



20
13

 UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

**Memoria
Anual
URCDP**





20
13

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

**Memoria
Anual
URCDP**

Índice

Prólogo Presidente de la URCDP

1. Campaña Nacional de Protección de Datos Personales “Tus datos valen. Cúdalos”

Tema: Los menores y las redes sociales

2. Principales temas analizados en el año 2013

Video vigilancia

Datos personales contenidos en Certificados de Defunción

Comunicación de datos personales

Sistema de referencias empresariales

Procedencia de la inscripción de una base de datos creada y regulada por ley y reglamento especial

Inclusión del diagnóstico del paciente en los certificados médicos que justifican ausencias por enfermedad

Alcance de los términos “listado” y “medios” utilizados en el artículo 9° literal C) de la Ley N° 18.331, y el literal B) del artículo 3° del Decreto N° 414/009, de 31 de agosto de 2009

Confidencialidad de datos personales

3. Avances de la normativa en protección de datos personales

Nacional

Ley N° 19.149, de 24 de octubre de 2013, artículo 45. Rendición de Cuentas y Balance de Ejecución Presupuestal Ejercicio 2012.

Internacional

Decreto Supremo N° 003-2013-JUS, de 21 de marzo de 2013, por el que se aprueba el Reglamento de la Ley N° 29.733, de Protección de Datos Personales de la República del Perú

Decreto N° 1377, de 27 de junio de 2013, por el cual se reglamenta la Ley N° 1581 de 2012 de la República de Colombia

Ley N° 172-13, de 26 de noviembre de 2013, sobre Protección de Datos de carácter personal, de la República Dominicana.

4. Jurisprudencia

Nacional

Internacional

5. Presentación de la Memoria 2012

6. Difusión y capacitación de la Unidad Reguladora y de Control de Datos Personales

Sitio web

Campaña Tus Datos Valen. Cúdalos.

Atención de consultas personalizadas.

Difusión en los medios

Relacionamiento internacional

Charlas impartidas en el año 2013

7. La URCDP en cifras

Registro de Bases de Datos según tipo de responsable

Distribución territorial

Datos sensibles

Transferencias internacionales

Tipos de información según su finalidad

Cesiones o comunicaciones de datos

Tipo de soporte de registro de bases de datos

Códigos de conducta

Bases de datos inscriptas en la URCDP

Cantidad de visitas al sitio web de la URCDP

Consultas a la mesa de ayuda de la URCDP

Expedientes presentados por consultas y denuncias

Resoluciones con sanción en 2013

Resoluciones y dictámenes realizados en 2013

Cantidad de informes realizados

8. La URCDP ante los nuevos retos en materia de protección de datos

Proyectos a realizar en el año 2014

Anexo Normativo

Prólogo del Presidente de la URCDP

La memoria anual que se presenta corresponde al año 2013. Un año que nos ha permitido concretar algunas expectativas albergadas desde el inicio de nuestra actividad como miembros del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales, en 2009.

Toda memoria anual requiere efectuar un balance de lo acontecido en el año, para dar cuenta a la población de las principales actividades desarrolladas. Pero como no hay un ¿dónde estamos?, sin antes preguntarnos ¿de dónde venimos?, no podemos prescindir de lo actuado en años anteriores.

Resulta difícil comparar el desempeño de 2013 con el alcanzado en el año 2012 que, tal como se reseña en el prólogo de la memoria anual de dicho año, alcanzó un cúmulo de sucesos de orden mayor, como haber alcanzado la declaración por parte de la Unión Europea de país adecuado en protección de datos en los términos de la Directiva 95/46/CE; haber ratificado el Convenio 108 del Consejo de Europa, que convirtió a nuestro país en el primero fuera del ámbito europeo; y haber sido país anfitrión para la realización de la exitosa 34ª Conferencia Internacional de Autoridades de Privacidad y Protección de Datos.

Sin embargo, la importancia de los tiempos de lo global no deben alejar nuestra atención de lo local, nuestro principal ámbito de acción. En tal sentido, el año 2013 tuvo como eje de desarrollo de la Unidad, el acercamiento con la población, para difundir y dar a conocer los derechos que se desprenden de la normativa vigente en protección de datos personales.

En particular debemos destacar el acercamiento con la población infantil, niñas y niños que son el Uruguay del mañana. Pero como no hay futuro sin presente, nuestra Unidad trabajó junto a educadores de CEIP, del Proyecto Gurí y del Plan Ceibal para elaborar la campaña formativa “Tus datos valen” dirigida a alumnos de sexto año de escuela.

Los resultados fueron formidables, tanto por el entusiasmo contagioso de los más pequeños, como de docentes y familiares, como por lo fermental de su trabajo. ¡Cuánto hemos aprendido! Es una renovada constatación que mejor forma de crecer y cultivar es ir a las raíces, en este caso escolares de sexto año, y muy especialmente en materia de derechos humanos.

Con estas palabras alentadoras, los invito a recorrer en detalle la memoria anual 2013 que sigue.

*Mag. Federico Monteverde
Presidente URCDP*



01

**Campaña Nacional
de Protección de
Datos Personales
"Tus datos valen. Cuidalos"**

"Tus datos valen. Cuidalos."
Datos Personales
de Protección de
Campaña Nacional

1. Campaña Nacional de Protección de Datos Personales "Tus datos valen. Cuidalos"

En la actualidad sensibilizar sobre la protección de los datos personales en Internet es clave y más aún a los niños que se encuentran expuestos a posibles peligros ocasionados por terceros. Por ello, el objetivo de esta primera campaña fue sensibilizar y capacitar a niños y niñas de 6° año de escuelas públicas y privadas de todo el país, sus maestros y familias, sobre la importancia que tiene el cuidado y la protección de los datos personales.

Para poder orientar a maestros y escolares sobre la temática referida, la Unidad Reguladora y de Control de Datos Personales (URCDP) generó un kit de materiales que incluyó un afiche, stickers y folletos para cada niño, una guía para el maestro, con una propuesta de actividad didáctica para trabajar la importancia que tienen los datos personales, y material para el uso de las carteleras en clase.

La campaña contó, además, con un concurso denominado "Cómo explicas qué son los datos personales". La consigna implicó la elaboración de un afiche por parte de los escolares, que tuviese como eje la protección de datos personales.

Asimismo se generó una sección en el sitio web de la Unidad con información relativa a la Campaña. También se crearon banners que fueron pautados en medios digitales, y se realizó una animación audiovisual que fue difundida en la pantalla de IMPO y en el canal Youtube.

La campaña nacional de Protección de Datos se convirtió en un aporte fundamental para que los niños, sus familias y los educadores conozcan y aprendan a cuidar adecuadamente tanto sus datos personales, como los de otras personas.

Esta campaña fue una iniciativa de la URCDP y contó con el apoyo de la Presidencia de República, el Consejo de Educación Inicial y Primaria (CEIP), el Plan Ceibal, la Dirección Nacional de Impresiones y Publicaciones Oficiales (IMPO), y la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC).



Tema: Los menores y las redes sociales

Desde hace unos años somos parte las redes sociales, fenómeno que potencia la socialización y genera relaciones de diferente índole - de amistad, académicas, empresariales, entre otras- en las que pueden intervenir tanto menores como mayores.

Se puede pensar que las redes sociales hacen que las personas, - ya sea en forma colectiva o individual -, transiten por las etapas de socialización que Peter Berger y Thomas Luckmann aplican a la socialización en general. Estas etapas se contemplan desde que el individuo comienza el proceso en el que se internaliza en la sociedad (socialización primaria), hasta que logra llegar a conocer los roles que ocupa en ella (socialización secundaria)¹.

Dentro de esta internalización que realizan los niños y adolescentes, la familia debería jugar un rol importante para que asimilen claramente los conceptos y puedan proteger su integridad y su privacidad, rol que no se cumple habitualmente, ya que la mayoría de las veces no se tiene conocimiento de cómo actúa el individuo dentro de ese "mundo paralelo". Mundo paralelo que de acuerdo con el Grupo de Trabajo sobre Protección de Datos del Artículo 29 de la Directiva 95/46/CE, en su Dictamen N° 5 de 12 de junio de 2009, se define como "plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes. En sentido jurídico, de acuerdo con la mencionada Directiva, las redes sociales son servicios de la sociedad de la información"².

Gracias al avance de la tecnología estos servicios son cada vez más accesibles. A su vez los niños y adolescentes conocen los cambios tecnológicos y tratan de mantenerse actualizados obteniendo equipamientos innovadores, como computadoras o celulares de última generación.

Ello hace que las redes sociales se conviertan en una forma más fácil y diferente de usar la red, en la que los usuarios quieren ser sus protagonistas. Para obtener esa posición ceden información sobre su persona, sus gustos, sus hábitos, su familia, sus amigos, a terceros conocidos y desconocidos. En muchos casos desconocen el significado o las consecuencias que puede acarrear el depósito en la red de sus datos o los datos de otras personas relacionadas con ellos en la red. Todo ello suscita múltiples preocupaciones por los posibles riesgos que pueda tener la utilización intensiva de estas plataformas, sobre todo cuando alimentan sus perfiles con datos, fotografías, videos e información privada.

A efectos de profundizar en este fenómeno y de acuerdo con el estudio presentado en 2013 por el Grupo Radar³, denominado "El Perfil del Internauta Uruguayo 2013", en nuestro país existen más de 1.500.000 usuarios de Internet. El 95% de estos usuarios usan redes sociales y son niños y adolescentes. La cifra aumentó respecto a 2012, en donde el porcentaje era del 80%. Entre las conclusiones a las que llega el Grupo se establece que el 66% de los niños y adolescentes ingresa a las redes sociales todos los días, el 24% cada dos o tres días, el 8% una vez a la semana, y el 1% con menos frecuencia. En este contexto Facebook es la red social con más usuarios, seguida de Twitter.

A estos niños y adolescentes se los denomina la "generación interactiva", los llamados nativos digitales, pero a su vez son la población más sensible de la red, sobre todo de las redes sociales. Además son la franja etaria que crece en el uso de las tecnologías, por lo que corren riesgos que requieren reglas y orientaciones flexibles y dinámicas para organizar su participación en este ámbito.

¹ Rodríguez Acosta, Beatriz. *Relación entre las Redes Sociales y la Protección de Datos en la Familia*. https://www.academia.edu/Relacion_entre_las_redes_sociales_y_la_proteccion_de_datos_personales_en_la_familia. Página visitada el 23 de enero de 2014.

² Dictamen 5/2009 sobre las redes sociales en línea. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf. Página visitada el 23 de enero de 2014.

³ Grupo Radar. *El Perfil del Internauta Uruguayo 2013*. <http://www.gruporadar.com.uy/01/wp-content/uploads/2013/10/El-Perfil-del-Internauta-Uruguayo-Resumen-ejecutivo.pdf>. Página visitada el 23 de enero de 2014.

Estos niños y adolescentes se caracterizan por exponer información sobre sí mismos con frecuencia, aspecto que forma parte de sus hábitos de consumo y marca su identidad.

La participación en las redes muchas veces supone una cultura participativa, la necesidad de sentirse popular, donde la consigna parece ser “cuanto más conectado, más popular soy”. Surgen en ellos sentimientos y actitudes de colaboración, participación, conexión, solidaridad, libertad de expresión, entre otros, que en la vida cotidiana muchas veces no tienen o manifiestan por diversos motivos. Su tiempo digital se intensifica según el uso que hagan de las redes sociales y restan tiempo a la familia, el estudio o la lectura, por ejemplo.

En general, las investigaciones realizadas a nivel mundial sobre este tema se basan en niños de más de 12 años y adolescentes. Sin embargo, actualmente hay autores como Sonia Livingstone⁴, que entienden que es necesario prestar atención a los niños menores de 12 años, ya que son ellos quienes usan las tecnologías cada vez con más frecuencia – en consecuencia las redes sociales – lo que aumenta su vulnerabilidad ante posibles riesgos. Por lo analizado anteriormente, se considera necesario determinar si los niños y adolescentes son conscientes de cuáles son los efectos que supone exponer su información de carácter personal, así como la revelación de datos de terceros en las redes sociales. Para ello es importante la intervención de la familia y los educadores para explicarles cuál es el alcance de esas conductas y sus consecuencias.

Los niños y adolescentes tienen derecho a proteger sus datos personales, por lo que es necesario que sepan que su imagen, su voz, su nombre y apellido, su dirección, su escuela, su correo electrónico y teléfono, entre otros, son datos personales que los identifican o los hacen identificables (artículo 4º lit. D de la Ley N° 18.331). Por este motivo deben tener especial cuidado cuando son compartidos con amigos o desconocidos en las redes sociales.

Hábitos, gustos u horarios, entre otros, son datos que tienen un valor más allá de lo que los menores se imaginan. Por ello, es muy importante tener presente las opciones que estas redes ponen a disposición para incrementar las medidas de seguridad.

Los niños y adolescentes deben ser conscientes que hay personas en las redes que se pueden presentar con identidades falsas, y solicitar sus datos personales para realizar actividades fuera de la ley. Se debe tener presente que lo mismo puede suceder con los datos que compartan de sus amigos.

El manejo de los datos personales por parte de los niños y adolescentes en las redes sociales es una preocupación que comparten los padres, maestros y autoridades, en virtud de que una vez que estos datos son subidos a la red, escapan de su círculo de confianza, y cambia la finalidad con la cual fueron compartidos (artículo 8º de la Ley mencionada).

Mantener la privacidad en la red es complejo, sobre todo en el caso de niños y adolescentes que interactúan en redes sociales.

Los datos que niños y adolescentes comparten en Internet sin las debidas precauciones, pueden ser divulgados sin el consentimiento del titular. Como se trata de menores de edad, en nuestro país, necesitan estar autorizados por sus padres o tutores, lo que en caso contrario puede contravenir la normativa vigente en la materia. Si el titular de la red social es un menor, tiene la obligación de contar con la presencia de sus padres o tutores para configurar su perfil.

Enumeramos a continuación algunos de los peligros a los que se enfrentan los niños en el uso de Internet.

- Las imágenes con contenido sexual que pueden implicar indicios de una conducta delictiva relacionada con pornografía infantil (Ley N° 17.815 sobre Violencia Sexual, Comercial o No Comercial cometida contra Adolescentes o Incapaces, de 18 de agosto de 2004) o que pueden provocar un uso ilegítimo de las imágenes robadas o

entregadas en forma privada. De esta manera se vulnera la intimidad y privacidad de la víctima, la cual queda sin protección y al arbitrio de agresiones o acosos por parte de terceros.

- El denominado ciberbullying, entendido como el acoso entre pares a través de las redes sociales que puede llegar a tener consecuencias irreparables para los niños y adolescentes.
- El llamado grooming. Éste se produce cuando un adulto se hace pasar por un menor estableciendo contacto con el niño o adolescente, que puede derivar en un acoso de características sexuales.

Aunque las redes se encuentren en un entorno virtual, se debe considerar que sus riesgos se asemejan a cualquier entorno real, y los daños causados son igual de reales. Una forma efectiva de proteger a los menores es educar, advertir, informar sobre los riesgos y aumentar las precauciones ante posibles usuarios sospechosos o extraños.

