Guía Comparada Protección de Datos Personales

Marzo 2025

www.compliancelatam.legal


Com
plian
ce
LATAM
Somos
un espacio
permanente,
cercano y
colaborativo que
permite crear
valor compartido
www.compliancelatam.legal

Introducción

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, Compliance Latam reúne a especialistas de destacadas firmas legales en 18 países de Latinoamérica, EE.UU. y España para ofrecer una visión clara y actualizada sobre los marcos normativos y últimas tendencias en protección de datos personales. A través de esta guía, brindamos 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.

Más allá del cumplimiento normativo, una adecuada gestión de la privacidad se ha convertido en un diferenciador competitivo. Contar con información precisa sobre las regulaciones en distintas jurisdicciones permite a las organizaciones anticiparse a los cambios, mitigar riesgos y fortalecer su posición en el mercado. Desde Compliance Latam, ponemos este conocimiento a disposición de nuestro ecosistema para apoyar la toma de decisiones estratégicas en esta materia.

índice

albagli zaliasnik

Autor:

Rodrigo Albagli, Socio.

Yoab Bitran, Director Grupo Compliance.

Antonia Nudman, Asociada Senior, Grupo IP, Tech and Data.

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

La protección de datos personales está garantizada como derecho fundamental por la Constitución Política de la República, en el artículo 19 N°4. La protección y el tratamiento de la información personal están regulado en la Ley N°19.628, de 1999. Sin embargo, recientemente se aprobó la Ley N°21.719, que modifica la normativa actual, elevando los estándares existentes junto con crear una Agencia de Protección de Datos Personales. Esta nueva regulación entrará en vigor el 1 de diciembre de 2026.

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 nueva Ley N°21.719 incorporó un nuevo tipo de modelo de prevención de infracciones de protección de datos personales (compliance), el cual comenzará a regir a partir del 1° de diciembre de 2026.

Los nuevos programas de compliance no son obligatorios, sin embargo, de implementarse y ser certificados por la futura Agencia de Protección de Datos Personales, servirán como atenuante de responsabilidad en caso de que la organización sea sancionada por dicho organismo.

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

El programa de cumplimiento deberá contener, al menos, los siguientes elementos:

a) La designación de un delegado de protección de datos personales.

b) La definición de medios y facultades del delegado de protección de datos.

c) La identificación del tipo de información que la entidad trata, el ámbito territorial en que opera, la categoría, clase o tipos de datos o bases de datos que administra, y la caracterización de los titulares de datos.

d) La identificación de las actividades o procesos de la entidad, sean habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de las infracciones señaladas en la ley.

e) El establecimiento de protocolos, reglas y procedimientos específicos que permitan a las personas que intervengan en las actividades en cuyo contexto se genere o incremente el riesgo de comisión de las infracciones señaladas en la ley, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de infracciones.

f) Los mecanismos de reporte interno sobre el cumplimiento de lo dispuesto en la presente ley y los mecanismos de reporte a la autoridad de protección de datos para el caso de vulneraciones de medidas de seguridad.

g) La existencia de sanciones administrativas internas, así como de procedimientos de denuncia o castigo de responsabilidades de las personas que incumplan el sistema de prevención de infracciones.

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 en protección de datos personales trae múltiples beneficios, entre ellos:

• Evita sanciones y multas al asegurar el cumplimiento normativo.

• Reduce riesgos reputacionales y genera confianza con clientes,colaboradores y socios.

• Protege la información sensible y minimiza el impacto de brechas de seguridad.

• Facilita la gestión de derechos de los titulares y mejora la transparencia.

• Optimiza procesos internos, promoviendo una cultura organizacional de privacidad y seguridad.

• Asegura la continuidad operativa, evitando interrupciones por incumplimientos legales.

Asimismo, en términos procesales, el modelo podría servir como medio de prueba para demostrar ante entidades públicas que se están tomando las medidas necesarias para cumplir la ley. Además, si el programa está certificado por la Agencia, podría servir como atenuante de responsabilidad según la nueva Ley N°21.719.

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

Sí, la nueva ley establece que los programas de prevención de infracciones serán certificados por la Agencia de Protección de Datos Personales, y serán incorporados en el Registro Nacional de Sanciones y Cumplimiento.

Además, se dictará un reglamento que establecerá los requisitos, modalidades y procedimientos para la implementación, certificación, registro y supervisión de los modelos.

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

En general no es obligatorio, pero si la compañía cuenta con un modelo de prevención de infracciones que someterá al proceso de certificación de la Agencia de Protección de Datos Personales, su incorporación es obligatoria.

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

Sí, bajo la legislación actual las multas son de hasta USD$3.500 U, Sin embargo, la Ley N°21.719, que entra en vigencia el 1° de diciembre de 2026, las incrementa ostensiblemente de la siguiente manera:

Infracciones leves: Amonestación por escrito y multa de hasta USD$350.000.

Infracciones graves: Multas de hasta USD $700.000.

Infracciones gravísimas: Multa de hasta USD $1.400.000.

En casos de reincidencia, las multas podrían triplicar el monto asignado como multa. Asimismo, cuando el infractor corresponda a una empresa de mediano o gran tamaño, que reincida en una infracción de carácter grave o gravísima, la multa podrá alcanzar a la más gravosa entre las señaladas anteriormente o hasta el monto correspondiente al 2% o 4% de los ingresos anuales por ventas,servicios y otras actividades del giro en el último año calendario, según se trate de infracciones graves o gravísimas, respectivamente.

Además, en caso de que se impongan multas por infracciones gravísimas reiteradas, en un período de veinticuatro meses, la Agencia podrá disponer la suspensión de las operaciones y actividades de tratamiento de datos que realiza el responsable de datos, hasta por un término de treinta días.

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

La normativa clasifica las conductas prohibidas en infracciones leves, graves y gravísimas.

Se consideran infracciones leves las siguientes conductas:

1. Falta de transparencia en el deber de información al titular de datos.

2. No contar con un medio de contacto actualizado (domicilio, correo electrónico o equivalente) para atender solicitudes de los titulares.

3. No responder, responder fuera de plazo o de forma incompleta las solicitudes de los titulares de datos.

4. No enviar a la Agencia las comunicaciones obligatorias establecidas en la ley.

5. Incumplir instrucciones generales de la Agencia, salvo que constituyan infracción grave o gravísima.

6. Otras infracciones menores a los derechos y obligaciones de la ley que no sean catalogadas como graves o gravísimas.

Se consideran infracciones graves las siguientes conductas:

1. Tratamiento ilícito de datos sin consentimiento o sin base legal válida.

2. Cesión o comunicación no autorizada de datos personales.

3. Uso de datos innecesarios para la finalidad del tratamiento.

4. Manejo de datos inexactos, incompletos o desactualizados.

5. Obstrucción o impedimento del ejercicio de derechos del titular (acceso, rectificación, supresión, oposición o portabilidad).

6. Negativa o demora injustificada en la respuesta a solicitudes de bloqueo temporal de datos.

7. Tratamiento indebido de datos de menores de edad.

8. Incumplimiento de requisitos específicos en organizaciones sin fines de lucro con fines políticos, filosóficos, religiosos, culturales, sindicales o gremiales.

9. Vulneración del deber de secreto o confidencialidad.

10. Incumplimiento de medidas de seguridad en el tratamiento de datos.

11. Falta de comunicación o registro de brechas de seguridad.

12. Deficiencias en la seguridad de datos con fines históricos, estadísticos o científicos.

13. Transferencia internacional de datos sin cumplir las normas legales.

14. Desacato a resoluciones o requerimientos de la Agencia.

Las siguientes conductas se consideran infracciones gravísimas según la ley:

1. Tratamiento fraudulento de datos personales.

2. Uso malicioso de datos para una finalidad distinta a la consentida o permitida por la ley.

3. Comunicación o cesión intencionada de datos inexactos o desactualizados.

4. Vulneración del secreto o confidencialidad de datos sensibles o sobre infracciones legales.

5. Tratamiento indebido de datos sensibles o de menores de edad.

6. Omisión deliberada de notificación de brechas de seguridad que afecten la integridad de los datos.

7. Uso masivo no autorizado de datos sobre infracciones penales, civiles o administrativas.

8. Transferencia internacional de datos en contravención a la ley.

9. Desacato a resoluciones de la Agencia en materia de derechos de los titulares.

10. Provisión intencional de información falsa en procesos de certificación del modelo de prevención de infracciones.

11. Incumplimiento de obligaciones específicas establecidas respecto de las evaluaciones de impacto.

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

Sí, actualmente existen varios organismos que ejercen estas laborares en forma parcelada. Por ejemplo, para el sector público existe el Consejo para la Transparencia y para el privado el Servicio Nacional de Protección del Consumidor, el que tiene estas atribuciones pero sólo respecto de las relaciones de consumo.

A partir del 1° de diciembre de 2026, será la Agencia la que tendrá dichas atribuciones en general.

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 Chile las organizaciones normalmente comienzan aplicando la nueva normativa de protección de datos personales identificando las brechas de cumplimiento y designando, de ser necesario, un Delegado de Protección de Datos (DPD), especialmente si manejan grandes volúmenes de datos, tratan datos sensibles y/o son multinacionales.

Además, debeben establecer un registro de actividades de tratamiento, evaluar los riesgos asociados a la gestión de datos y definir protocolos claros para la atención de los derechos de los titulares. Asimismo, debieran diseñar un programa de cumplimiento que contemple políticas internas, capacitaciones periódicas, medidas de seguridad adecuadas y procedimientos de auditoría.

También deben implementar controles robustos de seguridad de la información y definir estrategias para la gestión de incidentes y la notificación de brechas, garantizando así una adecuada gobernanza de los datos personales.

Finalmente, deben capacitar a sus colaboradores y, cuando corresponda, a sus proveedores, con el objetivo de sensibilizarlos sobre la importancia de proteger y gestionar responsablemente el tratamiento de datos personales de terceros, fomentando una cultura organizacional basada en la privacidad y el cumplimiento normativo.

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

En general, la ley se aplica a responsables y mandatarios establecidos o constituidos en Chile o a operaciones de tratamiento de datos personales que se realicen en el país. Sin embargo, podría tener aplicación extraterritorial en los siguientes casos:

• Cuando el mandatario, con independencia de su lugar de establecimiento o constitución, realice las operaciones de tratamiento de datos personales a nombre de un responsable establecido o constituido en el territorio nacional.

• Cuando el responsable o mandatario no se encuentren establecidos en el territorio nacional pero sus operaciones de tratamiento de datos personales estén destinadas a ofrecer bienes o servicios a titulares que se encuentren en Chile, independientemente de si a éstos se les requiere un pago, o a monitorear el comportamiento de titulares que se encuentran en el territorio nacional, incluyendo su análisis, rastreo, perfilamiento o predicción de comportamiento.

• La ley también se aplicará al tratamiento de datos personales que sea realizado por un responsable al que, sin estar establecido en el territorio nacional, le resulte aplicable la legislación nacional a causa de un contrato o del derecho internacional.

BARTOLOME & BRIONES

Autor:

Florencia Arrébola, Asociada Senior, Propiedad Intelectual, Media, Corporativo.

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

En España, la protección de datos personales está regulada principalmente por el Reglamento General de Protección de Datos (RGPD), que es una normativa de la Unión Europea aplicable a todos los Estados miembros. Este reglamento establece un marco armonizado para la protección de datos personales, asegurando derechos a los individuos y obligaciones a los responsables del tratamiento. El RGPD destaca principios como la responsabilidad proactiva, licitud, lealtad y transparencia, la limitación de la finalidad y la minimización de datos, que deben ser observados por cualquier entidad que maneje datos personales.

Además, la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) complementa y desarrolla el RGPD en el contexto español. Ambas normativas se fundamentan en principios esenciales de protección de datos, que no solo buscan salvaguardar la privacidad de los individuos, sino también fomentar la confianza en el uso de tecnologías digitales.

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, tanto el RGPD como la LOPDGDD establecen la obligación a los responsables y encargados del tratamiento de implementar medidas de cumplimiento en materia de protección de datos que se aplicarán atendiendo a la naturaleza, contexto, finalidad del tratamiento y los riesgos que el tratamiento de datos pueda implicar para los derechos y libertades de los ciudadanos. Estas medidas deben aplicarse desde el diseño y por defecto, es decir que deben tenerse en consideración desde el nacimiento y diseño de un proceso que implica el tratamiento de datos personales. En concreto, el artículo 24 del RGPD y el artículo 28 de la LOPDGDD exigen que los responsables adopten medidas técnicas y organizativas apropiadas. En este sentido, el principio de responsabilidad proactiva implica que cada responsable de tratamiento de datos deberá analizar y valorar cuáles son las medidas técnicas y organizativas que deben adoptarse en cada circunstancia para demostrar que se cumple con las obligaciones de la normativa frente a las autoridades de control y supervisión competentes.

Estas medidas pueden implicar no solo la creación de políticas y procedimientos internos, sino también la implementación de tecnologías adecuadas para proteger los datos. Por ejemplo, entre las medidas técnicas comúnmente utilizadas encontramos el uso de contraseñas seguras, actualización de los sistemas y copias de seguridad, y entre las medias organizativas destacamos la aplicación de políticas de privacidad, formación del personal, controles de acceso a la información y desarrollar auditorias regulares.

Por otro lado, el artículo 32 del RGPD describe las medidas de seguridad que se deben adoptar y enumera entre otras, técnicas como la seudonimización y cifrado de datos, garantizar la confidencialidad, integridad, disponibilidad y resiliencia de sistemas y servicios de tratamiento, capacidad para restaurar la disponibilidad y el acceso a los datos.

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

Como mencionamos en la respuesta anterior, si bien la normativa no determina las características de las medidas técnicas y organizativas que las organizaciones pueden adoptar, en la práctica, dichas medidas se caracterizan por los siguientes elementos:

Medidas técnicas:

• Uso de contraseñas seguras, para garantizar la seguridad del acceso a los sistemas e información de la organización.

• Actualización de los sistemas, a fin de que éstos sean más seguros frente a posibles amenazas externas.

• Copias de seguridad periódicas que permitan garantizar la recuperación de los datos en caso de que éstos sean eliminados o resulten dañados.

Medidas organizativas:

• Políticas de privacidad y protección de datos: documentos claros que informen a los empleados y a los interesados sobre cómo se manejan sus datos.

• Formación continua del personal sobre obligaciones en materia de protección de datos: en concreto se podrán llevar a cabo la capacitación regular para asegurar que todos los empleados conocen sus responsabilidades en el manejo de datos personales.

• Controles de acceso a la información: limitar el acceso a la información de manera que cuantas menos personas

tengan acceso a la información menor será el riesgo de que los datos personales se comprometan.

• Mecanismos de supervisión y auditoría interna: se basa en el desarrollo de herramientas para evaluar la efectividad de las políticas y detectar posibles fallos en el cumplimiento.

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

La adopción de las medidas técnicas y organizativas apropiadas ofrece beneficios significativos, tales como:

• Reducción de riesgos de incumplimiento y sanciones administrativas: un programa efectivo ayuda a identificar y mitigar riesgos potenciales, evitando así sanciones que pueden ser económicas y reputacionales.

• Mejora de la reputación y confianza con los clientes y usuarios: las organizaciones que demuestran un compromiso sólido con la protección de datos pueden ganar la confianza de sus clientes, lo que puede traducirse en lealtad y un incremento en la base de clientes.

• Fomento de una cultura de responsabilidad y ética en el manejo de datos: los programas de cumplimiento contribuyen a crear un entorno laboral donde se valora la privacidad y la protección de datos.

Asimismo, el compromiso con estas medidas y su adecuación a las características del tratamiento de datos y su finalidad, servirá para demostrar que se cumple con la normativa frente a las autoridades de control y supervisión competentes.

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

Sí, existen procesos de auditoría y certificación en materia de protección de datos, los cuales son reconocidos por el RGPD. En concreto la certificación "Europrivacy" aborda las obligaciones específicas del RGPD a la vez que funciona como esquema de certificación oficial y es aplicable al tratamiento de datos que se lleva a cabo en las organizaciones permitiendo evaluar y certificar su conformidad con el RGPD y LOPDGDD.

La certificación puede ser realizada por organismos de certificación acreditados que evalúan el cumplimiento de las normas de protección de datos, ofreciendo un mecanismo para demostrar la conformidad ante las autoridades y los interesados.

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

El RGPD y la LOPDGDD delimitan los supuestos en los que es necesario designar un Delegado de Protección de Datos (DPO).

En este sentido, la LOPDGDD regula este aspecto de forma más detallada, estableciendo los siguientes supuestos en los que los responsables y los encargados del tratamiento deberán designar un DPO:

• Los colegios profesionales y sus consejos generales.

• Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

• Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

• Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

• Las entidades de crédito (bancos, cajas de ahorro, cooperativas de crédito, el Instituto de Crédito Oficial).

• Los establecimientos financieros de crédito.

• Las entidades aseguradoras y reaseguradoras.

• Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

• Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

• Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

• Las entidades que desarrollen actividades de

publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

• Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

• Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

• Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

• Las empresas de seguridad privada.

• Las federaciones deportivas cuando traten datos de menores de edad.

Por otro lado, el RGPD establece la obligatoriedad de designar un DPO en los siguientes supuestos:

• Cuando el tratamiento de datos lo realiza una autoridad pública, excluyendo a los tribunales actuando en función judicial.

• Si las actividades principales del responsable o encargado del tratamiento implican la observación habitual y sistemática de datos personales a gran escala.

• Cuando se trata del tratamiento a gran escala de categorías especiales de datos, como el origen étnico, opiniones políticas, datos genéticos, entre otros.

Por lo tanto, el DPO deberá designarse obligatoriamente en los supuesto sindicados y de forma voluntaria en aquellos supuestos que las organizaciones así lo consideren. Tras la designación del DPO, la decisión se debe comunicar a la Agencia Española de Protección de Datos (AEPD).

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

Sí, el incumplimiento del RGPD y de la LOPDGDD puede derivar en la imposición de sanciones económicas o medidas como la suspensión temporal del tratamiento de datos o la obligación de rectificar o suprimir datos.

El RGPD en primer lugar, clasifica ciertas sanciones administrativas que pueden ascender hasta 10 millones de euros o el 2% del volumen de facturación anual global (es decir, del grupo de sociedades) del responsable o encargado, y, en segundo lugar, establece sanciones económicas más gravosas para aquellas infracciones consideradas muy graves, que podrán ascender hasta 20 millones de euros, o el 4% de la facturación anual global del responsable o encargado, la que sea mayor.

Además, la normativa establece criterios para graduar el importe de las sanciones, como por ejemplo la naturaleza, gravedad y duración de la infracción, acciones adoptadas para mitigar los daños ocasionados, los beneficios económicos obtenidos, la reincidencia, la intencionalidad de la infracción, categoría de datos comprometidos, así como cualesquiera otras circunstancias relevantes para determinar la culpabilidad.

Por otro lado, la LOPDGDD determina los diferentes importes que se indican a continuación:

• Incurrir en una infracción leve puede acarrear una sanción de hasta 40.000€.

• Incurrir en una infracción grave puede acarrear una sanción de entre 40.000€ hasta 300.000€.

• Incurrir en una infracción muy grave puede acarrear una sanción a partir de 300.000.

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

Las infracciones pueden clasificarse en leves, graves y muy graves, y las sanciones varían en función de la gravedad de la infracción.

Se consideran infracciones leves, por ejemplo, no proporcionar toda la información requerida al interesado en incumplimiento del principio de transparencia, no atender las solicitudes de ejercicios de derechos o no responder a la solicitud de supresión de los datos personales de una persona fallecida.

Tendrán la consideración de infracciones graves, por ejemplo, falta de consentimiento al tratamiento de datos personales de menores de edad, incumplimiento de medidas técnicas y organizativas necesarias o no disponer de actividades de registro de tratamiento.

Finalmente, se considerarán infracciones muy graves, por ejemplo, trata datos especialmente protegidos sin cumplir con los requisitos legales, ceder datos personales en supuestos no permitidos, realizar transferencias internacionales de datos sin contar con las garantías adecuadas, utilizar los datos personales para un finalidad incompatible con aquella para la que fueron recogidos originalmente, tratar datos personales relativos a condenas penales fuera de los supuestos permitidos, vulnerar los derechos de confidencialidad establecidos o incumplimiento de la obligación de bloqueo de los datos (previa a la eliminación de los mismos).

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

Sí, en España, la AEPD es el organismo encargado de supervisar y garantizar el cumplimiento de la normativa de protección de datos. La AEPD tiene la autoridad para investigar infracciones, imponer sanciones y facilitar orientación sobre la aplicación de la ley. Además, publica guías y recursos que ayudan a las organizaciones a entender sus obligaciones y a implementar prácticas adecuadas de protección de datos.

La AEPD también se encarga de promover la sensibilización sobre la importancia de la protección de datos, organizando campañas y formando alianzas con otras entidades para fomentar una cultura de privacidad en la sociedad.

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 comenzar con una auditoría de sus prácticas de tratamiento de datos, identificando flujos de datos y evaluando riesgos asociados. Este análisis inicial es crucial para entender qué datos se manejan, cómo se procesan y quién tiene acceso a ellos. A partir de esta auditoría, las organizaciones pueden desarrollar un plan de acción para abordar las necesidades y deficiencias de cada actividad o proyecto, a fin de adoptar las medidas necesarias para cumplir con la normativa.

Además, normalmente se establecen políticas y procedimientos internos que reflejen su compromiso con la protección de datos.

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

La normativa de protección de datos en España, a través del RGPD, se aplica a todas las organizaciones que procesan datos personales de individuos en la UE, independientemente de si están ubicadas dentro o fuera de la UE. Esto significa que empresas fuera de la UE que ofrezcan bienes o servicios a personas en la UE o que monitoricen su comportamiento están sujetas a las mismas obligaciones que las organizaciones dentro de la UE.

Esta aplicabilidad extraterritorial refleja el compromiso del RGPD de proteger los datos personales de los ciudadanos de la UE, asegurando que los estándares de protección se mantengan independientemente de dónde se realice el tratamiento de los datos. Esto también crea un marco de responsabilidad global para las empresas que operan en el entorno digital cada vez más interconectado de hoy.

BASHAM 1912

Autor:

Renata Buerón, Asociada, Privacidad, Protección de Datos y Tecnologías de Información.

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

México reconoce en su Constitución los derechos humanos, incluidos los derechos políticos y las libertades civiles. Además, México es parte de tratados internacionales de derechos humanos, como la Carta de Derechos Humanos de la ONU, la Convención Americana sobre Derechos Humanos, entre otros. Es importante mencionar que, en México, los derechos humanos incluidos en los tratados internacionales se encuentran al mismo nivel que la constitución, es decir, en la cúspide del sistema jurídico. La protección de datos personales está reconocida como un derecho humano autónomo por la Constitución mexicana (art. 16, párrafo II). Además, México se adhirió al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108) y su protocolo adicional relativo a las Autoridades de Control y los Flujos Transfronterizos de Datos, en vigor para México a partir del 1 de octubre de 2018. La Constitución mexicana establece garantías y recursos con respecto a los derechos humanos. El recurso más importante para la protección de los derechos humanos en México es el amparo.

En el sector público, la ley que rige la protección de datos personales en México es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017, así como las leyes locales que abordan el tema dentro de cada estado de la República Mexicana.

En el sector privado, la ley que rige la protección de datos personales en México es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), publicada en el Diario Oficial de la Federación el 5 de julio de 2010. La LFPDPPP regula el tratamiento legítimo de datos personales por parte de los responsables, así como el derecho de cada individuo a determinar si sus datos personales pueden ser tratados. Los principios generalmente aceptados de protección de datos también se incorporan a la LFPDPPP, es decir, los principios de legalidad, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

La legislación secundaria que complementa la LFPDPPP, incluye al Reglamento de la LFPDPPP, y los Lineamientos del Aviso de Privacidad, publicados en el Diario Oficial de la Federación el 21 de diciembre de 2011 y el 17 de enero de 2013, respectivamente.

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?

La LFPDPPP, y su reglamento (RLFPDPPP), determina diversas obligaciones con respecto al tratamiento de datos personales, y el artículo 48 del RLFPDPPP establece los medios para cumplir con el principio de responsabilidad, entre ellos desarrollar un programa de privacidad.

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

No se establece específicamente qué debe incluir ese programa, sin embargo del contenido de dicho artículo, los programas de privacidad por lo general deben: ser obligatorios y exigibles al interior de la organización del responsable; poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales; establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad; destinar recursos para la instrumentación de los programas y políticas de privacidad; instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos; revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran; establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales; disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento; establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la LFPDPPP y el RLFPDPPP, y establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.

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

El principal beneficio es minimizar riesgos en materia de seguridad de la información personal, lo que conlleva

a menores posibilidades de sufrir vulneraciones y, por tanto, inconformidades y demandas por parte de los afectados.

También se minimiza la posibilidad de ser sancionados por la autoridad de datos y por incumplir las leyes en la materia. Además, hay aspectos claves como la reputación y confianza por los consumidores/titulares de datos personales, junto a la protección de la marca.

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

N/A

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

Sí, el responsable del tratamiento debe nombrar a una persona o departamento específico de protección de datos. Esta persona o departamento será el encargado de promover la protección de los datos personales dentro de la organización, de verificar el cumplimiento de la ley y el reglamento, de responder a las solicitudes de los interesados cuando ejerzan sus derechos, entre otras obligaciones.

Asimismo, se debe contar con el delegado en todos los casos que una persona física o moral trate datos personales, no hay un criterio que delimite.

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

Las infracciones a la LFPDPPP o a su reglamento pueden ser sancionadas de la siguiente manera:

• Con una advertencia que instruya al responsable del tratamiento de los datos para que lleve a cabo las acciones solicitadas por el titular (en relación con el ejercicio de sus derechos)

• Con una multa que oscila entre las 100 y las 320.000 unidades denominadas UMA. Actualmente, el valor de una unidad llamada UMA es de 108.57 pesos mexicanos (aprox. USD 5.4). Por lo tanto, las multas oscilan entre aproximadamente USD 550 y USD 1' 500,000. Las multas pueden duplicarse si se trata de datos personales sensibles.

• Para las infracciones recurrentes, pueden imponerse multas adicionales y se calcularán sobre la misma base que en el párrafo anterior.

• Cuando se trata de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

Además, se puede imponer una pena de prisión a cualquier persona que infrinja ilegalmente las medidas de seguridad o facilite una violación de una base de datos bajo su custodia o que se beneficie ilegalmente del tratamiento de datos personales, aprovechando engañosamente cualquier error del titular.

Sanción	Conducta
Apercibimiento	No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada.
100 a 160,000 veces el valor de la UMA $108.57 ($11,000 a $17,500)	• Actuar con negligencia o dolo en la tramitación de solicitudes de acceso, rectificación, cancelación u oposición de datos personales. • Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable. • Dar tratamiento a los datos personales en contravención a los principios establecidos en la LFPDPPP. • Omitir en el aviso de privacidad o todos los elementos a que se refiere el artículo 16 de esta ley. • Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de estos que legalmente procedan cuando resulten afectados los derechos de los titulares. • No cumplir con el apercibimiento de la autoridad.
	• Incumplir el deber de confidencialidad. • Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin

200 a 320,000 veces el valor de la UMA ($22,000 a $35,000,000.00)	obtener nuevamente el consentimiento del titular. • Transferir datos a terceros sin comunicar a estos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos. • Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable. • Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos previstos en la LFPDPPP. • Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que este sea exigible. • Obstruir los actos de verificación de la autoridad. • Recabar datos en forma engañosa y fraudulenta. • Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el instituto o los titulares. • Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos ARCO. • Crear bases de datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

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

En caso de que persistan las infracciones, se impondrá una multa adicional que irá de 100 a 320,000 veces el valor de la UMA; y tratándose de faltas cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los importes establecidos.

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

La autoridad encargada de la observancia de la protección de datos es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). El INAI es un organismo constitucional y autónomo responsable de promover y difundir el derecho al acceso a la información pública, así como el derecho a la protección de datos dentro de organismos gubernamentales y partes privadas. Este organismo se compromete a trabajar con otras autoridades federales, estatales y municipales para promover la protección de datos en diferentes industrias y sectores, como los sectores financieros, educativo y de salud.

La Autoridad Mexicana de Protección de Datos (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, INAI), será disuelta tras una reciente reforma constitucional, aprobada el pasado mes de diciembre de 2024.

El INAI tiene entre sus funciones velar por la transparencia de las acciones que realizan las entidades del sector público y salvaguardar el derecho humano a la protección de datos personales en posesión tanto de entidades del sector público como de particulares.

El Gobierno mexicano determinará qué entidad de la Administración Pública Federal asumirá la responsabilidad de velar por la protección de los datos personales en posesión de particulares.

Tras la publicación del proyecto de ley en el Diario Oficial de la Federación (20 de diciembre de 2024), el Congreso mexicano tiene 90 días (marzo de 2025) para reformar la legislación mexicana de protección de datos, la Ley Orgánica de la Administración Pública Federal (LOAPF) y las leyes secundarias correspondientes para designar a la nueva autoridad de protección de datos encargada de gestionar los procedimientos relacionados con la protección de derechos, las verificaciones y la imposición de sanciones. Aún no se ha determinado la dependencia o ministerio específico encargado de salvaguardar los datos personales en posesión de entidades privadas.

Todas las acciones realizadas por el INAI con anterioridad a la promulgación de la legislación secundaria mantendrán plena eficacia jurídica. La disolución de los entes autónomos no se producirá hasta que dicha legislación secundaria entre en vigor.

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?

Se lleva a cabo una auditoria en la materia.

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

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su reglamento, son de aplicación extraterritorial en ciertos casos.

Antes de revisar los supuestos de aplicación extraterritorial, es importante conocer algunos conceptos clave que facilitan su identificación:

• **Responsable:** Persona física o moral del sector privado que decide sobre el tratamiento de datos personales.

• **Encargado:** Persona física o moral que trata datos personales en nombre y por cuenta del responsable.

• **Tratamiento:** Cualquier acción relacionada con datos personales, incluyendo su obtención, uso, divulgación o almacenamiento, ya sea por medios físicos o electrónicos. El uso comprende el acceso, manejo, aprovechamiento, transferencia o disposición de los datos personales.

• **Establecimiento:** Para personas físicas, se refiere al lugar donde se desarrollan sus actividades económicas o su domicilio. Para personas morales, es el lugar donde se encuentra su administración principal en México o cualquier instalación estable que permita el ejercicio real y efectivo de su actividad.

La LFPDPPP y RLFPDPPP resultan aplicables extraterritorialmente en los siguientes escenarios:

1. El responsable no está establecido en México, pero la legislación mexicana le resulta aplicable debido a la celebración de un contrato o en términos del derecho internacional.

2. El responsable no está establecido en México, pero utiliza medios situados en territorio mexicano, salvo que dichos medios se utilicen únicamente con fines de tránsito sin implicar tratamiento de datos.

Consideraciones sobre la aplicación extraterritorial

Es decir, la LFPDPPP y su reglamento serán aplicables incluso si el tratamiento central de datos no se lleva a cabo en México, pero cuando menos se recolectan en México. Por ello, si bien ni el responsable, ni el encargado realizan tratamiento de datos en territorio mexicano, la legislación mexicana resultaría aplicable en caso de que cuenten con medios localizados en nuestro país.

En la práctica es complejo que la autoridad de datos inicie y cumplimente una investigación por el incumplimiento de la LFPDPPP y su reglamento, por parte de una empresa o particular que no tenga representación en México.

BECCAR VARELA

Autores:

Florencia Rosatti, Socia, TMT, Privacidad y Protección de Datos Personales.

Andrea Sanchez Vicentini, Abogada Intermediate, IP, TMT y Privacidad.

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

El derecho a la privacidad está reconocido en el artículo 19 de la Constitución Argentina y en diversos Tratados Internacionales de Derechos Humanos suscritos y aprobados por Argentina, como el artículo 12 de la Declaración Universal de Derechos Humanos, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y el artículo 11 de la Convención Americana sobre Derechos Humanos. Estos tratados de derechos humanos tienen jerarquía constitucional conforme al artículo 75, inciso 22, de la Constitución Nacional.

Tras la reforma de 1994, la Constitución Nacional incorporó la acción de Hábeas Data en el artículo 43, tercer párrafo, y reconoció a las personas el derecho a acceder a sus datos personales, así como a solicitar su supresión, rectificación, confidencialidad o actualización.

La Ley de Protección de Datos Personales Nro. 25.326 (la "LPDP") es la norma marco general sobre la privacidad de los datos personales en Argentina. Establece las reglas para el tratamiento de la información, incluyendo la recopilación y el uso de datos personales, y está regulada por el Decreto Nro. 1558/2001 (el "DPDP"). Este marco se ve complementado por disposiciones inicialmente emitidas por la ex Dirección Nacional de Protección de Datos Personales (la "DNPDP") y, posteriormente, por resoluciones de la Agencia de Acceso a la Información Pública (la "AAIP"), la actual autoridad de protección de datos que reemplazó a la Dirección.

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?

En Argentina no existe regulación que establezca la obligación de tener un programa de prevención de infracciones o cumplimiento en materia de protección de datos personales.

Sin embargo, se han implementado varias medidas de prevención de infracciones y/o protección de los datos personales:

Registro de Responsables y de Bases de Datos: Las empresas que gestionan datos personales están obligadas a inscribirse e inscribir sus bases en el Registro de la AAIP. Esto busca garantizar transparencia en el tratamiento de los datos y asegurar el respeto de los derechos de los titulares.

Consultas ante la AAIP: Las personas humanas y las organizaciones pueden acceder a asesoramiento y consultas con la AAIP para resolver dudas sobre el cumplimiento de la ley y mejorar sus prácticas en protección de datos.

Facultades de la AAIP: La AAIP es el órgano encargado de la supervisión y el cumplimiento de la LPDP. La AAIP realiza actividades de control y fiscalización, investiga denuncias sobre infracciones, puede llevar a cabo auditorías para verificar que las empresas y organizaciones cumplan con la normativa de protección de datos personales. Si identifica infracciones, puede imponer sanciones que van desde advertencias hasta multas económicas. La AAIP también tiene una función educativa y promueve la conciencia sobre la protección de datos.

Registro de Integridad y Transparencia para Empresas y Entidades: En 2023 la AAIP creó el módulo sobre protección de datos personales (el "Módulo sobre PDP") dentro del Registro de Integridad para Empresas y Entidades ("RITE")[1] con el objetivo de que las organizaciones evalúen su nivel de cumplimiento con la normativa vigente en materia de protección de datos personales[2]. El RITE es una plataforma voluntaria, gratuita y federal impulsada por la Oficina Anticorrupción, un organismo desconcentrado de la Presidencia de la Nación, con el apoyo del Banco Interamericano de Desarrollo ("BID") y el Programa de las Naciones Unidas para el Desarrollo ("PNUD"), cuyo objetivo es contribuir al desarrollo y mejora de los programas de integridad, el intercambio de buenas prácticas y la promoción de ambientes transparentes.

El Módulo sobre PDP incluye una serie de preguntas organizadas en diferentes ejes temáticos. Estas preguntas analizan aspectos como el manejo del ciclo de vida del dato personal, la gestión de riesgos en su tratamiento y la existencia de un área dedicada a la

[1] https://shorturl.at/fzGLN
[2] Módulo sobre Protección de Datos Personales del RITE | Argentina.gob.ar; Nuevo módulo de RITE: Protección de Datos Personales | Argentina.gob.ar

protección de datos dentro de la organización. También se evalúa el nivel de compromiso de la alta dirección de la compañía, la implementación de medidas de responsabilidad proactivas y demostrables, así como la capacitación ofrecida a colaboradores, prestadores de servicios y clientes. Además, indaga sobre los canales de comunicación disponibles para gestionar consultas y reclamos relacionados con la privacidad. En algunos casos, solicita documentación de respaldo para evidenciar las prácticas implementadas.

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

Dado que en Argentina no es obligatorio tener un programa de cumplimiento en protección de datos personales, no existen requisitos específicos establecidos de manera oficial. Sin embargo, de existir, los programas de cumplimiento deben ajustarse a la LPDP y su normativa complementaria. También pueden seguir los lineamientos del Módulo sobre PDP del RITE.

Por lo tanto, deberían contemplarse los siguientes aspectos esenciales:

Bases de datos gestionadas: Identificación de todas las bases de datos que la empresa posee, junto con la especificación del área responsable de cada una de ellas.

Principios de la LPDP: Asegurar que se cumplan los principios establecidos por la LPDP en cuanto a la recolección, uso y almacenamiento de datos personales, los cuales incluyen la proporcionalidad y limitación de los fines, la transparencia, la exactitud de los datos, la seguridad de los datos y la confidencialidad.

Bases legales y derechos ejercidos: Llevar un registro detallado de las bases legales que se utilizan para cada procesamiento, y de los consentimientos otorgados por los titulares de los datos, así como de los derechos ejercidos por ellos y las acciones tomadas por la organización en respuesta.

Procedimientos internos: Definir y documentar los procedimientos internos de la empresa para la gestión de los derechos de los titulares de los datos, como el acceso, rectificación y supresión.

Contratos con prestadores de servicios: Celebrar acuerdos con los prestadores de servicios en los que se establezca que el encargado del tratamiento sólo tratará los datos personales siguiendo las instrucciones del responsable del tratamiento. Además, el acuerdo debe asegurar que el encargado cumpla con las obligaciones de seguridad y confidencialidad establecidas en la LPDP, que se abstenga de ceder los datos personales a terceros, incluso para su conservación, y que proceda a la destrucción de los datos una vez finalizada la prestación contractual, salvo que el responsable autorice expresamente su almacenamiento por un período adicional.

Transferencia internacional de datos: Documentar los países a los que se realice transferencia internacional, y contar con mecanismos para validar que las transferencias a países sin un nivel adecuado de protección se realicen bajo condiciones que aseguren la protección de los derechos de los titulares, como cláusulas contractuales modelo, normas corporativas vinculantes u otras medidas previstas por la LPDP, como el consentimiento.

Medidas de seguridad: Implementar y detallar las medidas técnicas y organizativas de seguridad necesarias para proteger los datos personales de conformidad con lo requerido por la LPDP, que sean de rigor equivalente o mayor al establecido en la Resolución AAIP 47/2018.

Gestión de incidentes de seguridad: Establecer un protocolo claro de respuesta ante incidentes de seguridad, que incluya preparar un informe interno del incidente, tomar medidas preventivas, establecer planes de acción correctivos en caso de vulneraciones y protocolos de seguridad para mitigar el impacto de los incidentes. Además, definir un procedimiento interno que permita evaluar en qué casos es necesario notificar a la AAIP y a los titulares de los datos.

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 en:

Reducción de riesgos legales: Las organizaciones con un programa de cumplimiento tienen un mayor control de sus flujos de datos personales y están mejor protegidas frente a sanciones o conflictos legales.

Gestión de riesgos: Ayuda a identificar y minimizar los riesgos relacionados con la seguridad de la información, reduciendo la probabilidad de incidentes de seguridad.

Adaptación a regulaciones internacionales: Cumplir con la LPDP facilita la adaptación a regulaciones internacionales, como el Reglamento General de

Protección de Datos ("RGPD"), lo cual es crucial para organizaciones que operan a nivel global.

Mejora de la reputación: Las organizaciones que demuestran un compromiso con la protección de los datos personales son percibidas como más responsables y confiables, lo que puede mejorar su imagen en el mercado.

Ventaja competitiva: Las organizaciones que cumplen con altos estándares de protección de datos pueden diferenciarse de sus competidores, atrayendo a clientes que valoran la privacidad y la seguridad.

Optimización operativa: La implementación de políticas y procedimientos claros para el manejo de datos personales contribuye a mejorar la eficiencia operativa y a evitar duplicación de esfuerzos.

Preparación para cambios regulatorios: Permite una transición más sencilla hacia futuras regulaciones que puedan reemplazar la LPDP, ya que las regulaciones emergentes tienden a exigir mayores niveles de "accountability" o responsabilidad demostrada en el tratamiento de datos personales.

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

En Argentina, no existen procesos de certificación formales para programas de cumplimiento en protección de datos personales.

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

La LPDP no exige la designación de un delegado de protección de datos ("DPO" por su sigla en inglés).

Existe actualmente un proyecto de ley que busca reemplazar la LPDP, que fue redactado por la AAIP y que aún está pendiente en el Congreso (el "Proyecto de Ley"), que sí incluye tal requisito. Sin embargo, el Proyecto de Ley perderá su estatus parlamentario el 28 de febrero del 2025 debido a que no ha sido tratado en el Congreso.

Adicionalmente, la Guía de Buenas Prácticas en Privacidad para el Desarrollo de Software Aplicativo emitida por la AAIP bajo la Resolución Nro. 18/2015 fomenta que los responsables de datos designen un DPO, mencionando que sus responsabilidades incluyen: (i) asegurar que el tratamiento de datos y el software cumplan con la normativa de protección de datos; (ii) revisar y mantener actualizada la política de privacidad del responsable de los datos; (iii) responder preguntas relacionadas con la política de privacidad, los derechos de los interesados y otros temas relacionados.

Asimismo, las Directrices para Auditorías emitidas por la AAIP bajo la Resolución Nro. 332/2020, que tienen como objetivo evaluar el grado de cumplimiento con la normativa de protección de datos, consideran relevante que el responsable de los datos haya designado un DPO dentro de su organización. En tal sentido, el Anexo II de dicha resolución establece como lineamiento a tener en cuenta para la fiscalización de la seguridad y confidencialidad si en la organización se encuentra designado un DPO.

Además, la Guía sobre Evaluaciones de Impacto en la Protección de Datos Personales aprobada por las autoridades de protección de datos de Argentina y Uruguay ("Guía de EIDP") hace referencia a la posible designación de un DPO, definiéndolo como una persona designada o contratada por el responsable de los datos, con experiencia y conocimientos comprobados en el área, para asesorar en la formulación, diseño e implementación de políticas de protección de datos personales.

Tipo de Infracción	Sanciones
Leves	Hasta dos apercibimientos y/o una multa de $1.000 a $80.000.
Graves	Hasta cuatro apercibimientos, suspensión de uno a treinta días y/o una multa de $80.001 a $90.000.
Muy Graves	Hasta seis apercibimientos, suspensión de treinta y uno a trescientos sesenta y cinco días, clausura o cancelación del archivo, registro o banco de datos y/o una multa de $90.001 a $100.000.

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

Sí, existen sanciones asociadas al incumplimiento de

la normativa sobre protección de datos personales en Argentina, de acuerdo con el artículo 31 de la LPDP y la Resolución Nro. 126/2024 de la AAIP. Las sanciones se clasifican en tres categorías: infracciones leves, graves y muy graves.

Además, la aplicación y cuantía de las sanciones se graduará atendiendo a varios factores, como la naturaleza y dimensión del daño, el beneficio económico obtenido, la reincidencia, la resistencia a la acción investigadora, entre otros.

Adicionalmente, las personas afectadas por el tratamiento ilícito de datos pueden presentar una demanda civil específica denominada "habeas data" (artículos 33 a 43 de la LPDP).

Además de esta acción de habeas data, el titular de los datos puede presentar una demanda general por daños. Sin embargo, al igual que en cualquier reclamo por daños, el éxito de la demanda está sujeto a cuatro requisitos básicos que deben ser probados por quien la presenta: (i) ilegalidad de la acción que causa el daño; (ii) daño real y efectivo; (iii) relación de causa y efecto entre la acción y el daño; o (iv) negligencia, conducta ilícita o responsabilidad objetiva.

Por otro lado, el artículo 117-bis (2) del Código Penal Argentino (Ley N° 11.179) establece que cualquier persona que a sabiendas proporcione a un tercero información falsa contenida en un archivo de datos personales podrá ser condenada a una pena de prisión de seis meses a tres años.

El artículo 117-bis (3) del Código Penal dispone que la pena puede incrementarse en una mitad de la pena mínima y una mitad de la pena máxima si como consecuencia de la conducta se produce un perjuicio a alguna persona.

Por otro lado, el artículo 156 del Código Penal establece que se podrá imponer una multa de entre ARS 1,500 a ARS 90,000 e inhabilitación especial de entre seis meses a tres años a los empleados que accedan a información confidencial, cuya divulgación pueda causar perjuicios, y la divulguen sin autorización y sin causa legal o justificada.

Finalmente, el artículo 157-bis del Código Penal establece que se podrá imponer una pena de prisión de uno a dos años a quien: (i) acceda de manera ilegítima y a sabiendas o violando los sistemas de confidencialidad y seguridad de los datos a cualquier base de datos personales; (ii) proporcione o divulgue ilegítimamente a terceros información registrada en una base de datos personal que deba ser mantenida confidencial según la ley; o (iii) inserte ilegítimamente datos en una base de datos, o lo permita.

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

La normativa en protección de datos personales en Argentina sanciona diversas conductas, clasificadas en infracciones leves, graves y muy graves. A continuación, se detallan las tipificaciones de cada tipo de infracción en formato cuadro:

Tipo de Infracción	Sanciones
Leves	• No inscribirse en el Registro Nacional de Bases de Datos. • No informar modificaciones, actualizaciones o bajas en tiempo y forma. • No proporcionar información solicitada por la DNPDP. • No acompañar documentación requerida en procedimientos de inspección. • No respetar el principio de gratuidad. • No informar medidas de seguridad y confidencialidad implementadas. • No acreditar el cumplimiento de requisitos para la cesión de datos personales.
Graves	• No inscribir la base de datos cuando haya sido requerido. • Declarar datos falsos o inexactos al registrarse. • Tratar datos sin una base de legitimación adecuada. • Recoger datos sin proporcionar el derecho de información. • No atender solicitudes de acceso, rectificación o supresión de datos. • Tratar datos que no sean ciertos, adecuados, pertinentes y no excesivos.

Graves	• Incumplir el deber de confidencialidad y seguridad. • Mantener bases de datos sin las debidas condiciones de seguridad. • Mantener datos más tiempo del legalmente establecido. • Tratar datos personales patrimoniales que excedan la información relativa a la solvencia económica. • No retirar o bloquear datos de publicidad cuando el titular lo solicite.
Muy Graves	• Omitir denunciar el domicilio legal y datos identificativos del responsable en Internet. • Conformar un archivo de datos con fines contrarios a las leyes o la moral pública. • Recoger datos mediante ardid, engaño o fraude. • Tratar datos de forma ilegítima o con menosprecio de los principios y garantías legales. • Impedir u obstaculizar el ejercicio de los derechos reconocidos en la LPDP. • Mantener datos inexactos o no efectuar las rectificaciones necesarias. • Transferir datos a países u organismos que no proporcionen niveles de protección adecuados. • Ceder datos ilegítimamente. • Recolectar y tratar datos sensibles sin consentimiento o sin razones legales. • Formar archivos que revelen datos sensibles sin autorización. • Incumplir el deber de confidencialidad y seguridad respecto a datos sensibles. • No cesar en el uso y tratamiento ilegítimo de datos cuando sea requerido. • Realizar maniobras para sustraerse o impedir la actividad de contralor de la DNPDP.

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

La AAIP es el órgano encargado de la supervisión y el cumplimiento de la LPDP. La AAIP realiza actividades de control y fiscalización, investiga denuncias sobre infracciones y emite sanciones en caso de incumplimiento de las normativas de protección de datos. La AAIP también tiene una función educativa y promueve la conciencia sobre la 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?

Las organizaciones suelen realizar un diagnóstico interno para conocer su situación actual en relación con el tratamiento de datos personales. Este diagnóstico les permite identificar las bases de datos que poseen, los procesos asociados al manejo de datos y cualquier posible incumplimiento de la normativa vigente. Después del mismo, se procede a enmendar o mejorar las deficiencias que se hayan identificado en el proceso, ajustando los procedimientos internos y las prácticas para cumplir con los requisitos establecidos por la LPDP.

Otro paso crucial es capacitar a los colaboradores sobre la LPDP, para que comprendan sus responsabilidades en cuanto al manejo y protección de los datos personales.

Aunque realizar una EIDP no es obligatorio de forma inicial, en caso de que el diagnóstico inicial revele que la organización realiza un tratamiento de datos que implique un alto riesgo para los derechos de los titulares (como el tratamiento masivo de datos sensibles, el procesamiento a gran escala de datos personales, la toma de decisiones automatizadas o el análisis de perfiles que afecten significativamente a los individuos), entonces sería recomendable llevar a cabo una evaluación de impacto para garantizar que se mitigan los riesgos asociados.

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

La LPDP no contiene una disposición explícita sobre su aplicación extraterritorial. El artículo 44 de LPDP establece que sus disposiciones se aplican en todo el territorio nacional, y la jurisdicción federal se aplica a las bases de datos interconectadas en redes de alcance interjurisdiccional, nacional o internacional. Por lo tanto,

la LPDP se aplica cuando los datos personales son tratados dentro del territorio argentino. Si el responsable del tratamiento no tiene presencia alguna en Argentina, podría interpretarse que queda fuera del alcance de las autoridades argentinas.

No obstante, en fecha 13 de abril del 2020, mediante Resolución Nro. 69/2020[3], la AAIP impuso una multa a Google LLC. La AAIP consideró en dicho caso que, a pesar de que Google LLC realizaba todo su procesamiento en el exterior, por procesar datos personales de argentinos por medio de bases de datos interconectadas en redes de alcance internacional, tal procesamiento quedaba sujeto a la aplicación de la LPDP.

Además, el 29 de noviembre de 2022, la AAIP introdujo un formulario web para el registro de responsables de datos que no residen en Argentina.

Por otra parte, el Proyecto de Ley incluye una disposición expresa sobre extraterritorialidad, al ampliar el ámbito de aplicación territorial en su artículo 4, estableciendo que se aplicará a:

(i) Responsables o encargados del tratamiento establecidos en Argentina, incluso cuando el tratamiento de datos tenga lugar fuera del país.

(ii) Responsables o encargados del tratamiento que no estén establecidos en Argentina, siempre que

a. Lleven a cabo el tratamiento de datos en el territorio argentino de personas que se encuentren en Argentina.

b. Realicen actividades de tratamiento relacionadas con la oferta de bienes o servicios a personas que se encuentren en Argentina, o con la elaboración de perfiles, monitoreo o control de los actos, comportamientos o intereses de dichas personas.

c. Estén establecidos en un lugar donde se aplique la legislación argentina en virtud del derecho internacional o contractual.

A la luz de lo anterior, el criterio de la AAIP es que la LPDP aplica en la medida en que se procesen datos de titulares de datos argentinos a través de bases de datos interconectadas en redes de alcance internacional, o cuando el tratamiento de datos se vincule con Argentina o produzca efectos en la República Argentina (interpretando el artículo 36.b de la LPDP). Este criterio ha sido respaldado por la justicia argentina, que ha reconocido que una filial local, constituida bajo la ley argentina y vinculada comercialmente con una entidad extranjera que procesa datos personales de argentinos, no puede eludir la aplicación de la normativa nacional en materia de protección de datos[4].

[3] rs-2020-25457045-apn-aaip_google.pdf
[4] P. A. E. c. Facebook Argentina SRL s/medida autosatisfactiva", CFed. Mendoza, sala B, 24/05/2019, AR/JUR/12577/2019.

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?

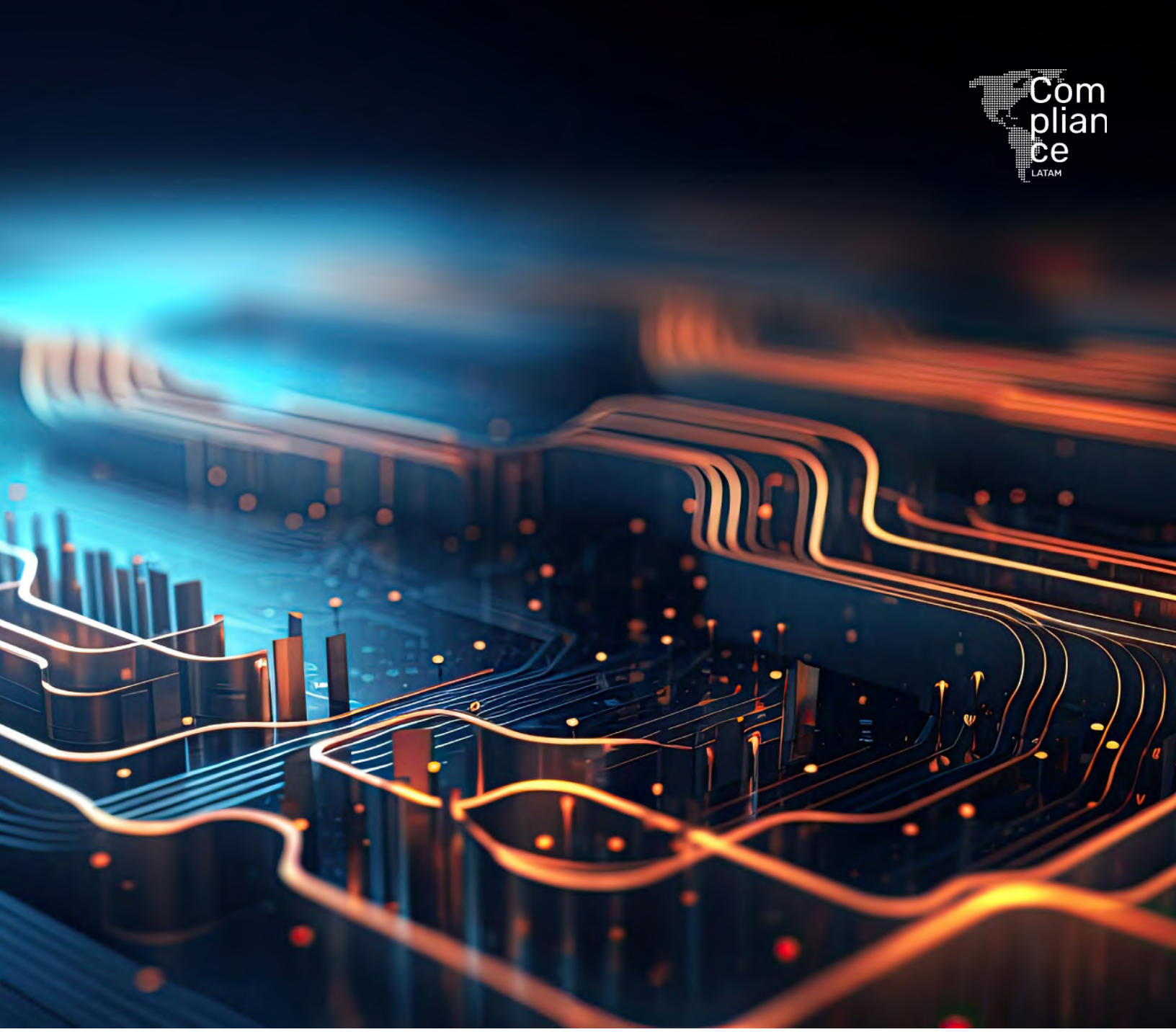
Sí, la Agencia de Protección de datos de los Habitantes (PRODHAB).

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.



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.

C|P|B
ABOGADOS

Autores:

Victor Bosleman, Abogado, Competencia, Protección de Datos Personales y Propiedad Intelectual.

Ayrton Huamán Nuñez, Abogado, Competencia, Protección de Datos Personales y Propiedad Intelectual.

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

El marco legal actual en materia de datos personales está conformado, principalmente, por las siguientes normas: (i) la Ley N° 29733 – Ley de protección de datos personales; (ii) su reglamento, aprobado por el Decreto Supremo N° 003-2013-JUS; y (iii) la Directiva N° 001-2020-JUS/DGTAIPD – Tratamiento de datos personales mediante videovigilancia, entre otras que pueden ser aplicables a sectores particulares.

Es importante considerar que el día 30 de noviembre de 2024, se publicó el nuevo Reglamento de Protección de Datos Personales, aprobado por el Decreto Supremo N° 016-2024-JUS, el cual entrará en vigencia a partir del 30 de marzo de 2025.

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?

La normativa actual no contempla programas obligatorios de prevención de infracciones en protección de datos personales. Sin embargo, una de las novedades del nuevo Reglamento de Protección de Datos Personales es la incorporación de los Códigos de Conducta como una herramienta opcional para fomentar el cumplimiento normativo.

Estos Códigos de Conducta son iniciativas voluntarias que las empresas o grupos empresariales pueden implementar para demostrar su compromiso con las obligaciones legales en esta materia. Su adopción no es obligatoria en ningún caso, pero, si se aplican antes del inicio de un procedimiento sancionador, pueden ser considerados como un factor atenuante de responsabilidad. Cabe señalar que la protección de datos personales resulta relevante para todas las empresas y por ello, recomendamos que se incorpore un programa de cumplimiento específico sobre esta materia dentro del sistema de compliance.

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

En el Perú, los Códigos de Conducta pueden ser adoptados por organizaciones representativas de un sector o por empresas y grupos empresariales. Mientras que los primeros pueden abarcar todos o algunos tratamientos de datos personales realizados por el sector, los Códigos de Conducta empresariales deben cubrir la totalidad de los tratamientos llevados a cabo por dicha empresa o grupo.

En ambos casos, el contenido mínimo de un Código de Conducta incluye:

• La definición de manera clara de las actividades, tratamientos y datos personales que regula el código.

• Disposiciones para garantizar el cumplimiento de los principios de datos personales aplicables al tratamiento o tratamientos indicados en el código.

• Procedimientos que permitan ejercer derechos ARCO.

• Identificación transferencias nacionales e internacionales que se prevean realizar y las garantías aplicables.

• Acciones para promover la protección de datos entre quienes los gestionan.

• Mecanismos para asegurar la confidencialidad de los datos personales por parte de quienes los traten.

• Mecanismos de monitoreo para garantizar el cumplimiento del código de conducta.

• Formatos de cláusulas para obtener el consentimiento de los titulares de datos personales al tratamiento o transferencia de sus datos personales.

• Formatos de cláusulas para informar a los titulares sobre el tratamiento de sus datos personales.

• Formatos para que los titulares puedan ejercer sus derechos ARCO.

• Formatos de cláusulas para la contratación del encargado del tratamiento, en caso se realice tratamiento de datos personales por encargo.

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 en protección de datos personales trae beneficios tanto reputacionales como legales. A nivel reputacional, la adopción de un Código de Conducta genera confianza entre trabajadores, clientes y socios, fortaleciendo la percepción de que la organización trata los datos personales de manera responsable y segura. A nivel legal, según el nuevo Reglamento de Protección de Datos Personales, contar

con un Código de Conducta puede ser considerado como un atenuante en un procedimiento sancionador, siempre que este se implemente antes de su inicio, lo que permite reducir posibles sanciones administrativas.

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

A la fecha, no se han establecido procesos de certificación de los Códigos de Conducta en Perú.

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

Sí, en ciertos casos. De acuerdo con el nuevo Reglamento de Protección de Datos Personales, las empresas que realicen tratamiento de grandes volúmenes de datos personales que pueda afectar a un gran número de personas, o que su giro de negocio comprenda el tratamiento de datos sensibles, tendrán la obligación de designar un oficial de datos personales. Esta obligación específica entrará en vigencia de manera gradual entre noviembre del año 2025 y noviembre del año 2028, dependiendo del nivel de ingresos anuales de la empresa. Para el caso de grupos económicos, se podrá designar un único oficial por grupo.

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

Sí. Las infracciones a la normativa sobre protección de datos personales se sancionan con multas que pueden ascender, como máximo, al equivalente a US$ 145,000 (ciento cuarenta y cinco mil dólares americanos) aproximadamente, por infracción. La graduación de la multa dependerá si la infracción se encuentra clasificada normativamente como leve, grave o muy grave.

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

Algunos ejemplos de infracciones leves son: El realizar tratamiento de datos personales que no sean necesarios ni pertinentes con la finalidad para los que son obtenidos, y atender fuera de plazo el ejercicio de los derechos del titular de los datos personales. Por el lado de las infracciones graves, tenemos como ejemplos: El realizar tratamiento de datos personales sin mediar consentimiento del titular, y no comunicar a la autoridad la ocurrencia de un incidente de seguridad. Por último, el realizar tratamiento de datos sensibles sin adoptar las medidas de seguridad correspondiente y generando con ello un perjuicio al titular es un ejemplo de una infracción considerada como muy grave.

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 Personales, órgano perteneciente al Ministerio de Justicia y Derechos Humanos, es la entidad encargada de fiscalizar el cumplimiento de la normativa de protección de datos personales en el Perú y de sancionar su eventual incumplimiento. Además, se encarga de dictar directivas que complementan y/o desarrollan la normativa de protección de datos personales, y de emitir opiniones consultivas que dan respuesta a consultas ciudadanas a partir de su interpretación de las normas.

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?

Recomendamos, como primer paso, obtener asesoría jurídica especializada para conocer las obligaciones sobre protección de datos personales aplicables a la organización considerando las particularidades del tratamiento y flujo de datos que realice, y sobre todo los riesgos de incumplimiento a los que podría estar expuesta. Una vez se cuenta con dicho diagnóstico, se puede proceder a implementar un sistema de protección de datos personales a la medida de la organización que tenga la finalidad de cubrir cada punto de riesgo detectado y cumplir con la normativa. En particular, este sistema también comprenderá la implementación de los Códigos de Conducta a los que nos hemos referido anteriormente.

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.

FERRERE

Autores:

Alberto Rivera, Asociado Senior Bolivia, Derecho Corporativo, Propiedad Intelectual, Derecho Administrativo y Regulatorio.

Jorge Plaza, Asociado Senior Bolivia, Derecho Corporativo, Fusiones y Adquisiones, Compliance, TMT, Privacidad y Tecnologías de la información.

Martín Pesce, Socio Uruguay, Protección de Datos, Nuevas Tecnologías.

María Canziani, Asociada Senior Uruguay, Derecho Administrativo y Corporativo.

Montserrat Puente, Asociada Senior Paraguay, Propiedad Intelectual y Asuntos Regulatorios.

Galo Molinas, Asociado Paraguay, Propiedad Intelectual y Asuntos Regulatorios.

Bolivia

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

Bolivia es uno de los pocos países de la región que no cuenta con una ley de protección de datos personales de carácter general. En su lugar, la protección de datos personales naturales es de carácter constitucional, complementada por regulación concreta para determinadas áreas reguladas.

A nivel constitucional, la Constitución Política del Estado Plurinacional de Bolivia reconoce la figura de la Acción de Protección de Privacidad mediante la cual toda persona individual que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de datos registrados por cualquier medio físico, electrónico, magnético o informático, o que afecten a su derecho fundamental a la intimidad y privacidad o a su propia imagen, podrá reclamar la restitución de sus derechos al juez o tribunal competente.

Por otra parte, la Ley General de Telecomunicaciones (Ley 164) y el Decreto Supremo No. 1793 que aprueba el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación (D.S. 1793) establecen, de manera escueta, normas generales sobre los derechos de usuarios de servicios de telecomunicaciones en materia de privacidad. Estos destacan la obligación de contar con el consentimiento previo, expreso e informado del titular de los datos, antes de su recopilación y tratamiento; y la obligatoriedad de implementar medidas de seguridad conforme con el estado de la tecnología y apropiados para la naturaleza de los datos almacenados.

Finalmente, la Ley de Servicios Financieros (Ley 393) también establece obligaciones específicas para la privacidad de usuarios de entidades financieras, como la regulación del secreto bancario.

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. El marco regulatorio boliviano, tanto en materia de protección de datos como en materia de compliance, no contempla la obligación de contar con programas de prevención de infracciones para el sector público o privado. No obstante, como indicamos en la respuesta anterior, el D.S. 1793 sí establece la necesidad de que los responsables del tratamiento de datos personales hayan establecido previamente las medidas de seguridad necesarias.

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

No aplicable, conforme a lo explicado en la respuesta anterior.

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

Aunque el sector privado no tiene la obligación de implementar programas de cumplimiento que aseguren la protección de datos personales tratados por dicha entidad, implementar voluntariamente este tipo de programas puede generar los siguientes beneficios:

- Generación de confianza entre los clientes de la entidad, proyectando una imagen de profesionalismo e incrementando su reputación dentro del mercado.

- Reducción de vulnerabilidades, anticipando respuestas y soluciones ante posibles amenazas de ciberseguridad.

- Mejoramiento de los procedimientos internos en el tratamiento de datos, evitando que personal de la entidad pueda comprometerla al vulnerar el derecho de privacidad de terceros durante el cumplimiento de sus funciones.

- Facilitación para justificar la implementación previa de medidas de seguridad adecuadas y procedimientos de mitigación eficaces, en caso de que se presenten incidentes de seguridad. Esto para disminuir el riesgo de responsabilidad y sanciones frente a estos sucesos.

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

No, debido a que la implementación de dichos programas de cumplimiento no es obligatoria en Bolivia.

No obstante, el Instituto Boliviano de Normalización y Calidad (IBNORCA), organización sin fines de lucro creada por el Decreto Supremo No. 23489 cuya finalidad es la realización de actividades de normalización técnica y certificación de calidad, sí ha establecido los lineamientos para la implementación de la norma ISO/IEC 27001 en empresas bolivianas. IBNORCA otorga

estas certificaciones, previo cumplimiento del proceso respectivo, a las entidades públicas o privadas que lo requieran.

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

No. El marco normativo boliviano en materia de protección de datos no contempla la figura del delegado de protección de datos personales.

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

Debido a que no existe una ley de protección de datos en Bolivia, tampoco existen sanciones específicas por el incumplimiento de obligaciones en cuanto al recojo y tratamiento de datos personales.

No obstante, dado que el Código Civil boliviano reconoce al derecho a la intimidad (entendido como el derecho a que nadie perturbe, ni divulgue la vida íntima de una persona) un derecho civil, quien se vea afectado en su derecho a la intimidad podría solicitar el resarcimiento por el hecho ilícito mediante un proceso ordinario en vía civil.

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

Dado que no existe una ley de protección de datos en Bolivia, tampoco existen sanciones por la realización de conductas que puedan afectar los derechos de los titulares de datos personales. En ese sentido, en virtud del principio de tipicidad reconocido en la Constitución Política del Estado, en la actualidad no se pueden implementar sanciones administrativas por el incumplimiento de obligaciones de protección de datos en los sectores regulados antes mencionados.

No obstante, sobre la base de las obligaciones establecidas en la Ley 164 y en el D.S.1793, las siguientes conductas contradicen lo establecido en materia de protección de datos:

• Recolección, conservación y procesamiento de datos personales sin el conocimiento previo y el consentimiento expreso de su titular.

• Transferencia de datos personales sin consentimiento previo y expreso del titular de los datos, o por orden escrita de la autoridad judicial competente.

• Acción omisa ante revocatoria del consentimiento otorgado.

• Utilización de los datos para finalidades distintas de las expresadas al momento de su recolección y registro.

• Afectación a los derechos de los titulares de los datos personales a solicitar el acceso, rectificación, actualización, cancelación, objeción y/o revocación de datos personales.

• No adopción de medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida o tratamiento no autorizado.

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 para proteger los derechos de usuarios y consumidores, de manera general, es el Viceministerio de Defensa del Consumidor.

En materia de protección de datos por medios de telecomunicación, la autoridad con competencia es la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT).

No obstante, ninguna de estas dos entidades ejerce de forma activa sus competencias en materia de protección de derechos de intimidad, privacidad y protección de datos de los usuarios. Tampoco se han emitido directrices en 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?

Cualquier organización que pretenda implementar un programa de cumplimiento de la normativa sobre protección de datos tiene que realizar los siguientes pasos:

• Realizar un diagnóstico inicial con el fin de determinar qué tipo de datos personales se suelen recolectar, la finalidad que se persigue para su tratamiento y la base legal que se requiere para obtener esos datos.

• Evaluar los posibles riesgos y determinar las medidas de seguridad necesarias para el tipo de datos identificados.

• Designación de funciones dentro del personal interno, para ejercer la tarea de supervisión de cumplimiento y gestión de la implementación de medidas de mitigación.

• Establecer los mecanismos de respuesta respectivos.

• Proceder con la redacción de la política de protección de datos.

• Relevamiento de acuerdos con proveedores.

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

El ámbito de aplicación está circunscrito al territorio boliviano, no existiendo un alcance extraterritorial conforme a la normativa local.

Paraguay

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

En Paraguay, el marco regulatorio para la protección de datos está dado por la Constitución Nacional (CN) que, a través del Habeas Data garantiza el derecho de toda persona a acceder a la información que, sobre ella misma, o sus bienes, obran en bases de datos públicas o privadas de carácter público. Además, la CN reconoce el derecho a la protección de la vida privada de todos los habitantes, estableciendo que la intimidad de la persona y de la familia y el respeto a la vida privada son inviolables, garantizando el derecho a la protección de la intimidad, la dignidad y la imagen privada de la persona. Por lo tanto, la protección a los datos personales y la intimidad personal se encuentran consagradas en la Constitución Nacional.

En concordancia con las disposiciones de la CN, la Ley N.° 6534/2020 "De Protección de la Información Crediticia" ("Ley 6534") establece lineamientos generales al respecto del tratamiento de datos personales, y en particular, al respecto del tratamiento de datos personales de carácter crediticio.

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. Si bien la Ley 6534 establece obligaciones para los responsables de tratamiento de datos, la norma no prevé la obligación de contar con un programa de prevención de infracciones o de cumplimiento en materia de protección de datos personales.

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?

•Aunque la normativa vigente no contempla incentivos específicos para la adopción de políticas internas de protección de datos, la implementación de un programa interno de cumplimiento en esta materia ofrece, sin duda, los siguientes beneficios:

• **Cumplimiento normativo:** La implementación de un programa de cumplimiento estructurado permite garantizar el cumplimiento de la normativa vigente, evitando multas, sanciones y responsabilidades legales derivadas de incumplimientos o malas prácticas.

• **Respuesta eficiente ante cambios y requerimientos regulatorios:** Contar con procedimientos claros y definidos facilita la gestión de solicitudes de autoridades regulatorias y titulares de datos, asegurando transparencia, cumplimiento de plazos y una rápida adaptación a los cambios normativos.

• **Reducción de vulnerabilidades:** Una política adecuada ayuda a prevenir ataques, y a optimizar la respuesta en casos de quiebres de seguridad.

• **Reputacional:** La adopción de programas de cumplimiento genera confianza y seguridad en los clientes, fortaleciendo la reputación de la empresa. Además, puede ser utilizada como una estrategia de marketing para diferenciarse en el mercado.

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

No, la Ley 6534 no prevé mecanismos de certificación de programas de cumplimiento en protección de datos. Sin embargo, no vemos impedimentos en obtener certificaciones a través de entidades extranjeras especializadas en la materia.

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

No, la Ley 6534 no obliga a los responsables a contar con un delegado o encargado de protección de datos.

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 6534 prevé sanciones para personas y empresas que incumplan las disposiciones de la ley. Estas varían según el ámbito de operación de la empresa y pueden ir desde apercibimientos hasta el cierre definitivo de operaciones.

Las sanciones se clasifican en:

• Apercibimiento.

• Multa de hasta 15.000 jornales mínimos (aproximadamente USD 206.000).

• Multa agravada por reincidencia: En caso de repetición de una misma infracción, la multa será el doble de la inicialmente aplicada y podrá elevarse hasta 50.000 jornales mínimos (aproximadamente USD 690.000) para personas físicas o jurídicas con una facturación anual superior a G. 6.000.000.000 (seis mil millones de guaraníes) (aproximadamente a USD 761.200,00).

• Implementación de medidas.

• Suspensión de actividades relacionadas con el tratamiento de datos por un período máximo de seis (6) meses.

• Cierre temporal de operaciones vinculadas al tratamiento de datos, en caso de no adoptar las medidas correctivas ordenadas por la autoridad de control dentro del período de suspensión.

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

• Inhabilitación para desempeñar cargos en el sistema financiero, crediticio y en sociedades de información de datos personales, por un período de seis (6) meses hasta cinco (5) años.

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

La normativa de protección de datos personales en Paraguay sanciona diversas conductas que vulneran los principios de licitud, transparencia, seguridad y confidencialidad en el tratamiento de datos. Entre las principales infracciones sancionadas se encuentran:

a. Infracciones relacionadas con la autorización y actividades de las entidades reguladoras:

1. Ejercer actividades reguladas por la ley sin autorización previa del ente regulador, o fuera del alcance de las autorizaciones obtenidos.

2. Incumplir limitaciones o prohibiciones temporales impuestas a la entidad, no acatar medidas correctivas, obligaciones legales o reglamentarias exigidas por el ente regulador.

3. Omitir información obligatoria o suministrar información incompleta o falsa al ente regulador.

4. Resistirse, excusarse o negarse a cumplir instrucciones o requerimientos de la Superintendencia de Bancos, supervisores o inspectores, incluyendo la falta de provisión de documentación solicitada.

5. Notificar de manera incompleta, tardía o defectuosa a la autoridad de protección de datos sobre una violación de seguridad.

b. Infracciones relacionadas con la protección de datos personales

1. Recopilación, uso o transferencia indebido de datos (ej. Sin consentimiento, para una finalidad distinta, etc.)

2. Negarse injustificadamente a dar acceso, rectificar o eliminar datos personales cuando así se solicite el titular del dato.

3. No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o portabilidad.

4. Tratar datos personales de un menor de edad sin su consentimiento, cuando tenga capacidad para ello, o sin el consentimiento de su representante legal.

5. No acreditar esfuerzos razonables para verificar la validez del consentimiento otorgado por un menor o su representante legal.

Obligaciones contractuales y medidas de seguridad

• No formalizar acuerdos entre corresponsables del tratamiento de datos o hacerlo de manera inexacta, o incumplir las estipulaciones contractuales en el tratamiento de datos personales sin justificación legal.

• No adoptar medidas técnicas y organizativas adecuadas para garantizar la protección de datos desde el diseño.

• Vulnerar el deber de confidencialidad sobre los datos personales.

• Recolectar, almacenar o transmitir datos personales por mecanismos inseguros o sin garantizar su integridad.

• Transferencias internacionales de datos

• Transferir datos personales a un tercer país u organización internacional sin cumplir los requisitos y garantías establecidos por la ley.

Favor notar que esta lista es enunciativa y no incluye a todas las posibles infracciones relacionadas a la protección o uso indebido 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 Ley 6534 en Paraguay dispone que las entidades competentes en materia de protección de datos son:

• Banco Central del Paraguay (BCP): El BCP debe velar por el cumplimiento de las disposiciones relativas a los burós de crédito y su funcionamiento.

• Secretaría de Defensa del Consumidor (SEDECO): Debe velar por el cumplimiento de las disposiciones de la norma relacionadas a los titulares de datos.

• A la fecha no se han emitido guías o directivas relacionadas al cumplimiento de la Ley 6534.

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?

Toda organización que desee realizar un diagnóstico sobre cumplimiento e implementación de un programa de cumplimiento debe seguir los siguientes pasos:

• Identificar los datos personales que son tratados por la organización.

• Determinar la base legal sobre la que los datos están siendo tratados.

• Elaboración de una política de datos / revisión y actualización de la política de datos.

• Implementación de protocolos y procedimientos internos.

• Revisión de medidas de seguridad vigentes.

• Relevamiento de los acuerdos con proveedores.

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

La aplicación de la Ley 6534 se limita a los datos recolectados o almacenados en Paraguay.

Uruguay

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

En Uruguay, la protección de datos personales está regulada por la Ley N° 18.331, el Decreto Reglamentario N° 414/009, los artículos 37 a 40 de la Ley N° 19.670 y el Decreto Reglamentario N° 64/2020 (“LPD”). Este marco legal garantiza a las personas el control sobre sus datos personales, protegiendo su derecho a la privacidad, en línea con la normativa internacional más avanzada en la materia, el Reglamento General de Protección de Datos de la Unión Europea (“RGPD”). Gracias a esta armonización, Uruguay ha obtenido la nota de adecuación de parte de la Comisión Europea, lo cual valida al país como adecuado para el tratamiento de datos personales.

La LPD establece principios clave que deben ser observados en todas las fases del ciclo de vida de los datos personales, desde su recolección hasta su destrucción, tales como el previo consentimiento informado, finalidad, legalidad (registro de la base de datos), confidencialidad, seguridad y reserva.

Como corolario, la LPD incorpora el principio de responsabilidad proactiva, que implica que tanto el responsable de tratamiento de los datos (propietario de la

base de datos) como el encargado (quien trata los datos personales por cuenta y orden del responsable) deben implementar medidas para garantizar la privacidad desde el diseño y por defecto, realizar evaluaciones de impacto en la protección de datos y designar delegado de protección de datos, cuando corresponda.

Adicionalmente, la LPD creó la Unidad Reguladora y de Control de Datos Personales ("URCDP"), autoridad encargada de supervisar el cumplimiento de la LPD y asegurar su aplicación.

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?

La LPD establece el principio de responsabilidad proactiva en virtud del cual los responsables y encargados de tratamiento de datos deben adoptar medidas técnicas y organizativas para garantizar el cumplimiento normativo. Esto incluye prácticas como privacidad desde el diseño y por defecto y la realización de evaluaciones de impacto cuando sea necesario.

Si bien la LPD no hace referencia expresa a la implementación de un "programa de cumplimiento", sí obliga a las organizaciones que recopilan y tratan datos personales, a documentar y revisar periódicamente las medidas adoptadas para garantizar el cumplimiento legal. Esta documentación debe incluir la forma, finalidad y medios del tratamiento de datos, mecanismos de cumplimiento normativo, protocolos de respuesta ante vulneraciones de seguridad, y cuando aplique, el rol del delegado de protección de datos.

Además, para ciertos tratamientos de datos específicos (grandes volúmenes, elaboración de perfiles, datos sensibles como negocio principal, datos especialmente protegidos o relativos a infracciones penales, civiles o administrativas, datos de menores de edad o personas con discapacidad, transferencias internacionales y otros que la URCDP pueda determinar, la LPD obliga a realizar una evaluación de impacto en la protección de datos ("EIPD"). Esta evaluación permite identificar y mitigar riesgos, además de servir como prueba de cumplimiento de la ley ante la autoridad de control.

En la práctica, aunque la LPD no mencione expresamente un "programa formal de compliance", sus requisitos generan un efecto equivalente, al exigir la documentación de las medidas técnicas y organizativas adoptadas para hacer el tratamiento conforme a la ley, así como también su revisión y gestión de riesgos en el tratamiento de datos personales.

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

La LPD establece que los responsables y encargados de tratamiento de datos deben documentar las medidas técnicas y organizativas que han adoptado para cumplir con la normativa. Esta documentación tiene un rol similar al de un programa de compliance, ya que ayuda a demostrar el cumplimiento de las normas sobre protección de datos.

Según la LPD, esta documentación debe incluir, al menos, detalles sobre la forma, los medios y la finalidad del tratamiento de datos, así como los procedimientos diseñados para cumplir con la normativa. También debe contemplar un protocolo de respuesta a incidentes de seguridad y definir el rol del delegado de protección de datos cuando corresponda.

Por otro lado, las EIPD, que son obligatorias y útiles para demostrar el cumplimiento de la LPD en tratamientos específicos, también deben cumplir con un contenido mínimo. Esto incluye una descripción sistemática de la actividad de tratamiento, una evaluación de su conformidad con la normativa, un análisis de los riesgos para los derechos de los titulares de los datos y un detalle de las medidas de seguridad implementadas junto con los mecanismos para demostrar el cumplimiento de la normativa.

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 en protección de datos personales asegura el cumplimiento normativo y reduce el riesgo de sanciones por parte de la URCDP y posibles reclamos de los titulares. A la vez, también protege la reputación de la empresa y fortalece la confianza de clientes, empleados y socios comerciales.

A nivel interno, optimiza la gestión de los datos con procesos claros y eficientes, facilitando la toma de decisiones estratégicas y la adaptación a posibles cambios regulatorios. Además, refuerza la seguridad en el tratamiento de la información, minimizando riesgos de vulneraciones y garantizando una mayor protección tanto para la empresa como para los titulares de los datos.

En definitiva, implementar un programa de cumplimiento

no sólo reduce riesgos legales, sino que también genera un entorno de confianza para quiénes voluntariamente proporcionan sus datos a las compañías para el acceso a bienes o servicios de su interés.

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

Actualmente, la LPD no contempla mecanismos de certificación de programas de cumplimiento en protección de datos, como sí ocurre en otras legislaciones a nivel comparado.

Para las EIPD que son requeridas por la LPD en marco de ciertas actividades de tratamiento y, que pueden integrarse en el programa de compliance, se establece que, si su resultado evidencia un riesgo significativo para los derechos de los titulares de datos, el responsable y el encargado deberán informarlo a la URCDP, proporcionando detalles sobre las medidas adoptadas o previstas, así como los plazos para su implementación.

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

De acuerdo con la LPD, están obligados a designar Delegado de Protección de Datos, las entidades públicas; entidades privadas total o parcialmente de propiedad estatal; las que traten datos sensibles como negocio principal; o traten grandes volúmenes de datos (es decir, datos de más de 35.000 titulares).

El Delegado de Protección de Datos tiene la función de asesorar a la organización en el cumplimiento de la normativa de protección de datos y ser el nexo con la URCDP, entre otras tareas.

La designación debe hacerse en plazo de 90 días desde el inicio de la actividad de tratamiento.

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

El incumplimiento de la LPD puede dar lugar a la aplicación de sanciones que oscilan desde una observación, apercibimiento, multas de hasta 500.000 Unidades Indexadas (aproximadamente, U$S 70.000), suspensión de la base de datos por un plazo de 5 días, o, en casos más graves, su clausura definitiva.

En ese sentido, la URCDP ha emitido la Resolución N° 105/2015 que contiene lineamientos para la determinación de sanciones. Entre los principales factores que se evalúan, se encuentran la gravedad de la infracción, el historial de incumplimiento del infractor, la naturaleza de los datos personales tratados, la adopción o no de medidas de seguridad, los derechos afectados, el volumen de datos tratados y los posibles perjuicios para las personas y terceros involucrados.

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

La LPD establece que tanto responsables como encargados deben cumplir con la normativa de protección de datos, pudiendo ser sancionados en caso de infracción.

Las infracciones incluyen, entre otras conductas, el tratamiento de datos sin una base legal válida; la falta de transparencia en la recopilación y uso de los datos personales; tratar datos personales para finalidades diferentes o incompatibles a las que motivaron su recolección; el incumplimiento de los derechos de los titulares; la falta de adopción de medidas de seguridad adecuadas para proteger la confidencialidad de los datos; llevar a cabo transferencias internacionales sin las garantías necesarias; la comunicación de datos sin base legal habilitante.

También son pasibles de sanción, conductas relacionadas con el incumplimiento de obligaciones formales como ser, la falta de registro de las bases de datos en URCDP, no brindar a la autoridad la información necesaria cuando ésta lo requiera en marco de investigaciones o afines, entre otras.

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

La LPD creó la URCDP como un organismo desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento ("AGESIC"), que cuenta con autonomía técnica para asesorar y tomar decisiones en materia de protección de datos. Su misión principal es garantizar el cumplimiento de la LPD, protegiendo los derechos de las personas en relación con sus datos personales.

Entre sus principales funciones se encuentran, asesorar a las personas sobre el alcance de la ley y los mecanismos legales para defender sus derechos; emitir normativas y directrices para el tratamiento adecuado de sus datos

personales; atender denuncias y reclamos de personas que consideren que sus datos han sido tratados de forma indebida; aplicar sanciones en caso de incumplimientos; capacitar a entidades públicas y privadas sobre buenas prácticas en materia de protección de datos.
En cumplimiento de sus cometidos, URCDP busca promover un uso responsable y seguro de la información personal en todos los ámbitos.

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 Uruguay, las organizaciones siguen una serie de pasos para garantizar el cumplimiento de la normativa de protección de datos. Primero, realizan un diagnóstico inicial para identificar qué datos personales se recolectan, su finalidad, los medios utilizados para su tratamiento, dónde se almacenan y con quién los comparten.

Con esta información, se elaboran políticas de privacidad para cumplir con el derecho de información de los titulares sobre la recopilación y tratamiento de sus datos. En este marco, establecen protocolos para atender las solicitudes de ejercicio de derechos de los titulares de datos (acceso, rectificación, actualización, supresión entre otros).

Asimismo, se implementan medidas técnicas y organizativas de seguridad orientadas a garantizar la confidencialidad, disponibilidad e integridad de los datos. Éstas pueden incluir controles de acceso, cifrado de datos, guardia física, capacitaciones del personal en gestión de datos, entre otras. Las medidas de seguridad pueden variar dependiendo de la forma de almacenamiento, la naturaleza de los datos tratados y otros factores, ya que la ley no establece expresamente qué medidas deben adoptarse.

En este contexto, las empresas también revisan sus contratos con terceros involucrados en el manejo de la información personal, para asegurarse que proveedores y aliados comerciales cumplan con la normativa, y, en caso de transferencias internacionales, adoptar medidas legales en la medida aplicable.

Posteriormente, las empresas cumplen con sus obligaciones formales, lo que incluye, el registro de sus bases de datos en URCDP – proceso en que deben declarar el cumplimiento de los pasos anteriores-. Además, cuando corresponde, designan un delegado de protección de datos para supervisar el cumplimiento normativo y actuar como ligamen con la autoridad de control.

De este modo, las organizaciones pueden incorporar la normativa de protección de datos en su programa de compliance, implementando protocolos de gestión de datos, auditorías internas y revisiones periódicas para evaluar la efectividad de sus medidas, garantizando así una mejora continua y adaptación a cambios regulatorios.

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

La LPD aplica al tratamiento de datos personales de personas físicas o jurídicas, en la medida en que el responsable de tratamiento (propietario de la base de datos) o el encargado (quien trata datos personales por cuenta y orden del responsable y bajo sus instrucciones) se encuentre establecido en Uruguay.

Adicionalmente, como en el caso del RGPD de la Unión Europea, la LPD tiene alcance extraterritorial. Por ende, aplica al responsable o encargado no establecido en Uruguay, cuando las actividades de tratamiento se encuentren relacionadas con la oferta de bienes o servicios dirigidos a habitantes uruguayos o se vinculen con el análisis de su comportamiento; cuando así lo disponen las normas de derecho internacional público o un contrato; o cuando en el tratamiento se utilizan medios situados en el país, como ser redes de información y de comunicación, centros de datos o infraestructura informática en general, recursos humanos u otros.

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.

Miller & Chevalier

Autor:

Facundo Galeano, Asociado, FCPA y Anticorrupción, Investigaciones Internas y AML.

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

Estados Unidos carece de una ley de protección de datos integral a nivel federal, pero hay un conjunto de leyes federales que regulan ciertas industrias y subcategorías de datos.

A nivel estatal, algunos estados han aprobado sus propias leyes de privacidad de datos que mantienen similitudes al sistema de la Unión Europea y su ley integral de privacidad de datos ("GDPR", por sus siglas en inglés).

La regla general es que todas aquellas compañías que no están reguladas a nivel federal o estatal pueden disponer de los datos de sus usuarios, como usar, vender, o compartir los datos sin notificárselo a los usuarios.

Algunas de las normativas más relevantes son:

Ley de la Comisión Federal de Comercio ("FTC", por sus siglas en inglés): es una herramienta importante para que los reguladores federales hagan cumplir las protecciones de privacidad de datos. La ley prohíbe los "actos o prácticas desleales o engañosas" ("UDAP", por sus siglas en inglés), lo que ha permitido a la FTC a interponer cientos de acciones legales basadas en denuncias de que las prácticas de protección de datos de una compañía violaban la prohibición de UDAP.

Ley de Privacidad de 1974: regula la recopilación y uso de datos sobre individuos por parte de las agencias federales. A grandes rasgos, aunque con algunas excepciones limitada, la ley prohíbe la revelación de datos personales sin el consentimiento del individuo, el cual se reserva sus derechos a solicitar sus datos personales registrados en dichas agencias, solicitar cambios o ajustes a datos en caso de ser inexactos o incompletos y a que las agencias protejan sus datos contra invasiones no autorizadas o injustificadas de sus datos.

Protecciones Generales de Datos "En Línea"

La Ley de protección de la privacidad en línea de los niños ("COPPA", por sus siglas en inglés): proporcionan requisitos de protección de datos para la información de los niños recopilada por los operadores en línea. COPPA se aplica a:

• Cualquier "operador" de un sitio web o servicio en línea que esté "dirigido a niños".

• Cualquier operador que tenga "conocimiento real de que está recopilando información personal de un niño".

COPPA establece varios requisitos con respecto a la recopilación y uso de datos, notificaciones de políticas de privacidad y seguridad de datos.

Ley de Comunicaciones de 1934: creó la Comisión Federal de Comunicaciones ("FCC", por sus siglas en inglés), incluye disposiciones de protección de datos para los operadores comunes (servicios de teléfono y telégrafo), operadores de cable y operadores de satélites.

Con respecto a los operadores de cable y los operadores de satélites, la Ley de Comunicaciones impone una serie de requisitos relacionados con:

• La recopilación y divulgación de datos.

• El acceso de los abonados a sus datos y su corrección.

• La destrucción de datos.

• La notificación de la política de privacidad.

• La seguridad de los datos.

Ley de Abuso y Fraude Informático: prohíbe el acceso no autorizado a "computadoras protegidas", que se define ampliamente como cualquier computadora utilizada en o que afecte el comercio o las comunicaciones interestatales, permitiendo de hecho que la ley se aplique a cualquier computadora conectada a internet.

Ley de Privacidad de las Comunicaciones Electrónicas de 1986 ("ECPA", por sus siglas en inglés): prohíbe el acceso no autorizado o la interceptación de comunicaciones electrónicas en almacenamiento o tránsito. ECPA es una ley integral sobre privacidad electrónica, pero su impacto en las prácticas de privacidad en línea ha sido limitado; los litigantes que intentan aplicar ECPA a la recopilación de datos en línea, o recopilación de datos comerciales, generalmente no han tenido éxito.

Industria financiera y otras protecciones al consumidor

Ley Gramm-Leach-Bliley: regula el uso por parte de las instituciones financieras de información personal no pública ("NPI", por sus siglas en inglés), generalmente relacionada con:

• Compartir NPI con terceros.

• Proporcionar avisos de privacidad a los consumidores.

• Proteger a NPI del acceso no autorizado.

Ley de Bolsa y Valores de 1934: exige que las empresas públicas y algunas otras empresas "diseñen y mantengan un sistema de controles contables internos suficiente para ofrecer garantías razonables" de que "las transacciones se ejecutan de acuerdo con la autorización general o específica de la gerencia" y que "el acceso a los activos solo se permite de acuerdo con la autorización general o específica de la gerencia".

La Ley de Protección Financiera del Consumidor: regula los actos injustos, engañosos o abusivos en relación con los productos o servicios financieros del consumidor. La Oficina de Protección Financiera del Consumidor ("CFPB", por sus siglas en inglés) tiene la autoridad para tomar medidas contra "actos o prácticas injustas, engañosas o abusivas".

La Ley de Informes de Crédito Justos: cubre la recopilación y el uso de los datos contenidos en los informes de los consumidores.

Protección de Datos en la Industria de la Salud

Ley De Portabilidad y Responsabilidad Del Seguro De Salud de 1996 ("HIPAA", por sus siglas en inglés): creó los estándares sobre el uso de datos personales de salud de un paciente por parte de los proveedores de salud y actores de la atención médica ("entidades cubiertas"). Las entidades cubiertas van desde los proveedores (médicos, dentistas, etc.), hasta la compañías de seguros de salud (incluyendo los planes gubernamentales) y los demás actores de la atención medica que procesan este tipo de información.

Leyes Estatales

En 2018, California aprobó la Ley de Privacidad del Consumidor de California ("CCPA", por sus siglas en inglés), la primera ley estatal integral de privacidad de datos y consumidores y considerada la ley más estricta del país.

Desde entonces, no solo California enmendó la ley, sino que varios estados han promulgado leyes integrales de privacidad de datos y consumidores, y otros estados ya han presentado proyectos de ley integrales que están en revisión.

Actualmente son 19 los estados que cuentan con leyes integrales de privacidad de datos y consumidores: California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennesse, Texas, Utah y Virginia[1].

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?

Debido a la falta de una sola ley integral que regule la protección de datos a nivel federal, habría que analizar cada una de las normativas para entender cuáles requieren de un programa de prevención o de cumplimiento y cuáles no.

A modo de ejemplo, en el caso de la FTC, la misma mantiene una norma para la salvaguardia de la información del cliente que proporciona orientación concreta a las empresas cubiertas —instituciones financieras sujetas a la jurisdicción de la FTC— y requiere que dichas empresas cubiertas desarrollen, implementen y mantengan un programa de seguridad de la información con salvaguardas administrativas, técnicas y físicas diseñadas para proteger la información del cliente.

En el caso de la HIPPA, la misma mantiene una regla de seguridad ("Regla de Seguridad") que establece un conjunto de normas nacionales de seguridad para proteger cierta información de salud mantenida o transmitida de forma electrónica. La Regla de Seguridad establece todas las salvaguardias administrativas, físicas y técnicas que las entidades cubiertas deben implementar para asegurar que la información electrónica esté protegida. En general, los estándares intentan:

• Asegurar la confidencialidad, integridad y disponibilidad de toda la información personal que crean, reciben,

[1] https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

mantienen o transmiten.

• Proteger contra amenazas razonablemente anticipadas a la seguridad o integridad de la información.

• Proteger contra usos o divulgaciones razonablemente anticipados e inadmisibles.

• Garantizar el cumplimiento por parte de su personal.

Las entidades cubiertas deberán también mantener políticas y procedimientos razonables y apropiados para cumplir con provisiones de las Regla de Seguridad, de forma escrita y disponible para el personal responsable de aplicar dichas políticas y procedimientos y actualizarlos de forma acorde. La Regla de Seguridad ha sufrido algunas modificaciones a través de los años con la implementación de leyes como la Ley de Tecnología de la Información Sanitaria para la Salud Económica y Clínica ("Ley HITECH", por sus siglas en inglés) y la Ley de No Discriminación de Información Genética.

En el caso de la Ley de Bolsa y Valores de 1934, la Comisión de Valores y Bolsa de los Estados Unidos ("SEC", por sus siglas en inglés) ha sugerido que las empresas deberían considerar las "amenazas relacionadas con la ciberseguridad" al formular controles contables. En julio de 2023, la SEC adoptó normas que obligaban a los solicitantes de registro a revelar los incidentes de ciberseguridad importantes que experimentaron y a revelar anualmente información importante sobre su gestión, estrategia y gobernanza de riesgos de ciberseguridad.

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

Tanto el contenido mínimo de un programa de cumplimiento como las diferentes auditorias y controles aplicables por parte de los reguladores relevantes dependerán de las leyes federales y/o estatales aplicables a la compañía. Debido a la disparidad de leyes federales y estatales relevantes, no existe una única guía que refleje los contenidos mínimos que deben tener las compañías para asegurar el cumplimiento de la protección de datos dentro de sus negocios, los cuales dependerán de la industria y la zona geográfica en la cual la compañía opere.

De todas maneras, las compañías deberán implementar algunos elementos que aseguren que la compañía está abordando las áreas claves para garantizar que los datos personales se manejan de manera segura y de acuerdo a las leyes relevantes:

• Inventario y clasificación de datos

• Redacción de Políticas y Procedimientos

• Políticas de protección de datos, detallando la forma en que la compañía recopila, usa, almacena y protege datos personales.

• Procedimientos adecuados para la implementación de dichas políticas, así como la implementación de mecanismos de respuesta a los consumidores, en caso de tener acceso a datos personales de los mismos.

• Procedimientos de seguridad en caso de hackeo o filtración de datos.

• Procedimientos adecuados de comunicación con las autoridades relevantes en caso de filtración de datos u otros reportes obligatorios (por ejemplo, cuando se transfieren largas cantidades de datos a otra jurisdicción).

• Nombramiento de un empleado responsable de supervisar la aplicación de las políticas y procedimientos

Algunas normas más complejas, como la CCPA, obligan también a las compañías a proporcionar en su política de privacidad o en su sitio web una descripción del "derecho a saber" de un consumidor y "uno o más métodos designados" para presentar solicitudes. La CCPA también exige a las empresas que eduquen a sus empleados responsables de atender las consultas de los clientes sobre las obligaciones de las empresas y cómo orientar a los consumidores en el ejercicio de sus derechos. Del mismo modo, con respecto al "derecho a optar por no participar", las empresas deben proporcionar un "enlace claro y visible" en su página de inicio titulado "No vender mi información personal".

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

Como todo programa de cumplimiento efectivo, son diversos los beneficios que acompañan su implementación. Algunos de ellos son:

• Reducir los riesgos de incumplimiento normativo y evitar sanciones por violaciones a las normativas de protección de datos aplicables.

• Eficiencia operacional en el manejo y almacenamiento

de datos, los cual mejora la productividad y reduce costos operativos.

• Ventaja competitiva y beneficios reputacionales al identificarse como una compañía con un programa de cumplimiento efectivo que maneja los datos personales de sus usuarios o clientes de manera responsable.

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

Los procesos de certificación dependerán de las normativas de protección de datos aplicable. De todas maneras, hay algunas certificaciones existentes para demostrar que la compañía cumple con los estándares de protección de datos personales aplicables. Estas certificaciones son:

• SOC 2 Compliance.

• ISO/IEC 27001.

• EU-U.S. Data Privacy Framework.

Adicionalmente, son varias las instituciones que ofrecen servicios de certificación de programas de cumplimiento en protección de datos en las diversas industrias. Las compañías podrán ofrecer a sus empleados la obtención de alguna de las certificaciones ofrecidas por la Asociación Internacional de Profesionales de la Privacidad (IAPP, por sus siglas en inglés) y/o el Consorcio Internacional de Certificación de Seguridad del Sistema de la Información (CISSP, por sus siglas en inglés) para demostrar que mantienen empleados expertos en el cumplimiento de la normativa de protección de datos aplicables.

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

La mayoría de las leyes de protección de datos relevantes no requieren del nombramiento de un oficial de protección de datos, pero ciertos estatutos requieren de la designación de una persona o personas que se encuentren encargadas de hacer cumplir los requisitos bajo dichos estatutos. En la mayoría de los casos no se requiere que la persona o personas mantengan cualificaciones específicas, ni se hace referencia a las responsabilidades especifica que esta persona o personas deben tener al interior de la entidad cubierta.

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

Cada normativa mantiene sus propias provisiones asociadas a las sanciones en caso de incumplimiento.

La Ley de la FTC no exige que las empresas cumplan proactivamente con políticas o prácticas específicas de protección de datos, y la ley se ha interpretado históricamente para no llegar a entidades que no han hecho declaraciones explícitas sobre la protección de datos. Además, la FTC no puede solicitar sanciones monetarias por violaciones de UDAP ante una primera violación, pero puede solicitar sanciones civiles después de que una empresa haya violado una orden de cese y desistimiento emitida por la FTC o un acuerdo.

En el caso de la HIPPA, esta mantiene un sistema de penalidades complejo, basado en cuatro niveles dependiendo de la violación, los cuales toman en cuenta factores como el conocimiento, la intencionalidad y el descuido de la compañía durante la violación y la intención de la misma en corregir o no la situación.

En el caso de la CCPA, esta exige a las empresas que informen a los consumidores sobre estos derechos de ciertas maneras específicas y proporcionen los medios para ejercerlos de forma gratuita. Si bien la CPRA prevé una causa de acción privada, esta causa de acción solo está disponible en el caso de un consumidor cuya "información personal no cifrada o no redactada" esté sujeta a "acceso no autorizado y exfiltración, robo o divulgación". Además, estas acciones sólo pueden interponerse si el consumidor notifica por escrito a la empresa con 30 días de antelación y le brinda la oportunidad de subsanar la infracción, a menos que el consumidor haya sufrido daños pecuniarios reales. El estatuto no especifica cómo una empresa podría "curar" una violación de este tipo. Los consumidores pueden recuperar daños bajo esta sección de no menos de $2,500 por cada violación o $7,500 por cada violación intencional a los consumidores a los que el negocio, contratista u otra persona tenía conocimiento real que era menor de 16 años.

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

Sin perjuicio de ya haber mencionado algunas de las conductas sancionadas por las diversas normativas de protección de datos personales, aquí describimos algunos ejemplos:

Como comentamos, la FTC prohíbe los "actos o prácticas desleales o engañosas". La FTC ha adoptado la posición de que las compañías actúan de manera "engañosa" cuando manejan datos personales de una manera que contradice las declaraciones o promesas que han hecho con respecto a la privacidad o el acceso no autorizado a los datos. La FTC también ha emprendido acciones legales contra compañías que aplican prácticas "desleales" de protección de datos, incluso cuando las compañías dificultan a los usuarios cambiar la configuración de privacidad predeterminada o cuando aplican retroactivamente políticas de privacidad revisadas.

Bajo la HIPPA, las entidades cubiertas no pueden hacer uso o compartir la información de salud de un paciente sin su consentimiento escrito y deben cumplir con el derecho de una persona a ver y/o corregir su información de salud. Es importante tener en cuenta que la información de salud que se comparte con una entidad que no esté cubierta no está sujeta a la regulación de la HIPAA. Esto significa que los datos de salud que se comparten, por ejemplo, en las redes sociales o se agregan a una aplicación de salud o nutrición, no se encuentran cubiertos bajo la HIPAA. En otros casos de organizaciones o instituciones que recopilan este tipo de información, como pueden ser las escuelas o los empleadores, aunque no están sujetas a la HIPPA, pueden estarlo a otras leyes federales o estatales.

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

Los organismos técnicos fiscalizadores son tantos como las normativas e industrias en las cuales operen las compañías, algunos de los cuales ya hemos mencionado en esta sección.

A modo de ejemplo, en el sector de la salud, la Ley HITECH requiere que el Departamento de Salud y Servicios Humanos de los Estados Unidos ("HHS", por sus siglas en inglés) realice auditorías periódicas a las entidades cubiertas para verificar su cumplimiento con los requisitos de la Ley HIPAA.

Cada Estado que mantiene una ley de protección de datos personales tiene a su vez un organismo técnico y fiscalizador local designado para hacer cumplir la norma. En el caso de California, la Agencia de Protección de Privacidad ("CPPA", por sus siglas en inglés) es el órgano encargado de implementar la CCPA.

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 la complejidad de la aplicación de normativas en protección de datos personales en Estados Unidos, es muy importante el primer paso: entender que normativas y regulaciones son aplicables a la compañía. Una vez establecido el ámbito regulatorio aplicable, la compañía deberá:

• Hacer una auditora que revise y contemple la forma en que la compañía recolecta, procesa, usa, comparte y almacena los datos (entre otros).

• Crear e implementar una política de privacidad y protección de datos a medida.

• Establecer protocolos claros de seguridad de los datos y respuesta en casos de hackeo o filtración de datos.

• Establecer procedimientos de respuesta a la solicitud de usuarios.

• Designar un responsable o responsables de la aplicación y cumplimiento de estas políticas.

• Entrenar a los empleados de la compañía.

Luego vendrán los demás controles, como son el monitoreo y revisión de las políticas y procedimientos para asegurar el cumplimiento de éstos y actualizar los mismos ante los cambios normativos o cambios dentro de la compañía que ameriten revisión de las mismas.

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

Como vimos en este capítulo, el ámbito de aplicación territorial dependerá de la normativa aplicable, siendo de forma general las normativas federales aplicables en todo el territorio nacional y las normativas estatales aplicables a las compañías que manejan datos personales de sus residentes.

A modo de ejemplo, la CCPA se aplica a cualquier compañía que recopila la información personal de los residentes de California, tiene fines de lucro, hace negocios en California y cumple con uno de los tres umbrales:

• A partir del 1 de enero del año civil, los ingresos brutos anuales superan los veinticinco millones de dólares (25

millones de dólares) en el año civil anterior.

• Solo o en combinación, anualmente compra, vende o comparte la información personal de 100.000 o más consumidores u hogares.

• Obtiene el 50 por ciento o más de sus ingresos anuales de vender o compartir información personal de los consumidores.

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.

Guía Comparada Protección de Datos Personales

Encuentra todas nuestras guías comparadas **aquí**

Compliance Latam @ComplianceLatam @ComplianceLatam

www.compliancelatam.legal