Guía didáctica sobre la Protección de Datos Personales

Autor

Unidad reguladora de control de datos personales (Urcdp)

Fecha de creación

13/07/2020

Tipo de publicación

Materiales didácticos

Resumen

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.

Los datos personales y su protección

Marco legal

- 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 art. 72
- La Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data (LPDP) de 11 de agosto de 2008.
- Los Decretos N° 664/008 de 22 de diciembre de 2008 y N° 414/2009 de 31 de agosto de 2009.
- Los Arts. 152 a 156 de la Ley N° 18.719 de 27 de diciembre de 2010, que introducen modificaciones a la Ley N° 18.331. • El art. 158 literales B) y C) de la Ley N° 18.719 de 27 de diciembre de 2010, sobre intercambio de información pública o privada entre organismos públicos, estatales o no.
- El art.43 Ley N° 18.996 de 7/11/2012 sobre definición de fuentes y documentos públicos o accesibles al público.
- La Ley N° 19.030 de 12/12/2012 regula la adhesión de Uruguay alConvenio Nº 108 y su Protocolo Adicional.

Conceptos generales

Los datos sensibles

Son aquellos que revelan un origen racial o étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referidas a la vida sexual de una persona.

La Ley identifica además datos que por sus características deben ser especialmente protegidos. Toda persona no está obligada a proporcionar datos sensibles. 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.

Los datos relativos a la salud

Se trata de los datos que son tratados en los establecimientos sanitarios, públicos o privados y por los profesionales de la salud quienes, guardando el deber del secreto profesional, manejan datos personales relativos a la salud de los pacientes, de acuerdo con la legislación sanitaria y de la protección de datos. Los datos también podrán ser tratados cuando sea necesario para salvaguardar la vida del afectado o de otra persona.

Los datos relativos a las telecomunicaciones

Las personas físicas o jurídicas, públicas o privadas, que actúen en el ámbito de las telecomunicaciones, en cualquiera de sus segmentos, como titulares o responsables de un servicio, deberán garantizar la protección de los datos personales cumpliendo con las exigencias legales.

Los datos relativos a bases de datos con fines publicitarios

Consisten en datos que se tratan con el propósito de establecer perfiles determinados con fines promocionales, comerciales o publicitarios, o que permiten establecer hábitos de consumo, cuando esos datos figuren en documentos accesibles al público, hayan sido facilitados por sus titulares u obtenidos con su consentimiento.

Los datos relativos a la actividad comercial o crediticia

Está autorizado el tratamiento de datos destinados a informar sobre la solvencia patrimonial o crediticia, cuando los mismos sean obtenidos de fuentes de acceso público o procedan de informaciones facilitadas por el acreedor o en las circunstancias previstas en la Ley. Para el caso de las personas jurídicas (empresas u organizaciones) también se permite el tratamiento de toda información autorizada por la normativa vigente.

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.

Reservado. 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.

Sobre la Ley

Datos personales: ¿por qué la Ley los protege?

A diario empresas, organismos públicos y particulares manejan información personal para fines 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.

¿Cuál es su alcance?

La Ley 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.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).

¿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 sólo 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.

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.
- Oponerse 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.

Toda persona tiene derecho a presentarse ante el responsable de una base de datos, pública o privada, para conocer qué datos se poseen sobre ella, la finalidad y el uso que se le dan a éstos y si se ha vulnerado alguno de sus derechos. También podrá denunciar la recepción de publicidad no deseada o consultar gratuitamente el Registro de base de datos de la URCDP.

Si su reclamo es desoído puede recurrir a la justicia mediante una acción de Habeas Data o denunciar la situación ante la URCDP personalmente o mediante su sitio web: https://www.gub.uy/unidad-reguladora-control-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 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 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 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. 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.

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 cuidado es requerida 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.

Tres consejos simples para cuidar nuestra privacidad en PC de uso compartido:

- Siempre recordar 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 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 situaciones de riesgo
- 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 cumplen con los pedidos hechos.
- Cuando se pide 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 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 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. Las mismas 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.

