Protección de Datos Personales en LATAM Guía de Consulta Rápida

EY Law | Latinoamérica
Octubre 2022

Haga clic para entrar

Building a better working world

Índice

Introducción

El contexto actual en constante evolución, en particular considerando el incremento acelerado de las mejoras tecnológicas, el uso a gran escala de datos, las nuevas tecnologías, y la "era digital", son realidades que no se pueden ignorar y que requieren mantenerse presente e informado. En esta línea, desde EY entendemos la necesidad que tienen las distintas empresas de adaptarse a la nueva realidad y estar lo mejor preparadas posible con una estrategia integral para la seguridad cibernética y la protección de datos personales, en particular mediante la identificación de los obstáculos legales y reglamentarios que deben superarse y actualizarse constantemente para mantenerse a la altura y velocidad de adaptación de las nuevas tecnologías. Por dicho motivo, desde EY Law decidimos lanzar esta segunda edición de la Guía de Consulta Rápida de Protección de Datos Personales en LATAM.

Al igual que en otras ediciones anteriores, destacamos que desde EY acompañamos a las empresas con una visión global y al mismo tiempo integrada con equipos multidisciplinarios que integran abogados especialistas en privacidad e informáticos especialistas en ciberseguridad permitiendo a nuestros clientes lograr el máximo nivel de protección y prevención.

Los datos continúan y seguirán siendo el combustible que alimenta la economía digital, un recurso sumamente valioso que permite llegar a más consumidores y de manera más precisa, buscando proteger a su vez, los derechos fundamentales de cada individuo como es el caso de la protección de los datos personales. La privacidad y la protección de datos personales se encuentran en el centro de atención del público en general y de diversos organismos de Gobierno.

A los fines de adaptarse a estas nuevas tecnologías, las organizaciones deben mantener seguros sus datos de posibles ataques cibernéticos para así ganar la confianza del público respecto a que sus datos serán tratados adecuadamente. Tanto los incidentes relacionados a la seguridad cibernética, como el incumplimiento de los requisitos para una adecuada protección de datos, podrían dañar la reputación, la marca o los negocios de una compañía. Es por ello que las compañías son directamente responsables por la protección de los datos personales que administran y no pueden desentenderse del uso -o abuso- de dichos datos personales.

La legislación de protección de datos personales en América Latina viene evolucionando significativamente en los últimos años y adaptándose a los más altos estándares internacionales. Por dicho motivo, el objetivo de esta guía es permitir al lector encontrar de manera rápida las respuestas iniciales a los interrogantes que en materia de protección de datos personales pudiera requerir para el desarrollo de sus negocios en América Latina. En esa línea, desde EY hemos articulado este trabajo sobre la base de una serie de preguntas disparadoras que se repiten en todas las legislaciones y que han sido en nuestra experiencia motivo de consulta frecuente. Las respuestas a estas preguntas servirán de guía para lograr una primera aproximación a la materia y entender preliminarmente el nivel de requerimientos exigidos por cada jurisdicción.

Téngase presente que la información contenida en esta guía está actualizada a la fecha de emisión de este documento y, en tal sentido, al momento de su consulta podría resultar relevante confirmar la efectiva vigencia de las normas referidas.

Esperamos que este material pueda resultar de utilidad y quedamos siempre abiertos a acompañarlos en caso de entender relevante la asistencia de nuestros especialistas en la materia.

Jorge Garnier
Socio EY Law
LATAM South Law Leader
jorge.garnier@ar.ey.com

Hernán Pacheco
Socio EY Law
LATAM North Law Leader
hernan.pacheco@cr.ey.com

EY Law es una firma global, caracterizada por su pensamiento de avanzada e innovación basada en los más altos estándares éticos y profesionales, que provee servicios legales comprensivos y multidisciplinarios a nuestros clientes. Estamos comprometidos a dar un excepcional servicio al cliente, conducidos por un servicio con alcance diferencial.

Pasión por la excelencia Servicios integrados

Nuestros abogados conocen y entienden la legislación y regulaciones vigentes, pudiendo aportar soluciones creativas y sólidas para su negocio. Ofrecemos una asesoría integral en las transacciones y operaciones de nuestros clientes y servicios de apoyo legal constante, lo que permite aumentar la eficiencia y reducir el costo de algunas actividades legales de rutina.

Enfoque regional - Firma integrada de América del Norte y América Latina

En América, nos encontramos en 18 países. Nuestras áreas de expertise incluyen Derecho Corporativo y Comercial, M&A, Impuestos, Antitrust, Contratos de Distribución y Franquicia, Comercio Internacional y Derecho Aduanero, Derecho Ambiental y Sustentable, Protección de Datos Personales, Derecho de la Tecnología, Propiedad Intelectual, Derecho Laboral, Litigación, Arbitraje y Resolución de Conflictos. También nos especializamos en innovación, start-ups, capital de riesgo e inversión de impacto, y proyectos de responsabilidad social corporativa y servicios pro-bono para las comunidades de la región.

Multidisciplinario y sector focalizado

EY, líder mundial en servicios profesionales, comprende los asuntos de negocios que son importantes para los altos ejecutivos. Con amplios conocimientos sobre el negocio y experiencia práctica en varias industrias, la organización mundial EY puede implementar una amplia gama de soluciones para asistir a las compañías en el crecimiento, mejora del desempeño financiero y administración del riesgo en cualquier parte del mundo.

Alcance global

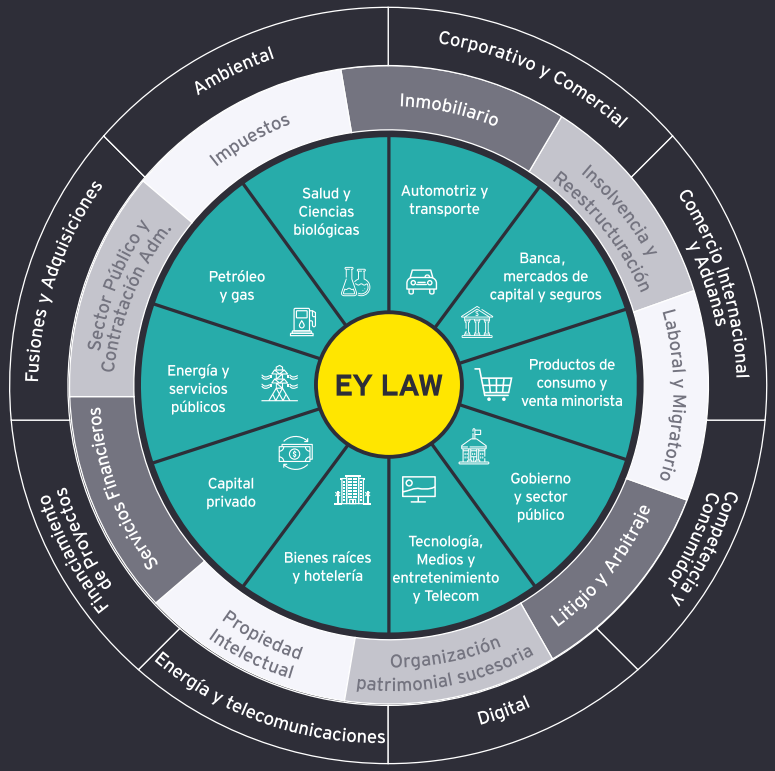
Con presencia en 95 países y más de 3.500 abogados, EY Law reúne a especialistas legales en todo el mundo y sigue creciendo a un ritmo acelerado. Nuestros equipos multidisciplinarios pueden prestar asistencia donde quiera que su negocio lo necesite. Cuenta con 261.000 profesionales en más de 150 países alrededor del mundo, quienes actúan como asesores confiables de negocios. En Argentina EY cuenta con cerca de 3.000 integrantes distribuidos en sus oficinas de la Ciudad de Buenos Aires y Córdoba.

Integrado

En EY Law somos una organización verdaderamente integrada tanto vertical como horizontalmente. No somos una conexión suelta de firmas a través de una alianza o afiliación, sino que somos todos miembros de EY, con toda la pericia, conocimiento y experiencia que ofrece el ser parte de una firma verdaderamente integrada y global. Esto nos permite trabajar junto con profesionales de otras prácticas de los negocios de EY, incluyendo Impuestos, Estrategia, Transacciones, Consultoría y Auditoría, entregando una experiencia excepcional de servicio al cliente. Al servir a nuestros clientes a través de las fronteras, nuestro enfoque sectorial y multidisciplinario significa que ofrecemos un asesoramiento integral y pertinente.

