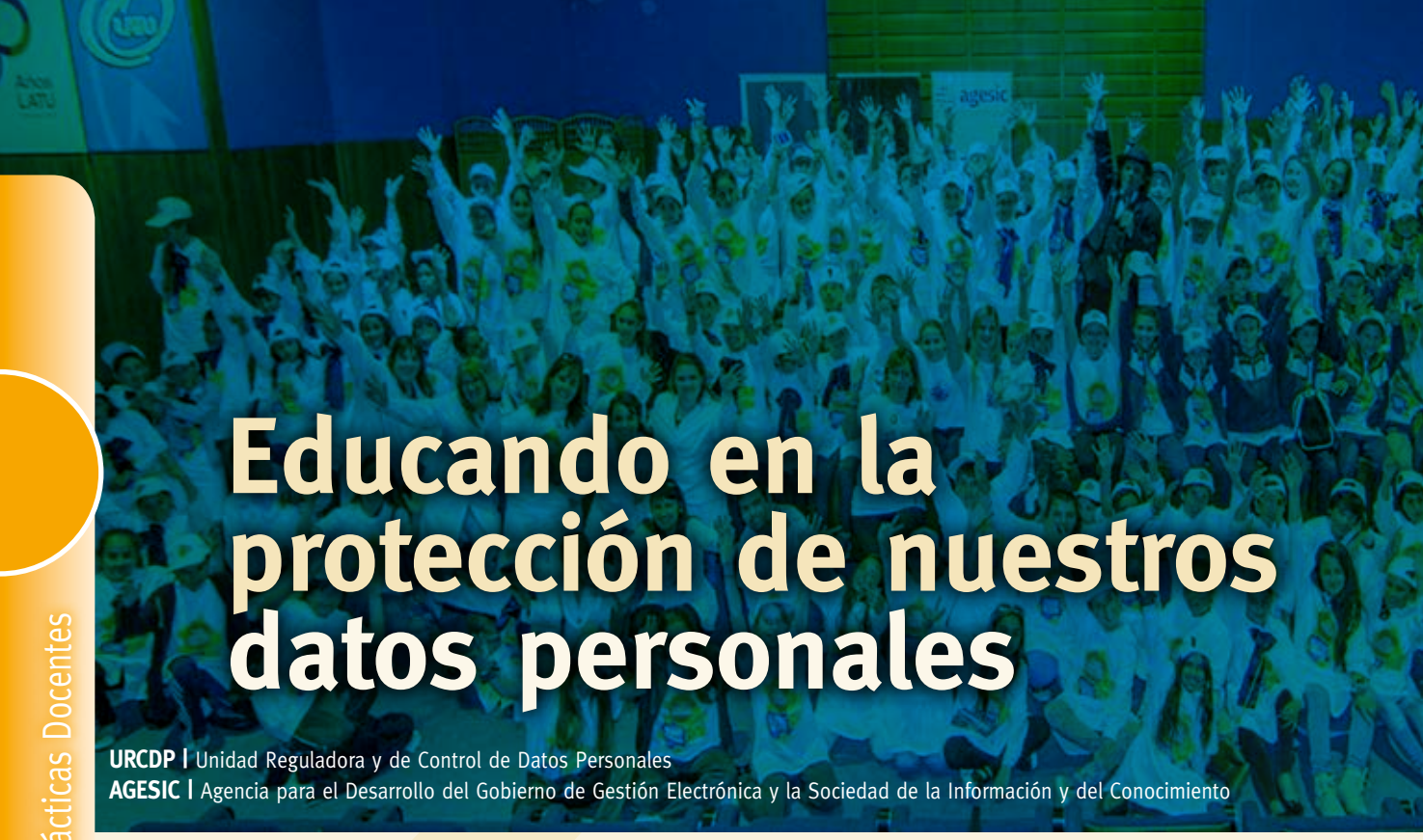


Educando en la protección de nuestros datos personales

URCDP | Unidad Reguladora y de Control de Datos Personales
AGESIC | Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento

Desde el año 2013, ANEP y la URCDP (Unidad Reguladora y de Control de Datos Personales) han trabajado en conjunto para sensibilizar y capacitar a niños y educadores en la protección de sus datos personales.

El objetivo de este artículo es presentar un marco conceptual de este derecho y su impacto en el ámbito educativo, así como relatar la experiencia de estos cuatro años de trabajo conjunto, invitando a que más maestros desarrollen actividades educativas en esta temática.

Conceptos generales

Para comenzar: ¿qué son los datos personales?

Un dato personal es cualquier tipo de información que nos pueda identificar directamente o nos hace identificables, ya sea nuestro nombre, dirección, teléfono, cédula de identidad, RUT, huella digital, número de socio, número de estudiante, una fotografía o hasta el ADN.

No todos los datos personales son iguales: datos personales sensibles

Los datos personales sensibles son aquellos que revelan el origen racial o étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referidas a la vida sexual de una persona.

Para recolectar y tratar este tipo de datos es necesario contar con el consentimiento expreso y escrito del titular, salvo la existencia de razones de interés general establecidas por Ley. En el caso de que el titular de estos datos sea un menor de edad, la autorización expresa debe ser otorgada por el adulto a su cargo.

En el ámbito escolar es común que maestros y directores estén tratando datos personales y datos personales sensibles de los alumnos, en especial aquellos relacionados con su salud, religión o algunos relativos a características de su núcleo familiar.

La Ley indica que estos datos sensibles, por sus características, deben ser especialmente protegidos.

Datos personales: ¿por qué la Ley los protege?

A diario, empresas, organismos públicos y particulares manejan información personal para fines educativos, laborales y comerciales, entre otros. Para proteger nuestra intimidad del mal uso o del uso incorrecto que se pueda hacer de nuestros datos, es que la protección de los datos personales se reconoce como un Derecho Humano.

Para ello, en Uruguay existe un marco legal de protección de los datos personales. Entre otros podemos mencionar los siguientes:

- La Declaración Universal de los Derechos Humanos.
- La Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica.
- La Constitución de la República, en especial su artículo Nº 72.
- La Ley Nº 18.331 de Protección de Datos Personales y Acción de *"Habeas Data"* del 11 de agosto de 2008.
- Los Decretos Nº 664/008 del 22 de diciembre de 2008 y Nº 414/009 del 31 de agosto de 2009.

Nuestros derechos y cómo ejercerlos

Resulta fundamental conocer las potestades que la ley otorga en relación con nuestros datos personales. Igualmente significativo es conocer cuáles son nuestros derechos.

Todos tenemos derecho a:

- Recibir información previa acerca de para qué se solicitan los datos.
- Conocer qué datos poseen sobre cada uno de nosotros.
- Rectificarlos o cancelarlos cuando sean inexactos o incompletos.
- Impugnar aquellas valoraciones personales con efectos jurídicos, que afectan de manera significativa y que se basan únicamente en un tratamiento automatizado de datos que evalúan determinados aspectos como el rendimiento laboral, crédito, fiabilidad, conducta, entre otros. La persona afectada tiene derecho a ser informada sobre el criterio de valoración y el programa utilizado para ello.
- Oponernos al tratamiento en determinadas circunstancias.
- Actualizarlos cada vez que se produzca un cambio en ellos.
- Solicitar la inclusión en alguna base de datos que no estemos y queramos estar.
- Presentarnos ante el responsable de una base de datos, pública o privada, para conocer qué datos nuestros poseen, la finalidad, el uso que se le da a estos y si se ha vulnerado alguno de nuestros derechos.
- También podremos denunciar la recepción de publicidad no deseada o consultar gratuitamente el Registro de base de datos de la URCDP. Si nuestro reclamo es desoído podemos recurrir a la justicia mediante una acción de *Habeas Data* o denunciar la situación ante la URCDP personalmente o mediante su sitio Web: www.datospersonales.gub.uy

La ley también establece obligaciones a quienes realizan tratamiento de datos personales, la misma se aplica a los datos personales registrados en cualquier soporte que permita tratarlos y usarlos posteriormente de diversos modos, tanto en el ámbito privado como público. Estos registros generalmente se constituyen en Bases de Datos.

Para que se considere la existencia de una base de datos, estos deben permitir un acceso ágil a la información: por orden alfabético o número de registro, por ejemplo.

Las bases de datos pueden ser informatizadas o manuales (llevadas en carpetas o biblioratos), y también mixtas (parte informatizada y parte en soporte papel).

