UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES
Andes 1365 piso 7, 11100, Montevideo, Uruguay
+598 2901 00 65 opción 3
www.datospersonales.gub.uy

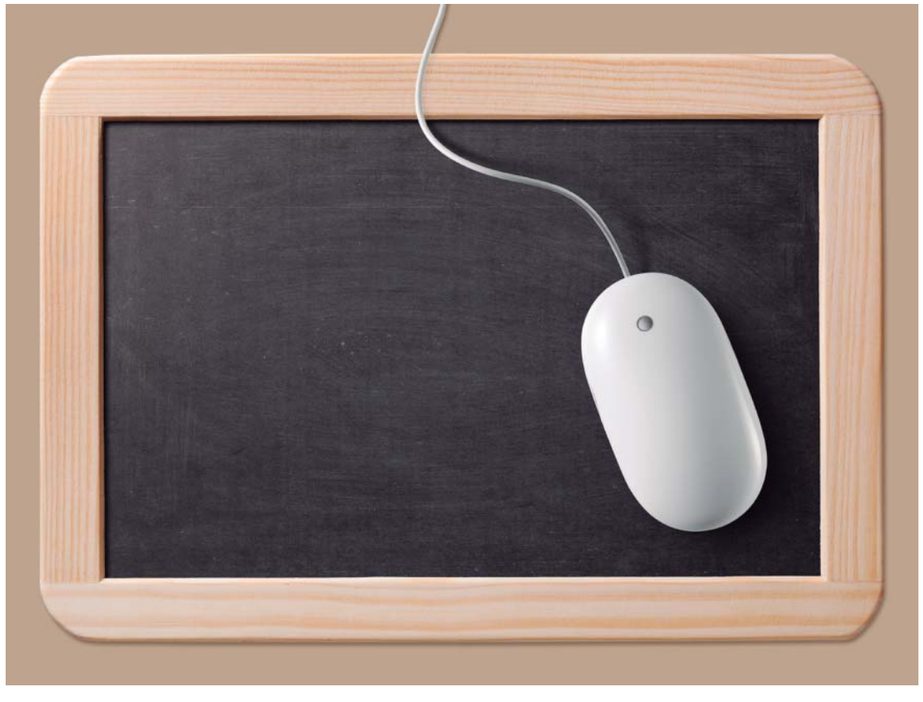
2 { EDUCACIÓN Y DATOS PERSONALES

EDUCACIÓN Y DATOS PERSONALES

Con la masificación de las Tecnologías de Información (TI) y su presencia extendida en el entretenimiento, el trabajo, la comunicación y la educación se torna cada vez más significativo el rol de los adultos (padres, tutores, educadores) en la tarea de ayudar a niños y jóvenes a aprovecharlas de forma efectiva y segura.

El diálogo llano y amigable es la herramienta más efectiva para transmitir la vulnerabilidad a la que los más jóvenes pueden estar expuestos haciendo un manejo incorrecto de sus datos personales, procurando evitar medidas como negar el acceso a Internet u otras tecnologías.

Tanto educadores como padres se enfrentan además al desafío de mantenerse informados y actualizados sobre las TI, ante un panorama donde muchas veces son los jóvenes los que cuentan con un manejo más fluido de la tecnología, aunque sin nociones cabales de sus posibles riesgos.



DATOS PERSONALES, JÓVENES E INTERNET

Lo primero que debemos hacer para que nuestros datos personales estén a resguardo es conocer cómo y cuándo la computadora almacena esa información.

Muchas de nuestras actividades dejan algún tipo de registro en una computadora. Por esa razón el acceso físico a la máquina implica uno de los mayores riesgos para nuestra información. En ella hay pistas que delatan gustos y preferencias y, por lo general, cantidad de información personal que nos expone a la apropiación de datos con fines comerciales o extorsivos.

Para evitar problemas de este tipo es recomendable controlar quién tiene acceso a las máquinas que usamos, eliminar oportunamente registros como el del navegador y utilizar medidas provistas por los sistemas como la protección con contraseña de la computadora y sus archivos.

Es fundamental que los jóvenes sean capaces de distinguir las señales de un engaño. Muchas de las herramientas que usamos para comunicarnos permiten, con relativa facilidad, tergiversar quién está del otro lado de una comunicación o sustituir la identidad de una persona de confianza.

Cuando se trata de menores de edad se requiere la máxima atención y cuidado, ya que lamentablemente existen quienes entablan relaciones sociales, camuflando su verdadera identidad con la finalidad de intercambiar fotos o videos de carácter sexual con personas de esa edad.

Aún sin acceso físico a la computadora, virus, troyanos y gusanos pueden convertirnos en blanco fácil de ataques informáticos.

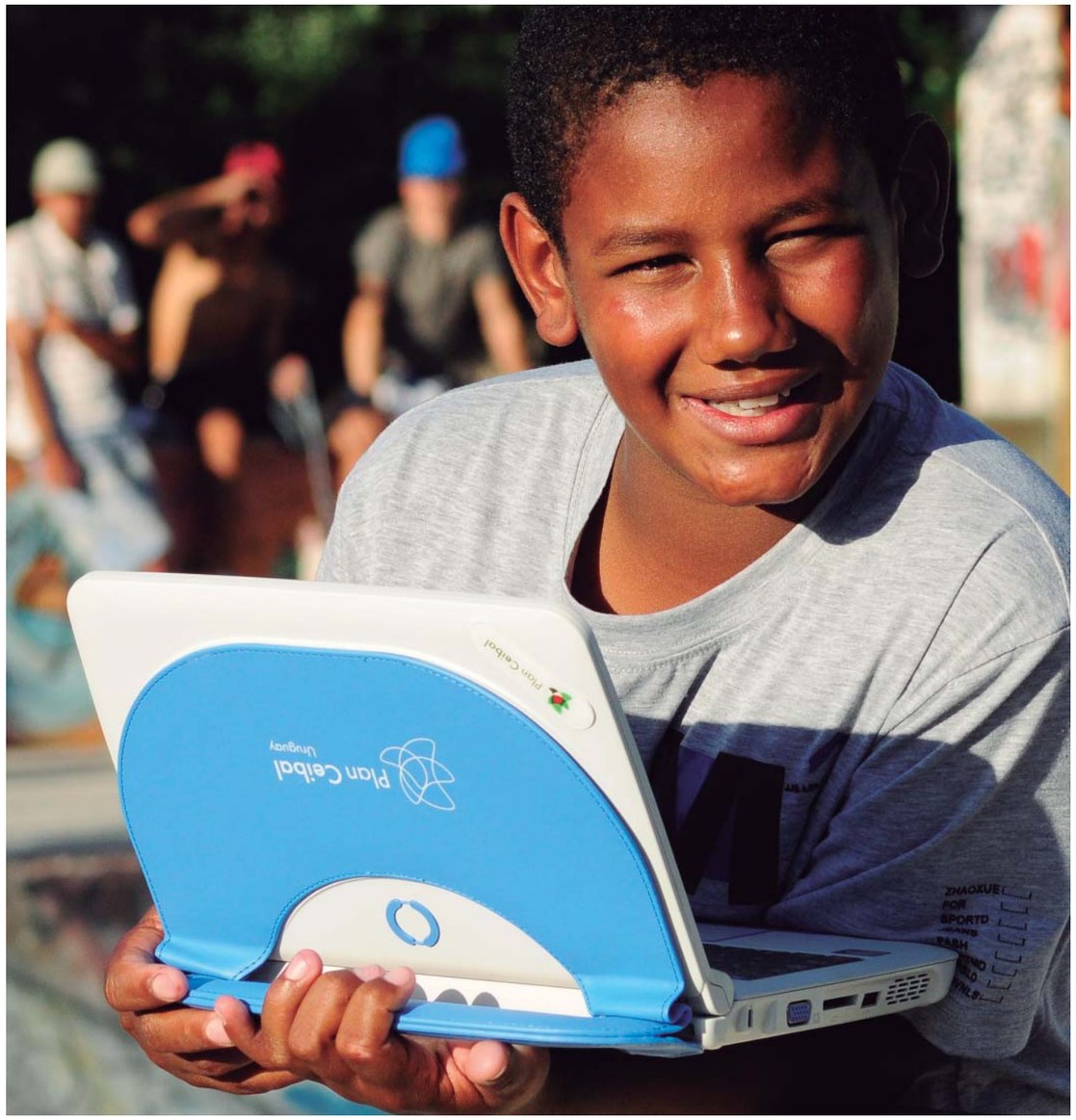
Es absolutamente imprescindible mantener los sistemas de antivirus y cortafuegos (o firewall) actualizados, además de navegar y descargar contenido únicamente de sitios Web de confianza.

TRES CONSEJOS SIMPLES PARA CUIDAR NUESTRA PRIVACIDAD CUANDO SE COMPARTEN COMPUTADORAS

Recordar siempre **cerrar la sesión** de cualquier cuenta a la que accedamos en Internet (correo, mensajería, redes sociales, etc.).

Luego de usar el navegador Web, **eliminar los archivos recientes** (también conocidos como caché) de imágenes y contenidos que visitamos.

Los sitios recientemente visitados son almacenados por nuestro navegador. **Borrar el historial** o desactivar esta opción es una forma sencilla de evitar que esa información sea vista por otros.



CÓMO IDENTIFICAR O EVITAR SITUACIONES DE RIESGO

Los criterios generales que podemos transmitirles a los niños y jóvenes para conducirse en Internet no son diferentes a los que les enseñamos para el mundo real. No deben confiar en desconocidos, aún cuando supongan que mantienen el anonimato. Esto incluye rechazar videoconferencias, envío de información o fotos, descarga de archivos y por supuesto, encuentros personales.

Recomendaciones respecto de Internet

- Evitar medios de intercambio sin controles adecuados.
- Existen espacios en Internet con medidas específicas para permitir que los niños se relacionen con otros niños en un ambiente con garantías.
- Evitar aceptar solicitudes con nombres de usuario asociados a dibujos animados, juguetes conocidos, entre otros.

Consejos en cuanto a la información

- El nombre de usuario no debe proveer información que delate las características personales del usuario tales como nombre o edad.
- Desconfiar de la excesiva amabilidad y promesas, así como de alabanzas al aspecto (aún sin haberlo visto), promesas de regalos, viajes o salidas son señales claras de un comportamiento sospechoso.
- Publicar datos o imágenes de la zona donde se habita, la dirección o el teléfono puede implicar grandes riesgos de seguridad.

Cómo identificar situaciones de riesgo

- Cuando la otra persona insiste en la obtención de fotos o videos.
- Cuando hay una amenaza de pérdida de interés en la conversación si no se cumplen con los pedidos hechos.
- Cuando se pide de forma explícita o implícita datos personales.
- Cuando alguien insiste en concretar un encuentro personal, y sobre todo cuando se pide o sugiere que sea sin compañía.

Conductas delictivas

La Constitución establece que la ley dispondrá las medidas necesarias para que la infancia y juventud sean protegidas contra el abandono corporal, intelectual o moral de sus padres o tutores, así como contra la explotación y el abuso.

En aplicación del mandato constitucional, el Estado ha creado delitos que tienden a la protección de los menores y adolescentes, muchos de las cuales se cometen mediante el uso de las nuevas tecnologías. A modo de ejemplo se sanciona la pornografía infantil, las amenazas y la violencia privada, entre otros.

Las Tecnologías de la Información, por sus especiales características, facilitan la creación de sitios específicamente dedicados a este tipo de conductas y a la difusión de material.

Grooming y Ciberbullyng

El **grooming** es un acoso ejercido por un adulto para establecer una relación y un control emocional sobre un niño o adolescente, con el fin de preparar el terreno para el abuso sexual de este. Se trata de situaciones de acoso con un contenido sexual explícito o implícito.

En el **ciberbullyng**, el acoso se verifica entre iguales. Se trata de insultos, humillaciones, agresiones, maltratos y amenazas a través de medios digitales. Puede darse en las redes sociales, foros, blogs, mensajes, fotologs o chats y se utilizan diversas modalidades para llevarlo a cabo:

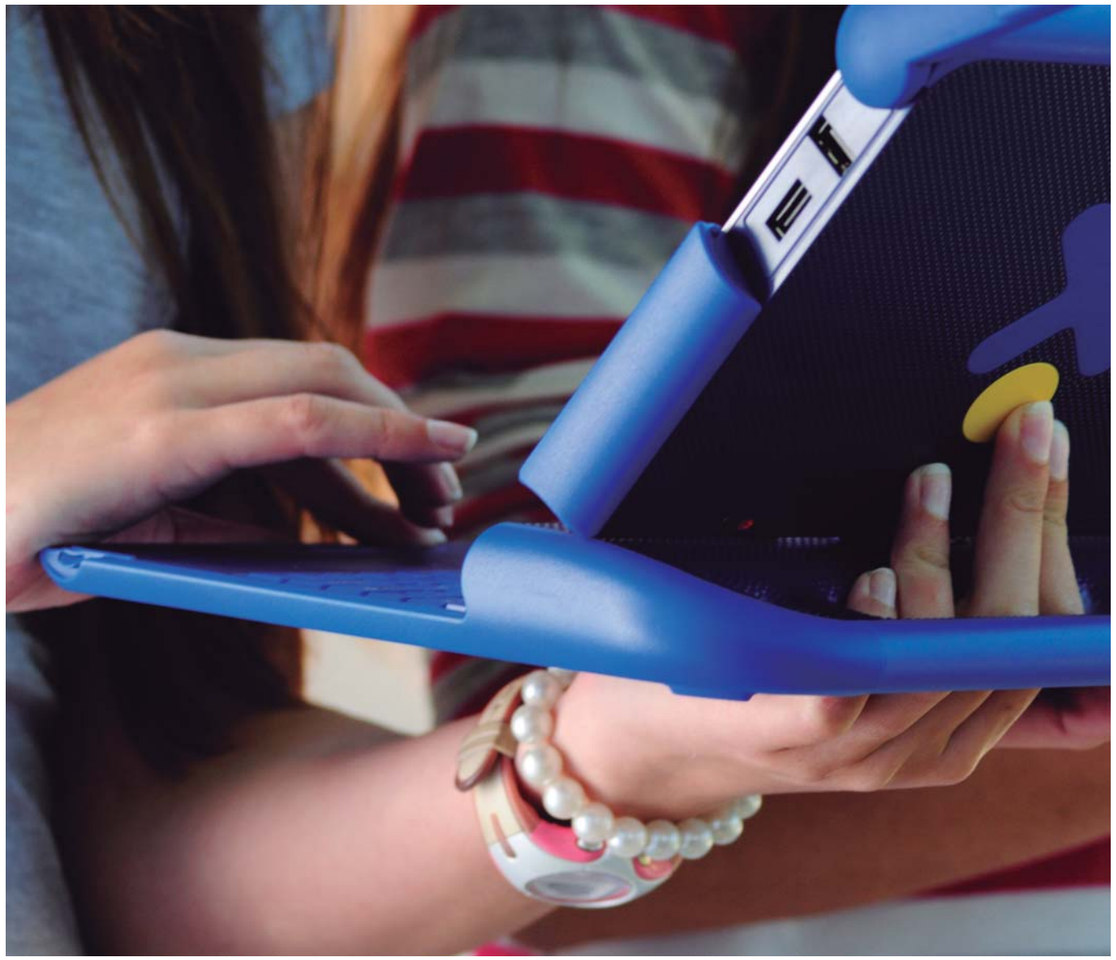
- Publicación o envío de fotografías como forma de desprecio y humillación a la persona.
- Comentarios y mensajes violentos o insultantes al celular o en redes sociales desde cuentas falsas o de forma anónima.
- Publicaciones con referencia a experiencias sexuales con una intención de humillación o burla.

Es importante que educadores y padres informen a niños y jóvenes sobre estos riesgos tratando de evitarlos y tomando conciencia de que pueden ser víctimas, pero también victimarios, provocando un daño irreversible a otro compañero o amigo, que inclusive podría dar lugar a la configuración de un delito.

Ante una situación de acoso es fundamental una actitud de apertura y atención desde los adultos, fomentando que los jóvenes compartan estas situaciones.
En caso de detectar una situación así, es importante conservar las pruebas y denunciar con agilidad la situación ante las autoridades correspondientes.

Contenidos inadecuados para niños y jóvenes.

La violencia, la pornografía y el racismo suceden también en medios como internet. Los adultos deben conocer y utilizar las herramientas disponibles para evitar que los menores entren en contacto con contenidos de este tipo.



Control Parental

Todos los navegadores Web y sistemas operativos modernos incluyen restricción de contenidos en su configuración. Los mismos permiten desactivar opciones como juegos o el acceso a determinados sitios, así como el registro de actividades o alertas ante conductas inapropiadas.

Asesor de Contenido

Las opciones de este filtro para la navegación Web permiten ajustar los contenidos que se muestran, más allá del sitio en el que se navega.

De esta forma se puede prevenir el acceso a contenido no deseado.

Esta herramienta permite restringir el acceso a contenidos como:

- Miedo e intimidación.
- Malos ejemplos para niños.
- Desnudez.
- Incitación o representación de daño.
- Lenguaje soez.
- Material y contenido sexual.
- Representación de apuestas.
- Representación de apuestas, uso de alcohol, de armas, de drogas y de tabaco.

Más allá de las distintas herramientas, no existe sustituto a la atención de las actividades que niños y jóvenes realizan en Internet y al dialogo fluido.

Una relación de confianza y honestidad recíproca es la mejor estrategia para evitar los riesgos mencionados en esta guía.