etiqampus
e-Learning en Integridad

Guía Comparada Protección de Datos Personales: caso Argentina

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 Argentina, escrita por las siguientes profesionales del estudio Beccar Varela:

- Florencia Rosatti, Socia, TMT, Privacidad y Protección de Datos Personales.
- Andrea Sanchez Vicentini, Abogada Intermediate, IP, TMT y Privacidad.

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



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.