Principios que deben orientar el uso de datos personales

Legalidad. *Las bases de datos personales deben cumplir con la normativa e inscribirse en el registro a cargo de la Unidad Reguladora y de Control de Datos Personales.*

Veracidad. *Los datos registrados deberán ser veraces, adecuados, ecuánimes (imparciales) y no excesivos en relación con la finalidad para la que se han obtenido. Será excesivo, por ejemplo, si se requiere preferencia política para afiliarse a un club deportivo.*

Finalidad. *Los datos no deben utilizarse para fines diferentes a los solicitados. Cumplida su finalidad, deben eliminarse.*

Previo consentimiento informado. *Se debe contar con el consentimiento del titular para tratar sus datos. El consentimiento debe ser:*

- ***Libre*** *(podrá brindarlo o no).*
- ***Previo*** *(recabado antes de solicitar los datos).*
- ***Expreso*** *(no tácito o implícito).*
- ***Documentado*** *(verificable).*
- ***Informado*** *(conocer la finalidad por la que se recolectan los datos y dónde ejercer sus derechos).*

Seguridad. *La normativa señala que se deben adoptar medidas de seguridad para proteger los datos recolectados.*

Finalidad. *Los datos deben utilizarse únicamente para la finalidad con la que se obtuvieron, y aplica el deber de confidencialidad a personas que tengan acceso a los mismos.*

Responsabilidad. *Recae sobre la persona física o jurídica responsable de la base así como los encargados de tratamientos, usuarios y terceros, con diferente alcance.*

¿Quiénes son los responsables de una base de datos?

Son todos aquellos que deciden la creación de la base, la finalidad, el contenido y uso de los datos almacenados en ella.

¿Qué bases de datos no deben ser inscriptas?

La Ley no se aplica a las bases de datos pertenecientes a personas físicas que tengan por finalidad un uso personal o doméstico. Tampoco se aplica a aquellas que tienen por objeto la seguridad pública, la defensa y seguridad del Estado, ni a las creadas y reguladas por leyes especiales.

¿Cuándo se pueden comunicar datos personales?

Los datos personales solo pueden ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo de quien los envía y de quien recibe, con el previo consentimiento del titular e informándolo sobre la finalidad de tal comunicación.

Quien recibe una comunicación de datos personales tiene las mismas obligaciones que quien recoge y envía los datos, respondiendo solidariamente ante el Órgano de Control y ante el titular de los datos.

¿Qué se entiende por tratamiento de datos personales?

Los tratamientos de datos personales están alcanzados por la ley cuando se realizan por un sujeto responsable de la base de datos, establecido en el territorio uruguayo, lugar donde ejerce su actividad, cualquiera sea su forma jurídica.

También los alcanza la ley si el responsable de la base de datos o tratamiento no está establecido en el territorio uruguayo, pero utiliza en el tratamiento medios situados en el país, salvo que estos se utilicen exclusivamente con fines de tránsito.

El rol de la Unidad Reguladora y de Control de Datos Personales (URCDP)

Es la autoridad de control, un órgano desconcentrado con autonomía técnica, cuya competencia es custodiar el cumplimiento de la legislación de protección de datos personales y el respeto de sus principios.

La Unidad tiene los siguientes cometidos:

→ Asesorar al Poder Ejecutivo y recomendar políticas en el tratamiento, seguridad y manipulación de los datos personales.

→ Informar sobre el alcance y los mecanismos de defensa previstos por la Ley.

- Inscribir las bases de datos y los códigos de conducta.
- Autorizar las transferencias de datos personales a países sin niveles de protección adecuados en la materia.
- Inspeccionar a las entidades públicas y privadas en relación con el tratamiento de los datos personales.
- Sancionar las infracciones según el marco jurídico existente en materia de protección de datos personales.

Protección de datos personales en el ámbito educativo

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 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 estos quedan registrados en los distintos dispositivos que utilizamos o en Internet.

Muchas de nuestras actividades dejan algún tipo de registro en un dispositivo (computadora, *tablet*, celular), en las distintas aplicaciones que utilizamos en nuestro ámbito laboral o personal así como diferentes ámbitos de Internet (foros, redes sociales, blogs, sitios Web). Por esa razón, el acceso físico a los dispositivos o aplicaciones implica uno de los mayores riesgos para nuestra información. En ellos, así como en la información que enviamos a Internet, hay pistas que delatan gustos y preferencias y, por lo general, cantidad de información personal sin resguardo 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 los dispositivos que usamos, eliminar oportunamente registros como el del navegador, cerrar la sesión cuando nos alejamos de los dispositivos y utilizar medidas provistas por los sistemas como la protección con contraseñas seguras y no compartidas.

Aun sin acceso físico a la computadora, *tablet* o celular, 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.

Otro gran riesgo que vulnera nuestros datos parte muchas veces de nosotros mismos. Es fundamental que los jóvenes sean capaces de distinguir las señales de un engaño cuando 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.

La máxima atención y el mayor cuidado son requeridos cuando se trata de menores de edad, 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.