EY Law | Principales Servicios

- Corporativo & Comercial
- Trabajo & Empleo
- Fusiones & Adquisiciones / Transacciones
- Financiación & Reestructuración



Argentina

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Normativa	¿Existe en el país una ley de protección de datos personales? En ese caso, identificar normativa aplicable.	Sí	La protección de datos personales está regulada por la Ley de Protección de Datos Personales Nº 25.326 ("LPDP"). Ese marco normativo se complementa con otras normas tales como: ‣ Constitución de la Nación Argentina en su Artículo 43, tercer párrafo. ‣ Decreto Nº 1558/2001, con sus modificaciones, reglamentario de la Ley de Protección de Datos Personales Nº 25.326 ("LPDP"). ‣ Ley 27.483 (adhesión al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, de Estrasburgo, Francia). ‣ Ley de Derecho de Acceso a la Información Pública Nº 27.275. ‣ Disposición E 60 / 2016 ‣ Resolución 159/2018 (Lineamientos y contenidos básicos de normas corporativas vinculantes). ‣ Protocolo Adicional 108+. (Firmado por Argentina. Pendiente de ratificación por normativa local).
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su Sitio Web.	Sí	Mediante el Decreto 746/2017, se establece como autoridad de aplicación a la Agencia de Acceso a la Información Pública, en adelante ("AAIP"), un organismo descentralizado en la órbita de la Jefatura de Gabinete de Ministros, dentro del Poder Ejecutivo. https://www.argentina.gob.ar/aaip
Ámbito de aplicación	¿Cuál es el ámbito de aplicación de la norma? Es decir, ¿su aplicación es estrictamente territorial, o aplica el concepto de extraterritorialidad?	Sí	Las normas de la LPDP son de orden público y de aplicación en lo pertinente en todo el territorio nacional argentino.
Recolección de datos	¿Cuáles son los requisitos o procesos legales exigidos para la recolección de datos personales? (por ejemplo, consentimiento del titular de los datos, proporcionar información sobre la finalidad del uso de los datos y derechos de su titular, entre otros).	Sí	El tratamiento de datos personales será licito cuando el titular hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de estos; e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	La LPDP define como dato personal a la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	**Datos sensibles:** Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. **Datos informatizados:** Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado. **Datos penales o contravencionales:** Datos relativos a los antecedentes penales y/o contravencionales que sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Situación de las sociedades y otras personas jurídicas	¿Alcanza la protección de la normativa en materia de datos personales, de las personas jurídicas o de existencial ideal?	Sí	La ley LPDP alcanza a los datos relativos a personas de existencia ideal o jurídicas, determinadas o determinables.
Consentimiento del titular de los datos	¿Se requiere la obtención previa del consentimiento del titular de los datos cuando se recaba su información? En tal caso, ¿existen condiciones para la obtención del consentimiento del titular de los datos? (por ejemplo, información previa que deba proporcionarse al titular de los datos.	Sí	La obtención del consentimiento debe ser previo, libre, expreso e informado. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara.
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resultennecesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes.
Contenido y alcance de la información a ser validada por el titular de los datos	¿Cuál es el contenido que debe incluir el consentimiento? (Por ejemplo, uso o destino de los datos, transferencia internacional de los datos, etc.).	Sí	Ver la respuesta en recolección de datos.
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales? ¿Hay requisitos aplicables en relación a la transferencia internacional de datos? (Ejemplo: cláusulas modelos, autorización por parte de la autoridad de control, entre otros).	Sí	En la LPDP está prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados. Sin embargo, la prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados no rige cuando el titular de los datos hubiera consentido expresamente la cesión. Por otro lado, a través de la Disposición Nº 60 - E/2016 publicada en el Boletín Oficial el 18 de noviembre de 2016, la Dirección Nacional de Protección de Datos Personales (ahora la AAIP) reguló aspectos referidos a las transferencias de datos personales. Conforme la LPDP, la transferencia a países que no son considerados adecuados en materia de protección de datos personales se encuentra prohibida. A la fecha, nunca se había determinado qué países cumplían ese standard de adecuación. La nueva Disposición establece que los siguientes países poseen legislación adecuada en materia de protección de datos personales: Estados miembros de la Unión Europea y miembros del Espacio Económico Europeo, Suiza, Guernsey, Jersey, Isla de Man, Islas Feroe, Canadá únicamente en cuanto al sector privado, Nueva Zelanda, Andorra y Uruguay. Es decir, se ha considerado a tal efecto las declaraciones de adecuación emitidas por la Unión Europea. Por su parte, la Disposición aprueba dos modelos de contratos para ser empleados en transferencias internacionales de datos a países no adecuados, tanto en caso de cesiones de datos como en los supuestos de prestación de servicios. Estos modelos siguen en muchos aspectos los lineamientos de las cláusulas contractuales modelo de la UE dispuestas en la Decisión 2001/497/CE y Decisión 2010/87/UE.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	Sí	A través de la Resolución 159/2018 la AAIP adoptó Normas Corporativas Vinculantes, a fin de ser consideradas en el diseño de documentos relativos a normas de autorregulación en empresas que conformen un mismo grupo económico, para la transferencia internacional de datos personales.
Datos sensibles	¿Qué se entiende por dato sensible? ¿Cómo es el tratamiento de los datos sensibles, de corresponder?	Sí	Se entiende por datos sensibles a los datos personales que revelan: ‣ Origen racial y étnico. ‣ Opiniones políticas. ‣ Convicciones religiosas, filosóficas o morales. ‣ Afiliación sindical. ‣ Información referente a la salud o a la vida sexual. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por la LPDP en su artículo 7.
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (ej. ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, tratamiento y/o uso de la misma? ¿Existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	Sí	Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro de la Agencia de Acceso a la Información Pública. Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro. El incumplimiento de estos requisitos dará lugar a las sanciones administrativas por parte de la AAIP, como expresa el artículo 29 de la LPDP.
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	Sí	En cuanto a las medidas técnicas y organizativas el responsable o usuario del archivo de datos, debe adoptar de modo que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado. A su vez, que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Ejemplo: rectificación, actualización o supresión). Identificar y explicar.	Sí	El titular de los datos tiene los siguientes derechos: ‣ Derecho de información y su contenido. ‣ Derecho de acceso. ‣ Derecho a actualización y/o rectificación. ‣ Derecho de supresión.
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	<u>Derecho de información y su contenido:</u> **Toda persona puede solicitar información, a la AAIP, relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables.** <u>Derecho de acceso del titular de datos personales:</u> El titular de los datos, previa acreditación de su identidad tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes. <u>Derecho a actualización, rectificación y supresión:</u> Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	Sí	Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo. Por otro lado, el cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros (data processing)? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	Sí	Cuando, por cuenta de terceros, se presten servicios de tratamiento de datos personales, estos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.
Conservación de datos	¿Hay obligación de retener/conservar los datos recolectados o procesados por un tiempo determinado? En dicho caso, ¿cuál es el plazo?	No	Sin embargo, una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.
Eliminación de datos	¿Existe una obligación de eliminar los datos recolectados o procesados? En dicho caso, ¿en qué supuestos y cuál es el plazo?	Sí	Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. Por otro lado, los datos deberán eliminarse en caso de que el titular del dato lo solicite.
Privacy Impact Asessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (Privacy Impact Assessment)?	No	No se prevé en la LPDP. Sin embargo, la AAIP junto con la Unidad Reguladora y de Control de Datos Personales de Uruguay elaboraron una guía de evaluación de impacto en el tratamiento de datos personales. Con el propósito de brindar un documento de referencia sobre los conceptos, contextos y metodologías en una evaluación de impacto en la protección de datos (EIPD). La guía tiene por objetivo actuar como una herramienta para la evaluación, de forma responsable y conforme a determinados estándares de seguridad e integridad, de las prácticas y proyectos que puedan afectar los derechos de las personas con relación al tratamiento de sus datos personales.
Incidentes	¿Hay obligación de reportar un incidente de seguridad u algún incumplimiento o las previsiones legales?	No	Si bien no existe un requerimiento local normativo vigente, en el año 2019, Argentina firmó el Protocolo Adicional (Convenio 108 +) que modifica el Convenio 108. A través del artículo 7 del mencionado Convenio, se establece que el responsable del tratamiento deberá notificar, sin demora, al menos a la autoridad de control competente, aquellas violaciones a los datos que puedan interferir gravemente con los derechos y las libertades fundamentales de los titulares de datos.
Sanciones	¿Existen sanciones frente al incumplimiento de dicha obligación? En caso de existir, identificarlas e indicar el monto de las sanciones o penalidad aplicable correspondiente.	Sí	El organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000) a cien mil pesos ($ 100.000), clausura o cancelación del archivo, registro o banco de datos.
Acciones legales	¿Existe alguna acción legal de protección de datos personales? ¿quién tiene derecho para ejercerla/ solicitarla?	Sí	La legislación contempla la acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado. Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.
Delegado o responsable de la protección de datos personales	¿Existe la figura del delegado de protección de datos (DPO) o similar? En dicho caso, ¿su designación es obligatoria? ¿debe ser designado localmente?	No	La ley no establece un requisito para designar un oficial de protección de datos.
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	La AAIP deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos. A su vez, puede controlar e imponer las sanciones administrativas.
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (ej. GDPR)? ¿Qué diferencias relevantes encuentra?	No	La normativa argentina no contempla todos los requisitos receptados por la normativa internacional. En este sentido, ya se presentaron ante el congreso proyectos para modificar la ley y adecuarla a los estándares internacionales.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Otras obligaciones	¿Existen otras consideraciones/ requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	N/A	

Brasil

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Normativa	¿Existe una ley de protección de datos personales en el país? En ese caso, identificar normativa aplicable.	Sí	La protección de datos personales se regula en: ‣ Ley General de Protección de Datos de Brasil ("LGPD"), Ley Federal Nº 13.709/2018. ‣ Modifica Ley, a la LGPD, Nº 13.853/2019. ‣ Modifica Ley, a la LGPD, Nº 14.010/2020. ‣ Decreto 10.474/2020 Adicionalmente, hay importantes instrumentos regulatorios sancionados por la Autoridad Nacional de Protección de Datos ("ANPD") tales como las Resoluciones CD/ANDP Nº 1/2021 y Nº 2/2022.
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su Sitio Web.	Sí	Actualmente, la principal autoridad estatal involucrada en la supervisión de los problemas de protección de datos personales es la Autoridad Nacional de Protección de Datos y su sitio web https://www.gov.br/anpd/
Ámbito de aplicación	¿Cuál es el ámbito de aplicación de la norma? Es decir, ¿su aplicación es estrictamente territorial, o aplica el concepto de extraterritorialidad?	Sí	La Artículo 3 de la LGPD establece que la ley se aplica a cualquier operación de procesamiento realizada por una persona física o jurídica regida por el derecho público o privado, independientemente del medio, del país en el que se encuentra su sede o del país en el que se encuentran los datos, proporcionados por el procesamiento, el propósito del procesamiento o los datos personales procesados de las personas ubicadas o recopiladas en el territorio brasileño. Artículo 3 de la LGPD: Se aplica a cualquier operación de tratamiento realizada por una persona física o por una persona jurídica de derecho público o privado, independientemente del medio, el país de su sede social o el país donde se encuentren los datos, siempre que: I - la operación de procesamiento se realice en el territorio nacional; II - el propósito de la actividad de procesamiento es ofrecer o suministrar bienes o servicios o procesar datos de personas ubicadas en el territorio nacional; o III - los datos personales tratados han sido recabados en el territorio nacional.
Recolección de datos	¿Cuáles son los requisitos o procesos legales exigidos para la recolección de datos personales? (por ejemplo, consentimiento del titular de los datos, proporcionar información sobre la finalidad del uso de los datos y derechos de su titular, entre otros).	Si	El tratamiento de los datos personales se realizará de buena fe y estará sujeto a los siguientes principios (Artículo 6): I. Finalidad. II. Idoneidad. III. Necesidad. IV. Acceso gratuito. V. Calidad de los datos. VI. Transparencia. VII. Seguridad. VIII. Prevención. IX. No discriminación. X. Rendición de cuentas. El tratamiento de los datos personales de los menores se llevará a cabo con el consentimiento específico y separado de al menos uno de los progenitores o del tutor legal. Los datos personales de los niños pueden recopilarse sin el consentimiento siempre que la recopilación sea necesaria para ponerse en contacto con los padres o el tutor legal. (Artículo 14). Además, el artículo 7 de la LGPD: El tratamiento de los datos personales sólo podrá llevarse a cabo cuando exista al menos una de las siguientes hipótesis autorizantes: I - mediante el consentimiento del titular; II - para el cumplimiento de la obligación legal o reglamentaria por parte del controlador; III. Por la administración pública, para el tratamiento y uso compartido de los datos necesarios para la ejecución de las políticas públicas previstas en las leyes y reglamentos o respaldadas por contratos, convenios o instrumentos similares, en cumplimiento de lo dispuesto en el Capítulo IV de esta Ley; IV - para la realización de estudios por parte del organismo de investigación, garantizando, siempre que sea posible, la anonimización de los datos personales; V - cuando sea necesario para la ejecución de un contrato o procedimientos preliminares relacionados con el contrato en el que el titular es parte, a petición del interesado; VI- para el ejercicio regular de derechos en procedimientos judiciales, administrativos o arbitrales, estos últimos conforme a la Ley Nº 9.307 de 23 de septiembre de 1996 (Ley de Arbitraje);

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
			VII - para la protección de la vida o la seguridad física del titular o de un tercero; VIII - para la protección de la salud, en un procedimiento realizado por profesionales de la salud o por entidades de salud; VIII. Para la protección de la salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridad sanitaria; IX - cuando sea necesario para satisfacer los intereses legítimos del controlador o de un tercero, excepto cuando prevalezcan los derechos y libertades fundamentales del interesado; O X - para la protección del crédito, incluso en lo que respecta a las disposiciones de la legislación pertinente.
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	De acuerdo con el LGPD, los datos personales consisten en la información relacionada con una persona física identificada o identificable. (Artículo 5).
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	La LGPD define dos categorías de datos en la Artículo 5: ‣ Datos sensibles como datos relacionados a orígenes raciales o étnicos, creencias religiosas, opiniones políticas, participación en sindicatos u organizaciones religiosas, políticas o filosóficas, datos relativos a la salud y vida sexual, información genética o biométrica, cuando sean en relación a una persona física. ‣ Datos anonimizados como datos relativos a un interesado que no pueda ser identificado, teniendo en cuenta el uso de medios técnicos razonables disponibles en el momento del tratamiento de los mismos. Además, de acuerdo al artículo 12 de la LGPD, los datos anonimizados no son considerados datos personales (excepto cuando el proceso de anonimización al que fueron sometidos es revertido, utilizando exclusivamente medios propios, o cuando, con esfuerzos razonables, pueda ser revertido). Además: el artículo 14 define procedimientos específicos para el procesamiento de datos personales de niños, niñas y adolescentes.
Situación de las sociedades y otras personas jurídicas	¿Alcanza la protección de la normativa en materia de datos personales, de las personas jurídicas o de existencia ideal?	No	N/A
Consentimiento del titular de los datos	¿Se requiere la obtención previa del consentimiento del titular de los datos cuando se recaba su información? En tal caso, ¿existen condiciones para la obtención del consentimiento del titular de los datos? (por ejemplo, información previa que deba proporcionarse al titular de los datos).	Sí	El consentimiento previo del titular de los datos es una de las diez hipótesis de autorización para el tratamiento de datos personales previstas en el artículo 7 de la LGPD. Si la base legal más adecuada (hipótesis autorizante) es el consentimiento, debe recopilarse de forma libre, informada e inequívoca asegurándose de que los interesados aceptan el procesamiento de sus datos personales para un propósito específico. El consentimiento debe proporcionarse por escrito o por cualquier otro medio que demuestre la manifestación de voluntad del interesado. También debe remitirse a fines definidos, y las autorizaciones genéricas serán nulas (Artículo 8).

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de los datos? En caso afirmación, identifique las excepciones.	Sí	Se renuncia al requisito de consentimiento para los datos manifiestamente hechos públicos por el interesado, salvaguardando los derechos del interesado y los principios previstos en esta Ley (Sección 7, Punto 4). Además, el artículo 7 de la LGPD trae otras 9 hipótesis de autorización para el tratamiento de datos que prescinde del consentimiento: II - para el cumplimiento de la obligación legal o reglamentaria por parte del responsable del tratamiento; III. Por la administración pública, para el tratamiento y uso compartido de los datos necesarios para la ejecución de las políticas públicas previstas en las leyes y reglamentos o respaldadas por contratos, convenios o instrumentos similares, en cumplimiento de lo dispuesto en el Capítulo IV de esta Ley; IV - para la realización de estudios por parte del organismo de investigación, garantizando, siempre que sea posible, la anonimización de los datos personales; V - cuando sea necesario para la ejecución de un contrato o procedimientos preliminares relacionados con el contrato en el que el titular es parte, a petición del interesado; VI. Para el ejercicio regular de derechos en procedimientos judiciales, administrativos o arbitrales, estos últimos conforme a la Ley Nº 9.307 de 23 de septiembre de 1996 (Ley de Arbitraje); VII - para la protección de la vida o la seguridad física del titular o de un tercero; VIII -Para la protección de la salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridad sanitaria; IX - cuando sea necesario para satisfacer los intereses legítimos del controlador o de un tercero, excepto cuando prevalezcan los derechos y libertades fundamentales del interesado; o X - para la protección del crédito, incluso en lo que respecta a las disposiciones de la legislación pertinente. Las hipótesis para el tratamiento de datos personales sensibles son más restringidas y se encuentran en el artículo 11 de la LGPD: Art. 11. El tratamiento de datos personales sensibles solo podrá producirse en los siguientes casos: I. Cuando el titular o su tutor legal consienta, de manera específica y destacada, para fines específicos; II - sin proporcionar el consentimiento del titular, en los casos en que sea indispensable para: a) el cumplimiento de la obligación legal o reglamentaria por parte del controlador; b) el tratamiento compartido de los datos necesarios para la ejecución, por parte de la administración pública, de las políticas públicas previstas en las leyes o reglamentos; c) la realización de estudios por parte de un organismo de investigación, garantizando, siempre que sea posible, la anonimización de los datos personales sensibles; d) el ejercicio regular de los derechos, incluso en los procedimientos contractuales, administrativos y arbitrales, estos últimos de conformidad con la Ley Nº 9.307 de 23 de septiembre de 1996 (Ley de Arbitraje); e) la protección de la vida o la seguridad física del titular o de un tercero; f) protección de la salud, en un procedimiento realizado por profesionales de la salud o por entidades sanitarias; o f) la protección de la salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridad sanitaria; o g) garantía de la prevención del fraude y la seguridad del titular, en los procesos de identificación y autenticación de registro en sistemas electrónicos, protegidos los derechos mencionados en el art. 9 de esta Ley y salvo en el caso de que prevalezcan los derechos y libertades fundamentales del titular que requieran la protección de datos personales.
Contenido y alcance de la información a validar por el titular de los datos	¿Cuál es el contenido que debe incluirse en el consentimiento? (Por ejemplo, uso o destino de datos, transferencia internacional de datos, etc.).	Sí	El interesado tiene derecho a facilitar el acceso a la información relativa al tratamiento de sus datos, que en gran medida se facilitará de manera clara, adecuada y ostensible, relativa, entre otras características previstas en el reglamento para el cumplimiento del principio de libre acceso: I – la finalidad específica del tratamiento; II – el tipo y la duración del tratamiento, observándose el secreto comercial e industrial; III. Identificación del responsable del tratamiento; IV – información de contacto del responsable del tratamiento; V – información sobre el uso compartido de los datos por parte del responsable del tratamiento y la finalidad; VI – Responsabilidades de los agentes que llevarán a cabo el tratamiento; y VII – los derechos del interesado, con mención explícita de los derechos. (Artículo 9).

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales? ¿Existen requisitos aplicables con respecto a la transferencia internacional de datos? (Ejemplo: cláusulas modelo, autorización por parte de la autoridad supervisora, entre otros).	Sí	La transferencia internacional de datos personales solo está permitida de acuerdo con las disposiciones establecidas en elArtículo 33. La transferencia internacional datos personales solo está permitida de acuerdo con las disposiciones establecidas en el Artículo 33. Artículo 33. La transferencia internacional de datos personales solo está permitida en los siguientes casos: I. Para países u organismos internacionales que proporcionen el grado de protección de datos personales adecuado a lo dispuesto en la Ley; II - cuando el responsable del tratamiento ofrezca y acredite garantías de cumplimiento de los principios, derechos del titular y el régimen de protección de datos previsto en la Ley, en la forma de: a) cláusulas contractuales específicas para una transferencia determinada; b) cláusulas contractuales tipo; c) normas corporativas mundiales; d) sellos, certificados y códigos de conducta expedidos periódicamente; III - cuando la transferencia sea necesaria para la cooperación jurídica internacional entre los organismos de inteligencia pública, investigación y persecución de conformidad con los instrumentos del derecho internacional; IV - cuando la transferencia sea necesaria para la protección de la vida o la seguridad física del titular o de un tercero; V - cuando la autoridad nacional autorice la transferencia; VI - cuando la transferencia resulte en un compromiso asumido en un acuerdo de cooperación internacional; VII.- Cuando la transferencia sea necesaria para la ejecución del orden público o atribución legal del servicio público, dándose publicidad de conformidad con el inciso I del caput del art. 23 de la Ley; VIII. Cuando el titular haya prestado su consentimiento específico y destacado la transferencia, con información previa sobre el carácter internacional de la operación, distinguiéndola claramente de otros fines; o IX. Cuando sea necesario para atender las hipótesis previstas en los incisos II, V y VI del art. 7 de la Ley.
BCR	¿Tienen reglas corporativas vinculantes (BCR)?	Sí	La LGPD prevé las reglas corporativas globales. Estos deben ser aprobados por la ANPD. (Artículo 35).

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Datos Sensibles	¿Qué se entiende por dato sensible? ¿Cómo es el tratamiento de los datos sensibles, de corresponder?	Sí	El concepto de datos sensibles se expresa en el apartado 5 de la LGPD. Los datos personales sensibles están previstos por la ley: datos personales sobre origen racial o étnico, convicciones religiosas, opinión política, afiliación a un sindicato u organización de carácter religioso, filosófico o político, dados en relación con la salud o la vida sexual, datos genéticos o biométricos, cuando estén vinculados a una persona física; las hipótesis para el tratamiento de datos personales sensibles son más restringidas y están previstas en el artículo 11 de la LGPD: Art. 11. El tratamiento de datos personales sensibles solo podrá producirse en los siguientes casos: I. Cuando el titular o su tutor legal consienta, de manera específica y destacada, para fines específicos; II - sin proporcionar el consentimiento del titular, en los casos en que sea indispensable para: a) el cumplimiento de la obligación legal o reglamentaria por parte del controlador; b) el tratamiento compartido de los datos necesarios para la ejecución, por parte de la administración pública, de las políticas públicas previstas en las leyes o reglamentos; c) la realización de estudios por parte de un organismo de investigación, garantizando, siempre que sea posible, la anonimización de los datos personales sensibles; d) el ejercicio regular de los derechos, incluso en los procedimientos contractuales, administrativos y arbitrales, estos últimos de conformidad con la Ley Nº 9.307 de 23 de septiembre de 1996 (Ley de Arbitraje); e) la protección de la vida o la seguridad física del titular o de un tercero; f) protección de la salud, en un procedimiento realizado por profesionales de la salud o por entidades sanitarias; o f) la protección de la salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridad sanitaria; o g) garantía de la prevención del fraude y la seguridad del titular, en los procesos de identificación y autenticación de registro en sistemas electrónicos, protegidos los derechos mencionados en el art. 9 de esta Ley y salvo en el caso de que prevalezcan los derechos y libertades fundamentales del titular que requieran la protección de datos personales.
Registro de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (por ejemplo, ante el organismo de ejecución correspondiente) una base de datos y/o la titularidad, tratamiento y/o uso de la misma? ¿Existe la obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	No	No existe una obligación general de hacer una notificación previa a la ANPD sobre los detalles de las actividades de procesamiento regulares.
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	Sí	Los agentes del tratamiento adoptarán medidas de seguridad, técnicas y administrativas que puedan proteger los datos personales de accesos no autorizados y situaciones accidentales o ilícitas de destrucción, pérdida, modificación, comunicación o cualquier forma de tratamiento inadecuado o ilícito. Las medidas técnicas pueden incluir la anonimización (Artículo 46 y 48).