Propuestas didácticas

Propósito y entorno de aplicación

Dar a conocer a través de una campaña de comunicación dirigida a niños que cursan los últimos años escolares, lo que son los datos personales, la importancia de cuidarse a la hora de brindarlos y que existe una ley y una Unidad Reguladora y de Control de Datos Personales (URCDP) que garantiza su protección.

Mediante estas propuestas didácticas se pretende que los niños reconozcan sus datos personales y el derecho a su protección. A su vez, que sean capaces de desarrollar una conducta responsable al respecto.

Las actividades se vinculan con los contenidos del Programa Escolar y podrán ser utilizadas para trabajar, en forma complementaria, los objetivos propuestos desde diferentes áreas del conocimiento, tales como:

- Área del Conocimiento de Lengua (argumentación, debate, texto argumentativo oral).
- Área del Conocimiento Social - Construcción de la ciudadanía (derechos).
- Área de Conocimiento Artístico - Artes Visuales (confección de un afiche colectivo).

Objetivos de la propuesta:

- Sensibilizar sobre la temática, a través de una actividad didáctica.
- Brindar elementos para comprender la importancia del cuidado de los datos personales.
- Generar espacios para discutir sobre la temática tanto en el ámbito escolar como en el ámbito familiar.
- Aproximarse al conocimiento de la protección de datos siendo capaces de replicar y enseñar a otros a cuidar los datos personales.

Secuencia didáctica

Se propone trabajar en una secuencia compuesta por 5 módulos. Cada maestro decidirá cómo y cuántos aplicar.

	Secuencia	
Módulo 1	Exploración de ideas previas	Puesta en común: identificación de los datos personales con los que vamos a trabajar.
Módulo 2	Subgrupos: • Enfrentar situación • Análisis de distitos puntos de vista • Argumentación • Toma de desiciones	Plenario: • Exponer (representar situación) • Argumentar • Evaluar • Conclusión (exposición del maestro)
Módulo 3	Subgrupos: • Enfrentar situación • Análisis de distitos puntos de vista • Argumentación • Toma de desiciones	Plenario: • Exponer (representar situación) • Argumentar • Evaluar • Conclusión (exposición del maestro)
Módulo 4	Subgrupos: • Enfrentar situación • Análisis de distitos puntos de vista • Argumentación • Toma de desiciones	Plenario: • Exponer (representar situación) • Argumentar • Evaluar • Conclusión (exposición del maestro)

Módulo 5	Subgrupos: • Seleccionar algunos datos personales • Ejemplificar	Plenario: • Creación de una cartelera colectiva

Propuestas didácticas para trabajar el tema Datos Personales

Módulo 1:

La intención de este módulo es que, mediante la técnica seleccionada por cada docente (como ejemplo se señala la tormenta de ideas), se indague sobre el conocimiento de la clase acerca del significado de los datos personales y la posibilidad de identificarlos. La idea es registrar todo lo que surja de la clase y guiar, si hace falta, la introducción a aquellos datos personales que no hayan sido identificados por los alumnos.

Una vez listado los datos personales, trabajar sobre la diferenciación entre datos personales y*datos personales sensibles que son aquellos que revelan un origen racial o étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical, información sobre la salud o referida a la vida sexual de una persona.*

Posteriormente, contar que se seleccionarán algunos datos de todo el listado para desarrollar la actividad. Sin pretender brindar un listado completo de todos los datos personales, se presentan algunos ejemplos que complementan la información: nombre y apellido, dirección, teléfono, cédula de identidad, imagen, voz, huella dactilar, ADN, nacionalidad, fecha de nacimiento, estado civil, edad, altura, salud, religión, origen étnico, listado de clases, correos electrónicos, contraseñas, listado de compañeros, celular, concurrencia a clase, orientación sexual, opiniones políticas, firma.

Módulos 2, 3 y 4:

- Formar equipos. La cantidad de equipos dependerá de las características de cada clase.
- A cada equipo se le reparten las consignas (ya que cada una representa a un Dato Personal).
- Frente a cada situación, cada equipo discute acerca de cuál sería la respuesta correcta.
- Argumentan y registran la justificación.
- Deciden si, en cada una de esas situaciones, es adecuado entregar ese dato personal.
- Designan un representante por equipo Plenario: para exponer la respuesta en plenario.
- Un representante de cada equipo expone la argumentación que desarrolló su equipo para responder a cada una de las situaciones planteadas.
- El docente lee la respuesta esperada, elaborada por la URCDP.
- Entre todos los integrantes de la clase se evalúa cuánto se acerca la respuesta de cada equipo a la respuesta esperada.

