etiqampus
e-Learning en Integridad

Guía Comparada Protección de Datos Personales: casos Bolivia, Paraguay y Uruguay.

Compliance Internacional

NIVEL INTERMEDIO

Fecha	Marzo 2025
Tpo. de lectura	27 min.

El avance tecnológico y la transformación digital han puesto la protección de datos personales en el centro del debate regulatorio a nivel global. En Latinoamérica, el desarrollo y fortalecimiento de normativas en esta materia reflejan la creciente necesidad de garantizar la privacidad y seguridad de la información en un entorno empresarial cada vez más interconectado.

La evolución de estas regulaciones y su aplicación práctica imponen nuevos desafíos a las organizaciones, que deben adaptar sus procesos y modelos de negocios para cumplir con estándares más altos y responder a las exigencias de las autoridades regulatorias y fiscalizadoras.

En este contexto, especialista de destacadas firmas legales de 18 países miembros de Compliance Latam, han elaborado esta guía que, además de dar una visión clara y actualizada sobre los marcos normativos y últimas tendencias en protección de datos personales, entrega herramientas clave para que las empresas comprendan y gestionen los riesgos asociados al tratamiento de datos, fomenten una cultura de cumplimiento y refuercen la confianza con sus clientes y socios comerciales.

A continuación te presentamos la sección dedicada a Bolivia, Paraguay y Uruguay y escrita por los siguientes profesionales del estudio Ferrere:

- Alberto Rivera, Asociado Senior Bolivia, Derecho Corporativo, Propiedad Intelectual, Derecho Administrativo y Regulatorio.
- Jorge Plaza, Asociado Senior Bolivia, Derecho Corporativo, Fusiones y Adquisiciones, Compliance, TMT, Privacidad y Tecnologías de la información.
- Martín Pesce, Socio Uruguay, Protección de Datos, Nuevas Tecnologías.
- María Canziani, Asociada Senior Uruguay, Derecho Administrativo y Corporativo.
- Montserrat Puente, Asociada Senior Paraguay, Propiedad Intelectual y Asuntos Regulatorios.
- Galo Molinas, Asociado Paraguay, Propiedad Intelectual y Asuntos Regulatorios.

FUENTE: el texto de esta portadilla se elaboró a partir de la introducción de la "Guía Comparada Protección de Datos Personales" publicada por la plataforma "Compliance Latam".

Guía Comparada Protección de Datos Personales

Marzo 2025



www.compliancelatam.legal



FERRERE

Autores:

Alberto Rivera, Asociado Senior Bolivia, Derecho Corporativo, Propiedad Intelectual, Derecho Administrativo y Regulatorio.

Jorge Plaza, Asociado Senior Bolivia, Derecho Corporativo, Fusiones y Adquisiones, Compliance, TMT, Privacidad y Tecnologías de la información.

Martín Pesce, Socio Uruguay, Protección de Datos, Nuevas Tecnologías.

María Canziani, Asociada Senior Uruguay, Derecho Administrativo y Corporativo.

Montserrat Puente, Asociada Senior Paraguay, Propiedad Intelectual y Asuntos Regulatorios.

Galo Molinas, Asociado Paraguay, Propiedad Intelectual y Asuntos Regulatorios.

Bolivia

1. ¿Cuál es el marco regulatorio de la protección de datos personales en tu jurisdicción?

Bolivia es uno de los pocos países de la región que no cuenta con una ley de protección de datos personales de carácter general. En su lugar, la protección de datos personales naturales es de carácter constitucional, complementada por regulación concreta para determinadas áreas reguladas.

A nivel constitucional, la Constitución Política del Estado Plurinacional de Bolivia reconoce la figura de la Acción de Protección de Privacidad mediante la cual toda persona individual que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de datos registrados por cualquier medio físico, electrónico, magnético o informático, o que afecten a su derecho fundamental a la intimidad y privacidad o a su propia imagen, podrá reclamar la restitución de sus derechos al juez o tribunal competente.

Por otra parte, la Ley General de Telecomunicaciones (Ley 164) y el Decreto Supremo No. 1793 que aprueba el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación (D.S. 1793) establecen, de manera escueta, normas generales sobre los derechos de usuarios de servicios de telecomunicaciones en materia de privacidad. Estos destacan la obligación de contar con el consentimiento previo, expreso e informado del titular de los datos, antes de su recopilación y tratamiento; y la obligatoriedad de implementar medidas de seguridad conforme con el estado de la tecnología y apropiados para la naturaleza de los datos almacenados.

Finalmente, la Ley de Servicios Financieros (Ley 393) también establece obligaciones específicas para la privacidad de usuarios de entidades financieras, como la regulación del secreto bancario.

2. ¿Existe en tu país regulación sobre programas de prevención de infracciones o de cumplimiento en materia de protección de datos personales? ¿Son obligatorios? ¿En qué casos?

No. El marco regulatorio boliviano, tanto en materia de protección de datos como en materia de compliance, no contempla la obligación de contar con programas de prevención de infracciones para el sector público o privado. No obstante, como indicamos en la respuesta anterior, el D.S. 1793 sí establece la necesidad de que los responsables del tratamiento de datos personales hayan establecido previamente las medidas de seguridad necesarias.

3. ¿Qué contenido mínimo deben tener los programas de cumplimiento en protección de datos personales en tu país?

No aplicable, conforme a lo explicado en la respuesta anterior.

4. ¿Qué beneficios trae contar al interior de la organización con un programa de cumplimiento en protección de datos personales?

Aunque el sector privado no tiene la obligación de implementar programas de cumplimiento que aseguren la protección de datos personales tratados por dicha entidad, implementar voluntariamente este tipo de programas puede generar los siguientes beneficios:

- Generación de confianza entre los clientes de la entidad, proyectando una imagen de profesionalismo e incrementando su reputación dentro del mercado.

- Reducción de vulnerabilidades, anticipando respuestas y soluciones ante posibles amenazas de ciberseguridad.

- Mejoramiento de los procedimientos internos en el tratamiento de datos, evitando que personal de la entidad pueda comprometerla al vulnerar el derecho de privacidad de terceros durante el cumplimiento de sus funciones.

- Facilitación para justificar la implementación previa de medidas de seguridad adecuadas y procedimientos de mitigación eficaces, en caso de que se presenten incidentes de seguridad. Esto para disminuir el riesgo de responsabilidad y sanciones frente a estos sucesos.

5. ¿Existen procesos de certificación de los programas de cumplimiento en protección de datos en tu país? ¿Quién realiza la certificación?

No, debido a que la implementación de dichos programas de cumplimiento no es obligatoria en Bolivia.

No obstante, el Instituto Boliviano de Normalización y Calidad (IBNORCA), organización sin fines de lucro creada por el Decreto Supremo No. 23489 cuya finalidad es la realización de actividades de normalización técnica y certificación de calidad, sí ha establecido los lineamientos para la implementación de la norma ISO/IEC 27001 en empresas bolivianas. IBNORCA otorga

estas certificaciones, previo cumplimiento del proceso respectivo, a las entidades públicas o privadas que lo requieran.

6. ¿En tu jurisdicción es obligatorio contar con un delegado de protección de datos personales? ¿En qué casos?

No. El marco normativo boliviano en materia de protección de datos no contempla la figura del delegado de protección de datos personales.

7. ¿Existen sanciones asociadas al incumplimiento de la normativa sobre protección de datos personales? ¿De qué tipo? ¿A cuánto ascienden las multas?

Debido a que no existe una ley de protección de datos en Bolivia, tampoco existen sanciones específicas por el incumplimiento de obligaciones en cuanto al recojo y tratamiento de datos personales.

No obstante, dado que el Código Civil boliviano reconoce al derecho a la intimidad (entendido como el derecho a que nadie perturbe, ni divulgue la vida íntima de una persona) un derecho civil, quien se vea afectado en su derecho a la intimidad podría solicitar el resarcimiento por el hecho ilícito mediante un proceso ordinario en vía civil.

8. ¿Qué tipo de conducta sanciona la normativa en protección de datos personales de tu país?

Dado que no existe una ley de protección de datos en Bolivia, tampoco existen sanciones por la realización de conductas que puedan afectar los derechos de los titulares de datos personales. En ese sentido, en virtud del principio de tipicidad reconocido en la Constitución Política del Estado, en la actualidad no se pueden implementar sanciones administrativas por el incumplimiento de obligaciones de protección de datos en los sectores regulados antes mencionados.

No obstante, sobre la base de las obligaciones establecidas en la Ley 164 y en el D.S.1793, las siguientes conductas contradicen lo establecido en materia de protección de datos:

• Recolección, conservación y procesamiento de datos personales sin el conocimiento previo y el consentimiento expreso de su titular.

• Transferencia de datos personales sin consentimiento previo y expreso del titular de los datos, o por orden escrita de la autoridad judicial competente.

• Acción omisa ante revocatoria del consentimiento otorgado.

• Utilización de los datos para finalidades distintas de las expresadas al momento de su recolección y registro.

• Afectación a los derechos de los titulares de los datos personales a solicitar el acceso, rectificación, actualización, cancelación, objeción y/o revocación de datos personales.

• No adopción de medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida o tratamiento no autorizado.

9. ¿Tu jurisdicción tiene un organismo técnico que dicte directrices y fiscalice el cumplimiento de las normas de protección de datos personales?

La autoridad competente para proteger los derechos de usuarios y consumidores, de manera general, es el Viceministerio de Defensa del Consumidor.

En materia de protección de datos por medios de telecomunicación, la autoridad con competencia es la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT).

No obstante, ninguna de estas dos entidades ejerce de forma activa sus competencias en materia de protección de derechos de intimidad, privacidad y protección de datos de los usuarios. Tampoco se han emitido directrices en la materia.

10. ¿Cuáles son los primeros pasos que toman las organizaciones en tu país para comenzar a aplicar la normativa en protección de datos personales en general y un programa de cumplimiento en particular?

Cualquier organización que pretenda implementar un programa de cumplimiento de la normativa sobre protección de datos tiene que realizar los siguientes pasos:

• Realizar un diagnóstico inicial con el fin de determinar qué tipo de datos personales se suelen recolectar, la finalidad que se persigue para su tratamiento y la base legal que se requiere para obtener esos datos.

• Evaluar los posibles riesgos y determinar las medidas de seguridad necesarias para el tipo de datos identificados.

• Designación de funciones dentro del personal interno, para ejercer la tarea de supervisión de cumplimiento y gestión de la implementación de medidas de mitigación.

• Establecer los mecanismos de respuesta respectivos.

• Proceder con la redacción de la política de protección de datos.

• Relevamiento de acuerdos con proveedores.

11. ¿Cuál es el ámbito de aplicación territorial de la normativa de protección de datos de tu país? ¿La normativa puede aplicarse extraterritorialmente?

El ámbito de aplicación está circunscrito al territorio boliviano, no existiendo un alcance extraterritorial conforme a la normativa local.

Paraguay

1. ¿Cuál es el marco regulatorio de la protección de datos personales en tu jurisdicción?

En Paraguay, el marco regulatorio para la protección de datos está dado por la Constitución Nacional (CN) que, a través del Habeas Data garantiza el derecho de toda persona a acceder a la información que, sobre ella misma, o sus bienes, obran en bases de datos públicas o privadas de carácter público. Además, la CN reconoce el derecho a la protección de la vida privada de todos los habitantes, estableciendo que la intimidad de la persona y de la familia y el respeto a la vida privada son inviolables, garantizando el derecho a la protección de la intimidad, la dignidad y la imagen privada de la persona. Por lo tanto, la protección a los datos personales y la intimidad personal se encuentran consagradas en la Constitución Nacional.

En concordancia con las disposiciones de la CN, la Ley N.° 6534/2020 "De Protección de la Información Crediticia" ("Ley 6534") establece lineamientos generales al respecto del tratamiento de datos personales, y en particular, al respecto del tratamiento de datos personales de carácter crediticio.

2. ¿Existe en tu país regulación sobre programas de prevención de infracciones o de cumplimiento en materia de protección de datos personales? ¿Son obligatorios? ¿En qué casos?

No. Si bien la Ley 6534 establece obligaciones para los responsables de tratamiento de datos, la norma no prevé la obligación de contar con un programa de prevención de infracciones o de cumplimiento en materia de protección de datos personales.

3. ¿Qué contenido mínimo deben tener los programas de cumplimiento en protección de datos personales en tu país?

N/A.

4. ¿Qué beneficios trae contar al interior de la organización con un programa de cumplimiento en protección de datos personales?

•Aunque la normativa vigente no contempla incentivos específicos para la adopción de políticas internas de protección de datos, la implementación de un programa interno de cumplimiento en esta materia ofrece, sin duda, los siguientes beneficios:

• **Cumplimiento normativo:** La implementación de un programa de cumplimiento estructurado permite garantizar el cumplimiento de la normativa vigente, evitando multas, sanciones y responsabilidades legales derivadas de incumplimientos o malas prácticas.

• **Respuesta eficiente ante cambios y requerimientos regulatorios:** Contar con procedimientos claros y definidos facilita la gestión de solicitudes de autoridades regulatorias y titulares de datos, asegurando transparencia, cumplimiento de plazos y una rápida adaptación a los cambios normativos.

• **Reducción de vulnerabilidades:** Una política adecuada ayuda a prevenir ataques, y a optimizar la respuesta en casos de quiebres de seguridad.

• **Reputacional:** La adopción de programas de cumplimiento genera confianza y seguridad en los clientes, fortaleciendo la reputación de la empresa. Además, puede ser utilizada como una estrategia de marketing para diferenciarse en el mercado.

5. ¿Existen procesos de certificación de los programas de cumplimiento en protección de datos en tu país? ¿Quién realiza la certificación?

No, la Ley 6534 no prevé mecanismos de certificación de programas de cumplimiento en protección de datos. Sin embargo, no vemos impedimentos en obtener certificaciones a través de entidades extranjeras especializadas en la materia.

6. ¿En tu jurisdicción es obligatorio contar con un delegado de protección de datos personales? ¿En qué casos?

No, la Ley 6534 no obliga a los responsables a contar con un delegado o encargado de protección de datos.

7. ¿Existen sanciones asociadas al incumplimiento de la normativa sobre protección de datos personales? ¿De qué tipo? ¿A cuánto ascienden las multas?

Sí, la Ley 6534 prevé sanciones para personas y empresas que incumplan las disposiciones de la ley. Estas varían según el ámbito de operación de la empresa y pueden ir desde apercibimientos hasta el cierre definitivo de operaciones.

Las sanciones se clasifican en:

• Apercibimiento.

• Multa de hasta 15.000 jornales mínimos (aproximadamente USD 206.000).

• Multa agravada por reincidencia: En caso de repetición de una misma infracción, la multa será el doble de la inicialmente aplicada y podrá elevarse hasta 50.000 jornales mínimos (aproximadamente USD 690.000) para personas físicas o jurídicas con una facturación anual superior a G. 6.000.000.000 (seis mil millones de guaraníes) (aproximadamente a USD 761.200,00).

• Implementación de medidas.

• Suspensión de actividades relacionadas con el tratamiento de datos por un período máximo de seis (6) meses.

• Cierre temporal de operaciones vinculadas al tratamiento de datos, en caso de no adoptar las medidas correctivas ordenadas por la autoridad de control dentro del período de suspensión.

• Cierre inmediato y definitivo de la operación cuando involucre el tratamiento de datos sensibles.

• Inhabilitación para desempeñar cargos en el sistema financiero, crediticio y en sociedades de información de datos personales, por un período de seis (6) meses hasta cinco (5) años.

8. ¿Qué tipo de conducta sanciona la normativa en protección de datos personales de tu país?

La normativa de protección de datos personales en Paraguay sanciona diversas conductas que vulneran los principios de licitud, transparencia, seguridad y confidencialidad en el tratamiento de datos. Entre las principales infracciones sancionadas se encuentran:

a. Infracciones relacionadas con la autorización y actividades de las entidades reguladoras:

1. Ejercer actividades reguladas por la ley sin autorización previa del ente regulador, o fuera del alcance de las autorizaciones obtenidos.

2. Incumplir limitaciones o prohibiciones temporales impuestas a la entidad, no acatar medidas correctivas, obligaciones legales o reglamentarias exigidas por el ente regulador.

3. Omitir información obligatoria o suministrar información incompleta o falsa al ente regulador.

4. Resistirse, excusarse o negarse a cumplir instrucciones o requerimientos de la Superintendencia de Bancos, supervisores o inspectores, incluyendo la falta de provisión de documentación solicitada.

5. Notificar de manera incompleta, tardía o defectuosa a la autoridad de protección de datos sobre una violación de seguridad.

b. Infracciones relacionadas con la protección de datos personales

1. Recopilación, uso o transferencia indebido de datos (ej. Sin consentimiento, para una finalidad distinta, etc.)

2. Negarse injustificadamente a dar acceso, rectificar o eliminar datos personales cuando así se solicite el titular del dato.

3. No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o portabilidad.

4. Tratar datos personales de un menor de edad sin su consentimiento, cuando tenga capacidad para ello, o sin el consentimiento de su representante legal.

5. No acreditar esfuerzos razonables para verificar la validez del consentimiento otorgado por un menor o su representante legal.

Obligaciones contractuales y medidas de seguridad

• No formalizar acuerdos entre corresponsables del tratamiento de datos o hacerlo de manera inexacta, o incumplir las estipulaciones contractuales en el tratamiento de datos personales sin justificación legal.

• No adoptar medidas técnicas y organizativas adecuadas para garantizar la protección de datos desde el diseño.

• Vulnerar el deber de confidencialidad sobre los datos personales.

• Recolectar, almacenar o transmitir datos personales por mecanismos inseguros o sin garantizar su integridad.

• Transferencias internacionales de datos

• Transferir datos personales a un tercer país u organización internacional sin cumplir los requisitos y garantías establecidos por la ley.

Favor notar que esta lista es enunciativa y no incluye a todas las posibles infracciones relacionadas a la protección o uso indebido de datos personales.

9. ¿Tu jurisdicción tiene un organismo técnico que dicte directrices y fiscalice el cumplimiento de las normas de protección de datos personales?

Sí, la Ley 6534 en Paraguay dispone que las entidades competentes en materia de protección de datos son:

• Banco Central del Paraguay (BCP): El BCP debe velar por el cumplimiento de las disposiciones relativas a los burós de crédito y su funcionamiento.

• Secretaría de Defensa del Consumidor (SEDECO): Debe velar por el cumplimiento de las disposiciones de la norma relacionadas a los titulares de datos.

• A la fecha no se han emitido guías o directivas relacionadas al cumplimiento de la Ley 6534.

10. ¿Cuáles son los primeros pasos que toman las organizaciones en tu país para comenzar a aplicar la normativa en protección de datos personales en general y un programa de cumplimiento en particular?

Toda organización que desee realizar un diagnóstico sobre cumplimiento e implementación de un programa de cumplimiento debe seguir los siguientes pasos:

• Identificar los datos personales que son tratados por la organización.

• Determinar la base legal sobre la que los datos están siendo tratados.

• Elaboración de una política de datos / revisión y actualización de la política de datos.

• Implementación de protocolos y procedimientos internos.

• Revisión de medidas de seguridad vigentes.

• Relevamiento de los acuerdos con proveedores.

11. ¿Cuál es el ámbito de aplicación territorial de la normativa de protección de datos de tu país? ¿La normativa puede aplicarse extraterritorialmente?

La aplicación de la Ley 6534 se limita a los datos recolectados o almacenados en Paraguay.

Uruguay

1. ¿Cuál es el marco regulatorio de la protección de datos personales en tu jurisdicción?

En Uruguay, la protección de datos personales está regulada por la Ley N° 18.331, el Decreto Reglamentario N° 414/009, los artículos 37 a 40 de la Ley N° 19.670 y el Decreto Reglamentario N° 64/2020 (“LPD”). Este marco legal garantiza a las personas el control sobre sus datos personales, protegiendo su derecho a la privacidad, en línea con la normativa internacional más avanzada en la materia, el Reglamento General de Protección de Datos de la Unión Europea (“RGPD”). Gracias a esta armonización, Uruguay ha obtenido la nota de adecuación de parte de la Comisión Europea, lo cual valida al país como adecuado para el tratamiento de datos personales.

La LPD establece principios clave que deben ser observados en todas las fases del ciclo de vida de los datos personales, desde su recolección hasta su destrucción, tales como el previo consentimiento informado, finalidad, legalidad (registro de la base de datos), confidencialidad, seguridad y reserva.

Como corolario, la LPD incorpora el principio de responsabilidad proactiva, que implica que tanto el responsable de tratamiento de los datos (propietario de la

base de datos) como el encargado (quien trata los datos personales por cuenta y orden del responsable) deben implementar medidas para garantizar la privacidad desde el diseño y por defecto, realizar evaluaciones de impacto en la protección de datos y designar delegado de protección de datos, cuando corresponda.

Adicionalmente, la LPD creó la Unidad Reguladora y de Control de Datos Personales ("URCDP"), autoridad encargada de supervisar el cumplimiento de la LPD y asegurar su aplicación.

2. ¿Existe en tu país regulación sobre programas de prevención de infracciones o de cumplimiento en materia de protección de datos personales? ¿Son obligatorios? ¿En qué casos?

La LPD establece el principio de responsabilidad proactiva en virtud del cual los responsables y encargados de tratamiento de datos deben adoptar medidas técnicas y organizativas para garantizar el cumplimiento normativo. Esto incluye prácticas como privacidad desde el diseño y por defecto y la realización de evaluaciones de impacto cuando sea necesario.

Si bien la LPD no hace referencia expresa a la implementación de un "programa de cumplimiento", sí obliga a las organizaciones que recopilan y tratan datos personales, a documentar y revisar periódicamente las medidas adoptadas para garantizar el cumplimiento legal. Esta documentación debe incluir la forma, finalidad y medios del tratamiento de datos, mecanismos de cumplimiento normativo, protocolos de respuesta ante vulneraciones de seguridad, y cuando aplique, el rol del delegado de protección de datos.

Además, para ciertos tratamientos de datos específicos (grandes volúmenes, elaboración de perfiles, datos sensibles como negocio principal, datos especialmente protegidos o relativos a infracciones penales, civiles o administrativas, datos de menores de edad o personas con discapacidad, transferencias internacionales y otros que la URCDP pueda determinar, la LPD obliga a realizar una evaluación de impacto en la protección de datos ("EIPD"). Esta evaluación permite identificar y mitigar riesgos, además de servir como prueba de cumplimiento de la ley ante la autoridad de control.

En la práctica, aunque la LPD no mencione expresamente un "programa formal de compliance", sus requisitos generan un efecto equivalente, al exigir la documentación de las medidas técnicas y organizativas adoptadas para hacer el tratamiento conforme a la ley, así como también su revisión y gestión de riesgos en el tratamiento de datos personales.

3. ¿Qué contenido mínimo deben tener los programas de cumplimiento en protección de datos personales en tu país?

La LPD establece que los responsables y encargados de tratamiento de datos deben documentar las medidas técnicas y organizativas que han adoptado para cumplir con la normativa. Esta documentación tiene un rol similar al de un programa de compliance, ya que ayuda a demostrar el cumplimiento de las normas sobre protección de datos.

Según la LPD, esta documentación debe incluir, al menos, detalles sobre la forma, los medios y la finalidad del tratamiento de datos, así como los procedimientos diseñados para cumplir con la normativa. También debe contemplar un protocolo de respuesta a incidentes de seguridad y definir el rol del delegado de protección de datos cuando corresponda.

Por otro lado, las EIPD, que son obligatorias y útiles para demostrar el cumplimiento de la LPD en tratamientos específicos, también deben cumplir con un contenido mínimo. Esto incluye una descripción sistemática de la actividad de tratamiento, una evaluación de su conformidad con la normativa, un análisis de los riesgos para los derechos de los titulares de los datos y un detalle de las medidas de seguridad implementadas junto con los mecanismos para demostrar el cumplimiento de la normativa.

4. ¿Qué beneficios trae contar al interior de la organización con un programa de cumplimiento en protección de datos personales?

Contar con un programa de cumplimiento en protección de datos personales asegura el cumplimiento normativo y reduce el riesgo de sanciones por parte de la URCDP y posibles reclamos de los titulares. A la vez, también protege la reputación de la empresa y fortalece la confianza de clientes, empleados y socios comerciales.

A nivel interno, optimiza la gestión de los datos con procesos claros y eficientes, facilitando la toma de decisiones estratégicas y la adaptación a posibles cambios regulatorios. Además, refuerza la seguridad en el tratamiento de la información, minimizando riesgos de vulneraciones y garantizando una mayor protección tanto para la empresa como para los titulares de los datos.

En definitiva, implementar un programa de cumplimiento

no sólo reduce riesgos legales, sino que también genera un entorno de confianza para quiénes voluntariamente proporcionan sus datos a las compañías para el acceso a bienes o servicios de su interés.

5. ¿Existen procesos de certificación de los programas de cumplimiento en protección de datos en tu país? ¿Quién realiza la certificación?

Actualmente, la LPD no contempla mecanismos de certificación de programas de cumplimiento en protección de datos, como sí ocurre en otras legislaciones a nivel comparado.

Para las EIPD que son requeridas por la LPD en marco de ciertas actividades de tratamiento y, que pueden integrarse en el programa de compliance, se establece que, si su resultado evidencia un riesgo significativo para los derechos de los titulares de datos, el responsable y el encargado deberán informarlo a la URCDP, proporcionando detalles sobre las medidas adoptadas o previstas, así como los plazos para su implementación.

6. ¿En tu jurisdicción es obligatorio contar con un delegado de protección de datos personales? ¿En qué casos?

De acuerdo con la LPD, están obligados a designar Delegado de Protección de Datos, las entidades públicas; entidades privadas total o parcialmente de propiedad estatal; las que traten datos sensibles como negocio principal; o traten grandes volúmenes de datos (es decir, datos de más de 35.000 titulares).

El Delegado de Protección de Datos tiene la función de asesorar a la organización en el cumplimiento de la normativa de protección de datos y ser el nexo con la URCDP, entre otras tareas.

La designación debe hacerse en plazo de 90 días desde el inicio de la actividad de tratamiento.

7. ¿Existen sanciones asociadas al incumplimiento de la normativa sobre protección de datos personales? ¿De qué tipo? ¿A cuánto ascienden las multas?

El incumplimiento de la LPD puede dar lugar a la aplicación de sanciones que oscilan desde una observación, apercibimiento, multas de hasta 500.000 Unidades Indexadas (aproximadamente, U$S 70.000), suspensión de la base de datos por un plazo de 5 días, o, en casos más graves, su clausura definitiva.

En ese sentido, la URCDP ha emitido la Resolución N° 105/2015 que contiene lineamientos para la determinación de sanciones. Entre los principales factores que se evalúan, se encuentran la gravedad de la infracción, el historial de incumplimiento del infractor, la naturaleza de los datos personales tratados, la adopción o no de medidas de seguridad, los derechos afectados, el volumen de datos tratados y los posibles perjuicios para las personas y terceros involucrados.

8. ¿Qué tipo de conducta sanciona la normativa en protección de datos personales de tu país?

La LPD establece que tanto responsables como encargados deben cumplir con la normativa de protección de datos, pudiendo ser sancionados en caso de infracción.

Las infracciones incluyen, entre otras conductas, el tratamiento de datos sin una base legal válida; la falta de transparencia en la recopilación y uso de los datos personales; tratar datos personales para finalidades diferentes o incompatibles a las que motivaron su recolección; el incumplimiento de los derechos de los titulares; la falta de adopción de medidas de seguridad adecuadas para proteger la confidencialidad de los datos; llevar a cabo transferencias internacionales sin las garantías necesarias; la comunicación de datos sin base legal habilitante.

También son pasibles de sanción, conductas relacionadas con el incumplimiento de obligaciones formales como ser, la falta de registro de las bases de datos en URCDP, no brindar a la autoridad la información necesaria cuando ésta lo requiera en marco de investigaciones o afines, entre otras.

9. ¿Tu jurisdicción tiene un organismo técnico que dicte directrices y fiscalice el cumplimiento de las normas de protección de datos personales?

La LPD creó la URCDP como un organismo desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento ("AGESIC"), que cuenta con autonomía técnica para asesorar y tomar decisiones en materia de protección de datos. Su misión principal es garantizar el cumplimiento de la LPD, protegiendo los derechos de las personas en relación con sus datos personales.

Entre sus principales funciones se encuentran, asesorar a las personas sobre el alcance de la ley y los mecanismos legales para defender sus derechos; emitir normativas y directrices para el tratamiento adecuado de sus datos

personales; atender denuncias y reclamos de personas que consideren que sus datos han sido tratados de forma indebida; aplicar sanciones en caso de incumplimientos; capacitar a entidades públicas y privadas sobre buenas prácticas en materia de protección de datos.
En cumplimiento de sus cometidos, URCDP busca promover un uso responsable y seguro de la información personal en todos los ámbitos.

10. ¿Cuáles son los primeros pasos que toman las organizaciones en tu país para comenzar a aplicar la normativa en protección de datos personales en general y un programa de cumplimiento en particular?

En Uruguay, las organizaciones siguen una serie de pasos para garantizar el cumplimiento de la normativa de protección de datos. Primero, realizan un diagnóstico inicial para identificar qué datos personales se recolectan, su finalidad, los medios utilizados para su tratamiento, dónde se almacenan y con quién los comparten.

Con esta información, se elaboran políticas de privacidad para cumplir con el derecho de información de los titulares sobre la recopilación y tratamiento de sus datos. En este marco, establecen protocolos para atender las solicitudes de ejercicio de derechos de los titulares de datos (acceso, rectificación, actualización, supresión entre otros).

Asimismo, se implementan medidas técnicas y organizativas de seguridad orientadas a garantizar la confidencialidad, disponibilidad e integridad de los datos. Éstas pueden incluir controles de acceso, cifrado de datos, guardia física, capacitaciones del personal en gestión de datos, entre otras. Las medidas de seguridad pueden variar dependiendo de la forma de almacenamiento, la naturaleza de los datos tratados y otros factores, ya que la ley no establece expresamente qué medidas deben adoptarse.

En este contexto, las empresas también revisan sus contratos con terceros involucrados en el manejo de la información personal, para asegurarse que proveedores y aliados comerciales cumplan con la normativa, y, en caso de transferencias internacionales, adoptar medidas legales en la medida aplicable.

Posteriormente, las empresas cumplen con sus obligaciones formales, lo que incluye, el registro de sus bases de datos en URCDP – proceso en que deben declarar el cumplimiento de los pasos anteriores-. Además, cuando corresponde, designan un delegado de protección de datos para supervisar el cumplimiento normativo y actuar como ligamen con la autoridad de control.

De este modo, las organizaciones pueden incorporar la normativa de protección de datos en su programa de compliance, implementando protocolos de gestión de datos, auditorías internas y revisiones periódicas para evaluar la efectividad de sus medidas, garantizando así una mejora continua y adaptación a cambios regulatorios.

11. ¿Cuál es el ámbito de aplicación territorial de la normativa de protección de datos de tu país? ¿La normativa puede aplicarse extraterritorialmente?

La LPD aplica al tratamiento de datos personales de personas físicas o jurídicas, en la medida en que el responsable de tratamiento (propietario de la base de datos) o el encargado (quien trata datos personales por cuenta y orden del responsable y bajo sus instrucciones) se encuentre establecido en Uruguay.

Adicionalmente, como en el caso del RGPD de la Unión Europea, la LPD tiene alcance extraterritorial. Por ende, aplica al responsable o encargado no establecido en Uruguay, cuando las actividades de tratamiento se encuentren relacionadas con la oferta de bienes o servicios dirigidos a habitantes uruguayos o se vinculen con el análisis de su comportamiento; cuando así lo disponen las normas de derecho internacional público o un contrato; o cuando en el tratamiento se utilizan medios situados en el país, como ser redes de información y de comunicación, centros de datos o infraestructura informática en general, recursos humanos u otros.