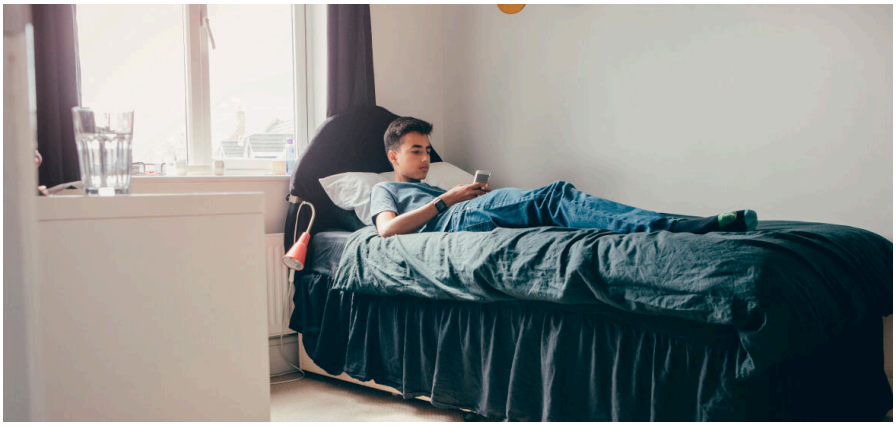
Privacidad



Qué es

Cuando un menor utiliza Internet proporciona gran cantidad de información sensible sobre sí mismo, construyendo la imagen que encontrarán los demás sobre él en la Red: su identidad digital.

La forma en que se maneja toda esa información personal que generamos y publicamos de forma voluntaria en la Internet se conoce como gestión de la privacidad. Es un concepto personal y subjetivo, por ello debemos buscar un equilibrio entre las ventajas que nos ofrece la exposición de información personal y los riesgos asociados. Cuidar nuestra privacidad es cuidar nuestra reputación online, es decir, procurar que nuestra imagen en Internet sea positiva, ya que puede tener serias implicaciones sobre nuestro futuro desarrollo personal y profesional.

Al contrario de lo que muchos adultos piensan, los menores sí cuidan su privacidad, pero entendiéndola de una forma diferente: buscan evitar que personas adultas como sus padres y profesores tengan acceso a su información en Internet. Sin embargo, no dan tanta importancia a las consecuencias de sus actos en Internet y les cuesta pensar en términos de futuro.

Se trata de establecer qué información queremos mantener al alcance sólo de algunas personas, en un ámbito privado, por nuestra seguridad. Este puede ser más íntimo o más amplio, y limitarse a más o a menos personas según nuestras preferencias. Además, no toda la información (datos personales, imágenes, aficiones, localización,...) que hay sobre nosotros en Internet la hemos publicado conscientemente, también puede tener otras procedencias:

- **Publicación inconsciente**. Información que se puede deducir a partir de una publicación propia.
- **Publicación ajena**. Datos de un usuario publicados en Internet por otras personas.
- **Publicación automática**. Información generada y publicada de forma automática por programas o servicios que los usuarios utilizan (por ejemplo última hora de conexión, sitios web visitados, geolocalización, versión del navegador utilizado, etc.)

En situación

Laura ha empezado el instituto hace unos días, y como recompensa por este cambio, sus padres le han regalado su primer móvil. Llevaba meses deseando que llegara este momento. Muchos de sus amigos ya tenían uno, y no soportaba tener que usar el móvil de sus padres para mandar mensajes de WhatsApp. Ahora ya tiene total libertad para hablar con quien quiera y cuando quiera...

Una de las primeras cosas que quiere hacer es hacerse un perfil en las redes sociales que tienen sus amigos. Decide hacerse unas cuantas fotos divertidas y atrevidas, y publicarlas en sus perfiles: no quiere seguir siendo una niña pequeña...

Unas semanas después, le llega un rumor en el Instituto: dicen que una de sus fotos más "atrevidas", en las que salía en bikini, está circulando por ahí. Después comprueba que es cierto, su foto está en otras páginas de Internet, grupos de WhatsApp, ¡e incluso impresas en papel colgadas por el instituto!

Laura se siente humillada, no dejan de difundir las imágenes y llegarle comentarios ofensivos al respecto. La situación está descontrolada. Laura nunca pensó que pudieran hacerle esto, y ahora se arrepiente de no haberlo pensado bien antes de publicar esas imágenes. Está intentando eliminar esos contenidos, pero no es fácil, ya lo tiene todo el instituto...

Cómo afecta a los menores

Una mala gestión de la información personal en Internet puede acarrear diversas consecuencias para los menores. La **pérdida de privacidad** es el principal riesgo al compartir información privada, conllevando la exposición pública de la intimidad de los menores. Una vez publicados en Internet, puede resultar difícil borrar esos contenidos, generando más problemas en el futuro. Esto puede suponer además:

- **Daños en su reputación**. Al exponer contenidos privados, estos pueden influir negativamente en la imagen que ofrecen a los demás a través de Internet.
- **Suplantación de identidad o perfiles falsos**. La publicación de información personal y privada puede facilitar la suplantación de identidad (creación de perfiles falsos), simplificando la deducción de contraseñas o preguntas de seguridad que permiten el acceso a cuentas personales.
- **Riesgos para la seguridad personal**. La publicación de información referente a ubicaciones, como domicilios, centros educativos o lugares de ocio habituales, así como horarios o rutinas, puede llegar a acarrear problemas ya que facilita que el menor pueda ser localizado físicamente.
- Ciberacoso. Cualquier contenido publicado en Internet puede ser utilizado en un acoso, siendo más grave cuanto más íntima es la información. Un ejemplo

de ello es la publicación de confidencias privadas para dañar o ridiculizar a la víctima.