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Ejemplo: rectificación, actualización o supresión). Identificar y explicar.	Sí	Los derechos de los titulares de los datos a los que se hace referencia en la LGPD como personas totalmente naturales se aseguran la propiedad de sus datos personales y la garantía de los derechos fundamentales a la libertad, la intimidad y la privacidad, de conformidad con las disposiciones de la LGPD, los interesados tienen derecho a obtener del controlador, en relación con los datos de los interesados procesados por dicho controlador, en cualquier momento y previa solicitud: ‣ Confirmación de la existencia del tratamiento. ‣ Acceso a los datos. ‣Corrección de datos incompletos, inexactos u obsoletos. ‣ Anonimización, bloqueo o eliminación de datos innecesarios o excesivos o de datos tratados en incumplimiento de lo dispuesto en la LGPD. ‣ Portabilidad de los datos a otros prestadores de servicios o proveedores de producto, previa solicitud, y observando los secretos empresariales e industriales, de acuerdo con la normativa del organismo de control. ‣ Eliminación de los datos personales tratados con el consentimiento de los interesados. ‣ Información de las entidades públicas y privadas con las que el responsable del tratamiento realizó el uso compartido de los datos. ‣ Información sobre la posibilidad de no dar su consentimiento y sobre las consecuencias de la denegación. ‣Revocación del consentimiento. (Artículos 17 y 18).
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	Los interesados tienen derecho a presentar una petición en relación con sus datos contra el controlador ante la autoridad de control. (Artículo 18). Previa solicitud al controlador.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Cesión de datos	¿Cuáles son los requisitos para la cesión de datos personales?	Sí	La información relativa a una persona física identificada o identificable puede ser transferida previo a su consentimiento y deberá observar la buena fe y los principios ya mencionados en la recogida de datos. (Artículo 5) **Artículo 7, § 5 de la LGPD:** El controlador que obtuvo el consentimiento mencionado en el punto I del caput de este artículo que necesite comunicar o compartir datos personales con otros controladores deberá obtener el consentimiento específico del titular para este fin, sujeto a las posibilidades de renuncia al consentimiento previstas en esta Ley. Artículo 11, § 3 de la LGPD: la comunicación o uso compartido de datos personales sensibles entre controladores con el fin de obtener una ventaja económica puede estar sujeta a sellado o regulación por parte de la autoridad nacional, previa audiencia de los organismos sectoriales del Poder Público, en el ámbito de sus competencias. Artículo 11, § 4 de la LGPD: no se permite la comunicación o el uso compartido entre controladores de datos personales sensibles relacionados con la salud con el fin de obtener una ventaja económica, excepto en las hipótesis relacionadas con la prestación de servicios de salud, atención farmacéutica y atención médica, siempre que se observe el párrafo 5 de este artículo, incluidos los servicios auxiliares de diagnóstico y terapia, en beneficio de los intereses de los interesados, y para permitir: Artículo 27 de la LGPD: la comunicación o uso compartido de datos personales de una persona jurídica de derecho público a una persona de derecho privado será informada a la autoridad nacional y dependerá del consentimiento del titular, excepto: I - en el caso de renuncia al consentimiento previsto en la Ley; II - en los casos de uso compartido de datos, en los que se dará publicidad de conformidad con el punto I del art. 23 de la Ley; o III. En las excepciones contenidas en el § 1 del Art. 26 de la Ley. Párrafo único. Se regulará la información a la autoridad nacional que se ocupe del caput de dicho artículo. Artículo 37. El responsable del tratamiento y el operador realizarán un seguimiento de las operaciones de tratamiento de datos personales que lleven a cabo, especialmente cuando se basen en un interés legítimo. **Artículo 38.** La autoridad nacional podrá decidir al responsable del tratamiento la elaboración de un informe de impacto sobre la protección de los datos personales, incluidos los datos sensibles, en relación con sus operaciones de tratamiento de datos, de conformidad con el Reglamento, de conformidad con los secretos comerciales e industriales. Párrafo único. De conformidad con lo dispuesto en el caput del presente artículo, el informe debe contener, como mínimo, la descripción de los tipos de datos recopilados, la metodología utilizada para la recopilación y garantía de la seguridad de la información y el análisis del responsable del tratamiento con respecto a las medidas, salvaguardias y mecanismos de mitigación de riesgos adoptados. **Artículo 39.** El operador llevará a cabo el tratamiento de acuerdo con las instrucciones proporcionadas por el controlador, quien verificará el cumplimiento de las instrucciones y las normas sobre el tema. **Artículo 40.** La autoridad nacional podrá establecer normas de interoperabilidad para la portabilidad, el libre acceso a los datos y la seguridad, así como sobre el tiempo de almacenamiento de registros, en particular con vistas a la necesidad y la transparencia. Párrafo único. Se regulará la información a la autoridad nacional que se ocupe del caput de este artículo.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros (data processing)? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	Sí	El controlador y el procesador mantendrán registros de las operaciones de procesamiento de datos personales realizadas por ellos, especialmente cuando se basen en un interés legítimo. Además, la autoridad nacional puede determinar que el responsable del tratamiento debe preparar un informe de impacto sobre la protección de los datos personales, incluidos los datos sensibles, que haga referencia a sus operaciones de tratamiento de datos, de conformidad con la normativa, sujeto al secreto comercial e industrial. El encargado del tratamiento llevará a cabo el tratamiento de acuerdo con las instrucciones proporcionadas por el responsable del tratamiento, que verificará la obediencia de las propias instrucciones y de las normas que rigen el tema. (Artículo 37 y 38).
Conservación de datos	¿Hay obligación de retener/conservar los datos recolectados o procesados por un tiempo determinado? En dicho caso, ¿cuál es el plazo?	No	Aunque es posible encontrar períodos específicos de conservación de datos en la legislación brasileña, no existe la obligación de conservar los datos recolectados o procesados en el marco de la LGPD.
Eliminación de datos	¿Existe una obligación de eliminar los datos recolectados o procesados? En dicho caso, ¿en qué supuestos y cuál es el plazo?	Sí	Los datos personales serán eliminados tras la terminación del tratamiento de los mismos, dentro del alcance y límites técnicos de las actividades, y la conservación será autorizada para los fines mencionados en el Artículo 16. El procesamiento puede considerarse finalizado en los supuestos previstos en el Artículo 15. Artículo 15. El cese del procesamiento de los datos personales se producirá en los siguientes supuestos: I - comprobación de que la finalidad fue alcanzada o de que los datos ya no son necesarios o pertinentes para alcanzar el fin específico buscado; II - expiración del plazo de procesamiento; III - comunicación de los interesados, incluso en el ejercicio de su derecho de revocación del consentimiento previsto en el párrafo 5 del artículo 8 de la referida Ley, al amparo del interés público; u IV - orden de la autoridad de control, en caso de incumplimiento de las disposiciones de la Ley. Artículo 16. Los datos personales deberán ser eliminados tras la finalización del procesamiento de los mismos de acuerdo al alcance y los límites técnicos de las actividades, y su conservación será autorizada para los siguientes fines: I - cumplimiento de una obligación legal o reglamentaria por parte del responsable del tratamiento; II - estudios por parte de un organismo de investigación garantizando, siempre que sea posible, la anonimización de los datos personales; III - cesión a terceros, previo cumplimiento de los requisitos de procesamiento de datos establecidos en la Ley; o IV - uso exclusivo del responsable del tratamiento, siempre que los datos estén anonimizados, entendiéndose que está prohibido el acceso a los mismos por parte de terceros.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Privacy Impact Assessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (Privacy Impact Assessment)?	Sí	La LGPD tiene como uno de sus principios una obligación general de rendición de cuentas. Esto requiere la demostración y adopción de medidas efectivas capaces de demostrar el cumplimiento de la ley de protección de datos y demostrar la efectividad de estas medidas. Además, la adopción de estas medidas es un factor atenuante si se imponen sanciones. La LGPD define la evaluación de impacto de la protección de datos como una documentación del responsable del tratamiento que contiene una descripción de los procesos de tratamiento de datos personales que podrían generar riesgos para las libertades civiles y los derechos fundamentales, así como medidas, salvaguardas y mecanismos para mitigar los riesgos. Sin embargo, no hay obligación de hacer una evaluación de impacto, excepto cuando sea requerido por la ANPD. La ANPD, podrá solicitar al responsable elaborar una evaluación de impacto de protección de datos, incluyendo datos sensibles, en relación con sus operaciones de procesamiento de datos, tal como lo establece la normativa, teniendo en cuenta los secretos comerciales e industriales (Artículo 38), y a los agentes gubernamentales la publicación de la evaluación de impacto de la protección de datos personales y sugerir la adopción de normas y buenas prácticas para el procesamiento de datos personales por parte del Gobierno (Artículos 16 y 32). Además, el Artículo 10, § 3 establece que la autoridad nacional puede solicitar al controlador/responsable que informe sobre la protección de datos personales, cuando el procesamiento se base en su interés legítimo, en interés de secretos comerciales e industriales. La LGPD brinda competencia a la ANPD para modificar las regulaciones y procedimientos sobre la protección de datos personales y privacidad, así como sobre la Evaluación de Impacto (Privacy Impact Assessment) para los casos en que el procesamiento representa un alto riesgo a la garantía de los principios generales de la protección de datos personales previstos en la ley. Hasta el momento, la ANPD no cuenta con un modelo oficial al respecto
Incidentes	¿Existe la obligación de informar de un incidente de seguridad o una violación o disposiciones legales?	Sí	El responsable del tratamiento deberá informar a la autoridad nacional y al titular de la ocurrencia de un incidente de seguridad que pueda causar un riesgo o daño significativo a los titulares. La comunicación se realizará en un plazo razonable, según lo definido por la autoridad nacional. La ANPD verificará la gravedad del incidente y podrá, en caso necesario, para salvaguardar los derechos de los titulares, determinar el responsable del tratamiento para adoptar medidas. (Artículo 48 y 49).

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Sanciones	¿Existen sanciones por el incumplimiento de esta obligación? Si existen, identificarlos e indicar el importe de las sanciones o sanciones aplicables correspondientes.	Sí	La violación de las disposiciones de la presente LGPD dará lugar a responsabilidades administrativas. Las disposiciones de este Artículo de la LGPD no reemplazan la imposición de sanciones administrativas, civiles o penales definidas por cualquier ley brasileña específica. Los agentes de tratamiento de datos de la ANPD, en relación con cualquier infracción de las normas establecidas en la LGPD, estarán sujetos a las sanciones administrativas del artículo 52. Artículo 52. Los agentes encargados del tratamiento de datos, por infracciones cometidas a las normas previstas en la presente Ley, están sujetos a las siguientes sanciones administrativas aplicables por la autoridad nacional: I. Advertencia, con indicación de un plazo para la adopción de medidas correctoras; II - multa simple, hasta el 2% (dos por ciento) de los ingresos de la persona jurídica de derecho privado, grupo o conglomerado en Brasil en su último año fiscal, excluyendo impuestos, limitado en total a R$ 50.000.000,00 (cincuenta millones de reales) por infracción; III - multa diaria, respetando el límite total a que se refiere el punto II; IV - publicidad de la infracción después de que se haya aclarado y confirmado debidamente su ocurrencia; V - bloqueo de los datos personales a que se refiere la infracción hasta su regularización; VI - eliminación de los datos personales a los que se refiere la infracción; VII - (VETADO); VIII - (VETADO); IX - (VETADO); X - (VETADO); (Incluido en la Ley Nº 13.853, 2019) (Promulgación de partes vetadas) XI - (VETADO); (Incluido en la Ley Nº 13.853, 2019) (Promulgación de partes vetadas) XII - (VETADO); (Incluido en la Ley Nº 13.853, 2019) (Promulgación de partes vetadas) XIII - suspensión parcial del funcionamiento de la base de datos a que se refiere la infracción por un plazo máximo de 6 (seis) meses, prorrogable por el mismo período, hasta la regularización de la actividad de tratamiento por parte del responsable del tratamiento; (Incluido en la Ley Nº 13.853, 2019) XIV - suspensión del ejercicio de la actividad de tratamiento de datos personales a que se refiere la infracción por un plazo máximo de 6 (seis) meses, prorrogable por el mismo plazo; (Incluido en la Ley Nº 13.853, 2019) XV - Prohibición parcial o total del ejercicio de actividades relacionadas con el tratamiento de datos. (Incluido en la Ley Nº 13.853, 2019).

