etiqampus
e-Learning en Integridad

Guía Comparada Protección de Datos Personales: caso Panamá

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 Panamá y escrita por la socia del estudio MDU Legal, Marlyn Narkis Assis.

Compliance Internacional

NIVEL INTERMEDIO

Fecha	Marzo 2025
Tpo. de lectura	23 min.

FGE

az albagli zaliasnik

MDU LEGAL

Com plian ce 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



Autor:

Marlyn Narkis Assis, Socia.

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

En la República de Panamá, el marco regulatorio de la protección de datos personales está principalmente establecido en la Ley 81 de 26 de marzo de 2019 "Sobre Protección de Datos Personales". Esta ley regula el tratamiento de los datos personales en el país y establece principios, derechos y obligaciones para garantizar su adecuada protección. A su vez, el Decreto Ejecutivo 285 de 2021 reglamenta la Ley 81 y proporciona lineamientos adicionales sobre el tratamiento de datos personales, las obligaciones de los responsables y encargados del tratamiento, y las medidas de seguridad que deben implementarse.

Adicionalmente, la Ley 51 de 2008, que regula el comercio electrónico y la firma electrónica, así como su reglamentación, contiene disposiciones relacionadas con la seguridad y protección de la información.
Otras normativas sectoriales, como las disposiciones específicas de la Autoridad Nacional para la Innovación Gubernamental, y de la Superintendencia de Bancos de Panamá para el sector financiero, así como regulaciones aplicables a los sectores de salud, telecomunicaciones, y la administración pública, pueden complementar la normativa de protección de datos en estos ámbitos específicos.

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?

Sí, la Ley 81 de 2019 y su reglamento establecen la obligación de adoptar medidas de seguridad para garantizar la protección de los datos personales. Aunque no se exige expresamente la implementación de un programa de cumplimiento, se requiere que las empresas y organizaciones que traten datos personales implementen protocolos, políticas y controles que aseguren la confidencialidad, integridad y disponibilidad de la información.

La implementación de programas de cumplimiento es altamente recomendado, y puede considerarse obligatorio para sectores regulados, como el financiero, telecomunicaciones, salud y el comercio electrónico, donde las regulaciones sectoriales pueden exigir medidas de seguridad específicas.

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

Aunque la legislación panameña no especifica un contenido mínimo obligatorio, un programa de cumplimiento efectivo debe incluir:

• Política de privacidad y protección de datos.

• Registro de actividades de tratamiento de datos.

• Evaluación de riesgos y medidas de seguridad.

• Procedimientos para la atención de solicitudes de derechos de los titulares.

• Capacitación y concienciación para el personal.

• Gestión de incidentes de seguridad y brechas de datos.

• Designación de un responsable o equipo de protección de datos.

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

Un programa de cumplimiento en protección de datos ofrece beneficios clave en términos legales, operativos y reputacionales:

a) Cumplimiento normativo y reducción de riesgos

• Garantiza el cumplimiento de la Ley 81 de 2019 y su reglamentación, evitando sanciones y litigios.

• Facilita la adaptación a normativas internacionales en caso de operar fuera de Panamá.

b) Reputación y confianza

• Refuerza la credibilidad ante clientes, socios y proveedores.

• Previene daños reputacionales por filtraciones o mal manejo de datos.

c) Seguridad y control de la información

• Reduce riesgos de fugas de datos, ciberataques y accesos no autorizados.

• Optimiza la gestión del ciclo de vida de los datos personales.

d) Eficiencia y reducción de costos

• Mejora la organización y acceso a la información.

• Minimiza costos asociados a incidentes de seguridad y litigios.

e) Cultura de privacidad y ventaja competitiva

• Fomenta la capacitación interna y el desarrollo de políticas alineadas con la normativa.
Brinda una ventaja competitiva, especialmente en sectores regulados como finanzas, salud y tecnología.

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

Actualmente, en Panamá no existe un proceso de certificación oficial a nivel gubernamental para programas de cumplimiento en protección de datos personales, sin embargo, las organizaciones pueden adoptar certificaciones internacionales.

Además, la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) supervisa el cumplimiento de la normativa y puede emitir directrices sobre buenas prácticas.

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

La Ley 81 de 2019 no exige expresamente la designación de un Delegado de Protección de Datos, pero sí requiere que las entidades responsables del tratamiento de datos implementen medidas de seguridad adecuadas. En sectores altamente regulados, como el financiero y el de salud, o entidades públicas, puede ser requerido por normativas específicas.

1) Designación voluntaria y requisitos
Si una entidad privada designa un Oficial de Protección de Datos para reforzar su programa de cumplimiento, debe cumplir con ciertas exigencias formales, incluyendo:

• Designación formal del Oficial de Protección de Datos.

• Notificación de su nombramiento a la ANTAI o a la entidad reguladora correspondiente.

• Garantizar que el Oficial de Protección de Datos tenga los conocimientos y la capacitación adecuada en la normativa de protección de datos.

2) Funciones del Oficial de Protección de Datos

El Oficial de Protección de Datos desempeña un papel clave dentro de la organización, con funciones como:

• Participar en asuntos relacionados con el cumplimiento de la normativa.

• Informar y asesorar al responsable del tratamiento sobre sus obligaciones legales.

• Actuar como punto de contacto entre la organización y los titulares de los datos.

• Servir como enlace con la ANTAI o la entidad reguladora correspondiente.

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 81 de 2019 sobre Protección de Datos Personales y su reglamentación mediante el Decreto Ejecutivo 285 de 2021, establecen sanciones por incumplimiento de sus disposiciones. La Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) es el organismo encargado de aplicar estas sanciones, las cuales pueden clasificarse en:

La Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) puede imponer sanciones a los responsables del tratamiento de datos personales y custodios de las bases de datos, cuando infrinjan los derechos del titular de los datos personales.
Sanciones aplicables:

• Para infracciones leves: Citación ante la ANTAI para abordar las faltas cometidas.

• Para infracciones graves: Multas que varían según la gravedad de la infracción, con montos entre B/.1,000.00 y B/.10,000.00.

• Para infracciones muy graves: Además de las multas mencionadas, se pueden imponer sanciones como la clausura de registros de bases de datos y la suspensión o inhabilitación, temporal o permanente, de actividades relacionadas con el almacenamiento y tratamiento de datos personales.

La ANTAI es la entidad facultada para imponer estas sanciones, considerando factores como la intencionalidad, reincidencia, naturaleza y magnitud del daño causado, duración de la infracción, beneficios obtenidos por el infractor, volumen de negocios afectado, relación del infractor con el tratamiento de

datos, posible contribución del afectado a la infracción, impacto en derechos de menores, designación de un oficial de protección de datos, adopción de medidas correctivas y proporcionalidad de la sanción respecto a la gravedad de la falta.

Además de las sanciones administrativas, el responsable del tratamiento de datos personales está obligado a indemnizar por daños patrimoniales y/o morales resultantes de un tratamiento indebido de los datos.

Los plazos de prescripción para las acciones sancionadoras son de un año para infracciones leves, tres años para graves y cinco años para muy graves. En cuanto a las sanciones impuestas, prescriben en tres años para las leves, cinco años para las graves, mientras que las muy graves son imprescriptibles.

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

La normativa panameña en materia de protección de datos personales sanciona diversas conductas que vulneran la seguridad y privacidad de la información de los ciudadanos. Estas infracciones se clasifican en leves, graves y muy graves, según su impacto y el nivel de incumplimiento de las obligaciones establecidas.

Clasificación de las infracciones:

• Infracciones leves: No proporcionar información requerida a la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) dentro de los plazos establecidos.

• Infracciones graves: Tratamiento de datos sin consentimiento, violación de principios y garantías establecidos, incumplimiento de confidencialidad, obstrucción de derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), falta de información al titular sobre el tratamiento de sus datos, almacenamiento sin medidas de seguridad adecuadas, desatención a requerimientos de la ANTAI y falta de cooperación durante inspecciones.

• Infracciones muy graves: Recolección fraudulenta de datos, incumplimiento en el tratamiento de datos sensibles, desobediencia a órdenes de suspensión de tratamiento emitidas por la ANTAI, transferencia internacional de datos en contravención a la ley y reincidencia en infracciones graves.

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

Sí, en Panamá la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) es el organismo técnico encargado de dictar directrices y fiscalizar el cumplimiento de las normas de protección de datos personales. La ANTAI, a través de su Dirección de Protección de Datos Personales, tiene las siguientes atribuciones y facultades:

Atribuciones de la ANTAI:

• Supervisión y fiscalización: Velar por la correcta protección y reserva de los datos personales en poder de entidades públicas y privadas.

• Sensibilización y capacitación: Promover la concienciación entre responsables y custodios de datos sobre sus obligaciones legales, incluyendo la realización de actividades de formación para servidores públicos y actores del sector privado.

• Asesoramiento: Brindar orientación a las entidades estatales sobre medidas legislativas y administrativas relacionadas con la protección de datos personales, emitiendo dictámenes y evaluaciones de impacto cuando sea necesario.
Funciones de la Dirección de Protección de Datos Personales:

• Evaluaciones y análisis: Realizar estudios y análisis de procedimientos que involucren el tratamiento de datos personales, pudiendo solicitar información y documentación pertinente a los responsables o custodios de dichos datos.

• Aprobación de mecanismos de autorregulación: Validar mecanismos de autorregulación vinculantes y modelos de cláusulas contractuales que aseguren el cumplimiento de las normativas de protección de datos.

• Inspecciones sectoriales: Llevar a cabo inspecciones, ya sea por iniciativa propia o a solicitud de terceros, para evaluar el cumplimiento de la Ley 81 de 2019 y sus reglamentaciones, contando con el apoyo de entidades reguladoras sectoriales y de la Autoridad Nacional para la Innovación Gubernamental en aspectos tecnológicos.

• Sanciones: Imponer sanciones a responsables y custodios de datos que infrinjan las disposiciones legales, aplicando multas y otras medidas correctivas según la gravedad de la infracción.

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?

Las organizaciones en Panamá suelen seguir estos pasos para cumplir con la normativa y establecer un programa de cumplimiento en protección de datos:

a) Diagnóstico inicial:

• Evaluar el estado actual del tratamiento de datos personales.

• Identificar los riesgos y vulneraciones en el cumplimiento.

b) Desarrollo de políticas y procedimientos:

• Crear una política de privacidad acorde con las regulaciones vigentes.

• Establecer protocolos para la gestión de datos y la respuesta a incidentes.

c) Registro de actividades de tratamiento:

• Identificar las bases de datos y documentar los procesos de recolección, almacenamiento y uso de datos.

d) Obtención del consentimiento y garantías legales:

• Asegurar que se obtenga el consentimiento de los titulares antes de tratar sus datos.

• Revisar contratos con terceros para garantizar la protección de la información.

e) Implementación de medidas de seguridad:

• Aplicar controles de acceso, cifrado y auditorías de seguridad.

• Garantizar la capacitación del personal en buenas prácticas de protección de datos.

f) Mecanismos para atender derechos de los titulares: Establecer canales para que las personas puedan ejercer sus derechos (acceso, rectificación, cancelación y oposición).

g) Supervisión y actualización continua:

• Realizar auditorías periódicas para verificar el cumplimiento.

• Adaptarse a nuevas regulaciones y recomendaciones de la ANTAI y entidades regulatorias.