- Sexting. Esta práctica de riesgo implica enviar a otra persona contenidos íntimos a través de Internet, como imágenes o vídeos, perdiendo en ese momento el control sobre los mismos.
- **Grooming**. Cuando un adulto trata de establecer relación con un menor a través de Internet teniendo intenciones de carácter sexual, el acercamiento suele incluir episodios de chantaje. El adulto utiliza la información íntima del menor como elemento de extorsión, para que éste acceda a sus deseos bajo la amenaza de hacer pública esa información.
- **Pérdidas económicas**. La información publicada puede facilitar datos de forma indirecta, como horarios, direcciones o nivel adquisitivo, de tal modo que puedan allanar el camino a ladrones y delincuentes. En otros casos puede proporcionar datos para el acceso a cuentas de banca y comercio online.

Prevención y fomento del uso seguro

La prevención siempre comienza fomentando una **comunicación sana** con los menores y haciéndoles partícipes de los riesgos a los que se enfrentan al administrar su información personal en Internet. Para ello, es fundamental aprender a diferenciar qué tipo de contenidos pueden ser públicos y cuáles deberíamos mantener en privado.

"Pensar antes de publicar" siempre es una buena pauta. Antes de compartir contenido deben reflexionar sobre qué pensará quien lo vea, cómo lo podrá utilizar y qué posibles consecuencias podría tener, tanto en el presente como en el futuro. Fomentando un uso más cuidado y menos impulsivo de su información personal también trabajamos la responsabilidad y la actitud crítica de los menores.

Fomentar este pensamiento crítico no sólo incluye pensar en la propia privacidad, sino también en la **de los demás**. A la hora de compartir información sobre otras personas, es necesario pedir permiso y guardar su intimidad.

Además, existen multitud de **medidas tecnológicas** que nos ayudarán a proteger la información que publicamos:

- **Opciones de privacidad**. Configurarlas adecuadamente es imprescindible en cada aplicación o servicio que utilicen los menores. A menudo puede resultarles complejo, por lo que podemos apoyarnos en los centros de ayuda de cada servicio y en los recursos que están a nuestra disposición, como la Guía de Privacidad y Seguridad en Internet de la OSI y la AGPD.
- **Opciones de seguridad**. Hoy en día cualquier servicio (redes sociales, servicios online, etc.) o dispositivo (ordenadores, tablets y teléfonos móviles), contiene mucha información privada que debe protegerse. El uso correcto de contraseñas robustas,

bloqueo de pantalla, preguntas de seguridad y otras opciones de acceso es esencial para limitar el acceso.

- **Control de contactos y amistades**. Es habitual que los menores añadan en sus redes sociales a personas que realmente no conocen, con lo que su información acaba en manos de personas totalmente extrañas. Es importante promover una lista de contactos segura, para que puedan controlar con quién comparten la información.
- **Sincronización**. Muchas aplicaciones conectan nuestra cuenta de usuario con otras aplicaciones (como por ejemplo, para tuitear automáticamente las fotos de Instagram). Debemos revisar los permisos de privacidad de cada aplicación, para evitar publicar información no deseada.
- **Uso de equipos públicos**. Es recomendable evitar su uso si se va a gestionar información sensible o privada. No obstante, de hacerlo, se recomienda utilizar la opción de navegación privada del navegador, no guardar las contraseñas y cerrar sesión de los servicios al finalizar para evitar que cualquiera que utilice el equipo a continuación pueda acceder a nuestro correo electrónico, redes sociales, banca online, etc.
- **Selección de aplicaciones y redes sociales**. Es importante leer las condiciones y permisos de cada servicio para saber si son adecuadas o suponen una amenaza para la privacidad. Esta situación también aparece al utilizar aplicaciones de terceros dentro de otros servicios, como juegos en redes sociales.

Cómo reaccionar en caso de conflicto

Apoyo al menor. Es fundamental reaccionar con calma y no culparle de la situación, manteniendo la comunicación y la confianza: cuenta con nuestra ayuda y comprensión.

Establecer nuevas medidas de seguridad. Si observamos que existe información privada publicada sin consentimiento, es necesario cambiar las contraseñas de los servicios online utilizados, ya que alguien puede haber accedido a ellos sin permiso.

Comunicación. Si otra persona ha difundido información personal del menor, la primera opción es contactar y hacerle ver que esa información es privada y debería borrarla.

Reporte al proveedor de servicios. Si el paso anterior no es suficiente, se debe contactar con los responsables del servicio donde se ha publicado para que tomen medidas.

Denuncia. Ante una situación de ciberacoso, grooming, o suplantación de identidad, así como problemas derivados de la práctica del sexting, es importante contactar con las Fuerzas y Cuerpos de seguridad. El centro de salud y su centro educativo pueden ofrecer al menor apoyo psicológico y emocional si es necesario.

¿Tienes dudas o necesitas ayuda de manera más personalizada en relación con el uso seguro y responsable de los menores en Internet? Contacta con nosotros en la Línea de Ayuda en Ciberseguridad de INCIBE, **017**. Es un servicio **gratuito** y **confidencial**.

Ayúdanos a mejorar

Tu opinión es muy importante para nosotros.

Compartir en Redes Sociales: