etiqampus
e-Learning en Integridad

Guía Comparada Protección de Datos Personales: caso Colombia

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 Colombia, escrita por Sarita Enríquez, Asociada del estudio Posse Herrera y Ruiz, a cargo de Competencia y Protección al Consumidor.

Compliance Internacional

●●○ NIVEL INTERMEDIO

Fecha	Marzo 2025
Tpo. de lectura	20 min.

FGE

albagli zaliasnik

POSSE HERRERA RUIZ

Compliance LATAM

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



POSSE HERRERA RUIZ

Autor:

Sarita Enríquez, Asociada, Competencia y Protección al Consumidor.

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

El marco regulatorio de protección de datos en Colombia se compone de la siguiente forma:

• Ley 1266 de 2008: Regula el manejo de la información financiera y crediticia de los consumidores. Establece derechos y deberes de los titulares de la información, así como las obligaciones de las entidades que manejan datos financieros.

• Ley 1581 de 2012: Establece disposiciones generales para la protección de datos personales. Define los principios, derechos de los titulares de datos y las obligaciones de los responsables y encargados del tratamiento de datos.

• Decreto 1377 de 2013: Complementa la Ley 1581 de 2012, regulando aspectos específicos relacionados con el tratamiento de datos personales. Además, establece procedimientos para la recolección y tratamiento de datos, así como para la autorización del titular.

• Decreto 1074 de 2015: Compila y unifica las normas relacionadas con la protección de datos personales y su tratamiento. Establece lineamientos para garantizar el cumplimiento de la Ley 1581 de 2012 y sus decretos complementarios.

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?

El régimen colombiano prevé la obligación de dar cumplimiento al Principio de Responsabilidad Demostrada o "Accountability".

Este principio se refiere a que los responsables del tratamiento deberán adoptar medidas apropiadas y efectivas para:

• Tratar los datos personales.

• Garantizar la seguridad de la información.

• Atender adecuadamente el ejercicio de los derechos de los titulares (reclamos y consultas).

• Conocer la normativa para reportar incidentes de seguridad.

Dicha obligación se materializa a través de la adopción de manuales y guías que permitan generar cultura interna sobre el tratamiento de datos para ejercer una adecuada gobernanza. Así mismo, la ley aplicable exige realizar capacitaciones y auditorías para mejorar y revisar el nivel de cumplimiento.

El Principio de Responsabilidad Demostrada es de obligatorio cumplimiento para todo aquel que trate datos personales en Colombia y podrá ser verificado por la Superintendencia de Industria y Comercio (SIC) a su entera discreción.

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

De conformidad con los artículos 26 y 27 del Decreto 1377 de 2013, los programas de cumplimiento deberán incluir la siguiente información:

• La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.

• La naturaleza de los datos personales objeto del tratamiento.

• El tipo de tratamiento.

• Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.

• La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012.

• La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.

• La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, con respecto a cualquier aspecto del tratamiento

Así mismo, un programa de cumplimiento deberá buscar el cumplimiento de todas las obligaciones del régimen de protección de datos en Colombia, esto es:

• Contar con autorización para el tratamiento de datos personales.

• Tener una política de tratamiento y en los casos en que sea necesario un aviso de privacidad.

• Llevar a cabo el registro de bases de datos en el Registro Nacional de Bases de Datos, así como sus actualizaciones (en caso de resultar aplicable).

• Tener un manual de políticas y procedimientos y dar cumplimiento al principio de Responsabilidad Demostrada o "Accountability".

• Cumplir con los requisitos para transmisión y transferencia de datos personales.

• Adoptar medidas de seguridad para prevenir la adulteración o acceso no autorizado a los datos personales.

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 de datos personales en Colombia ofrece múltiples beneficios significativos para las organizaciones. En primer lugar, reduce la probabilidad de requerimientos o sanciones por parte de las autoridades, lo cual no solo protege la reputación de la empresa, sino que también evita costos asociados a multas y litigios. Además, un programa robusto de cumplimiento promueve una mayor gobernanza y transparencia en el manejo de la información, lo que fortalece la confianza de los titulares de datos y mejora las relaciones con ellos.