Respecto del tratamiento de los datos personales de niños y adolescentes en las redes sociales, es necesario considerar las recomendaciones que surgen a nivel nacional o internacional (por ejemplo, el Memorandum de Montevideo, de 28 de julio de 2009), junto con la normativa vigente en nuestro país (Ley N° 18.331, sus modificativas y su decreto reglamentario). Además, la Unidad Reguladora y de Control de Datos Personales tiene por cometido el control y cumplimiento del derecho a la protección de datos personales, y se ha trazado como objetivo contribuir a la educación de niños, adolescentes, maestros y sus familias, en la protección de sus datos personales.



4 <http://www.lse.ac.uk/researchAndExpertise/Experts/s.livingstone@lse.ac.uk>. Página visitada el 23/1/2014.



02

**Principales temas
analizados
en el año 2013**

en el año 2013
analizados
principales temas

2. Principales temas analizados en el año 2013

En virtud de los cometidos asignados por la Ley N° 18.331 referidos al asesoramiento y asistencia a las personas, organismos y empresas, el Consejo Ejecutivo de la URCDP ha emitido varias resoluciones y dictámenes en temas de interés en la materia. La nómina que se detalla a continuación recoge los temas de mayor relevancia durante el año 2013.

Video vigilancia

Diversas empresas y organismos presentaron consultas y denuncias relacionadas con el uso de cámaras de video vigilancia:

- La Dirección Nacional de Sanidad Policial del Ministerio del Interior consulta sobre la instalación de cámaras con circuito cerrado de televisión en el Área de Cuidados Críticos del Hospital Policial con el objetivo de lograr una vigilancia más estrecha, que brinde mayor seguridad a los pacientes y al personal que allí se desempeña.

Por Dictamen N° 2, de 21 de febrero de 2013, se concluye que la video vigilancia debe usarse en forma proporcional a la finalidad. Se puede utilizar cuando no existan otros medios menos lesivos a la privacidad que permitan obtener los mismos resultados, y se debe atender a los principios consagrados en la Ley N° 18.331, prestando especial atención a los de legalidad, consentimiento informado y finalidad. También se recomienda la colocación de los logos de video vigilancia con la identificación del responsable, y si correspondiere, la inscripción de la o las bases de datos producto de ella.

- La Comisión Administradora del Edificio Poseidón consulta sobre la obtención del consentimiento de la copropiedad del Edificio respecto a la implementación de un área video vigilada, lo que fue resuelto por mayoría simple en Asamblea de Copropietarios y respecto al procedimiento adecuado para la implementación e instalación de cámaras que pretende realizar.

Mediante Dictamen N° 12, de 18 de abril de 2013, se expresa que en relación con la obtención del consentimiento de los copropietarios del Edificio para la implementación de un área video vigilada se aplica el régimen general de Propiedad Horizontal, no siendo competente la Unidad para expresarse en la materia.

Por otra parte, indica que en cuanto al procedimiento adecuado para la implementación e instalación de cámaras, se deberá proceder conforme lo expresado en el Dictamen N° 10, de 16 de abril de 2010.

- Un funcionario de la Facultad de Enfermería de la Universidad de la República presenta denuncia por la implementación de cámaras de video vigilancia, alegando que se ha instalado un nuevo sistema de reloj tarjetero que toma imágenes al momento de marcar las entradas y salidas del personal, y las posibles implicancias que éste puede generar en el uso de su imagen y sus datos personales. A ello agrega que no se ha informado al personal acerca de la recolección de imágenes.

La URCDP, mediante Resolución N° 8, de 21 de febrero de 2013, considera que ésta instalación es una manifestación del poder deber de supervisión que tiene la Facultad respecto a los funcionarios, pero no implica que las imágenes que se registren dejen por ello de ser datos personales que merecen protección, y que se ha debido informar a los funcionarios en forma previa, y en el caso de que correspondiera, identificar la existencia de éstas a través de los logos de acuerdo con el Dictamen N° 10, de 16 de abril de 2010.

De igual forma entendió que la Facultad debe cumplir con el principio de legalidad que regula la Ley N° 18.331, y proceder a la inscripción de las bases de datos en las cuales se almacenan esas imágenes.

Finalmente se procedió a sancionar con “observación” a la Facultad de Enfermería de la Universidad de la República por infracción a la Ley N° 18.331 en virtud del tratamiento dado a los datos personales de sus funcionarios.

- Otro de los puntos tratados este año fue la video vigilancia entre vecinos. En este marco, se presentó ante la Unidad una denuncia contra un vecino lindero por haber colocado cámaras en la pared medianera, enfocando hacia el patio del denunciante, y hacia la vereda ubicada frente al domicilio del denunciado.

La URCDP, por Resolución N° 91, de 17 de julio de 2013, entendió que le asistía razón y que la colocación de las cámaras violaba la normativa de protección de datos.

Luego de realizar una inspección en el lugar, debido a que la parte denunciada no se presentó a aportar las aclaraciones pertinentes, y considerando que la imagen es un dato personal cuyo tratamiento está sujeto a esta normativa, salvo las excepciones establecidas por ella, se resolvió sancionar con multa de 1000 Unidades Indexadas. Asimismo, se decidió realizar denuncia ante la justicia penal a efectos que fueran investigados dado que las circunstancias emergentes de éstos tenían apariencia delictiva.

Datos personales contenidos en Certificados de Defunción

Durante el año 2013, la Unidad ha recibido varias consultas relacionadas con los datos que lucen en los certificados de defunción.

- El Ministerio de Salud Pública, como consecuencia de un recurso presentado por una compañía aseguradora contra un acto administrativo en el cual se establecen una serie de requisitos para la entrega del certificado de defunción, consulta a la Unidad si debe proceder a realizar o no la entrega del referido certificado.

Mediante Dictamen N° 3, de 4 de marzo de 2013, se establece que el certificado de defunción es un documento que contiene datos personales de naturaleza sensible, especialmente protegidos por la Ley N° 18.331, por lo que sólo se pueden tratar con el consentimiento escrito y expreso de su titular. En el caso planteado, el contrato de seguro de vida es de carácter voluntario, prestando el tomador o suscriptor su consentimiento en forma libre, expresa y escrita.

Es importante tener en cuenta que se trata de un contrato cuya ejecución tendrá lugar una vez fallecido el suscriptor, y éste depende en varios casos de factores relacionados a la causal de su muerte que no lucen en la partida de defunción. En estos casos, es necesario que la empresa aseguradora conozca las causales de la muerte para poder determinar el curso que debe seguir el contrato de seguro de vida.

A los efectos de complementar lo expresado en cuanto al consentimiento, se hace referencia a que el artículo 9° de la Ley N° 18.331 prevé las hipótesis en que no se necesita el previo consentimiento del titular de los datos. Entre ellas, el literal a) indica que no es necesario “Cuando deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento”. En el caso del contrato de seguro de vida, la obtención de determinados datos es necesaria para dar cumplimiento a lo acordado entre las partes.

La Unidad, en base a todos los elementos anteriores, dictamina que es posible entregar la información objeto de la consulta, teniendo en cuenta que se tiene que armonizar la Ley N° 18.331, con las normas relativas a derechos y deberes de los usuarios de la salud, la Ley N° 18.335 de 15 de agosto de 2008, y las demás normas y disposiciones específicas en la materia que la complementan. Además, recomienda atender a los principios generales de la protección de datos personales a los efectos de resolver situaciones dudosas.

- La Unidad de Información Nacional de Salud (UINS) realizó una consulta a la Unidad sobre la pertinencia o no de incluir en la nueva versión del certificado de defunción impreso y electrónico, el número de teléfono celular y el correo electrónico del médico certificador.

Una vez realizado el estudio del tema, se entiende que se trata de una comunicación de datos excepcionada del requisito del previo consentimiento informado de su titular, conforme lo dispuesto en los literales B) y D) del artículo 9° de la Ley de Protección de Datos y Acción de Habeas Data, siendo el interés legítimo identificado la salud del paciente, en cuanto bien supremo, y entendiendo que el certificado forma parte de la historia clínica.

El Dictamen N° 6, de 21 de marzo de 2013, establece que la inclusión de los datos objeto del estudio en el certificado de defunción no contraría las disposiciones de la Ley vigente. Se trata de una comunicación de datos que está exceptuada del requisito del previo consentimiento informado del titular. El médico certificador tiene la obligación de llenar el certificado de defunción en forma completa e inteligible, integrando éste la historia clínica del paciente.

- La Dirección General de Registro de Estado Civil, realizó una consulta vinculada con el alcance que posee la Ley N° 18.331 respecto a la inclusión de la causa de muerte en el Acta y Certificado de Defunción del Maestro Julio Castro.

Mediante Dictamen N° 8, de 21 de marzo de 2013, se brinda respuesta a la consulta formulada.

Se establece que es preciso considerar que la Dirección General de Registro de Estado Civil dictó la Circular N° 2/2012, de 2 de marzo de 2012, en la que establece que al labrar acta de defunción, ya sea en certificado electrónico o en papel, no deberá dejarse constancia de la causa de la muerte si en el certificado no viene establecida. En caso que se haya indicado, deberá dejarse constancia de que esta información es reservada.

Además de la Circular mencionada, corresponde considerar lo dispuesto en la Ley N° 18.331, la Ley N° 18.335, el Decreto reglamentario N° 274/010, y la Ley N° 18.381, de Acceso a la Información Pública.

En esta consulta se tiene en cuenta, además de los datos que deben figurar en el certificado de defunción, que la causa de la muerte ha sido publicada en diversos medios de comunicación. Éstos son considerados por el artículo 43 de la Ley N° 18.996, de 7 de noviembre de 2012, por la que se le agrega a la Ley N° 18.331, el artículo 9° bis, fuentes públicas o accesibles al público, entre las que se mencionan, las publicaciones oficiales y las publicaciones en medios masivos de comunicación en cualquier soporte, así como todo registro o publicación en el que prevalezca el interés general en cuanto a que los datos personales en ellos contenidos, pueden ser consultados, difundidos o utilizados por parte de terceros.

También se procedió a analizar el papel que juega en este caso el interés general, excepción establecida en el artículo 17 de la Ley, considerando además la aplicación de las Leyes Nos. 18.381, de Acceso a la Información Pública; 18.596, de Actuación Ilegítima del Estado entre el 13 de junio de 1968 y 28 de febrero de 1985 y Reconocimiento y Reparación a las Víctimas, así como la normativa de Derecho Internacional de los Derechos Humanos, que nuestro país ha ratificado, y que garantizan derechos a las víctimas de terrorismo de Estado.

En base a los fundamentos expuestos, el Consejo Ejecutivo de la URCDP estimó que la Dirección General de Registro de Estado Civil se encuentra habilitada para incluir la causa de la muerte en el acta y en la partida de defunción.

Comunicación de datos personales

Varios organismos consultan acerca de la posibilidad de realizar determinadas comunicaciones de datos personales a terceros, o entre sí, sin el consentimiento del titular del dato.

- La Unidad de Acceso a la Información Pública (UAIP) recibió una consulta formulada por la Dirección Nacional de Medio Ambiente en relación con la habilitación legal para comunicar a terceros información que recibe de empresas acerca del Índice Ambiental de Operación (IAO), volumen de agua utilizada y su fuente, y efluentes. La UAIP desea saber si esta información puede considerarse “confidencial” y quedar cubierta por el artículo 10 numeral II) de la Ley N° 18.381.

Mediante Dictamen N° 1, de 21 de febrero de 2013, se determina que la información objeto de la consulta ingresa en la categoría de dato personal en la medida que constituyen rasgos o cualidades con suficiente fuerza para favorecer la determinación de sus titulares. En conclusión, salvo consentimiento del titular o aplicación de las excepciones previstas en los artículos 9° y 17 de la Ley de Protección de Datos Personales y Acción de Habeas Data, ésta información está alcanzada por la categoría de información confidencial en aplicación del artículo 10 numeral II) de la Ley de Acceso a la Información Pública.

- En forma conjunta consultaron el Banco de Previsión Social, el Ministerio de Educación y Cultura y las Asociaciones que vinculan a las Instituciones de Educación Privada respecto a si resulta acorde con la Ley de Protección de Datos Personales solicitarle a las mencionadas en último término, los datos de escolares y liceales necesarios para facilitar el otorgamiento y control del beneficio de la Asignación Familiar que sirve el primero de los nombrados.

Por Dictamen N° 5, de 14 de marzo de 2013, se dictamina que desde el punto de vista de la protección de datos personales es lícita la comunicación de datos entre las instituciones que plantean la consulta, no requiriendo el consentimiento de los titulares respecto a personas y grupos familiares que son atributarios o gestionantes del beneficio de la Asignación Familiar, a los efectos de facilitar y controlar su otorgamiento y mantenimiento.

Para otros casos, se tendrá por lícita la comunicación solamente con consentimiento del titular o sus representantes legales, en los términos que prevé la Ley.

Dicho dictamen se basa en que la comunicación de datos en los términos que se planteó, se enmarca en los principios que rigen en la normativa vigente de protección de datos personales, y que no necesita contar con el consentimiento de los titulares de los datos personales o de sus representantes legales, de acuerdo con los artículos 6°, 7°, 8° y 9° literales B) y C), y 17 literal B) de la Ley N° 18.331, así como en las Leyes Nos. 15.084, de 25 de noviembre de 1980, y 18.227, de 22 de diciembre de 2007.

- El Ministerio de Educación y Cultura se presenta ante la Unidad consultando en relación con una solicitud de acceso a la información pública recibida, en la que se le requería obtener el domicilio y el teléfono particular del titular de la Cartera.

Por Dictamen N° 9, de 21 de marzo de 2013, se considera que el artículo 7° de la Ley contempla la necesidad de que el tratamiento y comunicación de los datos personales deba ser proporcional a la finalidad que lo motiva, y mediante el artículo 8° de la misma norma, se establece que los datos objeto de tratamiento no podrán utilizarse para finalidades diferentes o incompatibles a aquéllas que dieron motivo a su recolección. A su vez, la finalidad implícita establecida en la Ley N° 18.381 es ejercer el control sobre la gestión y el funcionamiento de la Administración, pero para alcanzar estos fines no sería necesario dar acceso a la información personal del Ministro porque no alude a su cargo o a la función que cumple tal como lo establece el artículo 38, numeral 8°, del Decreto N° 232/010, de 2 de agosto de 2010, reglamentario de la Ley de Acceso a la Información Pública. Como conclusión se determina que no es proporcional ni se ajusta al principio de finalidad brindar acceso al domicilio y teléfono personal del Ministro.

- El Colegio de Contadores, Economistas y Administradores del Uruguay consulta acerca de la posibilidad de que la Caja de Jubilaciones y Pensiones de Profesionales Universitarios facilite a una empresa encuestadora los teléfonos de aquellos integrantes de una muestra aleatoria que no sean socios del Colegio.

Por Dictamen N° 11, de 11 de abril de 2013, la URCDP se pronuncia, estableciendo que la Caja de Jubilaciones y Pensiones de Profesionales Universitarios deberá obtener el consentimiento de los Profesionales, sean o no socios del Colegio, antes de proporcionar a la empresa encuestadora los teléfonos de quienes integran la muestra aleatoria.

Para ello, se consideró que no es posible omitir la solicitud de consentimiento dado que el teléfono no es un dato personal incluido en el artículo 9° literal C) de la Ley N° 18.331, y que para que la realización de la comunicación se encuentre amparada por la normativa vigente, debe cumplir con los requisitos mencionados en el artículo 17 de la Ley.

- La Comisión Honoraria de Salud Renal solicita el asesoramiento de la Unidad con respecto al alcance de la Ley N° 18.331, en cuanto a la comunicación de datos sensibles que se encuentran en el Registro Único de Pacientes con Enfermedad Renal al médico nefrólogo responsable de cada paciente, con la finalidad de mejorar su asistencia, facilitando la identificación de los casos de riesgo.

La Unidad manifiesta que los datos de salud están expresamente protegidos por la Ley de Protección de Datos Personales, integrando el grupo de los datos sensibles. Para su tratamiento es necesario el consentimiento expreso y escrito de su titular y la especial atención de los principios establecidos en la Ley.

Luego de realizado el estudio correspondiente, mediante Dictamen N° 13, de 18 de abril de 2013, se considera legítima la comunicación de datos en los términos de la consulta formulada y en el marco de lo expresado anteriormente.

Sistema de referencias empresariales

Se recibe consulta sobre la adecuación con la Ley de un sistema de referencias empresariales, donde cada empresa afiliada podrá ingresar datos de los empleados y una evaluación numérica que señale si lo recomienda o no.

Para realizar las búsquedas en el sistema mediante la cédula de identidad, las empresas deberán estar afiliadas al sistema y obtener el previo consentimiento de las personas. De acuerdo con lo informado por el consultante, el sistema no permite emitir listados ni navegar por la información de las personas si no brindaron el consentimiento para la realización de la consulta.

Se debe tener presente que por el artículo 17 de la Ley, los datos objeto de tratamiento podrán ser solo comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario, y con el previo consentimiento del titular de los datos. Si bien existe este interés, no se puede inferir el consentimiento del trabajador del contexto de la relación laboral o contractual, ni por la entrega de la cédula de identidad, ya que lo regulado por la Ley N° 18.331 no se basa en el consentimiento tácito sino en el expreso. Además, se debe tener en cuenta que los trabajadores, cuyos datos han sido ingresados al sistema, deben ser informados de la finalidad de la base y de esa eventual comunicación.

Por Dictamen N° 21, de 4 de julio de 2013, se dictaminó que debe recabarse el consentimiento en forma expresa mediante un formulario o cláusula específica que deberá ser firmada por los trabajadores conforme lo dispuesto en el artículo 9° de la Ley, y que deberán ser informados en los términos del artículo 13, así como cumplir con los principios de legalidad y seguridad.

Procedencia de la inscripción de una base de datos creada y regulada por ley y reglamento especial

La Ley de Protección de Datos y Acción de Habeas Data en el artículo 3° literal C) establece que su ámbito objetivo incluye a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por el ámbito público o privado.

Por Ley N° 18.242, de 27 de diciembre de 2007, y sus Decretos reglamentarios Nos. 393/2008 y 190/2012, de 11 de agosto de 2008 y 29 de mayo de 2012, respectivamente, se crea una base de datos que contendrá información sobre empresas elaboradoras y transformadoras de productos lácteos. La Institución responsable de la mencionada base, consulta sobre el alcance del artículo 3° literal C) de la Ley N° 18.331.

En el caso se consideró que existe un régimen legal propio que regula a la Institución. Se trata de una persona jurídica de derecho público no estatal, que lleva un registro de las empresas industrializadoras y comercializadoras de productos lácteos, la que para poder cumplir con esta obligación queda habilitada a solicitar toda la información que considere necesaria a efectos de cumplir con la normativa específica.

De acuerdo con lo mencionado anteriormente, mediante Dictamen N° 18, de 29 de mayo de 2013, se indica que de acuerdo con la normativa de protección de datos personales no deberá inscribirse en el registro que lleva la URCDP, la base de datos objeto de la consulta, pero deberán adoptar las medidas de seguridad necesarias para garantizar la confidencialidad y la reserva de los datos proporcionados.

Inclusión del diagnóstico en los certificados médicos que justifican ausencias por enfermedad

A la Unidad se presenta una consulta sobre la legalidad de exigir la inclusión del diagnóstico en los certificados médicos que justifican ausencias laborales por enfermedad.

Se procede a realizar el estudio de la consulta resultando que se deben abordar dos temas centrales sobre los cuales se sustenta la relación médico-paciente, como ser el secreto médico profesional, y el tratamiento de los datos sensibles, así como su comunicación en la especie.

Desde el punto de vista del primer tema, el diagnóstico está amparado en el secreto profesional regulado en el artículo 302 del Código Penal. Su relevamiento procede únicamente por justa causa, obligación legal, o autorización expresa y escrita del paciente. Desde el punto de vista del paciente, el diagnóstico es información sensible, especialmente protegida por la Ley de Protección de Datos Personales, y su comunicación procede únicamente mediante autorización expresa y por escrito.

Mediante Dictamen N° 23, de 4 agosto de 2013, se resuelve que no resulta ajustado a derecho exigir la inclusión del diagnóstico en el certificado médico laboral.

Alcance de los términos "listado" y "medios" utilizadas en el artículo 9° lit. C) de la Ley N° 18.331, y el literal B) del artículo 3° del Decreto N° 414/009, de 31 de agosto de 2009

Por Dictamen N° 26, de 8 de agosto de 2013, la Unidad se expide acerca del alcance de los términos "listados" y "medios" utilizados en el artículo 9° literal C) de la Ley N° 18.331, y en el literal B) del artículo 3° del Decreto N° 414/009, de 31 de agosto de 2009, de acuerdo a lo consultado por la Comisión de Protección de Datos Personales de la Contaduría General de la Nación.

La URCDP entiende que se aplican las reglas de interpretación de las leyes contenidas en el Título Preliminar del Código Civil. Los términos "listados" y "medios" no han sido definidos expresamente por el legislador en materia

de protección de datos personales, por lo que deben ser entendidos en sus sentidos naturales y obvios, según el uso general.

Confidencialidad de datos personales

La Dirección de Asuntos Jurídicos y Notariales de la Dirección Nacional de Aduanas consulta sobre el carácter de confidencialidad que eventualmente poseen los datos personales de firmas pertenecientes a las empresas Despachantes de Aduana cuyo acceso está permitido a terceros a través del Sistema Lucía.

Por Dictamen N° 27, de 8 de agosto de 2013, el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales considera que por los cometidos de la Dirección Nacional de Aduana (DNA), establecidos legalmente, no es necesario recabar el consentimiento de los involucrados o interesados, así como tampoco lo es, para comunicar ciertos datos a determinados organismos públicos, siempre y cuando, ello se corresponda con las funciones de cada uno de éstos, la finalidad del intercambio y su regulación legal.

Existen también algunos datos, que contiene la documentación de la DNA, que podrían haberse entregado en carácter de información confidencial de acuerdo con el artículo 10 de la Ley N° 18.381, de Acceso a la Información Pública, o tratarse de datos que no integran la nómina del artículo 9° literal C).

El Consejo Ejecutivo de la Unidad, mediante el Dictamen mencionado, estableció que en el caso de datos que requieran el previo consentimiento informado, corresponde recabarlo, o aplicar un mecanismo de disociación, o de lo contrario la publicación de la DNA debería limitarse solo a los datos incluidos en el artículo 9° lit. C). Indica que la DNA no requiere de dicho consentimiento cuando la comunicación o recolección es en el marco del cumplimiento de sus funciones, conforme lo establecido en el artículo 9 literal B) de la Ley.



03

Avances de la normativa en protección de datos personales

de datos personales
en protección
de la normativa
vigente

3. Avances de la normativa en protección de datos personales

Nacional

Ley N° 19.149, de 24 de octubre de 2013, artículo 75. Rendición de Cuentas y Balance de Ejecución Presupuestal Ejercicio 2012

Por el artículo 75, se determina que las empresas operadoras de servicios de telefonía móvil deberán llevar en forma actualizada una base de datos de los clientes que hubieran contratado servicios bajo cualquier modalidad, ya sea para servicios prepagos o postpagos. Esta base de datos estará amparada por la Ley N° 18.331, de 11 de agosto de 2008.

Internacional

Decreto Supremo N° 003-2013-JUS, por el que se aprueba el Reglamento de la Ley N° 29.733 de Protección de Datos Personales, de 21 de marzo de 2013, de la República del Perú

El 21 de marzo, mediante el Decreto Supremo N° 003-2013-JUS, se aprobó en la República del Perú, el Reglamento de la Ley N° 29.733 de Protección de Datos Personales. Éste entró en vigencia a los treinta días hábiles contados a partir del día siguiente de su publicación.

Entre los puntos de destaque se encuentra lo relacionado con los datos sensibles, siendo que determina que son tales: las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar y los hábitos personales que corresponden a la esfera más íntima. Además determina que el consentimiento escrito puede ser mediante firma manuscrita y electrónica, o por cualquier mecanismo de autenticación.

Decreto N° 1377, de 27 de junio de 2013, por el cual se reglamenta la Ley N° 1581 de 2012, de la República de Colombia

El 27 de junio, mediante el Decreto N° 1377, se reglamenta parcialmente la Ley N° 1581, de 2012, dictándose disposiciones generales para la protección de los datos personales.

El Decreto se divide en seis capítulos. El Capítulo I contiene las disposiciones generales, regulándose el tratamiento de datos personales en el ámbito personal o doméstico, e incluyendo algunas definiciones.

En el Capítulo II bajo el nombre "Autorización" se regula la recolección de los datos personales, la autorización para el tratamiento de datos personales, el modo de obtener la autorización, su prueba y su revocación. También se regulan los datos recolectados con anterioridad a la expedición del presente decreto. Además, se regulan las limitaciones temporales al tratamiento de los datos personales y los requisitos especiales para el tratamiento de datos de niños, niñas y adolescentes.

El Capítulo III regula las políticas de tratamiento de la información determinándose las políticas de tratamiento de la información, el contenido mínimo del aviso de privacidad, el deber de acreditar la puesta a disposición del aviso de privacidad y las políticas de tratamiento de información, y los medios de difusión del aviso de privacidad, el procedimiento para el adecuado tratamiento de los datos personales y las medidas de seguridad.

Por su parte, el Capítulo IV se refiere al ejercicio de los derechos de los titulares. Se regulan la legitimación para el ejercicio de los derechos del titular, el derecho de acceso, el derecho de actualización, rectificación y supresión, y los medios para el ejercicio de éstos.

El Capítulo V brinda un marco a las transferencias y transmisiones internacionales de datos personales.

Por último, el Capítulo VI refiere a la responsabilidad demostrada frente al tratamiento de datos personales, a la vigencia de la norma y disposiciones derogatorias.

Ley N° 172-13, de 13 de diciembre de 2013, sobre Protección de Datos de carácter personal, de la República Dominicana

En la República Dominicana, el derecho a la protección de datos personales ya se encontraba reconocido en el artículo 44 de la Constitución de la República. Dicha norma también regula los derechos ARCO. A ello, debe agregarse que el artículo 70 de la Constitución regula la Acción de Habeas Data.

Como antecedentes en la materia, es pertinente recordar que la República Dominicana también cuenta con una serie de leyes sectoriales que regulan aspectos relacionados con la protección de datos.

El 13 de diciembre de 2013, se promulga la Ley N° 172-13. Se trata de una ley general en la materia cuyo objetivo es la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamientos, sean éstos públicos o privados.

La referida Ley se divide en seis Capítulos. El Capítulo I contiene las disposiciones generales, entre las que se encuentran el objetivo, el ámbito de aplicación, las restricciones, los principios y las definiciones.

Por su parte, el Capítulo II regula los derechos de las personas (acceso, rectificación, cancelación, y oposición) y su ejercicio.

El Capítulo III refiere al órgano de control. Aquí se encuentra una de las particularidades de la norma que es que no se crea un órgano de control rector general.

Por otra parte, el Capítulo IV establece disposiciones procedimentales, y el Capítulo V regula las disposiciones relativas a infracciones y sanciones.

Por último, el Capítulo VI contiene las disposiciones transitorias y finales.



04

Jurisprudencia

Jurisprudencia



4. Jurisprudencia

Nacional

En este punto se hace referencia a aquellas sentencias que fueron dictadas durante el 2013 por los Tribunales nacionales, que se destacan en la temática de protección de datos personales.

Sentencia del Tribunal de Apelaciones en lo Civil de 1° Turno N° 13, de 6 marzo de 2013, confirmatoria de la Sentencia Interlocutoria del Juzgado Letrado de Primera Instancia en lo Civil de 6° Turno N° 1.906, de 13 de marzo de 2012. Se resuelve sobre la clausura de base de datos.

Sentencia del Juzgado de Paz de la Capital de 4° Turno N° 4, de 11 de marzo de 2013. Se resuelve sobre inclusión errónea en la base de datos de una entidad crediticia.

Sentencia del Tribunal de Apelaciones en lo Civil de 1° Turno N° 93, de 11 de junio de 2013. Se resuelve sobre errónea inclusión en una entidad crediticia de Salto.

Sentencia del Tribunal de lo Contencioso Administrativo N° 350, de 16 de julio de 2013. Se resuelve una acción de nulidad respecto a la Resolución N° 1.658/2010, de 15 de octubre de 2010, dictada por la Unidad Reguladora y de Control de Datos Personales.

Sentencia del Juzgado Letrado de Primera Instancia en lo Civil de 11° Turno N° 54, de 6 agosto de 2013. Se resuelve una acción de Habeas Data presentada contra una consultora de mercado en la que se pretende conocer los datos que ésta maneja en relación con las ventas del actor.

Sentencia del Tribunal de Apelaciones en lo Civil de 2° Turno N° SEF 005-000133/2013, de 4 de setiembre de 2013. Se confirma la primera instancia de la sentencia que desestima la Acción de Habeas Data contra una consultora de mercado a los efectos de conocer los datos que maneja acerca de las ventas del actor.

Sentencia del Tribunal de lo Contencioso Administrativo N° 516, de 10 de setiembre de 2013. Se desestima la solicitud de suspensión de ejecución de un acto dictado por la Dirección General Impositiva por el que se obliga a las Instituciones de Enseñanza Privada a identificar a quienes abonen las cuotas de los alumnos.

Sentencia del Juzgado Letrado en lo Penal de 7° Turno N° 223, de 28 de octubre de 2013. Se absuelve al imputado, acusado por haber violado el artículo 7° de la Ley N° 17.838, de 8 de setiembre de 2004.

Internacional

Sentencia de la Sala de 1° del Tribunal Constitucional de España, de 7 de octubre de 2013, relativa a una comunicación de datos sin consentimiento.

Sentencia 29/2013, de 11 de febrero de 2013, que resuelve el recurso de amparo 10522-2009 en relación con las Sentencias de del Tribunal Superior de Justicia de Andalucía y de un Juzgado de lo Social de Sevilla, referida a la impugnación efectuada a una sanción disciplinaria impuesta por la Universidad de Sevilla, en mérito a la utilización de imágenes captadas por cámaras de video vigilancia instaladas en el recinto universitario con una finalidad de supervisión laboral, sin información al trabajador.



05

Presentación de la Memoria 2012

Presentación de la Memoria 2012

5. Presentación de la Memoria 2012

En 2012 se alcanzaron importantes metas a nivel país en materia de protección de datos personales que merecen destacarse.

El lanzamiento de la Memoria de la URCDP se realizó en la Sala de Actos de la Presidencia de la República - Edificio Torre Ejecutiva contando con la presencia de las Autoridades de la Dirección Nacional de Impresiones y Publicaciones Oficiales (IMPO), Director Lic. Gonzalo Reboledo, del Consejo de Educación Inicial y Primaria (CEIP) Consejera Mag. Irupé Buzzetti, del Proyecto Plan CEIBAL, Presidente Ing. Miguel Brechner, y de la Unidad Reguladora y de Control de Datos Personales (URCDP), los Miembros del Consejo Ejecutivo Dr. Felipe Rotondo, Mag. Federico Monteverde e Ing. José Clastornik, representantes de organizaciones de la sociedad civil, empresas y academia.

Respecto a la Memoria Anual el Dr. Felipe Rotondo expuso sobre el relacionamiento internacional destacando que: "Desde ese punto de vista la legislación, aprobada por todos los partidos, fue reconocida por la Unión Europea a través de la adecuación. Uruguay es el segundo país en obtenerla no solo por el contenido de la Ley sino por su cumplimiento".

El Dr. Rotondo explicó que Uruguay a partir del 1º de agosto de 2012, es el primer miembro no europeo del Convenio N° 108 del Consejo de Europa para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal y del Protocolo Adicional al Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos, lo que fue aprobado por la Ley N° 19.030, de 12 de diciembre de 2012.

Otro de los puntos importantes, fue la reseña de los trabajos que se realizan en la Unidad durante el año 2012, destacándose las tareas relativas al asesoramiento a la ciudadanía, la realización de boletines informativos mensuales, las capacitaciones a diferentes sectores de la población y la elaboración de proyectos, así "estamos en un camino firme de consolidación institucional donde el trabajo diario es la labor más importante".



06

**Difusión y capacitación
de la Unidad Reguladora
y de Control
de Datos Personales**

de Datos Personales
y de Control
de la Unidad Reguladora

6. Difusión y capacitación de la Unidad Reguladora y de Control de Datos Personales

Sitio web

A los efectos de continuar con la comunicación e información a la ciudadanía de los trabajos realizados, y las novedades referentes al ejercicio de sus derechos, además del cumplimiento de sus obligaciones, la Unidad prosigue con la mejora de su sitio web oficial destacándose:

Campaña Tus Datos Valen. Cuídalos

Se ha llevado a cabo el lanzamiento de la Campaña “Tus Datos Valen. Cuídalos” que se mencionara en el punto dos de esta publicación, realizándose una sección en el sitio web de la Unidad especialmente para ella.

En dicho sitio se ha subido contenido referente a la descripción general de la Campaña propiamente dicha, así como información para maestros y niños relativa a la concientización del derecho a la protección de datos personales.

Además se puede encontrar una reseña sobre el concurso que se realizó para los alumnos de 6° año de las escuelas públicas y privadas de todo el país, bajo el eslogan “Cómo explicas qué son los datos personales”.

Para esta campaña se confeccionó un material didáctico de apoyo sobre la temática de datos personales así como también materiales para el concurso, los que fueron entregados a las escuelas públicas y privadas del país, llegando a un total de 3250 escuelas.



Atención de consultas a la ciudadanía

En el año 2013 la Unidad continuó con la atención a los ciudadanos en forma personalizada y telefónica.

Así se atendió en su sede, en forma personal a alrededor de 730 personas y se recibieron 865 llamadas telefónicas.

Mediante estas consultas los ciudadanos han solicitado asesoramiento sobre temas tales como video vigilancia, inscripción de bases de datos y códigos de conducta, transferencias internacionales de datos, cuáles son los países con nivel de adecuación y cuándo se requiere la autorización de la Unidad para la realización de una transferencia, así como sobre el estado del trámite de los expedientes de consultas y denuncias que han sido presentados ante la Unidad.

Difusión en los medios de comunicación

En el transcurso de 2013 la Unidad ha hecho difusión de sus actividades en diferentes medios de prensa escrita, radio y televisión.

Este año se ha visto incrementada su presencia en los medios debido al lanzamiento de la Campaña “Tus datos valen. Cuídalos” y del concurso realizado en las escuelas públicas y privadas de la República.

Es así que se ha asistido a varios programas de radio, a saber, el programa “De Diez a Doce” en Radio Uruguay, el programa “Cría Cuervos” en Radio Nacional, al que se concurrió en varias oportunidades. También se estuvo presente en los canales de televisión por aire: Canal 4, TNU Canal 5, Canal 10, y también en la televisión para abonados en Canal 20 TCC, programa Punto Tecno.

La campaña a su vez fue difundida en varios portales y páginas web de la capital y de diferentes departamentos del interior del país, así como en los diarios y semanarios de todo el territorio nacional.

Relacionamiento internacional

La Unidad cada año se propone como una de sus metas más importantes el relacionamiento con Autoridades y Organismos Internacionales bregando por una cooperación y colaboración cada vez más sólida.

- Del 23 al 25 de enero del año 2013, el Dr. Felipe Rotondo concurrió a la ciudad de Bruselas, Bélgica a la Conferencia denominada “Reloading Data Protection” en la que por iniciativa del Consejo de Europa se incluyó el panel denominado “Data Protection in Latin America”. Éste tuvo por objetivo considerar la evolución del derecho a la protección de datos y su impacto en Latinoamérica; fue dirigido por Sophie Kwasny de este Consejo y moderado por Artemi Rallo Lombarte, de la Universidad Jaume I de España, quien anteriormente se desempeñó como Director de la Agencia Española de Protección de Datos. Participaron, además, panelistas de Brasil, Colombia y México.
- Todos los 28 de enero se conmemora en Europa el Día de la Protección de Datos, en mérito a que se firmó en este día en 1981, el Convenio N° 108 relativo a la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Uruguay ha pasado a formar parte de él, al adherir a su texto en 2012, e internalizarlo a su normativa mediante la Ley N° 19.030, de 12 de diciembre de 2012.
- La Unidad recibió al Prof. Dr. Álvaro Sánchez Bravo de la Universidad de Sevilla, quien brindó una charla sobre la “Nueva normativa de la Unión Europea”. El catedrático indicó que el marco europeo de protección de datos

surge con la Directiva de 1995 que regula a nivel comunitario la protección de los datos personales, la que actualmente en muchos casos ha quedado obsoleta en razón de los entornos tecnológicos en que se vive actualmente.

Debido a esto se comenzó a trabajar en la Unión Europea, llegando a la conclusión de que la materia ya no va a ser regulada por una Directiva sino por un Reglamento, porque aquélla está dirigida a desarrollar las grandes políticas de la Unión Europea, dejando a los Estados miembros la capacidad de aplicarla conforme a su sistema jurídico e idiosincrasia, y si no lo hacen, el Estado es condenado a una sanción de carácter económico. Se considera que el Reglamento es, desde el punto de vista jurídico, la mejor opción, debido a que vincula a todos los Estados miembros de la Unión Europea y se aplica en forma automática.

El disertante concluyó que los temas más importantes que trata el Reglamento son: ámbito de aplicación; protección de los menores en los entornos tecnológicos; principio de tratamiento legal, lícito y transparente de los datos; derecho al olvido; portabilidad de los datos; evaluación de impacto de la protección de datos; protección de datos desde el diseño y por defecto; datos biométricos, genéticos y de salud.

- En el mes de abril la Unidad Reguladora y de Control de Datos Personales recibió la visita en su sede de la Jefa de la Oficina de Registros Públicos del Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad de Buenos Aires, Sra. Inés Tornabene y a la Sra. Agustina Callegari, que fueron recibidas en la Unidad por el Mag. Federico Monteverde, Miembro del Consejo Ejecutivo. En la reunión se trataron diferentes puntos referentes a la protección de datos personales, a la situación de ambos países en la materia y a las formas de cooperación y colaboración entre ambas autoridades, cumpliendo uno de los objetivos principales, que consistía en estrechar los lazos existentes y comenzar a gestionar procesos de intercambio en el avance de la temática de protección de datos personales en el Río de la Plata.
- Continuando con la visita de expertos extranjeros a la Unidad, se recibió la visita del profesor Dr. Ahti Saarempää, quien es Vicepresidente de la Junta de Protección de Datos de Finlandia, Profesor de Derecho Privado y Director del Instituto de Derecho e Informática en la Facultad de Derecho de la Universidad de Laponia, Finlandia.

El Dr. Saarempää como inicio de su exposición, abordó el tema del vínculo existente entre información y privacidad, y el desafío de combinar el derecho a la información con la privacidad.

Como segundo punto refirió a los cambios que producirá el nuevo Reglamento de Protección de Datos Personales de la Unión Europea, mencionando diferentes aspectos, siendo los más destacados, según su criterio, el derecho al olvido, la protección de los menores en Internet, la protección de datos por diseño y defecto, y las notificaciones en relación con la violación de datos personales.

- La Unidad participó como asistente en el Primer Congreso Internacional de Mobbing y Bullying en el que se destacaron los siguientes exponentes extranjeros: Marie France Hirigoyen (Francia), Iñaki Piñuel y Zabala (España), Sabino Delgado (España) y David González-Trijueque (España), referentes mundiales en la materia, entre otros expertos. La convocatoria se hizo bajo la consigna “hacer visible lo invisible”. La Lic. Silvana Giachero afirmó que este tipo de intercambio de conocimiento contribuye a ser “la mano que rescata a las víctimas del espiral de violencia restableciendo así la dignidad y la verdad, arrojando luz sobre los hechos”. El enfoque se realizó en forma multidisciplinaria, desde perspectivas sociológicas, psicológicas y jurídicas; las exposiciones se destacaron por su contenido conceptual y estadístico.
- En Quito, Ecuador, se realizó el Primer Foro Internacional de Registros de la Propiedad y Mercantiles de Ecuador. El evento estuvo dirigido a los Registradores Públicos del Ecuador, y contó con palabras inaugurales, así como de apertura y cierre, de importantes representantes del Ministerio de Telecomunicaciones y Sociedad de

la Información, del Ministerio Coordinador de Sectores Estratégicos y de la Dirección Nacional de Registros de Datos Públicos (DINARDAP). En la ocasión expusieron también varios jefes y técnicos de esta última, así como los especialistas en Derecho Registral Ab. Jaime Villalba Plaza (Ecuador) y Alberto Ruiz de Erenchun (Argentina).

Ecuador cuenta con una política destacada en materia de automatización y acceso ciudadano a los registros públicos, la que ejecuta a través de la DINARDAP, entidad estatal creada por ley en el año 2010 en cuya órbita funciona el Sistema Nacional de Registro de Datos Públicos SINARDAP. Sin embargo, no dispone hasta el presente de una Ley de Protección de Datos Personales que conjugue y se acople a dicho régimen. De ahí el interés de los organizadores del evento por conocer más a fondo la experiencia uruguaya.

Al evento, concurrió por invitación, el Dr. Marcelo Bauzá, Asesor Letrado de AGESIC, quien expuso sobre la “Protección de Datos y su Acceso”.

- El 6 y 7 de junio el Dr. Felipe Rotondo, participó en representación de la Unidad Reguladora y de Control de Datos Personales, del Primer Congreso Internacional de Protección de Datos Personales, en la ciudad de Santa Marta, Colombia.

El Congreso versó sobre la protección de datos en América Latina. Dentro de los países que participaron como invitados se encuentran Uruguay, Costa Rica, Perú, y Brasil. El Dr. Rotondo expuso sobre la Protección de Datos Personales en Uruguay. El Congreso se destacó por una buena afluencia de público y la participación activa.

Por otra parte, durante esos días se realizó, la Reunión de la Red Iberoamericana de Protección de Datos Personales (RIPD) en la que se trabajó sobre la revisión del Reglamento de la Red, llegando a consensos en varios aspectos. Esta reunión contó con la presencia de expertos en la temática de Iberoamérica, EEUU, Canadá y Francia, entre otros.

- En el marco de la 35ª Conferencia Internacional de Protección de Datos y Privacidad, la URCDP estuvo representada por el Dr. Felipe Rotondo, quien disertó en el Panel denominado “El reconocimiento mutuo entre las diferentes tradiciones de protección de datos”. La mesa estuvo integrada por Artemi Rallo de la Universidad Jaume I, España, como moderador, y como expositores participaron: Blair Stewart Asistente del Comisionado de Privacidad de Nueva Zelanda, Willem Debeuckelaere en su calidad de Presidente de la Autoridad de Privacidad de Bélgica, Giovanni Butarelli por parte del Asistente del Supervisor Europeo de Privacidad, y Joseph Alhadeff como Representante de Oracle.



Dicha Conferencia se desarrolló bajo el lema “A compass in turbulent world” y en ella se trataron los siguientes temas: la educación de privacidad en el mundo digital, la protección de datos y derecho comercial mundial, el acceso público a los datos del sector privado, la confidencialidad y seguridad cibernética, la evaluación de riesgos para la privacidad de los individuos, y la ejecución penal y administrativa de la protección de datos.

Del encuentro participaron autoridades de protección de datos personales y privacidad, académicos, empresarios y representantes gubernamentales.

- Siguiendo con el relacionamiento internacional, el 25 de setiembre de 2013, en Varsovia, Polonia, se firmó el Memorando de Entendimiento y Asistencia Recíproca para la Aplicación de Leyes de Protección de Datos en el Sector Privado con la Comisaría de Protección de Datos de Canadá. Del acto protocolar participó la Comisionada de Privacidad de Canadá Jennifer Sttodart y el Dr. Felipe Rotondo como Miembro del Consejo Ejecutivo de la URCDP.

La firma de este Memorando tiene como finalidad coordinar acciones de apoyo y colaboración entre ambos países para garantizar la protección de los datos personales de sus ciudadanos y la aplicación de la normativa vigente en la materia, así como también facilitar la investigación y la educación en lo relativo a la protección de datos personales.

En la actualidad se encuentran en marcha otros Convenios de Cooperación que se espera sean firmados durante el año 2014.

- En el mes de octubre se llevó a cabo en Cartagena de Indias el XI Encuentro de La Red Iberoamericana de Protección de Datos Personales (RIPD), encuentro al que acudió la Dra. Graciela Romero en representación de la Unidad. En él participaron representantes de las Autoridades de control de datos personales y personal de diferentes instituciones públicas iberoamericanas, procedentes del ámbito gubernamental, administrativo, legislativo, judicial y docente. Al mismo tiempo, se contó con la presencia del sector privado, tanto profesional (abogados, consultores o profesionales en TI) como empresarial (Google, Microsoft, Mercado Libre, Metlife, BBVA o IAB Spain).

En las jornadas se abordaron importantes temas como el llamado derecho al olvido, las garantías de los datos personales en la nube (cloud computing), la publicidad en Internet y los flujos transfronterizos de información.

- El Centro Latinoamericano de Administración para el Desarrollo (CLAD) organizó el XVIII Congreso Internacional sobre la Reforma del Estado y la Administración Pública.

A él concurrió por la Unidad, su Presidente Mag. Federico Monteverde, quien participó en el panel denominado “El impacto de la Protección de Datos en la Administración Pública”, que contó con una importante concurrencia, la que participó del debate y el intercambio de experiencias entre asistentes de diferentes países.

- Cerrando el ciclo de visitas de expertos extranjeros, en el mes de noviembre llegó a la Unidad Jesús Rubí, Adjunto al Director de la Agencia Española de Protección de Datos Personales.

En esta instancia el Sr. Rubí dio a conocer el trabajo que viene desarrollando la Agencia Española en cuanto a la realización de inspecciones y auditorías, así como la gestión de los ficheros y de las denuncias que recibe. Compartió su agenda con el grupo jurídico de Derechos Ciudadanos de AGESIC y realizó una disertación en el marco del Programa Salud.uy con especial énfasis en el tratamiento de los datos de salud en la historia clínica, el ejercicio de los derechos del titular y el rol de los responsables de tratamiento.

Charlas impartidas durante el 2013.

Otro de los retos de la Unidad es el relacionamiento y capacitación de la ciudadanía en cuanto al derecho a la protección de datos personales. Para ello se determinaron cuatro sectores en los que se comenzaría a concientizar a la población durante el 2013, con miras a reforzar esa capacitación en el año 2014: educación, responsables de acceso a la información pública telecomunicaciones y salud. En esta primera etapa se capacitó a los dos sectores mencionados en primer lugar.

- Durante el mes de abril la Unidad capacitó a directores y funcionarios de la División de Servicios Agrícolas del Ministerio de Ganadería, Agricultura y Pesca.

En el taller se difundieron los derechos y obligaciones contenidos en la Ley de Protección de Datos Personales, así como también, se analizó el procedimiento de inscripción de bases de datos y se efectuaron recomendaciones referidas a las medidas de seguridad y buenas prácticas a adoptar, para proteger y garantizar la confidencialidad así como la reserva de los datos personales.

- La Jefatura de Policía de Tacuarembó, dentro de su plan de capacitación en seguridad y educación policial, realizó los días 7 y 8 de Junio, el 2º Seminario de Seguridad Informática y Educación Policial, en la ciudad de Paso de los Toros. Departamento de Tacuarembó.

En dicho Seminario se trataron temas relativos a la protección de datos personales, la seguridad pública, las respuestas a incidentes, las formas de acoso a los niños (bullying), la seguridad en las redes sociales, la información y la inteligencia.

Este se realizó en el marco de la capacitación que se está efectuando a un grupo de efectivos policiales que conforman el grupo “UBUNTU”, dirigidos por el Lic. Mauro Amarillo y contó con la presencia del Jefe de Policía del Departamento de Tacuarembó. Los participantes pertenecían a diferentes departamentos del Ministerio del Interior (Informática, Delitos Complejos, Seguridad) y de Jefaturas de los Departamentos de Rivera, Maldonado, Treinta y Tres, Cerro Largo, Montevideo, Canelones, Paysandú, Rio Negro, entre otras, así como personal de la Gerencia del Área de Relacionamiento con la Comunidad de Antel.

- El 11 de setiembre la Unidad Reguladora y de Control de Datos Personales comenzó el ciclo de charlas sectoriales en la Cámara Uruguaya de Telecomunicaciones del Uruguay (CTU).

Se contó con la presencia de miembros de empresas telefónicas, call centers, proveedores de servicios de Internet y personal de la propia Cámara.

Los asistentes participaron activamente mediante preguntas y comentarios que realizaron a los especialistas de la Unidad sobre la temática.

- En el marco de la Campaña de Protección de Datos Personales y de la capacitación sectorial en materia de educación, se instruyó a docentes de escuelas primarias de Montevideo. Se realizaron dos talleres de formación con la participación de más de 100 docentes. Esta actividad contó con la colaboración de docentes del Consejo de Educación Inicial y Primaria (CEIP), integrantes del Programa GURÍ, quienes actuaron como moderadores y orientadores de la metodología de trabajo a seguir. Por la URCDP se realizó la capacitación en Protección de Datos Personales.

En la jornada, además, se expuso sobre la Campaña “Tus datos valen. Cuídalos” que la Unidad está llevando adelante y sobre el concurso “Cómo explicas qué son los datos personales”, el cual fue programado para alumnos de 6to año de las escuelas públicas y privadas de todo el país. Los asistentes contribuyeron con sus comentarios y preguntas a la realización de un diálogo ameno con las expositoras, en el que se intercambiaron diferentes opiniones.

- El 24 de octubre, la Unidad Reguladora y de Control de Datos Personales con la colaboración de la Cámara Uruguaya de Importadores de Máquinas de Oficina e Informática (CUIMOI), continuando con el programa de capacitación a la ciudadanía, se reunió con representantes de las empresas afiliadas a la mencionada Cámara.

7. La URCDP en cifras

Este capítulo tiene como objetivo presentar de manera cuantitativa y gráfica, datos que permitan realizar un análisis del estado de situación en Uruguay respecto a algunos aspectos de la protección de datos personales.

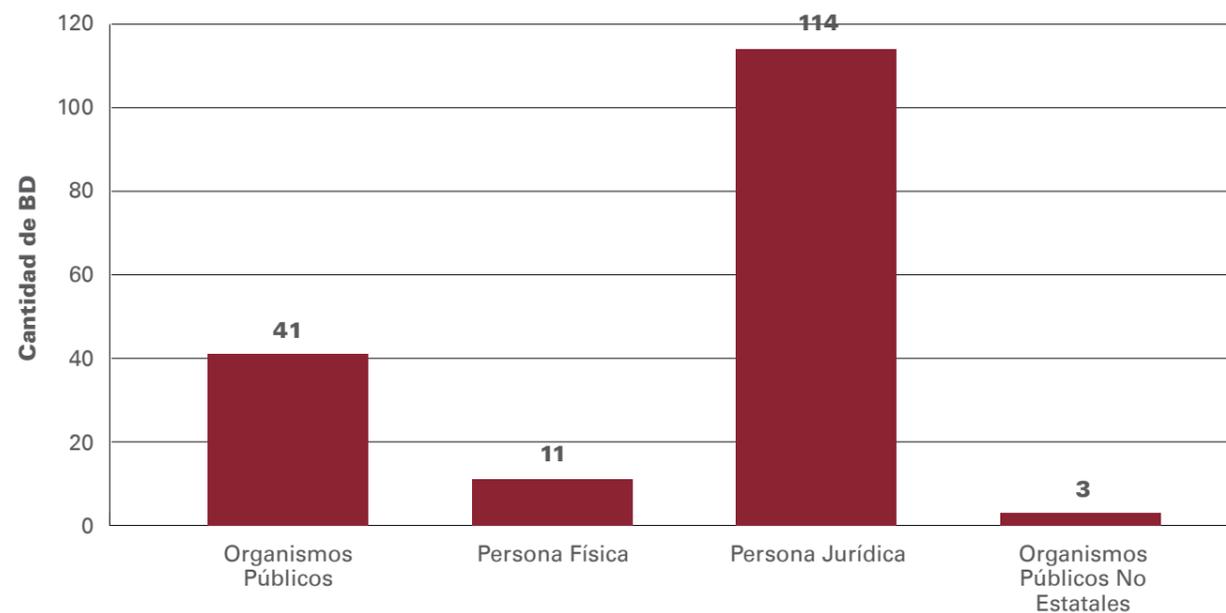
Registro de base de datos personales según el tipo de responsable

Desde el inicio de su actividad, la URCDP puso a disposición de los sujetos obligados un sistema informático que permite el ingreso vía Internet de los Formularios de Registro de Bases de Datos Personales. A continuación, se presentan y analizan los datos obtenidos como resultado del registro online de estos formularios durante el año 2013.

La tabla y el gráfico siguientes muestran las cantidades de base de datos según tipo de responsable presentados ante la Unidad durante el año 2013.

| Año 2013 | | |
|----------------------------------|----------------------------|--------------------------|
| Tipo de responsable | Cantidad de Bases de Datos | Cantidad de Responsables |
| Personas físicas | 11 | 9 |
| Personas Jurídicas | 114 | 72 |
| Organismos públicos | 41 | 10 |
| Organismos públicos no estatales | 3 | 1 |
| Totales | 169 | 92 |

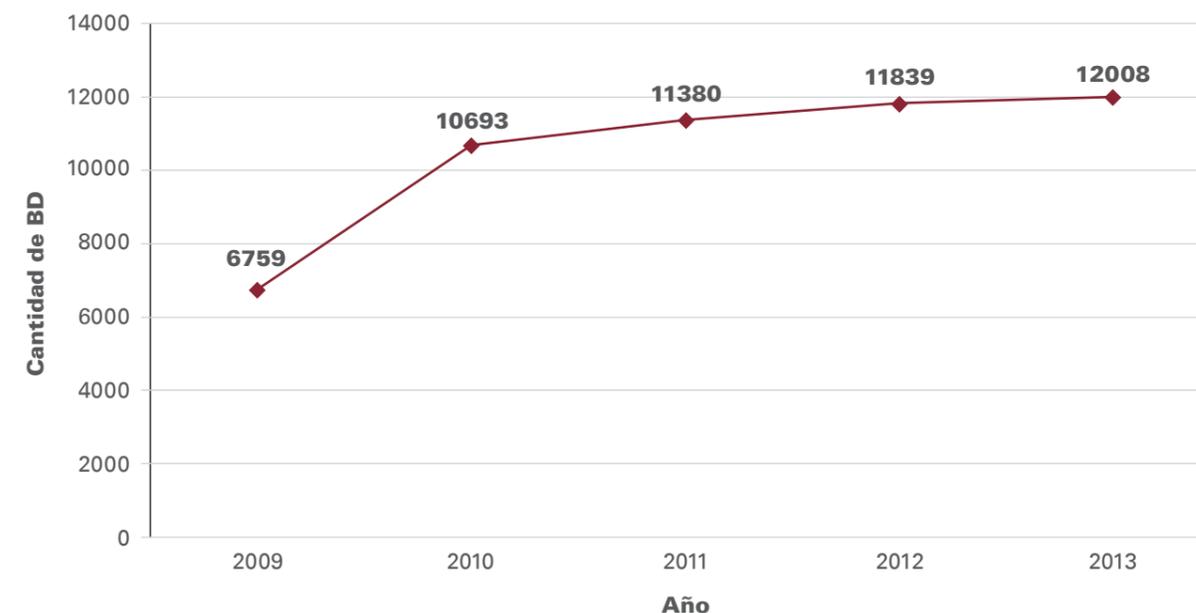
Cantidad de Bases de Datos por Tipo de responsable



Al igual que años anteriores, se observa por parte de las personas jurídicas la voluntad de cumplir con lo establecido en la normativa vigente en cuanto a la protección de datos personales, y en particular, con la obligación de inscribir las bases de datos personales que poseen.

En el gráfico siguiente se muestra la evolución en la cantidad de bases de datos totales presentadas ante la Unidad. En el mismo, se observa que durante 2013 el ritmo de inscripciones ha decrecido sensiblemente con respecto a años anteriores.

Evolución de la cantidad de BD presentadas



Distribución territorial

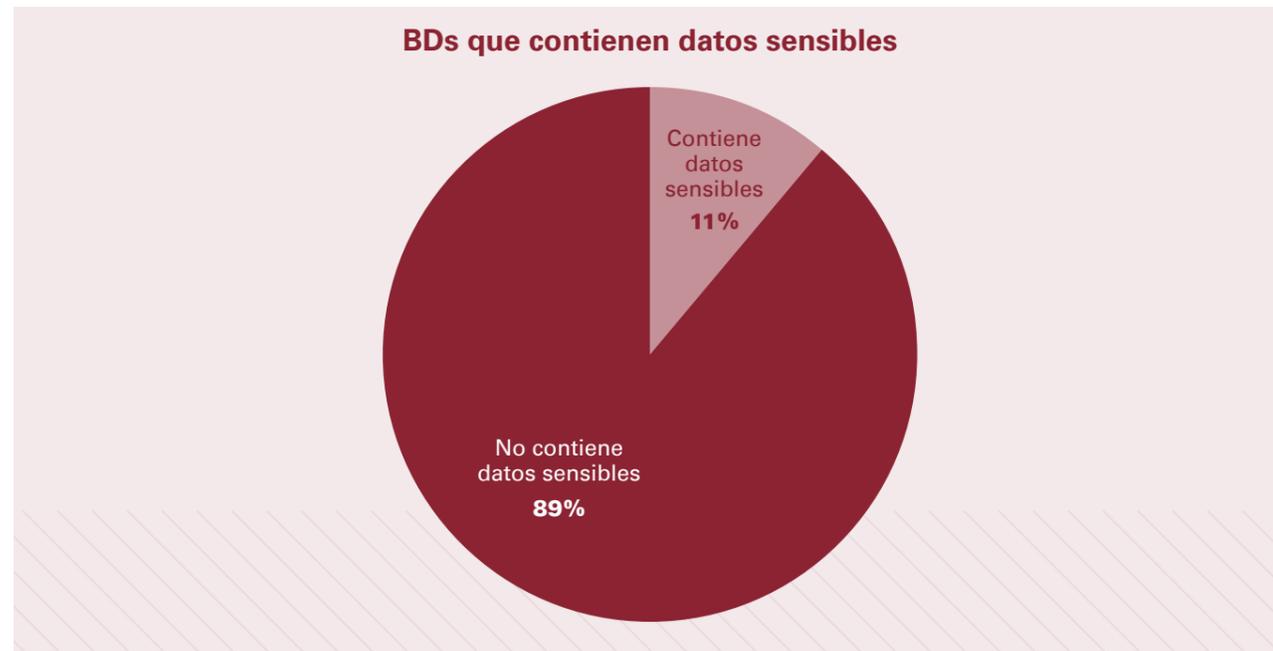
La siguiente tabla muestra la distribución territorial según la ubicación física de las bases de datos, agrupadas por departamentos, confirmándose una concentración en la capital de nuestro país, que coincide con la masa poblacional del Departamento.

| País | Departamento | Cantidad de BDs |
|-----------|----------------|-----------------|
| Uruguay | Montevideo | 121 |
| | Salto | 0 |
| | Canelones | 7 |
| | Maldonado | 7 |
| | San José | 1 |
| | Soriano | 2 |
| | Colonia | 13 |
| | Paysandú | 0 |
| | Lavalleja | 0 |
| | Cerro Largo | 1 |
| | Flores | 0 |
| | Rivera | 2 |
| | Tacuarembó | 0 |
| | Durazno | 2 |
| | Treinta y Tres | 0 |
| Rocha | 1 | |
| Florida | 1 | |
| Río Negro | 1 | |
| Artigas | 0 | |
| Otros | | 10 |

Datos sensibles

Interesa destacar la existencia de base de datos que contienen datos especialmente protegidos, como son los sensibles. A continuación, se muestra un gráfico con los resultados a la respuesta afirmativa en relación con quienes guardan datos relacionados con:

- Salud
- Vida sexual
- Convicciones Religiosas
- Preferencias Políticas
- Afiliaciones Sindicales
- Origen racial o étnico

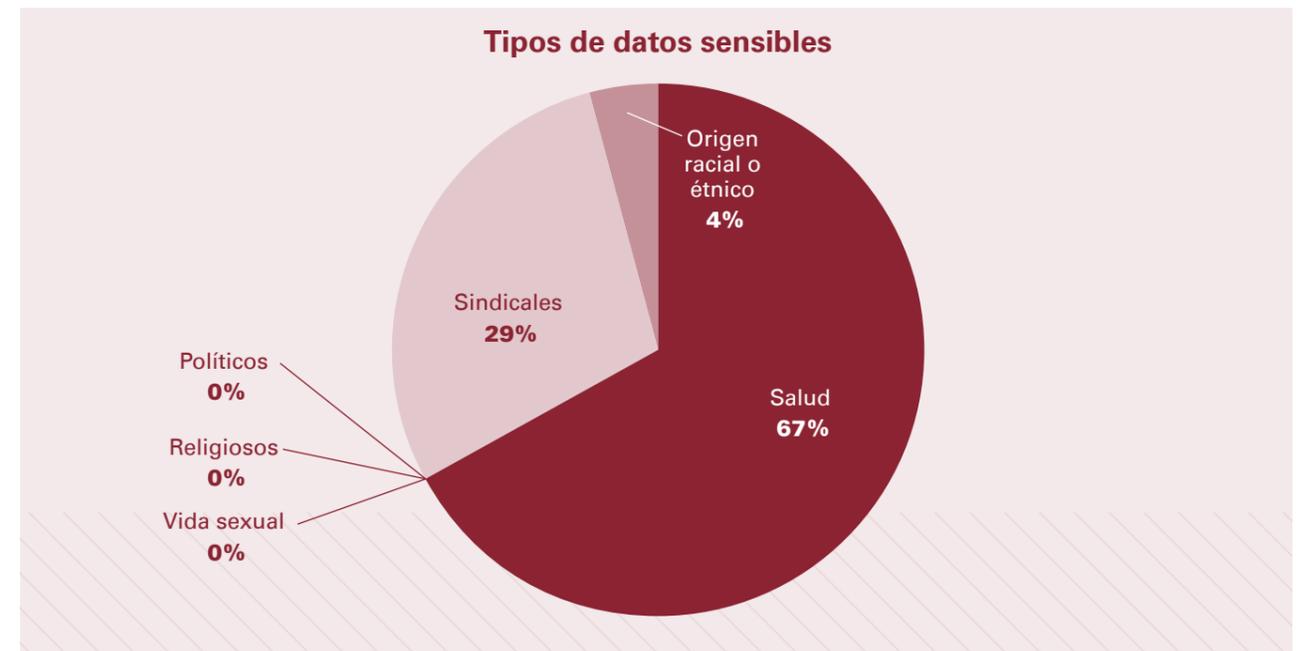


De los datos obtenidos, se observa que el 11% de las bases de datos registran datos sensibles.

En el siguiente gráfico se presenta el desglose de las bases que guardan datos sensibles. Al igual que años anteriores se mantiene predominancia de datos de salud y sindicales.

En Uruguay, las organizaciones sean públicas o privadas exigen a sus funcionarios la presentación del carné de salud con el que se certifica que la persona está apta para ejercer su función. Si bien las empresas solo tienen acceso al carnet propiamente tal, es declarado como dato de salud al momento de completar el registro.

En cuanto a los datos sindicales, las organizaciones sostienen que los datos sindicales son mantenidos con la única finalidad del descuento de la cuota de afiliación al sindicato.



Transferencias internacionales

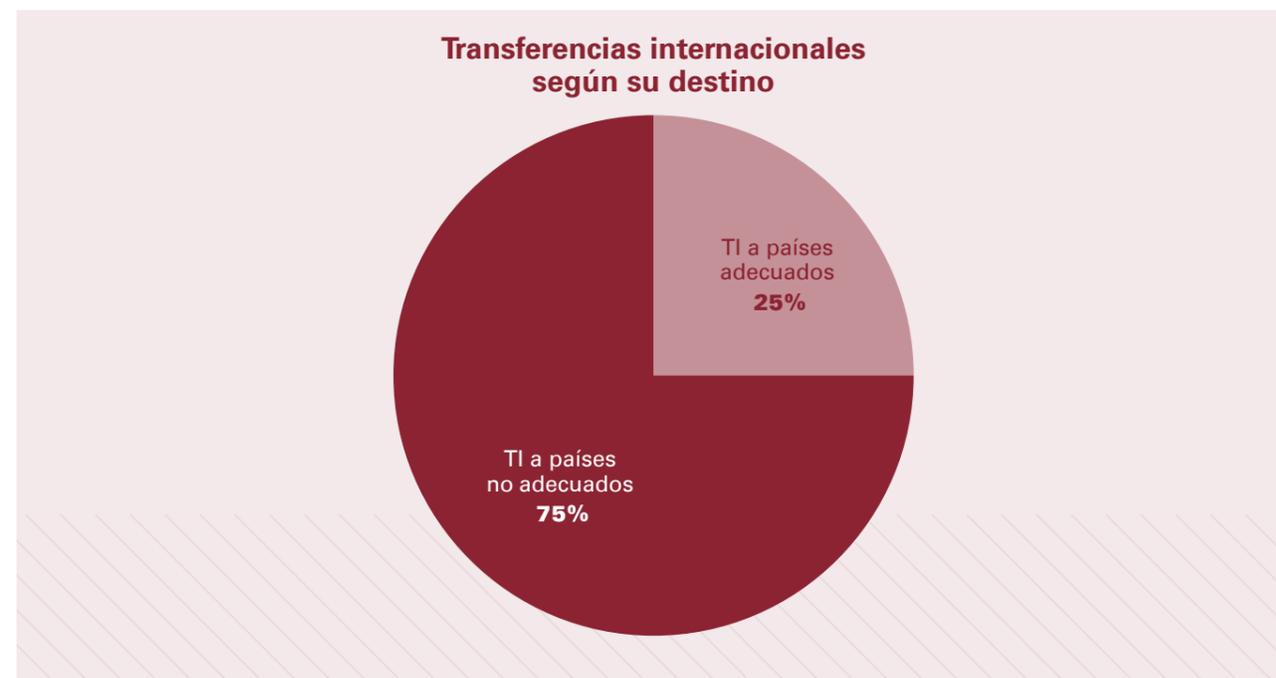
De acuerdo con el art. 23 de la Ley N° 18.331, los datos personales pueden ser transferidos internacionalmente siempre y cuando cumplan con los requisitos establecidos en el mencionado artículo. Por esta razón, interesa conocer datos estadísticos sobre transferencias internacionales y en particular a qué países.

Del total de bases de datos presentadas durante el 2013, aquellas que efectúan transferencias internacionales representan un 8% del total.



Resulta de interés clasificarlas considerando si el país de destino tiene o no nivel adecuado, de acuerdo con lo dispuesto por la Resolución N° 17, de 12 de junio de 2009, del Consejo Ejecutivo de la URCDP.

Se constata que una cuarta parte de las transferencias internacionales se realizan a países adecuados.



Durante el año 2013 la mayoría de las bases de datos presentadas que realizan transferencias internacionales lo hacen hacia Estados Unidos. Históricamente, el destino principal era Argentina, la cual ahora se encuentra en el segundo lugar.

La tabla siguiente presenta el ranking de los cinco países hacia donde se realiza la mayor cantidad de transferencias internacionales de datos desde Uruguay, como país de origen:

| Puesto | País |
|--------|-----------|
| 1 | EEUU |
| 2 | Argentina |
| 3 | Alemania |
| 4 | Brasil |
| 5 | Suecia |

Tipos de Información según su finalidad

Las bases de datos personales pueden almacenar diferentes tipos de información según su finalidad. La gran mayoría de las bases de datos sólo contienen datos identificatorios y de carácter personal. Sin embargo, hay muchas otras que adicionalmente almacenan otro tipo de información personal, que son datos especialmente protegidos de acuerdo con la normativa vigente.

Los datos especialmente protegidos son los siguientes:

- Datos sensibles
- Datos relativos a la salud
- Datos personales transferidos internacionalmente
- Telecomunicaciones (conservación de los datos de tráfico en las comunicaciones electrónicas)
- Datos de bases de datos con fines de publicidad
- Datos relativos a la actividad comercial o crediticia

La tabla siguiente muestra datos que reflejan la situación con respecto a las bases de datos que guardan diversos tipos de información, incluyendo algunos que están especialmente protegidos:

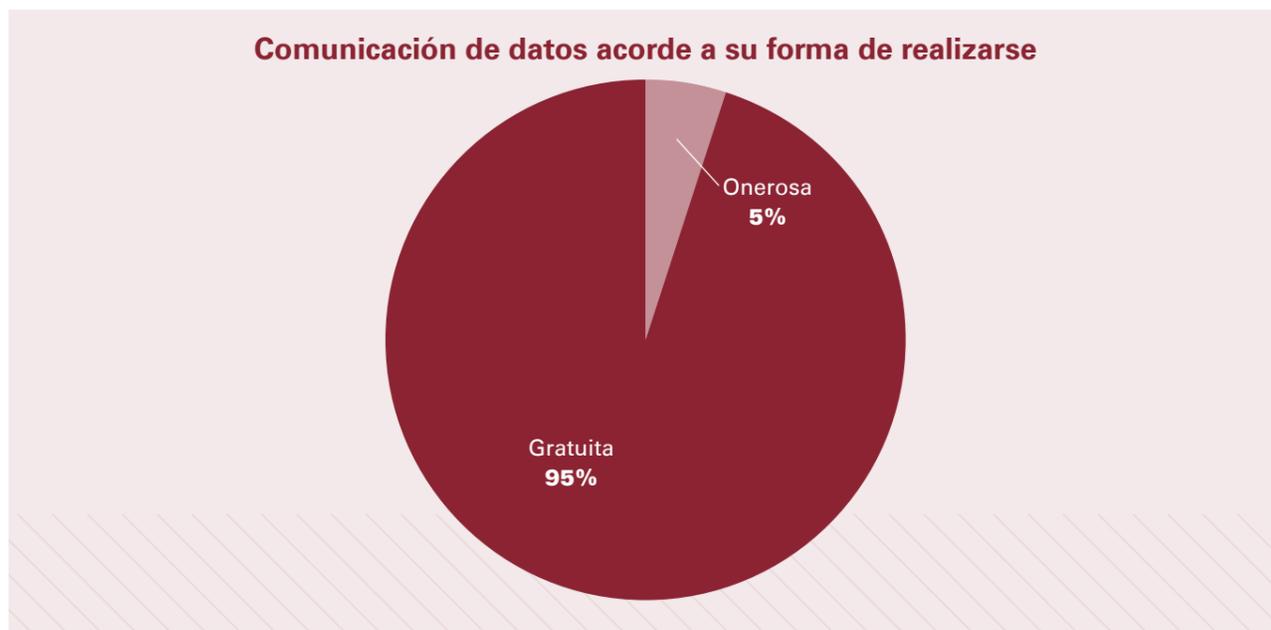
| Tipo de dato | % bases en 2013 |
|-----------------------------------|-----------------|
| Remuneraciones | 20,45 |
| Datos bancarios | 13,64 |
| Datos impositivos | 6,82 |
| Seguros | 3,41 |
| Deudas | 3,41 |
| Créditos, préstamos, avales | 3,41 |
| Estados contables | 5,68 |
| Historial créditos | 3,41 |
| Tarjetas de crédito | 9,09 |
| Hipotecas | 1,14 |
| Cuentas suspendidas y clausuradas | 4,55 |

Cesiones o comunicaciones de datos

La proporción de bases de datos de las cuales se realizan cesiones o comunicaciones de datos representa el 33% del total de bases presentadas, tal como se presenta en el siguiente gráfico.



De las bases de datos de las cuales se comunican o ceden datos personales interesa conocer en su desglose si la comunicación se realiza de forma gratuita u onerosa.

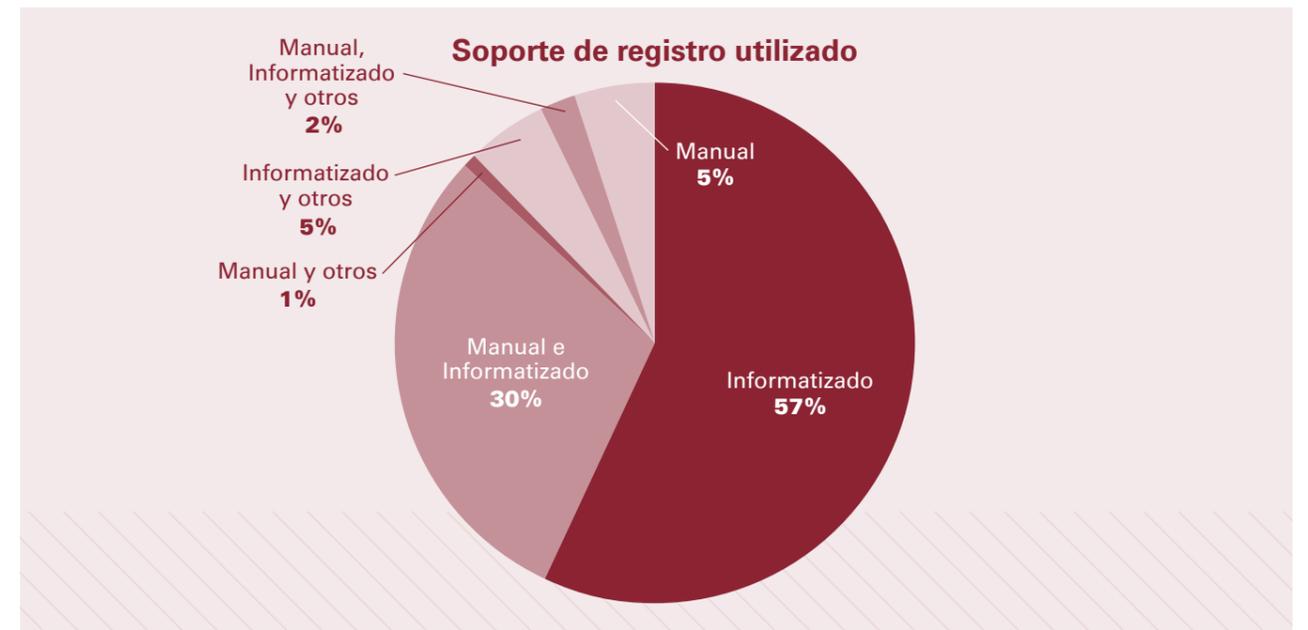


Tipo de soporte de registro de base de datos

Interesa en este punto destacar los soportes utilizados:

- Manual
- Informatizado
- Manual e informatizado (mixto)
- Otros

Tal como se puede observar en el gráfico, se verifica mayoritariamente el uso de soporte informatizado como forma de registrar datos.