Consignas para cada módulo y respuestas adecuadas

Se trata de situaciones a resolver. Analizar cómo corresponde resolverlas en cada caso y evaluar la pertinencia de entregar o no el Dato Personal solicitado.

Recordar que los niños a esta edad siempre deben estar asistidos y obtener el permiso de sus padres o tutores en el momento de brindar un dato sobre sí mismo, su familia o un tercero.

Módulo 2, aprendiendo a cuidar nuestros Datos Personales:

Situación planteada

• Una persona que no conocemos llama por teléfono y pregunta qué familia es… (Decidir si es pertinente/ adecuado darle el Dato Personal –nombre-).

Respuesta esperada

Le decimos que espere un momento y le pasamos la llamada a un adulto. Si bien el apellido (nombre de la familia) es un dato personal que no necesita permiso para brindarse, es mejor que cuando se trata de un desconocido hable directamente con nuestros padres o con el adulto que se encuentra a cargo de nosotros.

Situación planteada

Una empresa pide tu cédula de identidad para un sorteo…(Decidir si es pertinente/ adecuado darle el Dato Personal –CI-).

Respuesta esperada

No es adecuado porque en general los niños deben estar asistidos por los padres o tutores para participar de un sorteo. Sobre todo para brindar sus datos a los desconocidos. Por ello es muy importante estar preparados para el cuidado y protección de los datos personales, especialmente cuando éstos son solicitados por desconocidos.

Situación planteada

Un compañero de clase decide armar una agenda con información de toda la clase y quiere saber tu dirección…(Decidir si es pertinente/ adecuado darle el Dato Personal –dirección-).

Respuesta esperada

Se debe preguntar al compañero para qué quiere armar la agenda, luego conversar con los padres o tutores para ver si se lo puede dar o no.

Situación planteada

Una red social nos pide que ampliemos la información y pongamos el teléfono…(Decidir si es pertinente/ adecuado darle el Dato Personal –teléfono-).

Respuesta esperada

Para tener una red social se necesita el permiso de los padres o tutores, al igual que para agregar información solicitada por ella. Tienen que tener en cuenta que el teléfono es un dato que necesita la autorización de su titular.

Situación planteada

Para descargar un juego, nos piden el correo electrónico…(Decidir si es pertinente/ adecuado darle el Dato Personal –correo electrónico-).

Respuesta esperada

Cuando se entra al sitio web debe surgir que se va a necesitar correo electrónico para bajar juegos. En el momento de hacerlo se deberá pedir asistencia y autorización a los padres o tutores para agregar el correo porque es un dato personal que necesita el permiso del titular.

Situación planteada

Para un concurso nos piden que subamos una foto de nosotros a una red social…(Decidir si es pertinente/ adecuado darle el Dato Personal –imagen-).

Respuesta esperada

La foto es un dato personal y por lo tanto se necesita la autorización de sus padres o tutores para subir la imagen.

Situación planteada

Estamos en una Escuela Rural y hay que armar un botiquín que es muy importante porque el hospital queda a kilómetros. Para eso le piden información a los padres sobre las alergias de los alumnos para tener en cuenta a la hora de armarlo…(Decidir si es pertinente/ adecuado darle el Dato Personal Sensible –Salud-).

Respuesta esperada

No hay inconveniente en que la escuela solicite a los padres o tutores, información sobre la salud de los niños. Hay que tener presente que es parte de las funciones de la escuela el velar por la salud de los niños mientras permanecen en ella.

Módulo 3, conociendo quiénes deben tener nuestros Datos Personales:

Situación planteada

• Un padre le pide a la directora una lista con todos los nombres y teléfonos de los alumnos para invitarlos a un cumpleaños… (Decidir si es pertinente/ adecuado que la Directora de los Datos Personales – nombre y teléfono-).

Respuesta esperada

La dirección de la escuela deberá enviar un comunicado a todos los padres solicitando la autorización para comunicar los nombres y teléfonos de los alumnos. Si bien el nombre es un dato que no necesita el consentimiento, el teléfono sí lo necesita. También podría recabarlo en una reunión de padres. En ambos casos debe quedar documentado.

