etiqampus
e-Learning en Integridad

Guía Comparada Protección de Datos Personales: caso Brasil

Compliance Internacional

NIVEL INTERMEDIO

Fecha	Julio 2025
Tpo. de lectura	23 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 Brasil y escrita por los siguientes profesionales del estudio FCR Law:

- Marcelo Coimbra, Socio.
- Virgínia Coelho, Socia, Protección de Datos y Derecho Contractual.
- Stefano Fabbri, Asociado, Corporativo, Fusiones y Adquisiciones, Protección de Datos Personales.

FGE

albagli zaliasnik

FCR Law
Fleury, Coimbra e Rhomberg Advogados

Com plian ce LATAM

FUENTE: El texto de esta portadilla se elaboró a partir de extractos del documento que precede.

Guía Comparada Protección de Datos Personales

Marzo 2025



www.compliancelatam.legal



FCR Law

Fleury, Coimbra e
Rhomberg Advogados

Autores:

Marcelo Coimbra, Socio.

Virgínia Coelho, Socia, Protección de Datos y Derecho Contractual.

Stefano Fabbri, Asociado, Corporativo, Fusiones y Adquisiciones, Protección de Datos Personales.

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

El principal marco regulatorio en Brasil es la Ley General de Protección de Datos Personales (LGPD – Ley n.° 13.709/2018), que establece normas para el tratamiento de datos personales por parte de personas físicas y jurídicas, tanto públicas como privadas. La Autoridad Nacional de Protección de Datos (ANPD) es el órgano responsable de regular, supervisar y aplicar sanciones en materia de protección de datos.

Además de la LGPD, otras normativas también influyen en la protección de datos en el país, como el Marco Civil de Internet (Ley n.° 12.965/2014), que regula el uso de Internet y la privacidad de los usuarios, y el Código de Defensa del Consumidor (Ley n.° 8.078/1990), que protege a los consumidores contra el uso indebido de sus datos. Regulaciones específicas, como las del Banco Central de Brasil (Bacen) para el sector financiero y las directrices de la Agencia Nacional de Salud Suplementaria (ANS) para el sector sanitario, también imponen requisitos adicionales sobre seguridad y privacidad de datos.

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?

Aunque la LGPD no establece la obligatoriedad de un programa formal de cumplimiento en protección de datos, sí impone principios y obligaciones que, en la práctica, exigen la implementación de medidas organizacionales y técnicas para garantizar la prevención de infracciones y el cumplimiento de la normativa aplicable en materia de protección de datos personales.

Además, la ANPD fomenta la adopción de programas de gobernanza en privacidad, que deben estructurarse según el tamaño y el volumen de datos tratados por la organización. Las empresas que manejan grandes volúmenes de datos o que operan en sectores regulados (como el financiero, la salud y las telecomunicaciones) suelen estar sujetas a requisitos adicionales por parte de los organismos reguladores, lo que hace que estos programas sean esenciales.

Además, entre las funciones de los encargados de protección de datos (DPO) se incluye la elaboración, definición e implementación de reglas de buenas prácticas, gobernanza y programas de cumplimiento en privacidad.

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

Los programas de cumplimiento en protección de datos en Brasil deben incluir, como mínimo, los siguientes elementos:

I. Mapeo del tratamiento de datos: Identificación de los tipos de datos tratados, sus finalidades, bases legales y flujos de compartición, estructurando registros de las operaciones de tratamiento.

II. Política de privacidad y avisos de privacidad: Documentos que informan a los titulares, tanto internos como externos a la organización, sobre cómo se recopilan, utilizan y protegen sus datos.

III. Gobernanza y roles internos: Definición de responsabilidades dentro de la organización, incluyendo la designación del DPO, cuando corresponda.

IV. Gestión de riesgos e impactos en la privacidad: Implementación de procesos para evaluar y mitigar riesgos en el tratamiento de datos personales, incluyendo la elaboración de Informes de Impacto en la Protección de Datos (RIPD), cuando sea necesario.

V. Plan de respuesta a incidentes: Procedimientos para la identificación, contención, mitigación y notificación de incidentes de seguridad, en conformidad con los requisitos de la ANPD.

VI. Capacitación y concienciación: Programas educativos para los empleados sobre buenas prácticas, riesgos y obligaciones legales relacionadas con la protección de datos personales.

VII. Gestión de consentimientos y bases legales: Control sobre cómo se obtienen, almacenan y administran los consentimientos, además de la verificación del uso adecuado de otras bases legales previstas en la LGPD.

VIII. Mecanismos para garantizar los derechos de los titulares: Procedimientos internos para atender solicitudes de acceso, corrección, eliminación, portabilidad y demás derechos previstos en la LGPD.

IX. Adopción de medidas de seguridad: Implementación de controles técnicos y organizacionales para garantizar la autenticidad, integridad, confidencialidad y disponibilidad de los datos personales.

X. Monitoreo y auditoría: Revisión periódica del programa

de cumplimiento para evaluar su eficacia e identificar mejoras continuas.

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

Los principales beneficios de implementar un programa de cumplimiento en protección de datos incluyen:

I. Reducción de riesgos legales y financieros, evitando multas y otras sanciones de la ANPD, así como costos derivados de litigios civiles y laborales.

II. Mitigación del riesgo de no renovación o rescisión de contratos debido a la falta de acreditación de un programa de cumplimiento en protección de datos.

III. Mayor seguridad jurídica en operaciones de fusiones, adquisiciones y asociaciones, asegurando que los datos y contratos cumplan con la normativa.

IV. Transparencia y confianza por parte de clientes y socios, fortaleciendo las relaciones comerciales.

V. Mejora de la reputación y ventaja competitiva en el mercado, diferenciando a la empresa como referente en privacidad y protección de datos.

VI. Optimización de la gobernanza corporativa y la seguridad de la información, asegurando procesos más organizados y eficientes.

VII. Mayor protección frente a incidentes de seguridad, reduciendo pérdidas financieras y daños reputacionales.

VIII. Reducción del impacto operativo ante crisis relacionadas con la seguridad de la información, garantizando respuestas rápidas y eficaces.

IX. Facilidad para adaptarse a nuevas regulaciones y requisitos contractuales, especialmente en sectores regulados.

X. Mayor facilidad en la implementación de tecnologías innovadoras, asegurando que los nuevos procesos digitales se desarrollen de manera segura y conforme a la normativa.

XI. Mejora en la relación con empleados y stakeholders internos, fomentando una cultura organizacional enfocada en la protección de datos.

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

Actualmente, no existe una certificación oficial emitida o reconocida por la ANPD para acreditar la conformidad de las empresas con la LGPD. Sin embargo, la ANPD ya ha manifestado interés en regular los criterios para el reconocimiento de buenas prácticas y gobernanza en protección de datos, conforme lo previsto en sus Agendas Regulatorias para los bienios 2023-2024 y 2025-2026. Se espera que, en el futuro, puedan establecerse directrices para certificaciones o sellos oficiales, similares a los modelos adoptados en la Unión Europea bajo el GDPR.

Mientras tanto, las organizaciones que deseen demostrar su compromiso con la privacidad y la protección de datos pueden adoptar certificaciones reconocidas en el mercado, como, por ejemplo, la ISO/IEC 27701, que amplía la ISO/IEC 27001 para incluir requisitos específicos de privacidad, y el NIST Privacy Framework, que proporciona directrices para la gestión de riesgos de privacidad. Estas certificaciones son otorgadas por organismos de certificación independientes, acreditados por entidades como la International Organization for Standardization (ISO) y organismos nacionales de acreditación, como Inmetro en Brasil. Además, consultorías especializadas asisten a las empresas en el proceso de auditoría y conformidad con estos estándares. Aunque estas certificaciones no garantizan el cumplimiento legal de la LGPD, son ampliamente reconocidas como buenas prácticas para la estructuración de programas de gobernanza en privacidad, pueden representar un diferencial competitivo y constituyen un paso relevante en el camino hacia el cumplimiento de la legislación de protección de datos personales en Brasil.

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

En Brasil, la designación de un encargado del tratamiento de datos personales, o DPO, es obligatoria para la mayoría de los agentes de tratamiento. La ausencia de un encargado del tratamiento de datos personales, cuando su designación es requerida, puede afectar la evaluación de la conformidad de una organización y aumentar los riesgos regulatorios, haciendo que su nombramiento sea esencial para evitar sanciones y garantizar buenas prácticas en protección de datos. Además de la designación del encargado del tratamiento de datos personales, también es obligatoria la designación de un encargado suplente, que actuará en casos de ausencia, impedimento o vacancia del titular del cargo.

La ANPD establece criterios para que ciertos agentes de tratamiento puedan beneficiarse de flexibilizaciones en el cumplimiento de algunas obligaciones previstas en la LGPD, como la obligación de designar un encargado. Sin embargo, existen circunstancias en las que estas flexibilizaciones no se aplican y, por lo tanto, la designación del DPO es obligatoria:

• Tratamiento de alto riesgo: Agentes que realizan operaciones de tratamiento de datos consideradas de alto riesgo para los titulares. Se entiende por tratamiento de alto riesgo aquel que involucra, por ejemplo, vigilancia o control de zonas accesibles al público, decisiones automatizadas que afecten a los titulares o el uso de datos sensibles o de niños, entre otros criterios.

• Exceder el umbral de ingresos brutos: Agentes cuya facturación bruta anual supere los R$ 4.800.000,00, o R$ 16.000.000,00 en el caso de startups.

• Pertenencia a un grupo económico: Agentes que forman parte de un grupo económico cuya facturación global exceda los límites mencionados anteriormente.

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

Sí, la LGPD prevé las siguientes sanciones administrativas, que pueden ser aplicadas por la ANPD:

I. Advertencia.

II. Multa simple de hasta 2% de la facturación de la empresa o grupo económico en Brasil en el último ejercicio, limitada a R$ 50 millones por infracción.

III. Multa diaria, respetando el límite mencionado anteriormente.

IV. Publicación de la infracción.

V. Bloqueo o eliminación de los datos personales involucrados en la infracción.

VI. Suspensión del funcionamiento de la base de datos o de las actividades de tratamiento.

VII. Prohibición parcial o total del ejercicio de actividades relacionadas con el tratamiento de datos.

Además, las empresas pueden enfrentar acciones judiciales por parte de los titulares de datos y del Ministerio Público, según corresponda, así como sanciones impuestas por otros reguladores sectoriales.

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

El incumplimiento de la LGPD y de las resoluciones de la ANPD puede dar lugar a la aplicación de las sanciones mencionadas en el ítem 7. Las principales conductas sancionadas son:

I. Ausencia de medidas de seguridad: Defecto en la implementación de medidas técnicas y organizativas contra accesos no autorizados y otras formas de incidentes de seguridad.

II. No comunicación de incidentes de seguridad: Omisión en la notificación de incidentes a la ANPD y a los titulares, cuando sea requerido.

III. Incumplimiento de órdenes de la ANPD: Defecto en el cumplimiento de las determinaciones de la autoridad dentro de los plazos establecidos.

IV. Tratamiento de datos sin base legal adecuada: Cualquier forma de tratamiento de datos sin una justificación legal válida.

V. Uso indebido de datos sensibles o de niños y adolescentes: Tratamiento inapropiado de datos que requieren protección especial.

VI. Violación de derechos de los titulares: Negativa o demora injustificada en la atención a las solicitudes de los titulares en el ejercicio de sus derechos.

VII. No designación de un encargado: No designación del encargado (y del encargado suplente) en los casos en los que la legislación lo exija.

VIII. Exceso o desvío de finalidad en el tratamiento de datos: Utilización de datos para fines no informados o incompatibles con la recolección original.

IX. Compartir indebidamente datos: Transferencia de datos personales a terceros sin una base legal adecuada y/o sin el conocimiento de los titulares.

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

Sí. La Autoridad Nacional de Protección de Datos (ANPD) es el organismo responsable de:

• Regular e interpretar la LGPD.

• Fiscalizar el cumplimiento de la legislación.

• Aplicar sanciones.

• Emitir directrices y buenas prácticas para los agentes de tratamiento.

• Promover la educación sobre protección de datos.

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?

Como regla general, los primeros pasos incluyen:

I. Mapeo del tratamiento de datos.

II. Análisis de conformidad y riesgos (Gap Analysis).

III. Definición de un plan de adecuación a la LGPD.

IV. Creación de políticas internas y externas.

V. Implementación de medidas técnicas y organizativas de seguridad.

VI. Definición de procesos para atender los derechos de los titulares.

VII. Elaboración de un plan de respuesta a incidentes de seguridad.

VIII. Capacitación y concientización de los empleados.

IX. Revisión de contratos con clientes y proveedores.

X. Establecimiento de reglas de monitoreo para fines de auditorías internas.

XI. Seguimiento del escenario regulatorio.

11. ¿Cuál es el ámbito de aplicación territorial de la normativa de protección de datos de tu país? ¿La normativa puede aplicarse extraterritorialmente?
*(Considerar esta pregunta únicamente si tiene relevancia en el marco legal de Brasil)

La LGPD tiene aplicación territorial y extraterritorial, es decir, puede aplicarse a empresas y organizaciones dentro y fuera de Brasil, dependiendo de las circunstancias del tratamiento de datos.

La LGPD es aplicable a cualquier operación de tratamiento realizada por un agente de tratamiento, independientemente del medio, del país de su sede o del país donde se encuentren localizados los datos, siempre que:

• La operación de tratamiento se realiza en Brasil.

• La actividad de tratamiento tenga como objetivo la oferta o el suministro de bienes o servicios o el tratamiento de datos de individuos localizados en Brasil.

• Los datos personales objeto del tratamiento hayan sido recolectados en Brasil.