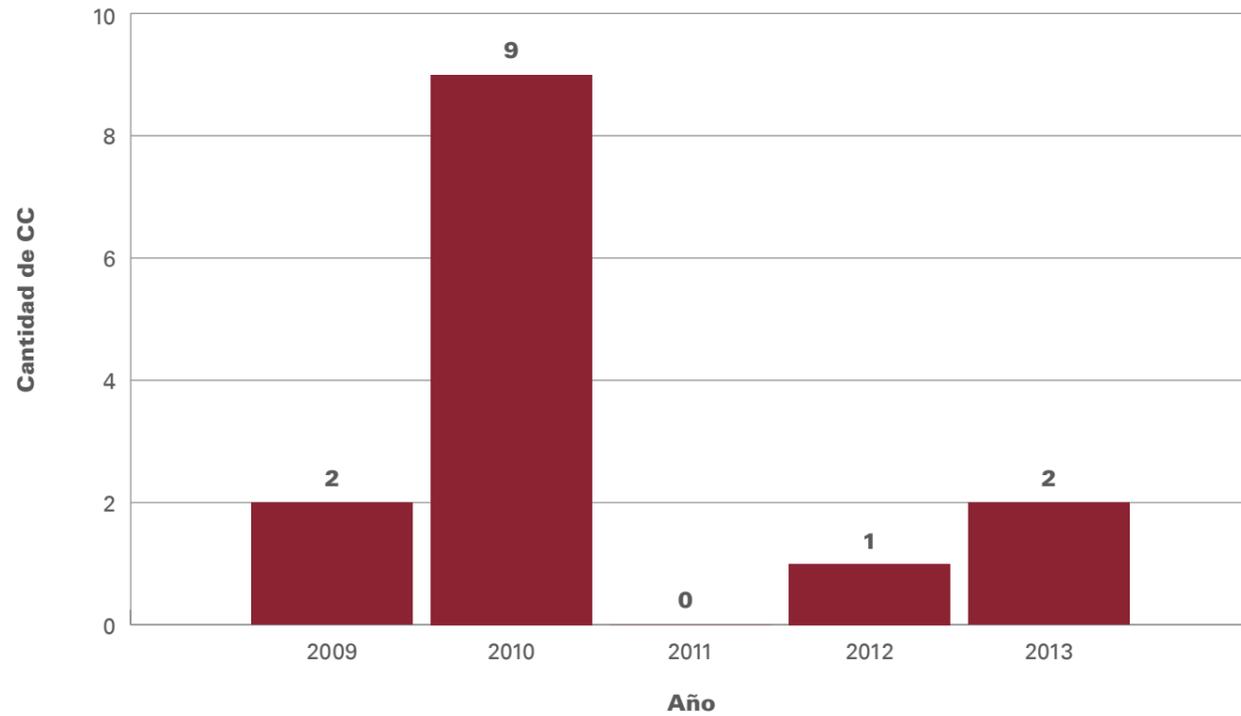


Códigos de conducta

Adicionalmente a la inscripción de base de datos personales los responsables pueden inscribir los códigos de conducta relativos al tratamiento de datos personales.

Durante el año 2013 se presentaron ante la Unidad dos códigos de conducta. A continuación, se muestra la evolución de la cantidad de inscripciones de códigos de conducta desde el inicio de la actividad de la URCDP.

Cantidad de Códigos de Conducta por año



Bases de datos inscriptas en la URCDP

Las bases de datos presentadas ante la URCDP pasan por un completo control de cumplimiento de la normativa vigente, el cual consiste en tres evaluaciones: jurídica, notarial y técnica.

La evaluación jurídica es realizada por un abogado que analiza si las bases de datos cumplen o no con la normativa vigente de protección de datos personales, y eventualmente solicita aclaraciones a su responsable si es necesario.

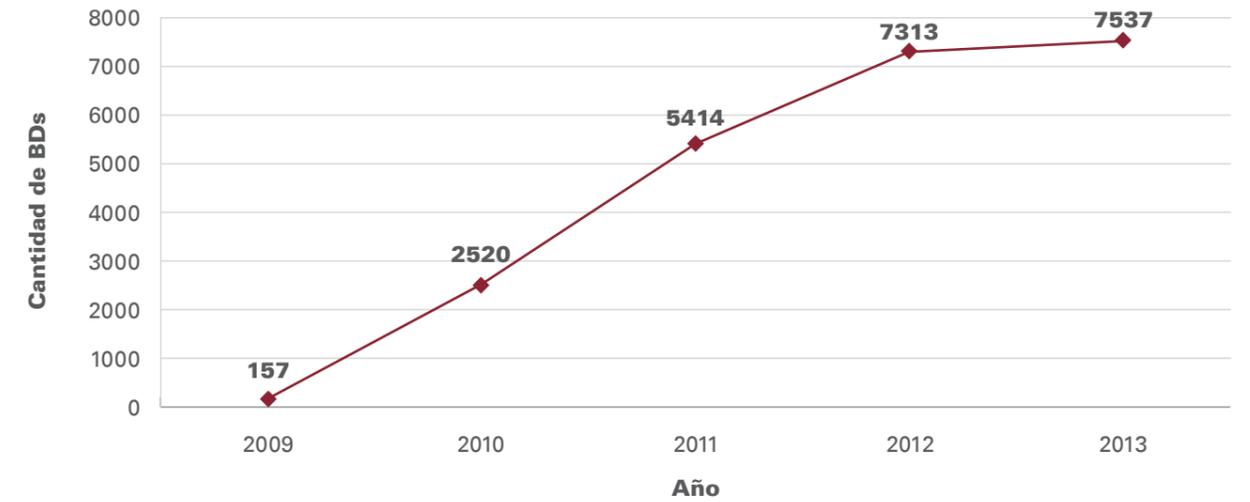
La evaluación notarial realizada por un escribano público, que analiza la correcta representación de la empresa que solicita la inscripción de la base de datos en cuanto a las formalidades y requisitos de representación, también puede solicitar aclaraciones si son necesarias.

La evaluación técnica donde un ingeniero en computación realiza las recomendaciones de seguridad pertinentes para las bases de datos que contengan datos especialmente protegidos o cuyas medidas de seguridad sean insuficientes.

Luego de realizados los controles, el Consejo Ejecutivo de la URCDP dicta la Resolución donde se establece que la base de datos queda efectivamente inscripta en el Registro de Bases de Datos Personales.

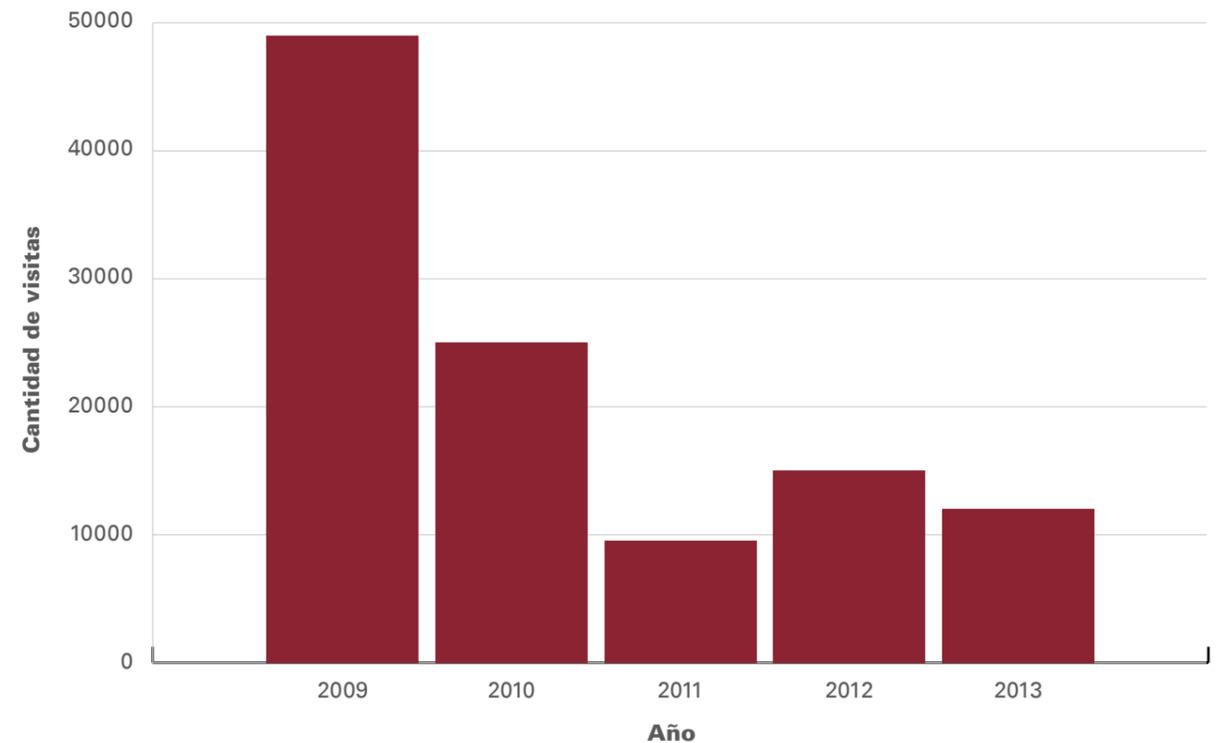
El gráfico siguiente muestra la evolución anual de la cantidad de base de datos inscriptas:

Evolución anual de la cantidad de BDs inscriptas



Cantidad de visitas al sitio Web de la URCDP

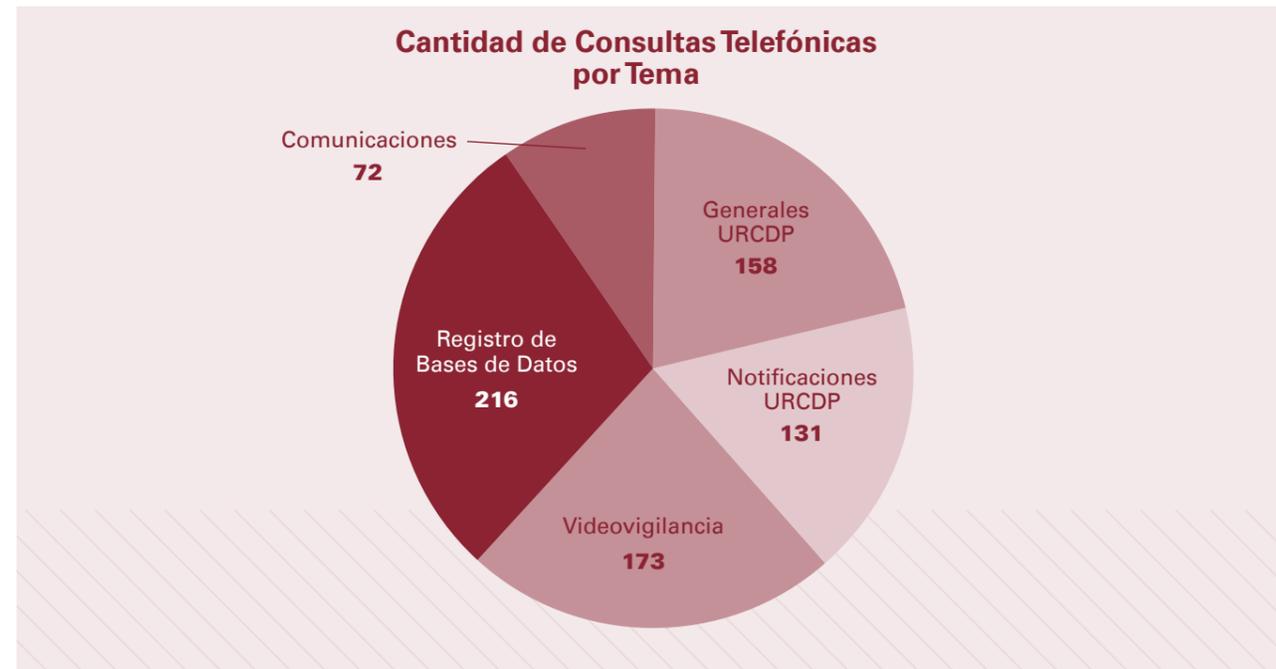
Respecto a las visitas registradas en números, se constata el registro de la mayor cantidad durante el año 2009, año de inicio de actividades de la URCDP y durante el cual vencía el plazo para la inscripción de bases de datos personales existentes.



Consultas a la mesa de ayuda de la URCDP

La mesa de ayuda de AGESIC atiende anualmente una importante cantidad de consultas formuladas a la Unidad. Las consultas son atendidas de manera personalizada en las oficinas de AGESIC, telefónicamente, vía correo electrónico y mediante el formulario de contacto de la web de la URCDP.

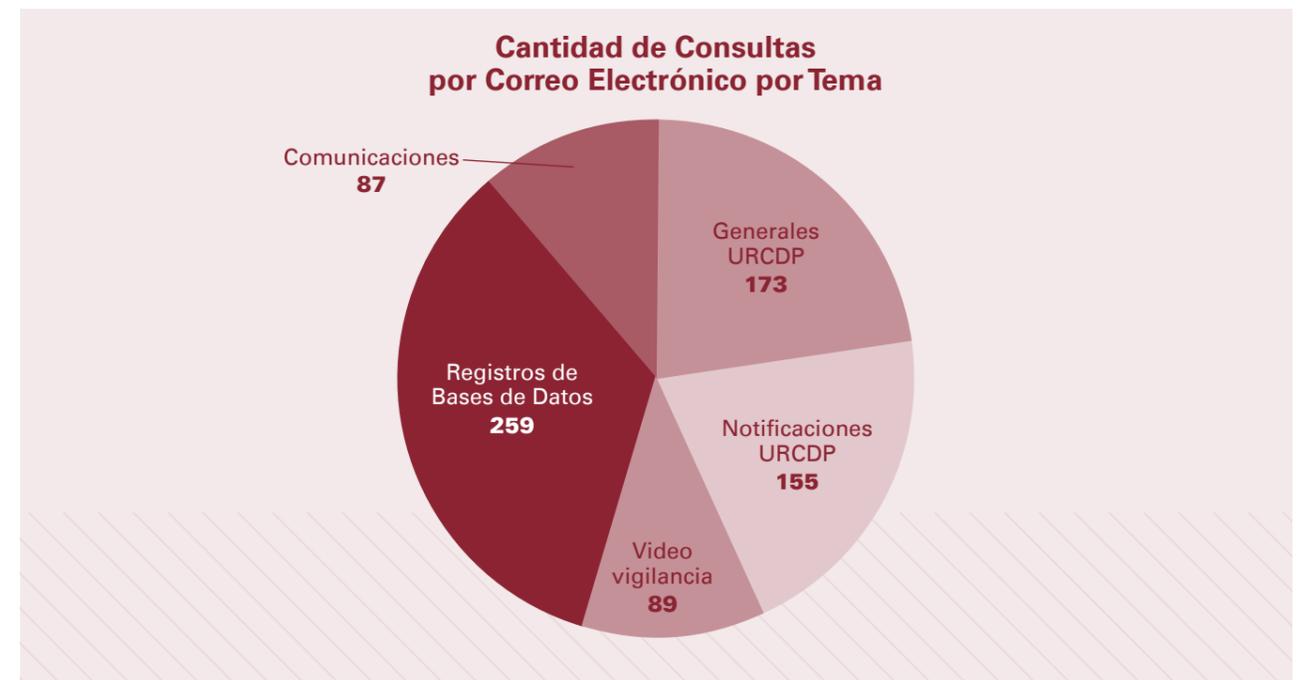
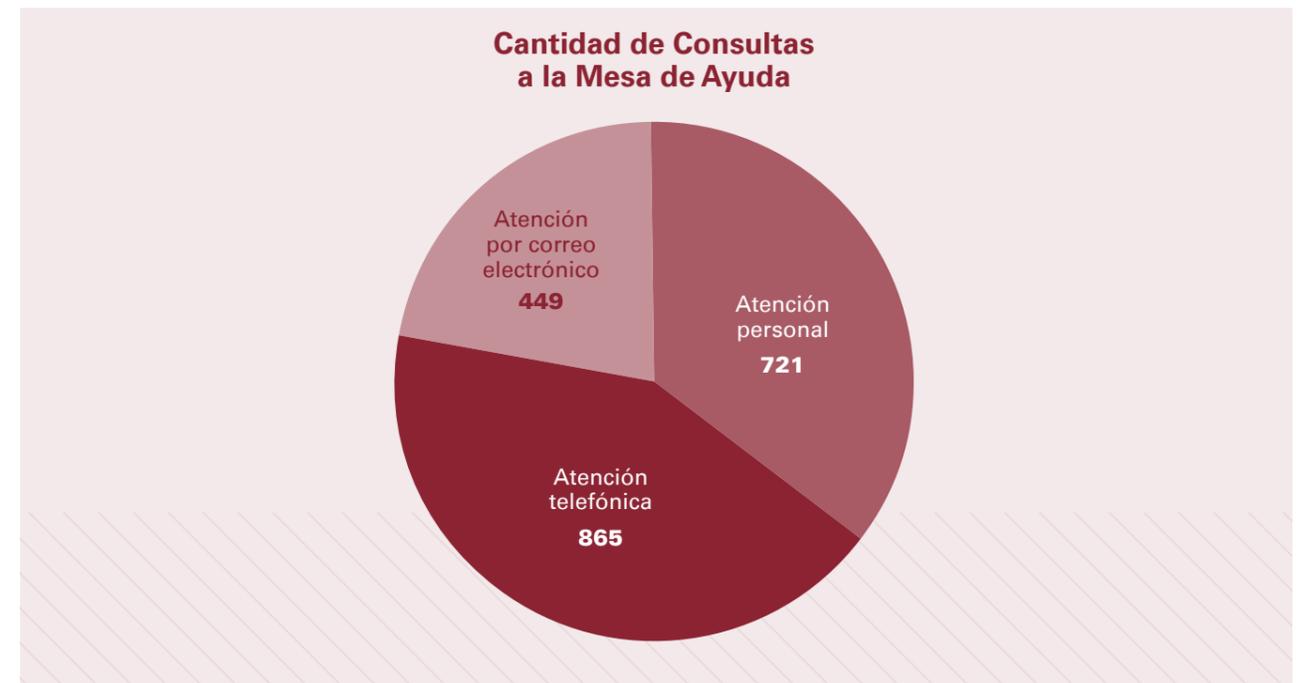
En el 2013 se recibieron 865 consultas telefónicas, las cuales se clasifican por tema en la gráfica siguiente:



La Unidad atiende en forma permanente a los ciudadanos a través del área de asesoría de la Gerencia de Derechos Ciudadanos de AGESIC.

Las consultas son recibidas y evacuadas en forma telefónica, vía correo electrónico, a través de la web y en forma personal.

Durante el año 2013 se recibieron 2035 consultas en total.



Expedientes presentados por consultas y denuncias

Debido a la difusión realizada por la Unidad y el mayor conocimiento de la ciudadanía respecto de sus derechos en materia de protección de datos personales, y al cumplimiento por parte de los organismos, empresas y personas físicas en los años que lleva la URCDP sensibilizando a la población en el tema, es que durante el año 2013 las denuncias han decrecido y las consultas se han mantenido respecto a las presentadas al año anterior.

Durante el 2013 la Unidad recibió 31 consultas y 43 denuncias.

Los principales motivos de denuncia fueron relativos a la video vigilancia, la comunicación de datos, la seguridad de los datos, y el ejercicio del derecho de acceso ante organismos del Estado.

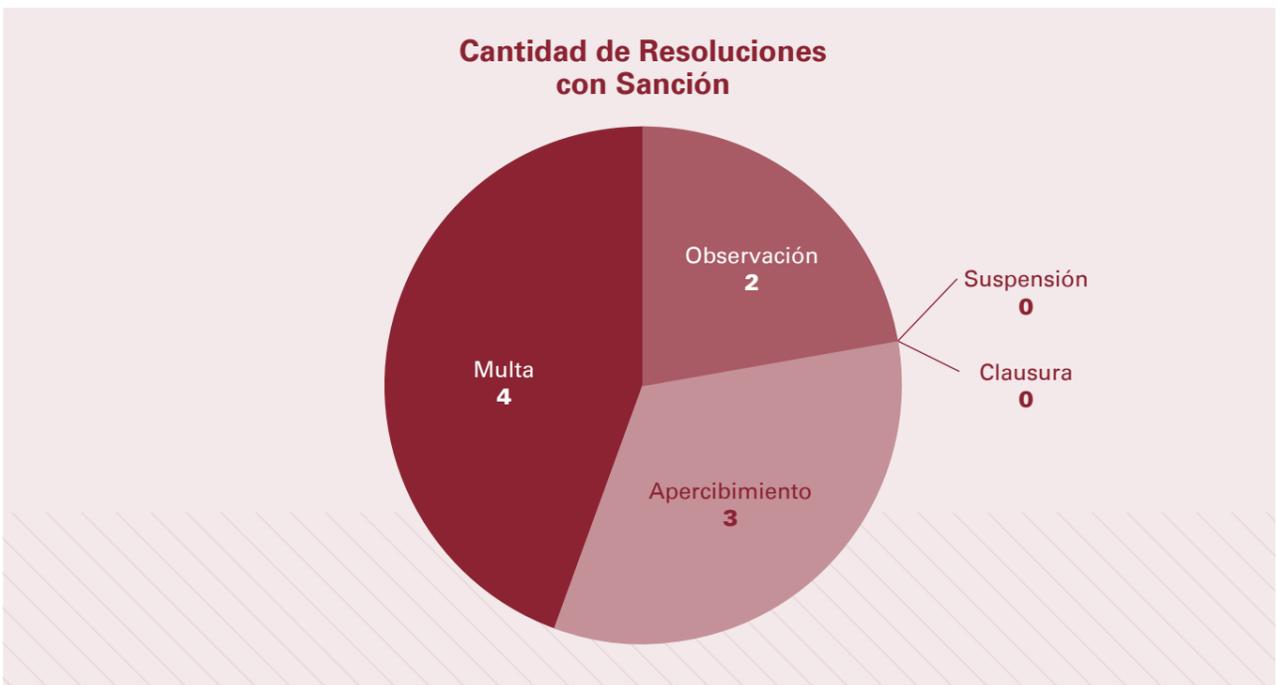
En lo referente a consultas realizadas ante la Unidad, los principales temas fueron: video vigilancia, comunicaciones de datos, relativas al alcance del artículo 22 de la Ley N° 18.331, transferencias internacionales de datos, publicidad, inscripción de base de datos, y trámite de los expedientes presentados.



Resoluciones que imponen sanciones

La Unidad, conforme lo dispuesto por el artículo 35 de la Ley, en la redacción dada por el artículo 152 de la Ley N° 18.719, de 27 de diciembre de 2010 podrá aplicar sanciones a los responsables de las bases de datos, encargados de tratamiento de datos personales y demás sujetos alcanzados por el régimen legal, en que se violen las normas de la presente ley, las que se graduarán en atención a la gravedad, reiteración o reincidencia de la infracción cometida, comenzando con una observación hasta llegar a la clausura de la base de datos mediante un procedimiento especial.

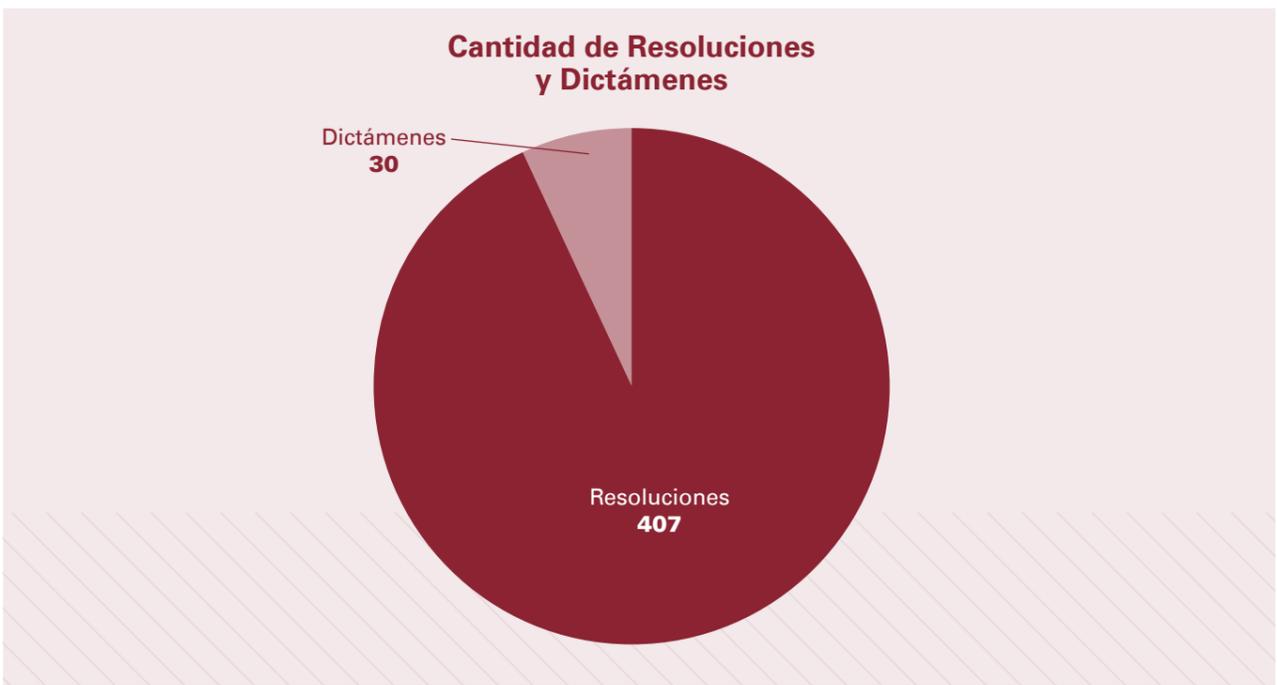
Durante el 2013 fueron aplicadas por contravenir la normativa vigente de protección de datos personales: 2 observaciones, 3 apercibimientos y 4 multas.



Resoluciones y dictámenes realizados en 2013

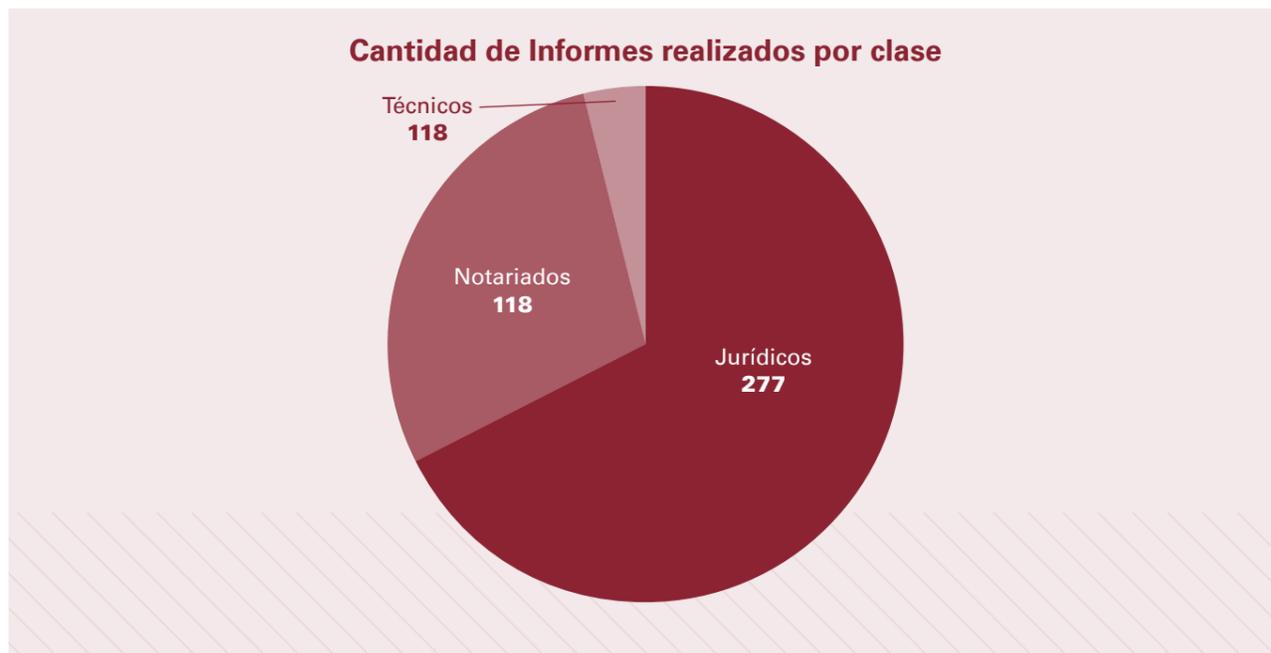
Durante el año 2013 se realizó el análisis de expedientes presentados ante la URCDP. Se expidieron 407 Resoluciones y 30 Dictámenes.

El ciudadano puede acceder a estos documentos a través del sitio web de la Unidad: <http://www.datospersonales.gub.uy>



Cantidad de informes realizados

El estudio de los diferentes expedientes que se han estudiado durante el año 2013 ha producido un total de 410 informes, los cuales se dividen en: jurídicos, notariales y técnicos.



Como se destaca en el gráfico, se realizaron 277 informes jurídicos, 118 notariales y 15 técnicos.



08

La URCDP ante los nuevos retos en materia de protección de datos

de protección de datos
nuevos retos en materia
de protección de datos

8. La URCDP ante los nuevos retos en materia de protección de datos

Proyectos a realizar en el año 2014

Para el 2014, la Unidad se ha fijado varias líneas de acción dedicadas a mejorar el relacionamiento con la ciudadanía en pro de la mejora de la protección de los datos personales.

Se continuará con la capacitación sectorial, reforzando iniciativas hacia los sectores de la salud y la educación. Sectores en los que se tratan gran cantidad de datos personales, sobre todo de una parte de la población sensible como son los niños y adolescentes, así como datos especialmente protegidos como los datos sensibles en el área de la salud.

Se aumentará la sensibilización de protección de datos personales en la ciudadanía mediante el fortalecimiento de los mecanismos de difusión como por ejemplo en eventos, lugares públicos y específicos con acceso a la población.

La Campaña “Tus datos valen. Cuídalos” continuará desarrollándose durante el 2014. Asimismo, se extenderán algunas acciones de sensibilización sobre la temática a los jóvenes.

Se generarán acciones específicas para aumentar el porcentaje de cumplimiento de la Ley en cuanto a su aplicación y alcance, fortaleciendo por ejemplo el registro de bases de datos de las instituciones públicas y privadas.

Se realizará un plan de procesos de auditorías, a nivel nacional, tanto para las instituciones públicas como privadas, manteniendo una actitud colaborativa con el administrado para solucionar las observaciones que se encuentren.

Se continuará con la mejora de la gestión simplificando los procesos de registros de bases de datos para que el ciudadano tenga más celeridad en el proceso.

Se profundizará el tema de cooperación internacional mediante la firma de convenios internacionales con las demás Autoridades de Protección de Datos Personales, la participación en los grupos de trabajo de la Red Iberoamericana de Protección de Datos Personales, del Consejo de Europa, de la Conferencia Internacional de Autoridades de Protección de Datos Personales y Privacidad.

Se trabajará para mantener la posición de Uruguay a nivel internacional como referente en la materia.

Anexo Normativo

Ley N° 19.149 de 24 de octubre de 2013, artículo 75. Rendición de Cuentas y Balance de Ejecución Presupuestal Ejercicio 2012

Información disponible

Decreto Supremo N° 003-2013-JUS, de 21 de marzo de 2013, por el que se aprueba el Reglamento de la Ley N° 29.733, de Protección de Datos Personales de la República del Perú

Información disponible

Decreto N° 1377, de 27 de junio de 2013, por el cual se reglamenta la Ley N° 1581 de 2012 de la República de Colombia

Información disponible

Ley N° 172-13, de 26 de noviembre de 2013, sobre Protección de Datos de carácter personal, de la República Dominicana

Información disponible