Situación planteada

¡La clase participó en un concurso y ganó! La lista de ganadores es publicada en Internet con los números de cédula…(Decidir si es pertinente/ adecuado que la escuela publique los Datos Personales – CI-).

Respuesta esperada

Este listado se puede colgar en Internet para anunciar a los ganadores del concurso, porque la cédula de identidad y el nombre en listados son datos que no necesitan autorización para ser difundidos o comunicados. Si necesitará el consentimiento de padres o tutores si el listado se utiliza para una finalidad diferente.

Situación planteada

Un vendedor de libros que vino a la escuela le pide a la escuela el teléfono de la casa de los alumnos que se interesaron en los libros para ofrecérselos a sus padres…(Decidir si es pertinente/ adecuado que la escuela de los Datos Personales – teléfono-).

Respuesta esperada

La escuela deberá recabar el consentimiento de los padres o tutores de los niños, utilizando alguna forma de comunicación, ya sea mediante una reunión o el cuaderno de comunicaciones.

Situación planteada

Recibimos un correo de la escuela donde estaban todos los alumnos copiados. Luego un padre envía a todas esas direcciones una promoción de su empresa. ¿Está bien lo que hicieron la escuela y el padre?... (Decidir si es pertinente/ adecuado que la escuela y el padre den los Datos Personales – correo electrónico-).

Respuesta esperada

La escuela debió enviar el correo con las direcciones de correo electrónico ocultas, porque este es un dato que requiere la autorización del titular para poder ser entregado a otra persona.

El padre no debió usar esa lista de correos para una finalidad diferente para la que lo envió la escuela, que era comunicarse con los padres.

Situación planteada

Vinieron a la escuela de la televisión y nos hicieron entrevistas a los alumnos. ¿Habría que hacer algo más antes de que las entrevistas salgan en la tele?... (Decidir si es pertinente/ adecuado dar el Dato Personal – imagen-).

Respuesta esperada

La escuela debe informar a los padres o tutores que los alumnos van a ser entrevistados, sobre qué trata la entrevista y sobre todo, que van a salir en la televisión. Luego de ser informados y de obtener el consentimiento, los niños podrán ser filmados y sus imágenes podrán salir en la Televisión. Hay que recordar que nuestra imagen es un dato personal.

Si los padres o tutores no dieron su autorización deben sacar la imagen de ese alumno o mostrarla de forma borrosa (pixelarla) para que no se pueda identificar al niño.

Situación planteada

El guardavidas de la piscina del gimnasio o del club está preocupado porque uno de los niños tiene problemas de salud y no debería ir a la piscina. Por esa razón solicita ver los carné de salud de todos. (Decidir si es pertinente/ adecuado dar el Dato Personal –Salud-) (podríamos cambiarle la enfermedad, sería igual la respuesta)

Respuesta esperada

El presidente del club debe exigir que todos los niños tengan el carné de salud al día para poder ir a la piscina, pero no debe entregar esta documentación al guardavidas, ya que los datos que se encuentran en él son datos sensibles, especialmente protegidos, que necesitan la autorización para ser divulgados. Sí podría darlos si hay una epidemia y ello es necesario para colaborar con su control.

Módulo 4, aprendiendo a cuidar los Datos de tus amigos:

Situación planteada

Tus padres quieren saber los nombres de tus compañeros de clase… (Decidir si es pertinente/ adecuado darles los Datos Personales –nombre-).

Respuesta esperada

Está bien que se los digas porque en el caso de los nombres, si bien son datos personales, no necesitas el consentimiento de los titulares para poder comunicarlos a otras personas.

Situación planteada

Encontraste una cédula de identidad perdida, ¿la ponés en la cartelera para que el dueño la vea o harías otra cosa?... (Decidir si es pertinente/ adecuado publicar el Dato Personal –CI-).

Respuesta esperada

Se debe entregar a la maestra para que disponga lo necesario para encontrar a su titular y devolverla, porque si la dejas en la cartelera esos datos estarían expuestos y se pueden tomar con otra finalidad que no es la de encontrar a la persona.

Situación planteada

Una persona en Facebook dice que es el tío de uno de tus amigos y que no se acuerda dónde vive su sobrino ¿le daríamos la dirección?... (Decidir si es pertinente/ adecuado darle el Dato Personal –dirección-).

Respuesta esperada

No debes darle la dirección, es un desconocido. Necesitamos la autorización de tu amigo para darle el dato. Recuerda que en las redes sociales no se deben dar datos de tus amigos ni tuyos, a desconocidos sin permiso de los padres.

Situación planteada

Un compañero de clase te pide el teléfono de otro compañero de clase. ¿Se lo damos?... (Decidir si es pertinente/ adecuado darle el Dato Personal –teléfono-).

Respuesta esperada

No debes dárselo sin la autorización de tu compañero. Primero debes consultarlo.

Situación planteada

Te anotaste en un sorteo y te ofrecen más chances de ganar si anotás las direcciones de correo de tres amigos. ¿Deberías hacerlo?... (Decidir si es pertinente/ adecuado darle los Datos Personales –correo electrónico-).

Respuesta esperada

No, porque los correos electrónicos son datos que necesitan la autorización de su titular por lo que es necesario consultarlos para que den su consentimiento previo permiso de sus padres o tutores.

Situación planteada

Tenés unas fotos super divertidas de tus amigos, ¿tendrías que tener algo en cuenta antes de subirlas a una red social?... (Decidir si es pertinente/ adecuado publicar el Dato Personal –imagen-).

Respuesta esperada

Sí, debes consultar a tus amigos y a sus padres o tutores para que den el consentimiento, además configurar en la red la privacidad para que solo lo vean tus amigos. Tienes que decirles a ellos que hagan lo mismo con su privacidad para que la imagen, que es un dato personal, no se difunda por la red a personas desconocidas.

Situación planteada

Un amigo está enfermo y querés saber cómo está. Por casualidad el doctor que lo atendió es tu tío. ¿Está bien que le preguntes por tu amigo?... (Decidir si es pertinente/ adecuado conocer el Dato Personal –Salud-).

Respuesta planteada

Si, puedes preguntarle a tu tío por la salud de tu amigo. El responsable de guardar los datos de salud de tu amigo es tu tío, por lo que no debe dar detalles de su enfermedad, ya que son datos sensibles que deben ser cuidados con mayor seguridad y para divulgarlos se necesita el consentimiento de los padres o tutores de tu amigo.

Módulo 5, creando una cartelera sobre Protección de Datos:

Cada equipo trabajará sobre uno o dos Datos Personales propuestos en la actividad y deberán plantear situaciones en las que ese dato se vea afectado. La clase deberá crear en forma conjunta una cartelera que permita transmitir a la Escuela qué son los Datos Personales utilizando las situaciones desarrolladas por cada equipo.

Aclaraciones:

Están disponibles espacios de comunicación con la URCDP para plantear consultas o dudas.

Teléfono de consultas: 2901 00 65 interno 3

infourcdp@datospersonales.gub.uy

Propuestas didácticas para trabajar los datos de naturaleza sensible

Datos de naturaleza sensible

Hay ciertos datos personales que se consideran de naturaleza sensible porque describen los aspectos más cercanos o delicados de una persona y que pertenecen a su esfera más intangible, razón por la cual nadie está obligado a proporcionarlos y sólo pueden ser objeto de tratamiento con el consentimiento expreso y escrito de su titular, salvo la existencia de razones de interés general establecidas por ley. Se trata de datos que, de divulgarse de manera indebida, afectarían la esfera más íntima del ser humano. Estos datos son los que revelen el origen racial o étnico, las preferencias políticas, las convicciones religiosas o morales, la afiliación sindical y las informaciones referentes a la salud o la vida sexual. La escuela o el colegio son ámbitos en los cuales se tratan datos personales de los niños que muchas veces pueden ser de naturaleza sensible. Por ello, estas instituciones y quienes trabajan en ellas deben cumplir con la normativa en materia de protección de datos personales.

Cuando te pidan información personal te tienen que avisar *para qué* la quieren; si no lo hacen, pregúntales para qué la necesitan.

