etiqampus
e-Learning en Integridad

Guía Comparada Protección de Datos Personales: casos de Guatemala, El Salvador, Honduras, Nicaragua y Costa Rica

Compliance Internacional

NIVEL INTERMEDIO

Fecha	Marzo 2025
Tpo. de lectura	26 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 Guatemala, El Salvador, Honduras, Nicaragua y Costa Rica y escrita por León Weinstok, Director, Ciberseguridad y Protección de Datos, Publicidad, Mercadeo y Protección al Consumidor del estudio Business Law Partners, BLP.

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



Business Law Partners.

Autor:

León Weinstok, Director, Ciberseguridad & Protección de Datos, Publicidad, Mercadeo y Protección al Consumidor.

Guatemala

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

Actualmente, Guatemala no cuenta con una ley marco para la protección de datos personales. Se cuenta con una ley de orden público que establece normas y procedimiento para garantizar acceso a la información pública, la Ley de Acceso a la Información Pública (Decreto 57-2008 del Congreso de la República), que regula únicamente la protección de datos personales que se encuentra dentro de archivos del organismos del Estado, que incluye municipalidades, instituciones autónomas y descentralizadas y las entidades privadas que perciban, inviertan o administren fondos públicos, incluyendo fideicomisos constituidos con fondos públicos, obras o servicios públicos sujetos a concesión o administración.

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 existen programas ni obligatoriedad por la falta de regulación local. En cuanto a información pública, de conformidad con la Ley de Acceso a la Información Pública, cada Sujeto Obligado, es decir, cada organismo del Estado sujeto a esta ley deberá contar con programas de actualización permanente (interna) en materia de protección de datos personales de los particulares. Estos programas son obligatorios y administrados por cada unidad dentro de la institución.

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

No existen lineamientos por la falta de regulación legal. En cuanto a la información pública, tampoco existen requisitos o lineamientos establecidos para cumplir con los programas internos para el fortalecimiento de la protección de datos personales dentro de organismos del Estado, cada institución del Estado, a través de sus Unidades de Acceso a la Información Pública planifican de manera personalizada.

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

No existen comentarios por la falta de regulación local.

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

No existen.

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

No es obligatorio por la falta de regulación local.

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

En materia de información pública, existen sanciones para funcionarios y empleados públicos. Las sanciones son penales sin perjuicio de la responsabilidad civil y administrativa. Las sanciones pueden ser de prisión 1 a 8 años y multas que pueden ascender a US$13,500 aproximadamente.

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

• Comercialización de datos personales (protegidos por la ley de acceso a la información pública).

• Alteración o destrucción de información en archivos públicos.

• Retención de información pública.

• Revelación de información confidencial o reservada.

En cuanto a la comercialización de datos personales fuera del ámbito de la administración pública, la Corte de Constitucionalidad (Tribunal de mayor jerarquía en Guatemala) ha establecido en un fallo constitucional (Expediente 863-2011) la prohibición de comercializar datos personales sin el consentimiento de la persona. Este fallo constitucional representa un hito dentro del territorio nacional pues se reconoce el derecho a la autodeterminación informativa del individuo que va íntimamente ligado al derecho a la intimidad y privacidad de la persona. Si bien la conducta no se encuentra tipificada como delito, existe el primer fallo de la Corte de Constitucional en la cual ordena a empresas privadas cesar la comercialización de datos personales sin el consentimiento de las personas. Debido a que este fallo ha pasado a formar parte de la jurisprudencia del país, toda conducta en la misma línea podrá ser sancionada con multas no substanciales por parte del tribunal

juzgador o bien con ordenar el cese de la conducta.

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

En materia de información pública, cada una de las instituciones de gobierno debe contar con una Unidad de Acceso a la Información Pública que se encarga de cumplir con la ley de 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?

Debido a que no existe una ley de la materia cada una de las organizaciones locales aplican políticas propias para el manejo y protección de datos personales sin ninguna directriz en particular.

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

N/A

El Salvador

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

Ley de protección de Datos Personales (LPDP).

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, no existe hasta el momento regulación al respecto.

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

Actualmente no existe una regulación respecto a este tema, únicamente establece obligaciones generales respecto a que los datos deben de estar almacenados "cumpliendo las exigencias mínimas de seguridad de la información", pero no se especifica.

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

Bajar el riesgo de un incumplimiento por parte de la empresa a la LPDP.

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

No, actualmente no existe.

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

Sí, la LPDP establece la obligación por parte de las empresas de tener un Delegado de Protección de Datos personales (Art. 15 de la LPDP) a todas las empresas que tengan una base de datos.

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

Si existen sanciones por el incumplimiento, las mismas se clasifican en leves, las cuales son sancionadas con multa desde US$365 hasta US$3,650, las graves, que van con multa desde US$4,015 hasta US$9,125 y las muy graves, que van desde una multa de US$9,490 hasta US$14,600.

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

Estas se encuentran en el Art. 56 de la LPDP:

Infracciones

Art. 56.- Las infracciones se clasificarán en leves, graves y muy graves:

a) Son consideradas infracciones leves, las siguientes:

1. No informar al titular de los datos personales acerca de sus derechos antes de ser recolectados.

2. No publicar los datos de contacto del encargado del tratamiento.

3. Omitir notificar respecto de las vulneraciones a la seguridad de los datos personales acaecidas a los sujetos pertinentes, de conformidad con lo dispuesto en el artículo 25 de la presente ley.
4. Acceder a un banco de datos, base de datos,

repositorio, sistemas o registros, tanto manuales como informáticos, sin autorización del responsable de éstos.

5. Dar un tratamiento a los datos personales de forma inexacta o falsa.

6. Modificar los datos suministrados en el documento que autoriza el tratamiento de datos personales.

7. Exigir pago para atender las solicitudes que en la presente ley se establecen como gratuitas.

8. Incumplir con el Derecho de Información frente a la Recolección de Datos contenido en el artículo 7 o la obligación de informar del artículo 48, ambos de la presente ley.

9. No atender las solicitudes realizadas por parte de la ACE en materia de protección de datos personales.

b) Son consideradas infracciones graves, las siguientes:

1. Proporcionar de forma incompleta o inexacta la información relativa a los datos personales que del titular se traten, ya sean recolectados o inferidos, cuando este ejerza su derecho de acceso.

2. No atender las solicitudes de derechos ARCO-POL, en el tiempo y forma establecidos por la presente ley.

3. Procesar, recopilar o destinar datos personales con finalidad diferente para la que se otorgó el consentimiento o se habilito su tratamiento.

4. Obstaculizar el desarrollo de las auditorías o inspecciones que realice la ACE.

5. No implementar las medidas, controles técnicos o lineamientos que establezca la ACE en materia de protección de datos.

6. Incurrir en las prohibiciones establecidas en el artículo 59 de la presente ley.

7. No cumplir con las medidas de seguridad establecida en las políticas de actuación emitidas por la Agencia.

c) Son consideradas infracciones muy graves, las siguientes:

1. Tratar datos personales sin el consentimiento previo, de conformidad con lo establecido en el artículo 26 de la presente ley.

2. Denegar las solicitudes realizadas para el ejercicio de los derechos ARCO-POL en contravención a lo establecido en esta ley.

3. El uso de los datos personales de niños, niñas y adolescentes sin el previo consentimiento de sus padres, representantes o tutores, de conformidad con las leyes vigentes o tratados internacionales debidamente suscritos y ratificados por El Salvador.

4. Tratar datos personales de personas declaradas incapaces sin el consentimiento de su titular o su representante.

5. Realizar transferencia internacional de datos personales a países que no cumplan como mínimo con el nivel de protección exigido por la presente ley.

6. Realizar transferencia de datos personales sin el consentimiento de su titular o su representante, o en contravención de las excepciones que establezca la ley.

7. Comercializar datos personales a cualquier título sin el consentimiento de su titular.

8. Revertir la seudonimización de los datos personales sin el consentimiento del titular.

9. Tratar datos personales a pesar de la revocación del consentimiento otorgado por el titular.

10. No hacer efectiva la revocación del consentimiento ante la solicitud del titular cuando ésta proceda.

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

Sí, es la Agencia de Ciberseguridad del Estado (ACE) (Art. 50 LPDP)

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?

La LPDP fue aprobada en noviembre del 2024, por lo que actualmente las empresas están iniciando su cumplimiento, lo primeros pasos que están realizando es el nombramiento del Delegado de Protección de Datos Personales para que este se encargue internamente de la adecuación de la sociedad a la ley.

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

Con respecto a los efectos extraterritoriales de la recientemente promulgada Ley para la Protección de Datos Personales, la ley proporciona un lenguaje muy limitado sobre este tema, mencionando únicamente en el Artículo 2 que los funcionarios públicos están sujetos a la ley cuando trabajan fuera del territorio de El Salvador.

Para los actores privados, no se menciona ningún efecto fuera del país, aunque podría interpretarse que las actividades relacionadas con datos que ocurren en El Salvador por actores sin presencia física o jurídica en el país están dentro del alcance de la ley (por ejemplo, un servicio de streaming que recopila datos de residentes salvadoreños en el extranjero a través del uso de su plataforma en el país). No obstante, no parece haber un alto riesgo de aplicación de la ley contra actores sin activos o presencia legal en El Salvador.

Cabe considerar que el Artículo 60 de la ley establece que la Agencia de Ciberseguridad del Estado deberá emitir políticas, medidas, directrices y cualquier otro documento necesario para la aplicación de la ley dentro de los primeros tres meses desde su entrada en vigor (a mediados de febrero de 2025). Sin embargo, hasta la fecha, no se ha hecho público ningún avance en este asunto.

Honduras

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

No existe una ley específica, pero algunas disposiciones podemos identificarlas en la Constitución de la República y la Ley Sobre Justicia Constitucional.

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, no existe regulación que aborde programas de este tipo.

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?

La implementación de un programa de cumplimiento en materia de datos personales permite el cumplimiento de la empresa con la normativa aplicable.

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

No, no existen.

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

No, no es obligatorio.

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

Sí, podrían llegar hasta cincuenta (50) salarios mínimos mensuales.

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

Aquellas infracciones no constitutivas de delito, mismas que serán sancionadas con amonestación por escrito, suspensión, multa, cesantía o despido. Las multas de entre medio salario hasta cincuenta (50) salarios mínimos mensuales, serán impuestos por el Instituto de Acceso a la Información Pública, (IAIP), dependiendo de la gravedad de la infracción, debiendo ser enterados dichos valores en la Tesorería General de la República.

Quien:

• Estando obligado por Ley, no proporcionare de oficio o se negare a suministrar la información pública requerida en el tiempo estipulado o de cualquier manera obstaculizare su acceso;

• Copie, capte, consulte, divulgue o comercialice información reservada cuando la Ley lo prohíbe o en el caso de datos personales, se negare a proporcionarlos a su legítimo titular, sus sucesores o autoridad

competente;

• Elimine, suprima o altere, información pública o reservada y los instrumentos que la contengan, sin seguir el procedimiento de depuración previsto en la Ley.

• Fuera de los casos previstos en la Ley, recoja, capte, transmita o divulgue datos personales, o se niegue a rectificarlos, actualizarlos o eliminar información falsa en los datos personales confidenciales contenidos en cualquier archivo, registro o base de datos de las Instituciones Obligadas por la Ley; y,

• Estando obligado, de conformidad con el Artículo 4, segundo párrafo, de la Ley, no envíe la información relativa a los procedimientos de contratación y las contrataciones mismas a la Oficina Normativa de Contratación y Adquisiciones.

Todo lo anterior enmarcado a la obligatoriedad de proporcionar información dirigido a *"Instituciones Obligadas"* o entidades gubernamentales.

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

No, no existe un organismo técnico específico.

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?

Considerando que no existe una normativa específica, las organizaciones comienzan a aplicar sus procedimientos internos en aras de velar por la protección de datos personales, con especial atención a las pocas disposiciones que regulan este tema en Honduras.

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

N/A

Nicaragua

1. ¿Cuál es el marco regulatorio de la protección de datos personales en tu jurisdicción?
Ley No. 787, Ley de protección de Datos Personales (2012).

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, no existe regulación al respecto.

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

No hay normativa específica sobre este tema.

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

Facilitará el cumplimiento con las normativas locales con antelación. Por el momento, la autoridad (Dirección de Protección de Datos Personales) fue instituida por Ley, pero es inoperante al no estar creada por el Ejecutivo todavía.

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

No, no existen.

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

Sí. La ley contempla a un responsable, o encargado, para el tratamiento de datos y gestión de sus ficheros.

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

Si existen sanciones administrativas por el incumplimiento, que pueden incluir: apercibimientos, suspensión temporal o definitiva y multa (no se especifican montos).

8. ¿Qué tipo de conducta sanciona la normativa en

protección de datos personales de tu país?

El Artículo 44 establece como infracciones leves: tratar datos sin consentimiento cuando sea requerido, no atender solicitudes de modificación o eliminación de datos, incumplir instrucciones de la autoridad, recopilar datos sin informar sobre su uso y enviar publicidad no deseada.

El Artículo 45 define como infracciones graves: tratar datos de forma fraudulenta, impedir el ejercicio de derechos sobre los datos, violar el secreto profesional, reincidir en infracciones leves, no garantizar seguridad en el manejo de datos y obstruir inspecciones de la autoridad.

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

Sí, la Dirección de Protección de Datos Personales tiene las facultades para dictar normas y disposiciones administrativas.

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?

Por el momento, ante la falta de un regulador activo, las organizaciones están comenzado a desarrollar políticas internas alineadas a la Ley 787 y capacitar a su personal.

Costa Rica

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

La protección de datos personales se encuentra regulada principalmente en la Ley de Protección de la Persona frente al tratamiento de sus datos personales No. 8968 y su reglamento.

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, no existe regulación al respecto.

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

No hay normativa específica sobre este tema.

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

Legalmente no hay ningún beneficio establecido.

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

No, no existen.

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

No contamos con esta exigencia

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

Se establecen faltas que pueden ser leves, graves o muy graves. La sanción más elevada puede ser de hasta 30 salarios base (US$ 15,000 aproximadamente).

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

Se establecen las siguientes faltas:

Faltas leves:

1. Recolectar datos personales para su uso en base de datos sin que se le otorgue suficiente y amplia información a la persona interesada, de conformidad con las especificaciones del artículo 5, apartado I.

2. Recolectar, almacenar y transmitir datos personales de terceros por medio de mecanismos inseguros o que de alguna forma no garanticen la seguridad e inalterabilidad de los datos.

Faltas graves:

1. Recolectar, almacenar, transmitir o de cualquier otra forma emplear datos personales sin el consentimiento informado y expreso del titular de los datos, con arreglo

a las disposiciones de esta ley.

2. Transferir datos personales a otras personas o empresas en contravención de las reglas establecidas en el capítulo III de esta ley.

3. Recolectar, almacenar, transmitir o de cualquier otro modo emplear datos personales para una finalidad distinta de la autorizada por el titular de la información.
4. Negarse injustificadamente a dar acceso a un interesado sobre los datos que consten en archivos y bases de datos, a fin de verificar su calidad, recolección, almacenamiento y uso conforme a esta ley.

5. Negarse injustificadamente a eliminar o rectificar los datos de una persona que así lo haya solicitado por medio claro e inequívoco.

Faltas gravísimas:

1. Recolectar, almacenar, transmitir o de cualquier otra forma emplear, por parte de personas físicas o jurídicas privadas, datos sensibles, según la definición prevista en el artículo 3 de esta ley.

2. Obtener, de los titulares o de terceros, datos personales de una persona por medio de engaño, violencia o amenaza.

3. Revelar información registrada en una base de datos personales cuyo secreto esté obligado a guardar conforme la ley.

4. Proporcionar a un tercero información falsa o distinta contenida en un archivo de datos, con conocimiento de ello.

Realizar tratamiento de datos personales sin encontrarse debidamente inscrito ante la Prodhab, en el caso de los responsables de bases de datos cubiertos por el artículo 21 de esta ley.

5. Transferir, a las bases de datos de terceros países, información de carácter personal de los costarricenses o de los extranjeros radicados en el país, sin el consentimiento de sus 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 Agencia de Protección de datos de los Habitantes (PRODHAB).

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?

No se establece legalmente ningún tipo de guía o recomendación en este sentido. Sin embargo, lo recomendado es iniciar por un análisis del tratamiento de datos que se realiza, preparar los procedimientos y protocolos necesarios y por último la implementación y capacitación.

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

De conformidad con lo establecido en el artículo 3 del reglamento, esto es aplicable “a los datos personales que figuren en las bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos, en tanto surtan efectos dentro del territorio nacional, o les resulte aplicable la legislación costarricense derivada de la celebración de un contrato o en los términos del derecho internacional”. Por ende, si podría tener una aplicación extraterritorial en caso de celebrarse un contrato que le resulte aplicable la ley costarricense.