Recomendaciones respecto de Internet

Evitar medios de intercambio sin controles adecuados.

Existen espacios en Internet con medidas específicas para permitir que 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, dirección, teléfono puede implicar grandes riesgos de seguridad.

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, aun cuando supongan que mantienen el anonimato. Esto incluye rechazar videoconferencias, envío de información o fotos, descarga de archivos y, por supuesto, encuentros personales.

Algunas situaciones de riesgo pueden ser las siguientes:

- Cuando la otra persona insiste en la obtención de fotos o video.
- Cuando hay una amenaza de pérdida de interés en la conversación si no se cumple con los pedidos hechos.
- Cuando se piden de forma explícita o implícita datos personales.
- Cuando se insiste en concretar un encuentro personal, y muy especialmente se debe evitar 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 la 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 los 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 *ciberbullying*

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 *ciberbullying* 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:

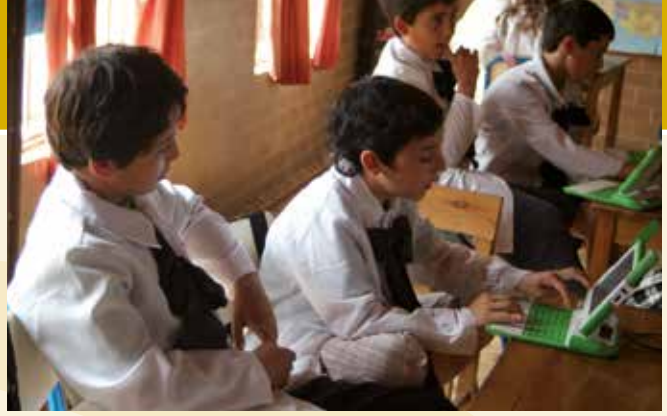
- Publicación o envío de fotografías como forma de desprecio y humillación a la persona.
- Comentarios y mensajes violentos o insultantes al celular o en redes sociales desde cuentas falsas o de forma anónima.
- Publicaciones con referencia a experiencias sexuales con una intención de humillación o burla.

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 accidental o aquel que se trata de un contenido no deseado pero en un sitio que normalmente está permitido.

Esta herramienta permite ajustar 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 uso de alcohol.
- Representación de uso de armas.
- Representación de uso de drogas.
- Representación de uso 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.

El trabajo conjunto de ANEP y la URCDP

A partir de la creciente sensibilidad acerca de la importancia de introducir la temática de Protección de Datos Personales en el ámbito educativo y formar a los niños en el conocimiento y la comprensión de su derecho y las buenas prácticas para su protección, es que desde el año 2013, ambas instituciones han desarrollado diversas actividades conjuntas entre las que destacan la capacitación a maestros de todo el país, la elaboración y difusión de una Guía didáctica para el desarrollo de actividades en clase y la realización de un concurso anual.

Para lograr el objetivo de dar a conocer el derecho y generar prácticas y habilidades en los niños, era necesario contar con socios estratégicos que reprodujeran la campaña y sus contenidos, aportando el alcance territorial, el contacto directo y la especialidad técnico-didáctica. Para ello se trabajó en conjunto con ANEP (Administración Nacional de Educación Pública), órgano rector de la educación en Uruguay.

A su vez, se sumó como socio a Ceibal, que se encarga en Uruguay de gestionar el Programa para la Conectividad Educativa de Informática Básica para el Aprendizaje en Línea (Plan Ceibal), tendiente a promover la inclusión digital para un mayor y mejor acceso a la educación y a la cultura. Y además a IMPO (Centro de Información Oficial).

Específicamente con el CEIP-ANEP definimos algunas líneas de acción que se enumeran a continuación:

1) Capacitación presencial a docentes. Para llegar a nuestro público objetivo que son los niños, necesitamos docentes capacitados y comprometidos en dar a conocer esta temática y trabajarla en cada aula del país.
2) Concurso anual donde los niños mostraban sus conocimientos sobre Datos personales mediante diversas herramientas (afiches, cómics, audiovisuales, cuentos).
3) Elaboración de materiales específicos para docentes. En conjunto con referentes técnicos de la ANEP diseñamos guías didácticas para que los docentes pudieran conocer el tema y trabajarlo en clase.
4) Capacitación en línea certificable a los docentes.
5) Colaboración a nivel estructural de ANEP, asesorando a todo el órgano sobre la aplicación de esta ley, lo cual genera un alto impacto ya que la ANEP es uno de los organismos públicos donde se maneja la mayor base de datos del Uruguay.

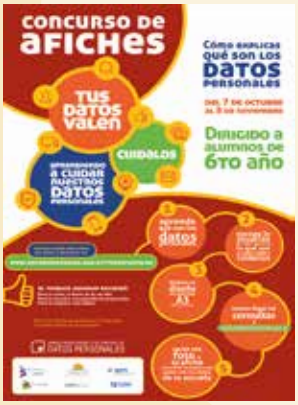
Líneas de acción

- Promoción y sensibilización de nuestros derechos.
- Formación y capacitación en todo el territorio nacional.
- Articulación y construcción de capacidades en red.

Cuatro años, cuatro concursos, miles de niños de todo el país aprendiendo a cuidar nuestros datos personales

► Concurso 2013:

"Tus datos valen. Cuídalos"



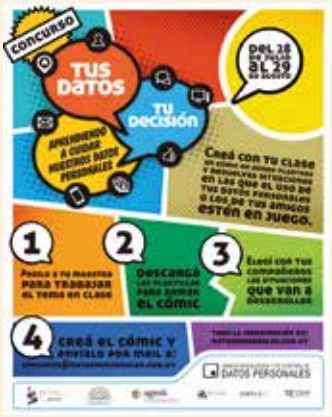
Consigna: Elaborar un afiche donde explique qué son los datos personales.

Resultados:

- 3700 alumnos participaron de la propuesta.
- 150 afiches presentados.
- Participaron 127 escuelas públicas y colegios privados de los 19 departamentos.

► Concurso 2014:

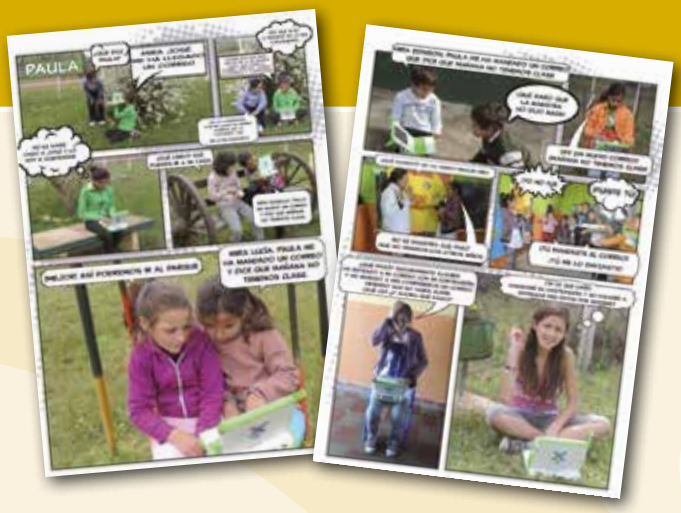
"Tus datos. Tu decisión"



Consigna: Elaborar un cómic que identifique y resuelva situaciones en las que el uso de los datos personales esté en juego.

Resultados:

- 1100 alumnos participaron de la propuesta.
- 40 cómics presentados.
- Participaron 33 escuelas públicas y colegios privados de 11 departamentos.



► Mini-Concurso

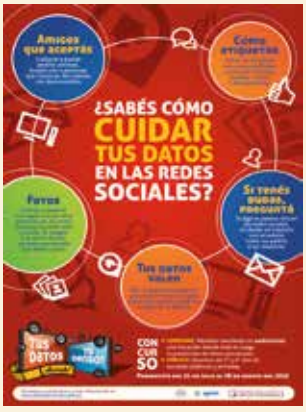
de Verano 2015
Centros CAIV de Maldonado

Consigna: Elaborar un afiche, cómic o animación que identifique situaciones en las que el uso de los datos personales esté en juego.
Resultados:

- 350 niños participaron de la propuesta.
- 160 trabajos presentados.
- Participaron 21 escuelas públicas del departamento de Maldonado.

► Concurso 2015:

"Tus datos, tu decisión. Animate"



Consigna: Elaborar un audiovisual (en dos categorías: animación, video o filmación) donde esté en juego la protección de datos personales.
Resultados:

- 900 niños participaron de la propuesta.
- 32 trabajos presentados.
- Participaron 27 escuelas y colegios del país de 12 departamentos.

► Concurso 2016:

"Tus datos cuentan"

Consigna: elaborar un cuento corto colectivo cuyo tema principal fuera la protección de los datos personales.
Resultados:

- 1860 niños participaron de la propuesta.
- 62 trabajos presentados.
- Participaron 56 escuelas y colegios del país de 14 departamentos.