Asimismo, al implementar políticas y procedimientos claros, se asegura una mejor calidad en los datos recolectados y tratados, lo que se traduce en decisiones más informadas y efectivas. Esto también facilita la identificación y mitigación de riesgos asociados al tratamiento de datos, promoviendo un entorno más seguro.

En última instancia, un enfoque proactivo en el cumplimiento de la normativa de protección de datos no solo beneficia a la organización desde el punto de vista legal, sino que también puede convertirse en una ventaja competitiva en el mercado, al demostrar un compromiso con la privacidad y la protección de los derechos de los titulares.

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

En Colombia no existen procesos de certificación de programas de cumplimiento en protección de datos. Sin embargo, y tal como se anticipó, la SIC puede solicitar que una compañía evidencie que cuenta con medidas apropiadas y efectivas para el tratamiento de datos.

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

La normativa aplicable dispone que las organizaciones deben contar con una estructura administrativa que permita dar seguimiento al cumplimiento del régimen aplicable. En esta medida, la SIC ha determinado que las empresas podrían contar con un área encargada o con un oficial de protección de datos para garantizar el cumplimiento del régimen.

Por otro lado, en sistemas como el Registro Nacional de Bases de Datos, la SIC permite que facultativamente, las organizaciones registren a su oficial de protección de datos, sin embargo, lo anterior aún no es de obligatorio cumplimiento.

A la fecha hay distintos proyectos de ley que, entre otras iniciativas, pretenden imponer como obligación la designación de un oficial de protección de datos. Sin embargo, dichos proyectos siguen en trámite legislativo.

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

Sí, de conformidad con el artículo 23 de la Ley 1581 de 2012, la SIC se encuentra facultada para imponer las siguientes sanciones:

• Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción (para 2025 COP 2.847.000.000). Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

• Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.

• Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.

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

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

La SIC se encuentra facultada para sancionar cualquier incumplimiento de las obligaciones enunciadas en la respuesta No. 3.

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 en materia de protección de datos personales es la SIC. Dicha autoridad emite guías y circulares para reforzar el cumplimiento del régimen aplicable.

Las más recientes son aquellas relacionadas con:

• La implementación de Inteligencia Artificial (IA) en el tratamiento de datos personales. Proporciona directrices sobre cómo las entidades deben manejar la IA de manera ética y responsable, asegurando la protección de los derechos de los titulares de datos.

• La circular relacionada con la responsabilidad de administradores en el manejo y tratamiento de datos personales dentro de las organizaciones. Establece que los administradores deben garantizar el cumplimiento de la normativa de protección de datos y tomar medidas adecuadas para proteger la información.

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 Colombia, el primer paso que deben tomar las organizaciones para aplicar la normativa en protección de datos personales es determinar el flujo de captura y tratamiento de datos dentro de su estructura. Esto implica identificar qué datos se recolectan, cómo se almacenan, quiénes tienen acceso a ellos y con qué propósito se utilizan. Este diagnóstico inicial es crucial, ya que permite a la organización comprender su situación actual en relación con la protección de datos y detectar posibles áreas de riesgo. Una vez que se tiene claridad sobre el flujo de datos, las organizaciones pueden avanzar hacia la implementación de un programa de cumplimiento efectivo.

El siguiente paso es asesorarse con expertos en la materia para elaborar las herramientas necesarias que garanticen el cumplimiento de las obligaciones establecidas en la normativa. Esto incluye la creación de políticas de privacidad, procedimientos de gestión de datos y mecanismos de respuesta ante incidentes. La implementación de estas herramientas debe ir acompañada de un esfuerzo por fomentar una verdadera gobernanza y cultura de protección de datos dentro de la organización.