etiqampus
e-Learning en Integridad

Guía Comparada Protección de Datos Personales: caso Ecuador

Compliance Internacional

NIVEL INTERMEDIO

Fecha	Marzo 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 Ecuador y escrita por los siguientes profesionales del estudio Bustamante Fabara:

- Esteban Dávila Caicedo, Asociado Senior, Competencia
- Económica, Compliance, Privacidad y Protección de Datos Personales.
- Rafael Gabela, Asociado, Protección de Datos Personales.

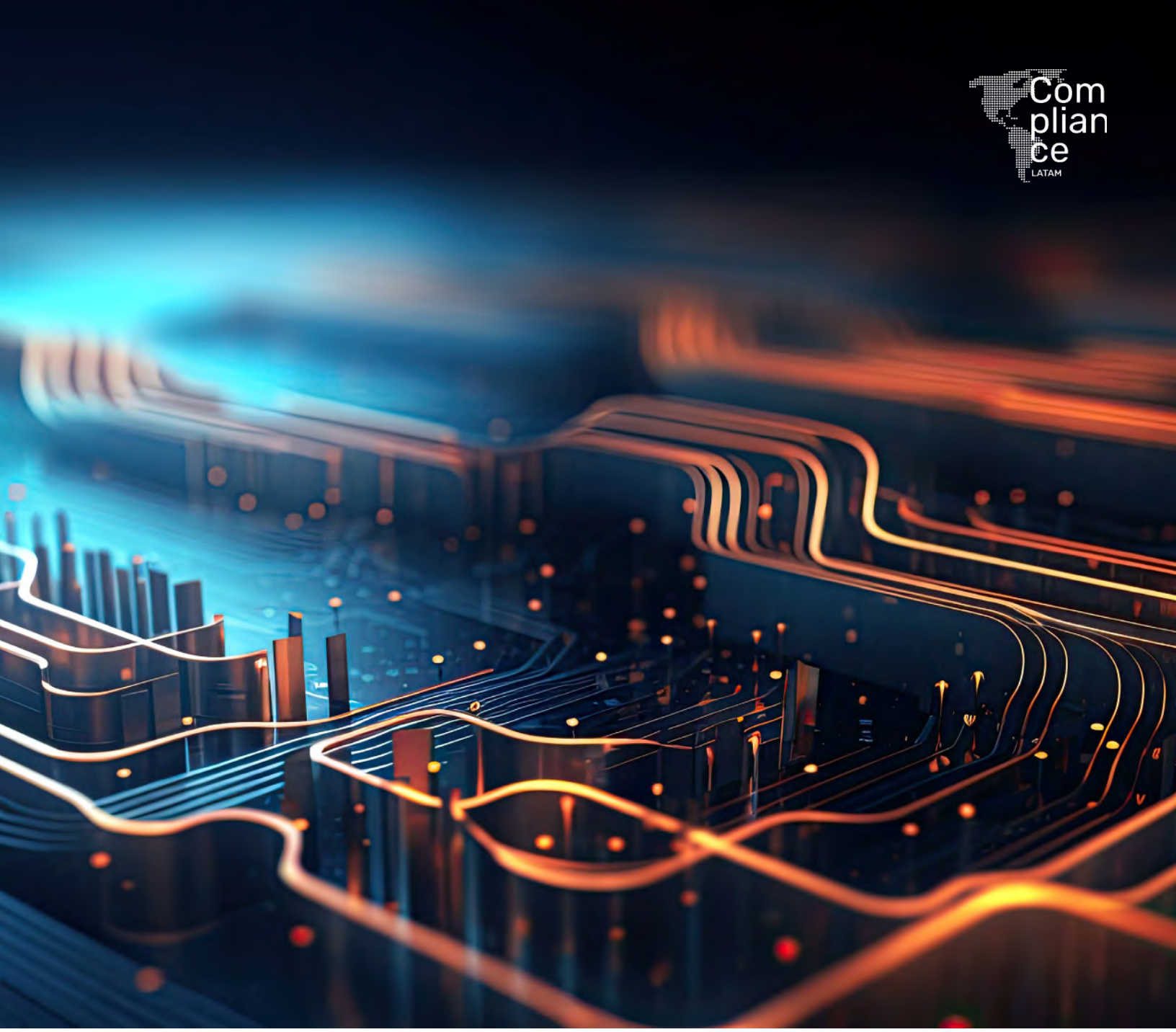
FUENTE: el texto de esta portadilla se elaboró a partir de la introducción de la “Guía Comparada Protección de Datos Personales” publicada por la plataforma “Compliance Latam”.

Guía Comparada Protección de Datos Personales

Marzo 2025



www.compliancelatam.legal



BUSTAMANTE FABARA

Autores:

Esteban Dávila Caicedo, Asociado Senior, Competencia Económica, Compliance, Privacidad y Protección de Datos Personales.

Rafael Gabela, Asociado, Protección de Datos Personales.

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

En Ecuador, el marco regulatorio principal es la Ley Orgánica de Protección de Datos Personales ("LOPDP"), promulgada el 26 de mayo de 2021. Esta ley tiene como objetivo garantizar el ejercicio del derecho a la protección de datos personales, incluyendo el acceso y decisión sobre información personal, así como la protección de derechos como la intimidad y privacidad. Ecuador también cuenta con regulación secundaria a la LOPDP, específicamente el Reglamento a la LOPDP expedido el 13 de noviembre de 2023.

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 LOPDP establece la obligación de implementar medidas de responsabilidad proactiva para garantizar el cumplimiento de la normativa de protección de datos. Entre estas medidas, se incluye la designación de un Delegado de Protección de Datos Personales en ciertos casos específicos, como cuando el tratamiento de datos se realiza por entidades del sector público o cuando las actividades del responsable o encargado requieren un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades del tratamiento. Los preceptos de la LOPDP son de cumplimiento obligatorio para todas las instituciones, públicas o privadas, que traten datos personales de titulares.

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

Los programas de cumplimiento deben incluir medidas técnicas, jurídicas y organizativas apropiadas para garantizar y demostrar que el tratamiento de datos se realiza conforme a la ley. Esto incluye:

1. Aplicar e implementar procesos de verificación, evaluación y valoración periódica de la efectividad de las medidas técnicas, jurídicas y organizativas implementadas.

2. Implementar políticas de protección de datos personales afines al tratamiento de datos personales que realice la organización por sus diferentes procesos.

3. Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento de datos y las partes involucradas en dicho tratamiento.

4. Realizar evaluaciones de seguridad previas al tratamiento de datos personales.

5. Establecer protocolos de notificación a la Autoridad de Protección de Datos Personales y a los titulares cuando sucedan violaciones de seguridad de los datos personales en los plazos y condiciones que prevé la ley.

6. Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales.

7. Establecer protocolos para asegurar que el encargado del tratamiento de datos personales ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme a lo establecido en la LOPDP.

8. Elaborar un registro de actividades de tratamiento de datos personales (RAT);.

9. Designar un delegado de protección de datos personales en los casos que la ley establece como obligatorio dicha designación.

10. La adopción de códigos de conducta y la aplicación de mecanismos de certificación.

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

Implementar un programa de cumplimiento en protección de datos personales ayuda a las organizaciones a:

• Garantizar el respeto a los derechos de los titulares de los datos.

• Evitar sanciones legales derivadas del incumplimiento de la normativa, las cuales pueden ser muy cuantiosas ya que una sanción grave puede llegar a equivaler hasta el 1% del volumen de negocio de una compañía.

• Generar confianza entre clientes y usuarios al demostrar un compromiso con la privacidad y seguridad de la información.

• Diferenciar a la organización en el mercado al demostrar su compromiso con la privacidad.

• Empresas con programas robustos de privacidad pueden acceder a mercados con regulaciones estrictas.

• Facilita alianzas estratégicas con organizaciones que exigen cumplimiento en privacidad como requisito.

• Reduce el riesgo de brechas de datos y ciberataques.

• Reduce el impacto reputacional en caso de incidentes relacionados con datos personales.

• Mejorar la gestión y calidad de los datos dentro de la organización.

• Facilita la respuesta ante solicitudes de derechos de los titulares (acceso, rectificación y eliminación, entre otros).

• Un programa de cumplimiento bien estructurado permite adaptarse fácilmente a nuevas regulaciones.

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

La ley contempla la posibilidad de que la Autoridad de Protección de Datos Personales establezca mecanismos de certificación para responsables y encargados del tratamiento de datos. Sin embargo, los detalles específicos sobre estos procesos y las entidades encargadas de la certificación deberán ser definidos por la Autoridad de Protección de Datos Personales y, a la presente, no han sido definidos.

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

Sí, es obligatorio designar un Delegado de Protección de Datos Personales (DPO) en los siguientes casos:

a. Cuando el tratamiento de datos es realizado por entidades del sector público.

b. Cuando las actividades del responsable o encargado del tratamiento requieren un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades.

c. Cuando se traten categorías especiales de datos a gran escala.

d. Es obligatorio designar a un DPO si la organización pertenece a los siguientes sectores:

• Hospitales, clínicas e instituciones que conforman el Sistema Nacional de Salud.

• Entidades que traten datos de desplazamiento de personas en el sistema de transporte público de una ciudad.

• Entidades que tratan datos de geolocalización de personas en tiempo real.

• Compañías de seguros, corredores, agentes, prestadores y medicina prepagada.

• Instituciones financieras.

• Entidades que realicen tratamiento de datos personales para publicidad comportamental por un motor de búsqueda.

• Empresas de servicios de telefonía o internet.

La Autoridad de Protección de Datos Personales puede definir condiciones adicionales para la designación de este delegado.

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 establece sanciones por el incumplimiento de la normativa, que pueden ser de tipo administrativo y económico. Las multas varían según la gravedad de la infracción y pueden alcanzar montos significativos. Para infracciones leves, las multas pueden ser de entre el 0,1% al 0,7% del volumen de negocios; mientras que, las graves, de entre el 0,7% al 1% del volumen de negocios del infractor en el año inmediatamente anterior al de la imposición de la multa.

La Autoridad de Protección de Datos también puede imponer medidas correctivas a las organizaciones infractoras. Dichas medidas correctivas pueden consistir, entre otras, en: (i) el cese del tratamiento, bajo determinadas condiciones o plazos; (ii) la eliminación de los datos; (iii) la imposición de medidas técnicas, jurídicas, organizativas o administrativas para garantizar un tratamiento adecuado de datos personales.

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

La normativa sanciona conductas como:

• Recopilar, almacenar, procesar o transferir datos personales sin el consentimiento expreso e informado del titular cuando este sea requerido.

Utilizar bases de datos sin contar con una base jurídica válida (consentimiento, contrato, obligación legal,

interés legítimo, etc.).

• No respetar los principios de licitud, lealtad, transparencia, minimización de datos, exactitud, limitación de conservación y seguridad.

• Conservación indefinida de datos sin base e legal.

• No implementar medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos.

• No notificar una brecha de seguridad dentro de los plazos establecidos.

• Transferir datos personales a terceros países que no cuenten con un nivel adecuado de protección, sin aplicar medidas adicionales.

• No formalizar acuerdos de corresponsabilidad o encargos de tratamiento con proveedores o terceros que accedan a datos personales.

• Negar, obstruir o no responder dentro de los plazos legales las solicitudes de los titulares sobre sus derechos de acceso, rectificación, eliminación, oposición, portabilidad y limitación del tratamiento.

• Procesar datos sensibles (origen étnico, salud, orientación sexual, biometría, etc.) sin cumplir con requisitos más estrictos de seguridad y consentimiento.

• No mantener actualizado el Registro Nacional de protección de datos personales.

• No designar al Delegado de Protección De Datos personales cuando corresponda.

• No implementar protección de datos desde el diseño y por defecto.

• No mantener disponibles políticas de protección de datos personales afines al tratamiento 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 Autoridad de Protección de Datos Personales es el organismo encargado de supervisar la aplicación de la ley, emitir directrices y lineamientos, y fiscalizar el cumplimiento de las normas de protección de datos en Ecuador. Dicha autoridad funciona a través de una Superintendencia, denominada como Superintendencia de Protección de Datos Personales.

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 suelen iniciar con:

• Realizar un diagnóstico del tratamiento de datos personales: identificar qué datos personales se recopilan, procesan, almacenan y transfieren dentro de la organización.

• Evaluar la base legal del tratamiento de datos (consentimiento, ejecución de un contrato, cumplimiento de una obligación legal, entre otras).

• Analizar los flujos de datos dentro y fuera de la organización.

• Detectar posibles riesgos y brechas de cumplimiento respecto a la normativa.

• Elaborar y adoptar Políticas de Protección de Datos Personales, alineadas con la LOPDP.

• Diseñar procedimientos internos para garantizar el ejercicio de los derechos de los titulares (acceso, rectificación, eliminación, portabilidad, entre otros).

• Establecer protocolos para la gestión de incidentes y notificación de brechas de seguridad.

• Crear registros de actividades de tratamiento para documentar cómo se manejan los datos personales.

• Determinar si la organización está obligada a designar un Delegado de Protección de Datos Personales (DPO), especialmente si maneja datos sensibles o realiza tratamientos a gran escala.

• Sensibilizar y entrenar a todos los colaboradores en principios de protección de datos y buenas prácticas.

• Desarrollar programas de formación específicos para equipos clave (TI, RRHH, Marketing, Atención al Cliente, Legal, entre otros).

• Establecer medidas técnicas y organizativas para garantizar la seguridad de los datos.

• Realizar Evaluaciones de Impacto en la Protección de Datos (EIPD) en tratamientos que puedan implicar

riesgos elevados para los derechos y libertades de los titulares.

• Diseñar planes de acción para mitigar riesgos identificados en el diagnóstico inicial.

• Implementar auditorías y revisiones periódicas para garantizar el cumplimiento con la normativa.

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

Con base en lo previsto en el artículo 3 de la LOPDP, dicha norma aplica:

1. Para el tratamiento de datos personales que se realice en cualquier parte del territorio ecuatoriano.

2. Cuando un responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional.

3. Cuando se realice tratamiento de datos personales de titulares que residan en el Ecuador por parte de un responsable o encargado no establecido en el Ecuador, cuando las actividades del tratamiento estén relacionadas con: (i) La oferta de bienes o servicios a dichos titulares, independientemente de si a estos se les requiere su pago, o, (ii) del control de su comportamiento, en la medida en que este tenga lugar en el Ecuador.

4. Para el responsable o encargado del tratamiento de datos personales, no domiciliado en el territorio nacional, le resulte aplicable la legislación nacional en virtud de un contrato o de las regulaciones vigentes del derecho internacional público.