologías aportan a los menores, es el ser también conscientes de que en Internet pueden existir situaciones constitutivas de riesgos para nuestros hijos e hijas.

¿Qué nos preocupa a padres y madres?

De forma paralela al avance de las Tecnologías de la Información y Comunicación aparecen situaciones que pueden constituir riesgos para los menores. Los padres y madres se enfrentan a una situación nueva, que abordan con interés y responsabilidad.

En ocasiones lo que consideran "grave" puede responder más al eco mediático –del que, evidentemente, los padres son conscientes: como por ejemplo, el uso abusivo del ordenador – que al peligro objetivo que entraña. Precisamente por ello, los padres y madres necesitan pautas que les ayuden a valorar objetivamente la gravedad de las situaciones a las que se enfrentan sus hijos e hijas.

En general, se trata de comportamientos que no tienen su origen en las TIC en un sentido estricto, sino en situaciones y actitudes humanas preexistentes, que han encontrado en Internet un canal rápido de difusión. Algunos de estos riesgos son los siguientes:

- ***Ciberbullying*** o acoso entre iguales (entre menores) ocurrido a través de un medio tecnológico. Las manifestaciones de acoso son múltiples y, en general, incluyen cualquier comportamiento que genera en la víctima una sensación de agobio: chantaje, vejaciones, insultos, difusión de rumores falsos sobre la persona, publicación de fotografías humillantes… Lo relevante en este caso es que acosador y víctima son niños, y que se utiliza un dispositivo tecnológico (Internet y teléfono móvil, principalmente) para llevar a cabo la acción.

- ***Grooming*** o acoso sexual ejercido por un adulto y se refiere a las acciones realizadas deliberadamente con el fin de establecer una relación y un control emocional sobre un niño o niña y así preparar el terreno para un abuso sexual del menor. Se podría decir que son situaciones de acoso con un contenido sexual explícito o implícito. Utilizando el chantaje emocional, el depredador sexual busca conseguir gratificaciones que pueden ir desde el envío de imágenes o vídeos hasta propuestas de encuentros en persona. Se trata de situaciones que, si bien no son frecuentes desde un punto de vista estrictamente numérico, comportan consecuencias muy graves para la integridad física y emocional del menor. La lucha es desigual: un adulto especializado en la "caza" de menores, contra un niño inmerso en una situación que, con frecuencia, no puede controlar ni compartir.

- **Amenazas a la privacidad:** la facilidad de publicación de datos, fotografías y vídeos y la enorme fluidez de circulación a través de Internet suponen que, una vez hecho público un contenido en la Red, sea prácticamente imposible frenar su difusión. Así, facilitar datos personales en contextos y a personas inadecuados puede comprometer la seguridad del titular de los datos. Todo ello, unido a la tendencia de los niños a *compartir* la información (frente a la conducta opuesta que tenemos los adultos de *retenerla*) coloca a los menores en una posición vulnerable. ¿Qué ocurre si circula por Internet una foto de nuestro hijo?; ¿o si él mismo facilita datos personales tales como su domicilio o el colegio en el que estudia? Esta información, en manos de personas malintencionadas, puede constituir una amenaza a la privacidad de nuestro hijo. El éxito creciente entre los jóvenes de las redes sociales (por ejemplo: *Tuenti*, *Fotolog*, *Facebook*), plataformas en las que los usuarios crean sus propios contenidos y los hacen visibles entre su red de contactos, puede contribuir a que proliferen estas actitudes susceptibles de afectar a la privacidad del menor.

Otras situaciones ante las que los padres y madres debemos estar alerta son la posibilidad de **uso abusivo o adicción a Internet** (excesivo tiempo de conexión por el menor, que puede implicar incluso dependencia o renuncia a la realización de otras actividades) y el **acceso a contenidos inapropiados** (como de carácter sexual, xenófobo, que hagan apología del terrorismo o de las sectas, que favorezcan trastornos tales como la

anorexia y la bulimia, que incluyan información falsa o que vulneren gravemente los valores en los que educamos a los hijos e hijas, entre otros ejemplos).

En estos casos, ¿dónde está el límite? Debemos ser los padres y madres los que, atendiendo a las circunstancias concretas (edad y madurez del niño, tolerancia o intolerancia hacia determinados contenidos, etc.), determinemos normas precisas de utilización de la Red. Como veremos más adelante, existen herramientas que pueden ayudarnos a poner en práctica un control sobre el tiempo de uso de Internet y el tipo de contenidos a los que acceden los chavales.

No podemos bajar la guardia ante otro tipo de riesgos que, si bien no son considerados graves por la mayoría de los padres, ocurren en un alto grado. Nos referimos a **riesgos de carácter técnico***:* virus, troyanos, gusanos y otras manifestaciones de malware (código malicioso) que pueden suponer un funcionamiento inadecuado del equipo, pérdida de información, etc.

Ante todas estas situaciones descritas, los niños y adolescentes se encuentran en situaciones de especial vulnerabilidad. Su edad, inexperiencia o inmadurez pueden facilitar la incidencia de alguna de estas situaciones. Además, los riesgos son dinámicos y evolucionan constantemente empujados por las nuevas posibilidades técnicas que surgen casi a diario. Por tanto, las situaciones descritas en este artículo no definen una realidad estática: es previsible que evolucionen a la misma velocidad que lo hace la tecnología.

¿Cómo enfrentarnos ante estas situaciones?

En primer lugar, es importante que los menores sepan identificar y manejar los riesgos con la misma destreza con la que utilizan el resto de funcionalidades de la Red, para poder aprovechar todas las ventajas que ponen a su alcance las TIC.

Del mismo modo, también nosotros como protagonistas indiscutibles en la educación de nuestros hijos tenemos la responsabilidad de conocer el uso que nuestros hijos hacen de Internet y las situaciones que pueden ocurrir, para así ser capaces de darles una respuesta. Sólo con un conocimiento profundo de los riesgos existentes en Internet seremos capaces de identificarlos y combatirlos. Existe multitud de información disponible al respecto – como no podía ser de otro modo – en Internet.

Antes de avanzar sobre las medidas concretas a implantar para fomentar un uso seguro de Internet por parte de nuestros hijos e hijas, es importante destacar una idea: una adecuada cultura de seguridad procede, de un lado, de las herramientas instaladas en los equipos y, de otro, de los hábitos o pautas generales de comportamiento adoptados por el menor. Cuando se trata de asegurar que nuestro hijo o hija utiliza Internet de forma segura, tan importantes son las herramientas como los hábitos. Veamos en profundidad ambos conceptos.

Pautas y consejos de seguridad

Los padres y madres podemos ayudar a nuestros hijos siguiendo una serie de pautas que contribuyen a una navegación segura:

- Supervisad la actividad de vuestro hijo en Internet. Es necesario saber qué hace nuestro hijo o hija mientras navega. En función de la edad y autonomía del menor,

este seguimiento podrá consistir en el acompañamiento físico (recomendable cuando los niños son pequeños y están empezando a utilizar la Red) o en un control a posteriori: preguntando qué páginas han visitado, o comprobándolo nosotros mismos a través de la revisión del historial de navegación. Del mismo modo, podemos convertirnos en usuarios de las páginas visitadas por nuestro hijo: ¿qué mejor forma de conocer cómo utiliza su red social favorita que participando en ella?

- En la medida de lo posible, colocad el ordenador del menor en una zona de uso común. De este modo, podemos realizar más eficazmente la supervisión de la navegación, minimizamos el riesgo de que se produzcan situaciones delicadas a través de la webcam o accesos a páginas de contenidos inapropiados y evitamos que el niño o niña esté conectado más allá del tiempo que hayamos dispuesto.

- Estableced unas normas de uso claras referidas al tiempo, servicios y contenidos.

- Hacedles conscientes de la necesidad de velar por su privacidad y respetar la de los demás. Deben saber la importancia de no difundir determinada información personal y las consecuencias negativas que puede implicar la falta de privacidad. Inculcadles normas de comportamiento respetuoso en Internet, y hacedles ver que en el mundo online se deben respetar las mismas pautas que en el mundo físico.

- Ofrecedles ayuda a la hora de crear su nombre de usuario o apodo y sus contraseñas y claves de acceso. Los apodos no deben dar pistas sobre datos personales como género y edad del usuario (por ejemplo, evitar nicks del tipo *marta1995* o *julio14*). Las claves de acceso deben ser seguras y confidenciales, y el niño debe aprender a cambiarlas periódicamente y a no revelarlas a terceras personas.

- Alertadles acerca de los peligros existentes en ciertos comportamientos y, si es el caso, prohibid o limitad situaciones como: citas con desconocidos, publicación de fotografías personales, realización de transacciones económicas, descarga de archivos en redes p2p, etc.

- Habladles acerca de los efectos negativos de los virus o código malicioso**,** proporcionándoles pautas para evitar las infecciones de los equipos informáticos: siempre han de escanearse los archivos que se vayan a descargar con un antivirus actualizado y, en ningún caso, deben descargar archivos procedentes de fuentes o personas que no conocen.

- Instalad y mantened actualizadas las herramientas de seguridad del equipo de vuestro hijo o hija.
- Sobre todo, debéis transmitir a vuestro hijo o hija la suficiente confianza para que os implique y os pida ayuda en situaciones que le pueden resultar incómodas.

Herramientas de control parental

Son herramientas que sirven para restringir y monitorizar el uso que nuestro hijo hace de Internet. Hay infinidad de herramientas de este tipo en el mercado, bien integradas en los sistemas operativos, bien ofrecidas por los propios proveedores de Internet, bien en forma de programas específicos (tanto gratuitos, como bajo licencia de pago).

¿Qué utilidades ofrecen estas herramientas?

- Controlan el tiempo que nuestro hijo puede estar conectado a Internet: podemos limitar el tiempo diario de conexión, el horario y los días a la semana de uso. Resulta muy útil, por ejemplo, cuando los niños están solos en casa.

- Bloquean el acceso a páginas que contienen ciertas palabras: la herramienta impide al menor visitar webs donde aparezcan los términos que hayamos predefinido, y que implican un contenido que consideramos inapropiado para el menor (por ejemplo, sexo, apuestas, drogas, casino…).

- Revisan las páginas visitadas por el menor: ofrece una relación de los sitios a los que el niño ha accedido (o ha intentado acceder). De este modo, nos permite conocer cuáles son los hábitos de navegación de los menores.

- Impiden la ejecución o descarga de determinados programas (por ejemplo, mensajería instantánea), así como la salida de determinada información (datos personales, bancarios, etc.).

- Determinan las páginas por las que les es permitido navegar a los menores, a través de un sistema de definición de listas blancas (webs a las que se permite el acceso) y listas negras (webs con acceso denegado).

Padres, madres y educadores no están solos en esta tarea

La forma en la que las diferentes Administraciones Públicas estamos materializando acciones con este objetivo de sensibilización y formación es muy variada: elaboración de guías y materiales didácticos e interactivos, difusión de buenas prácticas, publicación de estudios, creación de páginas web, realización de charlas, seminarios y cursos, etc.

En este sentido, desde el **Instituto Nacional de Tecnologías de la Comunicación (INTECO)**, dentro de nuestra labor de formación, información y difusión de la cultura de la seguridad, ofrecemos a través de su página web www.inteco.es pautas, consejos y herramientas para garantizar un uso seguro de las nuevas tecnologías. Algunas de nuestras acciones en este ámbito son:

- Oficina de Seguridad del Internauta:
  www.osi.es
  Línea telefónica de soporte a denuncias (hotline): 901.111.121
  Línea telefónica de ayuda e información (helpline): 901.111.121

- Sección Web "Menores en la Red":
  http://osi.es/econf/Protegete/Menores_en_la_red

- Guía para padres y madres de menores en Internet: www.inteco.es/extfrontinteco/img/File/intecocert/Proteccion/menores/guiapadresymadres.pdf

- Guía para menores en Internet: www.inteco.es/extfrontinteco/img/File/intecocert/Proteccion/menores/guiaparamenoreseninternet.pdf

- Guía para la protección legal de los menores en el uso de Internet: www.inteco.es/Seguridad/Observatorio/area_juridica/Guias_Legales/Guia_para_la_proteccion_legal_de_los_menores_en_el

- Guía legal sobre las redes sociales, menores de edad y privacidad en la Red: www.inteco.es/Seguridad/Observatorio/area_juridica/Guias_Legales/guia_redes_menores

- Guía sobre ciberbullying y grooming http://www.inteco.es/Seguridad/Observatorio/manuales_es/guiaManual_gromin g_ciberbullying

- Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/Estudio_ninos

- Estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/Estudio_moviles_menores

- Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/est_red_sociales_es

- Estudio sobre medidas de seguridad en plataformas educativas http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/Estudio_plataformas_educativas

- Nota: La utilización segura de la mensajería instantánea por parte de los adolescentes http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/utilizacion_segura_mensajeria_instantanea_1

- Nota: Los controles parentales: cómo vigilar a qué contenidos de Internet acceden nuestros hijos http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/Articulo_control_parental_11

- Herramientas de seguridad gratuitas: tanto programas de control parental mencionados, como aquellos relacionados con la protección de los equipos ante amenazas técnicas (virus, correo no deseado):
  www.inteco.es/Seguridad/INTECOCERT/Proteccion/tiles_Gratuitos_2/

- Guía de herramientas de seguridad para hogares:
  www.inteco.es/extfrontinteco/img/File/intecocert/Proteccion/menores/guiaparamenoreseninternet.pdf

- Guía práctica sobre cómo activar y configurar el control parental de los sistemas operativos:
  www.inteco.es/Seguridad/Observatorio/area_juridica/Guias_Legales/guia_activacion_contol_parent

- SecuKid®, juego para móviles desarrollado por INTECO sobre seguridad en el uso de las TIC dirigido a niños y adolescentes:
  www.secukid.es

- Juego educativo online TriviRal sobre riesgos en Internet:
  http://www.navegacionsegura.es

Es nuestra responsabilidad como padres y madres conocer los hábitos de navegación de nuestros hijos, los riesgos existentes en Internet y la forma de combatirlos. Todo ello para ayudarles a aprovechar al máximo los beneficios y posibilidades que presentan las nuevas tecnologías. Pero, además es clave saber que, en esa tarea, los padres y madres no están solos. Por un lado, existen organismos públicos (como INTECO) y fundaciones, asociaciones y empresas del ámbito privado que ofrecemos ayuda, información, formación, consejos y herramientas prácticas y útiles, con un tratamiento riguroso y especializado, y en la mayoría de los casos de forma gratuita. Por otro lado, las Fuerzas y Cuerpos de Seguridad del Estado disponen de unidades especializadas para la denuncia y persecución de los delitos contra los menores realizados a través de Internet.

Así pues, con responsabilidad, sin temor y con confianza, nuestros niños y jóvenes podrán disfrutar de todas las oportunidades que Internet les ofrece.