Preguntar por un dato sensible es una situación de incomodidad. No insistas para que te den un dato sensible, cada persona por mas amigo que sea, tiene derecho a preservarlo.

Situación planteada

Si una persona llama por teléfono a tu casa y te pregunta qué vota tu papá, mamá o tutor ¿qué haces?

Respuesta esperada

Le decimos que aguarde un momento y llamamos a un adulto. Las preferencias políticas son un dato sensible y requieren el consentimiento de tu papá, mamá o tutor.

Situación planteada

En la clase estamos estudiando las religiones y la maestra me pregunta qué religión tiene mi familia. ¿Puedo negarme?

Respuesta esperada

Sí, por que nadie está obligado a proporcionar datos de naturaleza sensible.

Situación planteada

En la escuela estamos armando un botiquín. ¿La maestra puede preguntarnos si somos alérgicos a algún medicamento?

Respuesta esperada

No hay problema en que la maestra recabe ese dato para garantizar nuestra salud mientras estamos en la escuela. Pero debe pedirlos nuestro papá, mamá o tutor.

Situación planteada

En una entrevista para postular a un trabajo nos preguntan cuál es nuestra religión. ¿Podemos negarnos a dar esa información?

Respuesta esperada

Sí, nadie está obligado a proporcionar datos de naturaleza sensible.

Imagen

Los datos personales son aquellos que nos identifican o nos hacen identificables, por lo tanto, nuestra imagen también es un dato personal, que merece ser protegido. Por ello, es importante que seamos responsables respecto al manejo de nuestra imagen y la de los demás. Esto interesa también a las instituciones que trabajan directamente con los niños, jóvenes y sus familias, ya que, en su actividad y en las publicaciones que pudiera difundir, puede registrar o publicar imágenes de menores. Por ello, deben pedir consentimiento expreso (escrito) a los padres y madres o tutores legales para tomar imágenes de sus hijos/hijas y especificar claramente el uso y el tipo de divulgación de que pueden ser objeto.

Situación planteada

La maestra crea un blog abierto de la escuela con fotos de los niños y las actividades que realizan. ¿Está bien?

Respuesta esperada

Para ello debe pedir consentimiento por escrito a los padres o tutores. La foto es un dato personal y por lo tanto se necesita la autorización de papá, mamá o tutor a cargo para subir la imagen.

Situación planteada

¿Puedo grabar a mis compañeros con la XO?

Respuesta esperada

Sí, pero debes avisarles que los vas a grabar. Debes ser cuidadoso en el uso que hagas de esas imágenes una vez que las tengas.

Situación planteada

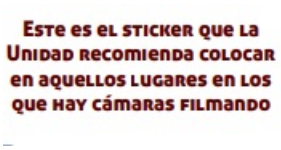
Vinieron a la escuela de la televisión y nos hicieron entrevistas. ¿Hay que hacer algo antes de que las entrevistas salgan en la tele?

Respuesta esperada

Sí. La escuela debe informar a papá, mamá o tutor que los alumnos van a ser entrevistados, sobre qué trata la entrevista y sobre todo, que van a salir en la televisión. Luego de ser informados y de obtener el consentimiento (por escrito), los niños podrán ser filmados y sus imágenes podrán televisarse. Si papá, mamá o tutor no dieron su autorización deben sacar la imagen de ese alumno o mostrarla de forma borrosa (pixelarla) para que no se pueda identificar al niño.

Videovigilancia

Puede definirse la videovigilancia como toda grabación, captación, transmisión, conservación y almacenamiento de imágenes y en algunos casos de sonidos mediante la utilización de videocámaras u otro medio análogo. Esta información es considerada personal y sus finalidades refieren a la protección de las personas físicas, la propiedad, el interés público, así como la detección y prevención de delitos, entre otros intereses legítimos. En este tema se deben aplicar los principios de la protección de datos, y se deben garantizar los derechos establecidos en la Ley así como cumplir las obligaciones que se encuentran consignadas en ella.



Situación planteada

En el Supermercado que hay cerca de la Escuela, hay un sticker que dice que me están filmando. ¿Está bien?

Respuesta esperada

Si entrás a un lugar que tiene cámaras es correcto que te avisen que te están filmando por que están captando tu imagen.

Recomendaciones para aplicar en redes sociales

- Aceptá solamente a gente que conozcas.
- No intercambies información personal, contraseñas o datos de tu familia con desconocidos ni los subas a sitios públicos. En Internet cualquiera puede hacerse pasar por otro. Compartí con tus padres o alguien mayor en quien confíes, cualquier duda o situación que te parezca extraña. Utilizá las etiquetas de manera positiva. Nunca para insultar, humillar o dañar a otras personas.
- Pregúntate qué información de otras personas expones y asegúrate de que no les importa.
- Para etiquetar a otras personas debes asegurarte de que no les molesta que lo hagas.
- Como regla general no publiques fotos o videos en las que salgan otras personas sin tener su permiso.

Red Conceptual

- **DDHH**
  - Posicionamiento
  - Discurso
    - Juicios
    - Argumentos
- **Democracia**
  - Acuerdos / Desacuerdos
  - Participación
  - Conflictos
  - Relaciones de poder
    - Igualdad / Desigualdad
    - Libertad / Opresión
    - Justicia / Injusticia
    - Identidad / Alteridad
- **Convivencia**
- **Cultura/s**
  - Moral/es
  - Sociedad/es
  - Tradiciones
  - Creencias
  - Estereotipos culturales
  - Géneros
  - Etnias
  - Clases
  - Mitos
  - Valores
- **Diversidad**
- **Ciudadanía**

DATOS PERSONALES

Selección de Contenidos

Área del Conocimiento de Lengua

Oralidad
Quinto año
Los debates en distintas situaciones sociales.
Sexto año
El debate. Los roles de los participantes. Los mensajes y las conclusiones implícitas y explícitas.

Lectura
Quinto año
Lectura hipermedial.

Escritura
Cuarto año
Los diferentes modos de organización de la información. las abreviaturas y las siglas.
Quinto año
La organización del texto argumentativo.
Sexto año
La jerarquización de los argumentos en los textos de opinión.
Los modelos de archivos de organización personal de la información: El Esquema

Área del Conocimiento Artístico

Artes visuales
Quinto año
La creación de imágenes a través de cartel usando soporte material y/o digital.
Sexto año
La persuasión de la imagen en propaganda.

Expresión corporal
Sexto año
La representación de escenarios sociales imaginados.

Área del Conocimiento Social

Historia
Sexto año
La vigencia de la Constitución y los derechos individuales.
EMERGENTES:
- Protección de datos personales amparados en la Constitución: Artículo 72
- Derechos del niño y el adolescente: 20 de noviembre día internacional de los Derechos del niño

Construcción de la ciudadanía
Derecho
Segundo año
El derecho a la integridad física y moral. El derecho a la intimidad.
Tercer año
El derecho a la protección social. El marco Legal para la seguridad ciudadana en el hogar y en la comunidad.
Ética
Sexto año
Los derechos humanos como conquista. Derechos de los Estados y su compromiso con el cumplimiento de los derechos.
Los derechos, deberes y garantías en el Sistema Jurídico

DATOS PERSONALES


Ley 18.331
del 11/08/08
Protección de Datos Personales
Especial protección
• Datos sensibles
• Datos relativos a la salud
• Datos relativos a las telecomunicaciones
• Datos relativos a bases de datos con fines publicitarios
• Datos relativos a la actividad comercial o crediticia
PDP
Es un DERECHO con el que se nace, es "inherente a la persona humana"
Tus datos valen
• Tu nombre. Tu apellido
• Lo que chateas
• Tus Fotos
• Tu dirección
• Tu mail
• Tu celular
• Tu perfil en las Redes Sociales
Principios
• Legalidad
• Veracidad
• Finalidad
• Previo consentimiento informado
• Seguridad
• Reserva
• Confidencialidad
Creación de URCDP
UNIDAD REGULADORA Y CONTROL DE DATOS PERSONALES
Garantiza el cumplimiento de lo establecido en la Ley sobre tratamiento de datos.
Derechos sobre datos personales
• Derecho a acceso
• Derecho a rectificación y actualización
• Derecho a supresión
• Derecho a inclusión
24/04/09
Asume Consejo Ejecutivo de URCDP
COMETIDOS
• Asesorar al Poder Ejecutivo
• Informar sobre el alcance y los mecanismos de defensa previstos en la ley
• Autorizar las transferencias de datos personales a países sin niveles de protección adecuada en la materia
• Inspeccionar entidades Públicas y privadas en relación con los datos personales
• Sancionar infracciones según el marco jurídico existente en materia de PDP.
Derecho gratuito
Plazo de 5 días hábiles a partir de que el titular solicitó ejercer alguno de los derechos
UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES


TUS DATOS VALEN
CUIDALOS
APRENDIENDO A CUIDAR NUESTROS DATOS PERSONALES
Protección de Datos Personales
Basados en la
Constitución
y garantizados por
Derechos del niño y del adolescente
implican
Derecho a la protección social
suponen
Derecho a la intimidad
Derechos como conquista
son
Garantizados por el sistema Jurídico
sensibilización a través de
La actividad lúdica
Representación de escenarios sociales imaginados
El debate
La lectura hipermedial
Replicándolos con
Creación de un cartel
UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Glosario

- **Base de datos:** es el conjunto organizado de datos personales que son objeto de tratamiento o procesamiento, en forma electrónica o no, cualquiera sea la característica por la cual se forma, almacena, organiza o accede.
- **Bloqueo de datos:** procedimiento por el cual los datos son reservados con el fin de impedir su tratamiento, con la excepción que pueden ser puestos a disposición de los Poderes del Estado, de instituciones que estén legalmente habilitadas, a los efectos de estar pendiente de las posibles responsabilidades que puedan surgir del tratamiento.
- **Cancelación o Supresión de datos:** procedimiento mediante el cual el responsable de la base de datos detiene el uso de los datos. La supresión o cancelación reservará los datos con el fin de impedir su durante el plazo establecido en la normativa vigente, vencido éste se deberá proceder a su eliminación definitiva.
- **Cesión de datos o comunicación de datos:** es toda revelación de datos realizada a una persona distinta del titular de los datos.
- **Consentimiento del titular:** toda manifestación de voluntad del titular del dato realizada de forma libre, inequívoca, específica e informada, mediante la cual apruebe el tratamiento de datos personales que le pertenece.
- **Dato personal:** es toda información referida a personas físicas o jurídicas determinadas o que puedan ser determinadas.
- **Dato sensible:** es toda información referida a persona físicas o jurídicas determinadas o que puedan ser determinadas, que manifiesten el origen racial y étnico, sus preferencias políticas, sus creencias religiosas o morales, su afiliación sindical y toda información que se refiera a la salud o a la vida sexual.
- **Dato personal relacionado con la salud:** son las informaciones concernientes a la salud pasada, presente y futura, física o mental, de una persona. Entre otros, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad o a su información genética.
- **Destinatario:** es la persona física o jurídica, pública o privada, que recibe comunicación de datos, se trate o no de un tercero.
- **Disociación de datos:** todo tratamiento de datos personales de manera que la información obtenida no pueda ser vinculada a una persona determinada o que pueda ser determinada.
- **Encargado del tratamiento:** persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento.
- **Exportador de datos personales:** la persona física o jurídica, pública o privada, situada en territorio uruguayo que realice, una transferencia de datos de carácter personal a otro país.
- **Fuentes accesibles al público:** aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin norma que lo impida o con el pago de una contraprestación.
- **Importador de datos personales:** la persona física o jurídica, pública o privada, que reciba datos de otro país, cuando se realice una transferencia internacional de éstos, ya sea responsable o encargado del tratamiento, o tercero.
- **Interesado o titular del dato:** es la persona cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la ley de protección de datos.
- **Responsable de la base de datos o del tratamiento:** es la persona física o jurídica, pública o privada, que es la propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.
- **Transferencia internacional de datos:** es cuando se realiza el tratamiento de los datos enviándolos fuera del territorio nacional, constituyendo una cesión o comunicación, y teniendo por objeto la realización de un tratamiento por cuenta del responsable de la base de datos o tratamiento establecido en territorio uruguayo.
- **Tratamiento de datos:** es la realización de operaciones y procedimientos ordenados, de forma automatizada o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.
- **Usuario de datos:** toda persona, pública o privada, que realice a su saber y entender el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos.