etiqampus
e-Learning en Integridad

Guía Comparada Protección de Datos Personales: caso Estados Unidos

Compliance Internacional

NIVEL INTERMEDIO

Fecha	Marzo 2025
Tpo. de lectura	25 min.

El avance tecnológico y la transformación digital han puesto la protección de datos personales en el centro del debate regulatorio a nivel global. En Latinoamérica, el desarrollo y fortalecimiento de normativas en esta materia reflejan la creciente necesidad de garantizar la privacidad y seguridad de la información en un entorno empresarial cada vez más interconectado.

La evolución de estas regulaciones y su aplicación práctica imponen nuevos desafíos a las organizaciones, que deben adaptar sus procesos y modelos de negocios para cumplir con estándares más altos y responder a las exigencias de las autoridades regulatorias y fiscalizadoras.

En este contexto, especialista de destacadas firmas legales de 18 países miembros de Compliance Latam, han elaborado esta guía que, además de dar una visión clara y actualizada sobre los marcos normativos y últimas tendencias en protección de datos personales, entrega herramientas clave para que las empresas comprendan y gestionen los riesgos asociados al tratamiento de datos, fomenten una cultura de cumplimiento y refuercen la confianza con sus clientes y socios comerciales.

A continuación te presentamos la sección dedicada a Estados Unidos, escrita por Facundo Galeano, Asociado de Miller & Chevalier y encargado de FCPA y Anticorrupción, Investigaciones Internas y AML.

FGE

az albagli zaliasnik

Miller & Chevalier

Com plian ce LATAM

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

Guía Comparada Protección de Datos Personales

Marzo 2025



www.compliancelatam.legal



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.