Topic	Concept	Yes / No/NA (Not Applicable)	Remarks / Comments
Acciones legales	¿Existe alguna acción legal de protección de datos personales? ¿quién tiene derecho para ejercerla/ solicitarla?	Sí	La defensa de los intereses y derechos del interesado podrá ejercerse en los tribunales, individual o colectivamente, en forma de las disposiciones de la ley aplicable (LGPD), sobre los instrumentos de protección individual y colectiva. Además, los datos personales relacionados con el ejercicio regular de los derechos por parte de los interesados no pueden utilizarse en su contra. (Artículo 21 y 22).
Delegado o responsable de la protección de datos personales	¿Existe la figura del delegado de protección de datos (DPO) o similar? En dicho caso, ¿su designación es obligatoria? ¿Debe ser designado localmente?	Sí	En LGPD la figura de DPO se define como una persona física designada por el controlador, que actúa como un canal de comunicación entre el controlador y los interesados y la autoridad de control. El responsable del tratamiento indicará un delegado de protección de datos. La identidad y los datos de contacto del DPO se divulgarán pública, clara y objetivamente, preferiblemente en el sitio web del controlador. La ANPD podrá establecer la designación obligatoria, de acuerdo con la naturaleza y el tamaño de la entidad o el volumen de las operaciones de tratamiento de datos, normas complementarias sobre la definición y las funciones del delegado de protección de datos, incluidos los casos en que no sea necesario nombrar a dicho DPO. (Artículo 41). Artículo 41, § 3 - La autoridad nacional podrá establecer normas complementarias sobre la definición y atribuciones del responsable, incluidas hipótesis de dispensa de la necesidad de su indicación, en función de la naturaleza y el tamaño de la entidad o del volumen de las operaciones de tratamiento de datos.
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	En caso de incumplimiento de la LGPD, como consecuencia del tratamiento de datos personales por parte de organismos públicos, la autoridad de control como la ANPD, podrá enviar una comunicación con las medidas aplicables para cesar la infracción. Asimismo, la Resolución CD/ANPD Nº 01/2021 prevé que la ANPD puede actuar de oficio en las tareas de control (Artículo 16).
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (ej. GDPR)? ¿Qué diferencias relevantes encuentra?	Sí	Sí, en general, la LGPD es muy similar al GDPR.
Otras obligaciones	¿Existen otras consideraciones/ requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	Sí	La LGPD establece que la ANPD estará a cargo de definir algunas disposiciones importantes para asegurar el cumplimiento de la ley. En este sentido, regulaciones futuras sobre privacidad y protección de datos personales pueden ser dictadas por la ANPD.

Chile

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Normativa	¿Existe en el país una ley de protección de datos personales? En ese caso, identificar normativa aplicable.	Sí	La protección de datos personales está regulada principalmente en la Ley Nº 19.628, sobre la protección de la vida privada ("LPDP"). Asimismo, la Ley Nº 20.575, incorpora el principio de finalidad con relación al procesamiento de datos personales de carácter económico, financiero, bancario o comercial. Por otro lado, la Constitución de la República de Chile, en su artículo 19 Nº 4, consagra el derecho a la protección de la vida privada y los datos personales, por lo que este derecho se encuentra protegido constitucionalmente.
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su Sitio Web.	Si	En la actualidad, no hay una autoridad dedicada específicamente a supervisar asuntos relacionados con la protección de datos personales. Sin embargo, recientemente se le otorgaron facultades legales al Servicio Nacional del Consumidor (SERNAC) para la fiscalización del cumplimiento de la LPDP en el contexto de relaciones de consumo. El sitio web del SERNAC se encuentra en el siguiente enlace.
Ámbito de aplicación	¿Cuál es el ámbito de aplicación de la norma? Es decir, ¿su aplicación es estrictamente territorial, o aplica el concepto de extraterritorialidad?	Sí	El ámbito de aplicación es territorial. No se prevé su aplicación fuera del país.
Recolección de datos	¿Cuáles son los requisitos o procesos legales exigidos para la recolección de datos personales? (por ejemplo, consentimiento del titular de los datos, proporcionar información sobre la finalidad del uso de los datos y derechos de su titular, entre otros).	Sí	De acuerdo al artículo 4 de la LPDP, el tratamiento de datos personales, incluyendo su recolección, debe ser autorizado por el titular de manera previa, expresa y por escrito, o por medios electrónicos equivalentes. Asimismo, el titular de los datos debe ser debidamente informado, respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	La LPDP, en su artículo 2º, define el concepto de dato personal como cualquier información concerniente a personas naturales, identificadas o identificables.
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	Las categorías de datos personales definidas en el artículo Nº 2 de la LPDP son: ‣ Dato caduco: el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna. ‣ Dato estadístico: dato que, en su origen o por su tratamiento, no puede ser asociado a un titular identificado o identificable. ‣ Datos sensibles: datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
Situación de las sociedades y otras personas jurídicas	¿Alcanza la protección de la normativa en materia de datos personales, de las personas jurídicas o de existencia ideal?	No	La definición de "dato personal" entregada por la LPDP, en su artículo 2º, se limita a la información relativa a personas naturales, dejando afuera, por tanto, a las personas jurídicas.
Consentimiento del titular de los datos	¿Se requiere la obtención previa del consentimiento del titular de los datos cuando se recaba su información? En tal caso, ¿existen condiciones para la obtención del consentimiento del titular de los datos? (por ejemplo, información previa que deba proporcionarse al titular de los datos).	Sí	De acuerdo al artículo Nº 4º de la LPDP, el procesamiento de datos personales requiere el consentimiento previo, explícito y por escrito – o por medios electrónicos equivalentes - del titular de los datos. Antes de dar su consentimiento, el interesado debe ser informado del propósito del procesamiento de datos y su posible comunicación al público.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	Las excepciones al consentimiento del titular, es decir, las ocasiones en que el responsable del tratamiento no requerirá del consentimiento del titular para el procesamiento de sus datos son: ‣ Cuando el tratamiento se encuentre autorizado por la ley. ‣ Cuando se trate de información proveniente o recolectado de fuentes accesibles al público, cuando se trate de datos de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limitan a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios. ‣ En cuanto a datos personales sensibles, no se requerirá el consentimiento del titular cuando se trate de datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.
Contenido y alcance de la información a ser validada por el titular de los datos	¿Cuál es el contenido que debe incluir el consentimiento? (Por ejemplo, uso o destino de los datos, transferencia internacional de los datos, etc.).	Sí	El titular del dato debe ser debidamente informado respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales? ¿Hay requisitos aplicables en relación a la transferencia internacional de datos? (Ejemplo: cláusulas modelos, autorización por parte de la autoridad de control, entre otros).	Sí	Si bien no existen disposiciones específicas sobre la transferencia de datos personales, las transferencias nacionales, así como las transferencias transfronterizas, están sujetas a las normas generales sobre procesamiento de datos. Por tanto, la transferencia de datos personales será legítima, por regla general, cuando ésta se base en el consentimiento otorgado de manera expresa y por escrita – o por medios electrónicos equivalentes – por el titular de los datos. Asimismo, cabe señalar que la LPDP, en su artículo 5º, admite la posibilidad de una transmisión automatizada de datos.
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	No	No está regulado en la LPDP.
Datos sensibles	¿Qué se entiende por dato sensible? ¿Cómo es el tratamiento de los datos sensibles, de corresponder?	Sí	Los datos sensibles se encuentran definidos en el artículo Nº 2º de la LPDP, son aquellos que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como: ‣ Hábitos personales ‣ Origen racial ‣ Ideologías y opiniones políticas ‣ Creencias o convicciones religiosas ‣ Condiciones de salud física o psíquica, y ‣ La vida sexual El tratamiento de datos de carácter sensible solo es legítimo cuando la ley lo autorice, cuando exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (ej. ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, tratamiento y/o uso de la misma? ¿Existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	No	La LPDP no establece ninguna obligación de registro en cuanto a las bases de datos, su titularidad, tratamiento o uso, en la medida en que éstas sean privadas. En cuando a organismos públicos, el artículo Nº 22º de la LPDP establece que el Servicio de Registro Civil e Identificación deberá llevar un registro de los bancos de datos personales a cargo de organismos públicos.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	No	La LPDP establece en su artículo Nº 11º que el responsable del tratamiento debe cuidar los datos con la debida diligencia. A su vez, el artículo 7º de la LPDP establece que las personas que trabajan en el tratamiento de datos personales, sea en el ámbito público como privado, están obligados a guardar el secreto sobre los mismos.
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Ejemplo: rectificación, actualización o supresión). Identificar y explicar.	Sí	La LPDP reconoce explícitamente los siguientes derechos a los titulares en su artículo Nº 12º: ‣ El derecho a ser informado sobre los datos relativos a su persona, su procedencia y destinario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente; ‣ El derecho a rectificar datos, esto es, a que sean modificados en caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos; ‣ El derecho a que sus datos sean eliminados o bloqueados en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos; cuando se hayan proporcionado voluntariamente o se usen para comunicaciones comerciales y el titular no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal. La información, modificación o eliminación de los datos debe ser absolutamente gratuita, debiendo proporcionarse, además, a solicitud del titular, una copia del registro alterado en la parte pertinente. Si se realizaren nuevas modificaciones o eliminaciones de datos, el titular también podrá obtener, de manera gratuita, una copia del registro actualizado, siempre que hayan transcurrido al menos 6 meses desde la última oportunidad en la que se solicitó copia del registro.
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	Con respecto al ejercicio de los derechos previamente señalados, la LPDP establece en su artículo Nº 16º que, si el responsable no se pronunciare sobre la solicitud del titular en dos días hábiles, el titular podrá recurrir ante un juez de letras en lo civil. Asimismo, el artículo Nº 23º de la LPDP señala que los responsables del tratamiento deberán indemnizar a los titulares por el daño patrimonial y moral que cause un tratamiento indebido de los datos, además de eliminar, modificar o bloquear los datos según lo solicitado por el titular o bien lo ordenado por el tribunal si corresponde. Para ello, el titular debe interponer una acción ante tribunales civiles. Finalmente, el derecho a la protección de los datos personales y la intimidad es un derecho consagrado constitucionalmente, por lo que las acciones constitucionales, como el recurso de protección, también son herramientas para ejercer los derechos de los titulares de datos, en la medida en que se hubieren visto vulnerados.
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	Sí	La cesión de datos personales se rige por las reglas generales para el procesamiento, esto es, se debe contar con la autorización expresa y por escrito – o por medios electrónicos equivalentes – del titular de los datos. Asimismo, de acuerdo al artículo Nº 5º de la LPDP, el responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión, siempre que se deje constancia de: a) La individualización del requirente; b) El motivo y el propósito del requerimiento, y c) El tipo de datos que se transmiten.
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros (data processing)? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	Sí	Sí se pueden prestar servicios de procesamiento de datos por cuenta de terceros. De acuerdo al artículo Nº 8º de la LPDP, en el caso que se procesen datos por mandato, se aplicarán las reglas generales del mismo. Adicionalmente, el mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Conservación de datos	¿Hay obligación de retener/conservar los datos recolectados o procesados por un tiempo determinado? En dicho caso, ¿cuál es el plazo?	No	La LPDP no establece un plazo específico para retener/conservar los datos. Sin embargo, el artículo N° 6° de la LPDP establece que los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado.
Eliminación de datos	¿Existe una obligación de eliminar los datos recolectados o procesados? En dicho caso, ¿en qué supuestos y cuál es el plazo?	Sí	De acuerdo al artículo N° 6° de la LPDP, los datos personales deberán ser eliminados o cancelados cuando su almacenamiento no tenga una base legal o cuando haya expirado
Privacy Impact Asessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (Privacy Impact Assessment)?	No	La LPDP no regula las evaluaciones de impacto.
Incidentes	¿Hay obligación de reportar un incidente de seguridad u algún incumplimiento a las previsiones legales?	No	La LPDP no provee ninguna obligación de reporte de incidentes de seguridad. Por su parte, la LPDP solo contempla una obligación general de seguridad de datos que le impone al responsable de la base de datos en su artículo N° 11°: "cuidar de ellos con la debida diligencia, haciéndose responsable de los daños". Esta obligación no contiene medidas concretas de seguridad que deban aplicarse por el responsable.
Sanciones	¿Existen sanciones frente al incumplimiento de dicha obligación? En caso de existir, identificarlas e indicar el monto de las sanciones o penalidad aplicable correspondiente.	No	Por regla general la LPDP no establece sanciones ni multas asociadas al incumplimiento de obligaciones legales. La única multa establecida en la LPDP se encuentra en su artículo N° 16°, que señala que en caso de acogerse la reclamación ante tribunales por la falta de pronunciamiento del responsable ante el ejercicio de derechos de los titulares, el tribunal podrá aplicar una multa de aproximadamente USD 65 a USD 650 (1 a 10 Unidades Tributarias Mensuales). Con todo, de acuerdo al artículo N° 23 de la LPDP, los responsables del tratamiento deben indemnizar el daño patrimonial y moral causado por el tratamiento indebido de datos personales, además de eliminar, modificar o bloquear los datos según sea solicitado por el titular u ordenado por tribunales. No obstante, para ello será necesaria la presentación de una acción ante tribunales civiles por parte del titular.
Acciones legales	¿Existe alguna acción legal de protección de datos personales? ¿quién tiene derecho para ejercerla/ solicitarla?	Sí	De conformidad con lo señalado previamente, el artículo N° 23° de la LPDP, establece que los responsables del tratamiento deben indemnizar el daño patrimonial y moral causado por el tratamiento indebido de datos personales, además de eliminar, modificar o bloquear los datos según sea solicitado por el titular u ordenado por tribunales. No obstante, para ello será necesaria la presentación de una acción ante tribunales civiles por parte del titular. a Por otro lado, dado que la protección de datos personales y la privacidad es un derecho consagrado constitucionalmente, también existe la posibilidad de interponer la acción de protección constitucional, que tiene por objetivo que la Corte ordene todas las medidas necesarias para reestablecer el derecho vulnerado y asegurar su protección.
Delegado o responsable de la protección de datos personales	¿Existe la figura del delegado de protección de datos (DPO) o similar? En dicho caso, ¿su designación es obligatoria? ¿Debe ser designado localmente?	No	La LPDP no establece la figura del DPO. No obstante, la Ley N° 20.575, de finalidad en el uso de los Datos Personales, en su artículo 4, establece que los responsables de tratamiento de datos que procesan datos económicos, financieros, bancarios y comerciales deberán designar a una persona física como oficial de protección de datos ante quien los titulares pueden ejercer los derechos que les otorga la LPDP.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	N/A	
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (ej. GDPR)? ¿Qué diferencias relevantes encuentra?	No	La LPDP data del año 1999 y, si bien ha sufrido algunas reformas, aún dista mucho de los estándares comúnmente incorporados en normas internacionales como el GDPR. Si bien la LPDP contiene estándares exigentes teóricamente (se requiere el consentimiento expreso y por escrito de los titulares), la inexistencia de otras fuentes de legitimidad, la falta de una autoridad competente exclusivamente dedicada a fiscalizar esta materia y la ausencia de multas y procedimientos administrativos que faciliten el ejercicio de los derechos de los titulares de datos, en concreto ha significado que el cumplimiento de la LPDP sea prácticamente inexistente. Por ejemplo, no regula las mismas bases legales ni principios para el tratamiento de datos, no establece obligaciones precisas al responsable del tratamiento, no hay autoridad a cargo de la materia, no considera sanciones, ni consagra el derecho de portabilidad de los datos, entre otras diferencias. Finalmente, es importante destacar que actualmente, se encuentra en tramitación un proyecto de ley que modifica la actual LDPD y que incorpora estándares de protección muy similares al GDPR. El contenido de este proyecto de ley se encuentra mayoritariamente zanjado y existe bastante transversalidad en el mundo político respecto de él. Alguna de sus novedades sería la creación de una Agencia para la Protección de Datos Personales, el establecimiento de multas por incumplimiento, la incorporación de nuevas fuentes de legitimidad (interés legítimo, cumplimiento contractual, consentimiento tácito, etc.), la incorporación del derecho de portabilidad, entre otras. Asimismo, es un proyecto que ha sido calificado como prioritario para el gobierno actual, por lo que se espera que su tramitación avance para que sea prontamente aprobado.
Otras obligaciones	¿Existen otras consideraciones/ requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	N/A	

Colombia

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Normativa	¿Existe en el país una ley de protección de datos personales? En ese caso, identificar normativa aplicable.	Sí	La normativa colombiana en materia de protección de datos se detalla a continuación: ‣ Arts. 15 y 20, Constitución Política de Colombia. ‣ Ley Estatutaria Nro. 1266/2008 (“Ley 1266”) ‣ Decreto Nro. 2952/10 (“Dec. 2952”), compilado en el Decreto Nro. 1074 de 2015 (“Dec. 1074) ‣ Decreto Nro. 1727/2009 (“Dec. 1727”), compilado en el Decreto Nro. 1074 de 2015 (“Dec. 1074) ‣ Ley 1273 de 2009 (“Ley 1273”) ‣ Ley Estatutaria Nro. 1581/2012 (“Ley 1581”) ‣ Decreto Nro. 1377/2013 (“Dec. 1377”), compilado en el Decreto Nro. 1074 de 2015 (“Dec. 1074) ‣ Ley Nro. 1712/2014 (“Ley 1712”) ‣ Decreto Nro. 886/2014 (“Dec. 886”), compilado en el Decreto Nro. 1074 de 2015 (“Dec. 1074) ‣ Ley Nro. 1928/2018 (“Ley 1928”) ‣ Decreto 090 de 2018 (“Dec. 090”) ‣ Decreto Nº 255/2022 (“Dec. 255”) por el cual se adiciona el artículo 7 al Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Dec. 1074. ‣ Circular Única Jurídica de la Superintendencia de Industria y Comercio
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su Sitio Web.	Sí	La Superintendencia de Industria y Comercio es la autoridad nacional de protección de la competencia, los datos personales y la metrología legal, protege los derechos de los consumidores y administra el Sistema Nacional de Propiedad Industrial, a través del ejercicio de sus funciones administrativas y jurisdiccionales. https://www.sic.gov.co/tema/proteccion-de-datos-personales
Ámbito de aplicación	¿Cuál es el ámbito de aplicación de la norma? Es decir, ¿su aplicación es estrictamente territorial, o aplica el concepto de extraterritorialidad?	Sí	Será aplicable a todos aquellos datos personales susceptibles de tratamiento en el territorio colombiano, por entidades tanto de naturaleza pública como privada, o cuando al responsable o encargado del tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. Art. 2, Ley 1581.
Recolección de datos	¿Cuáles son los requisitos o procesos legales exigidos para la recolección de datos personales? (por ejemplo, consentimiento del titular de los datos, proporcionar información sobre la finalidad del uso de los datos y derechos de su titular, entre otros).	Sí	Por regla general se requiere la autorización previa, expresa e informada del titular para el tratamiento de datos personales, a no ser que se trate de datos personales de naturaleza pública, o que se configure alguna otra excepción de las consagradas en el artículo 10 de la Ley 1581. Las regulaciones y requisitos establecidos para la recolección de datos bajo la normativa colombiana se encuentran dispuestos en el artículo 12 de la Ley 1581 y los artículos 4, 5, 6 y 7 del Decreto 1377.
Concepto legal de “dato personal”	¿Qué se entiende por dato personal?	Sí	Se considera “dato personal” a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Art. 3, inc. c), Ley 1581.

1. Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Art. 3, inc. g) - Ley 1581/2012)

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	La normativa establece cinco categorías diferentes de datos: ▸ **Datos personales:** considerado como cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. ▸ **Datos personales financieros:** cualquier pieza de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, referida al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen y que sea vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. ▸ **Datos públicos:** el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas. ▸ **Dato semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios. ▸ **Dato privado:** es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. Incluye los datos sensibles. ▸ **Datos sensibles:** son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos. Arts. 3 inc. c) y 5, Ley 1581 y Art. 3, inc. 2), Dec. 1377.
Situación de las sociedades y otras personas jurídicas	¿Alcanza la protección de la normativa en materia de datos personales, de las personas jurídicas o de existencial ideal?	Sí	La normativa en materia de datos personales únicamente protege la información de las personas jurídicas en relación a su información financiera, comercial y de cumplimiento de obligaciones dinerarias, al tenor de la Ley 1266.
Consentimiento del titular de los datos	¿Se requiere la obtención previa del consentimiento del titular de los datos cuando se recaba su información? En tal caso, ¿existen condiciones para la obtención del consentimiento del titular de los datos? (por ejemplo, información previa que deba proporcionarse al titular de los datos).	Sí	Se requiere la autorización previa, expresa e informada del titular. La misma deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior, como medios escritos, verbales o conductas inequívocas. Para la recolección de datos sensibles únicamente podrá hacerse uso de medios escritos o verbales. La SIC ha hecho énfasis en que el silencio del titular no puede en ningún caso ser entendido como el otorgamiento de la autorización mediante una conducta tácita o inequívoca, y que bajo ninguna circunstancia puede confundirse el aviso de privacidad con la autorización previa, expresa e informada, dado que este primero tiene finalidades sustancialmente diferentes a las de una autorización y, por lo tanto, de ninguna manera la suple (cf. Resolución número 59001 de 2020 de la SIC -Radicación 19-47344-). Arts. 3, inc. a), 4, inc. c) y 9, Ley 1581y el Art. 5, Dec. 1377.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	La autorización del titular del dato no será necesaria cuando se trate de los supuestos detallados a continuación: (i) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial. (ii) Datos de naturaleza pública. (iii) Casos de urgencia médica o sanitaria. (iv) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos. (v) Datos relacionados con el Registro Civil de las Personas. La transmisión internacional de datos personales (entre un responsable y un encargado) no requerirá ser informada al titular ni contar con su consentimiento cuando exista entre responsable y encargado, un contrato que se sujete a los términos dispuestos en el artículo 2.2.2.25.5.2., del Dec. 1074. Art. 10, Ley 1581 Art. 2.2.2.25.5.1. Dec. 1074.
Contenido y alcance de la información a ser validada por el titular de los datos	¿Cuál es el contenido que debe incluir el consentimiento? (Por ejemplo, uso o destino de los datos, transferencia internacional de los datos, etc.).	Sí	El responsable del tratamiento al momento de solicitar al titular la autorización, deberá informarle de manera clara y expresa lo siguiente: (i) El tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; (ii) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes; (iii) Los derechos que le asisten como titular; (iv) La identificación, dirección física o electrónica y teléfono del Responsable del tratamiento. Art. 12, Ley 1581 de 2012, Art. 7, Dec. 1377 y Arts. 2.2.2.25.2.3 y 2.2.2.25.2.4 del De. 1074.
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales? ¿Hay requisitos aplicables en relación a la transferencia internacional de datos? (Ejemplo: cláusulas modelos, autorización por parte de la autoridad de control, entre otros).	Sí	La Ley 1581 en su artículo 26, prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la SIC sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la ley exige a sus destinatarios, según lo establecido en el Art. 3, inc. 3.1 de la Circular Externa N°.005 Bogotá D.C. Esta prohibición no regirá cuando se trate de: a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia; b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública; c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable; d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad; e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular; f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

2. https://www.sic.gov.co/sites/default/files/normatividad/082017/Circular_Externa_005_de_2017.pdf

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
			En los casos no contemplados como excepción, corresponderá a la SIC, proferir una declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente está facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación. Las anteriores disposiciones son aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266. Art. 26, Ley 1581 y Art. 3, inc. 3.1, 3.2 y 3.3), Circular Externa No. 005 Bogotá D.C ,
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	Sí	La Ley 1581, en el artículo 27, establece que es facultad del Gobierno Nacional expedir la reglamentación correspondiente a Normas Corporativas Vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países. El Decreto 255 establece las condiciones mínimas de las Normas Corporativas Vinculantes ("NCV"), las cuales pueden ser adoptadas por los grupos empresariales que realicen transferencia de datos personales a un responsable del mismo grupo, fuera del territorio colombiano. Las NCV corresponden a las políticas, principios de buen gobierno o códigos de buenas prácticas empresariales de obligatorio cumplimiento asumidas por el responsable del tratamiento de datos personales que se encuentre establecido en el territorio colombiano, para realizar transferencias o un conjunto de transferencias de este tipo de datos a un responsable que se encuentre ubicado por fuera del territorio colombiano y que haga parte de su mismo grupo empresarial. Estas normas se materializan mediante sistemas de autorregulación que confieren derechos a los titulares de información personal e imponen deberes y obligaciones en cabeza del grupo empresarial y cada uno de sus miembros. Todas las empresas del grupo empresarial y cada uno de sus miembros serán solidariamente responsables del cumplimiento de las NCV, por lo que la SIC está facultada a requerir, investigar y sancionar al responsable del tratamiento que se encuentre establecido en Colombia, por aquellas infracciones que cometa cualquiera de los miembros del grupo empresarial. La SIC está facultada para aprobar las NCV que (i) sean jurídicamente vinculantes y se apliquen a todos los miembros que hacen parte del mismo grupo empresarial; (ii) confieran expresamente a los titulares de los datos la facultad de ejercer los derechos previstos en las normas aplicables; y (iii) cumplan los requisitos establecidos en el Decreto 255. Las NCV solo podrán ser sometidas a la autorización de la SIC cuando hayan sido aprobadas por el órgano corporativo competente, de conformidad con los estatutos de la sociedad respectiva o los acuerdos del grupo empresarial. Por lo tanto, estas normas solo podrán ser implementadas en el momento en que hayan surtido su trámite corporativo y la SIC haya posteriormente aprobado su contenido y emitido la certificación de buenas prácticas, esto último debiendo informarse en la página web del responsable del tratamiento. Las NCV no serán de obligatorio cumplimiento cuando el grupo empresarial aplique otros mecanismos de transferencia de datos establecidos en la legislación colombiana, como por ejemplo las declaratorias de conformidad expedidas por la SIC. Art 27, Ley 1581 y Arts. 3, inc.4) y 5), 24 y 25, Dec. 1377. A su vez Compilados en los arts. 2.2.2.25.1.3, 2.2.2.25.5.1 y 2.2.2.25.2.2 de Dec. 1074, respectivamente. Dec. 255.

2. https://www.sic.gov.co/sites/default/files/normatividad/082017/Circular_Externa_005_de_2017.pdf

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Datos sensibles	¿Qué se entiende por dato sensible? ¿Cómo es el tratamiento de los datos sensibles, de corresponder?	Sí	Se entiende por dato sensible a aquel que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos. En cuanto a su tratamiento, el mismo se encuentra regulado en el art. 6 de la Ley 1581 y art. 6 del Dec. 1377. A su vez Compilado en el art. 2.2.2.25.2.3 del Dec. 1074. Igualmente, la Superintendencia de Industria y Comercio ha señalado que deben tomarse medidas de seguridad reforzada frente a estos datos. Arts. 5 y 6, Ley 1581 y Art. 6, Dec. 1377.
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (ej. ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, tratamiento y/o uso de la misma? ¿Existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	Sí	El responsable del tratamiento tiene la obligación de inscribir y actualizar ante el Registro Nacional de Bases de Datos (RNBD) administrado por la Superintendencia de Industria y Comercio, cada una de las bases de datos que contengan datos personales sujetos a tratamiento, siempre que se trate de una sociedad o entidad sin ánimo de lucro que tenga activos totales superiores a 100.000 Unidades de Valor Tributario (UVT). También están obligadas a dicho registro y actualización las personas jurídicas de naturaleza pública. Para ello, deberán aportar la información dispuesta en el art. 5 del Dec. 866. A su vez Compilado en el art. 2.2.2.26.2.1 del Dec. 1074. Si bien no existe obligación de presentar informes periódicos ante el Registro Nacional de Base de Datos, los responsables deberán actualizar la información inscrita cuando haya cambios sustanciales. Los cambios no sustanciales deben ser actualizados entre el 2 de enero y el 31 de marzo de cada año. Art. 25, Ley 1581 y Arts. 3, 5, 6 y 14, Dec. 866. A su vez Compilados en los arts. 2.2.2.26.1.3, 2.2.2.26.1.4 y 2.2.2.26.2.2 del Dec. 1074, respectivamente.
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	Sí	No existen medidas de seguridad expresas en la normativa vigente en la materia. Sin embargo, todas las empresas y entidades públicas están obligadas a implementar las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento y a conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Siguiendo esta línea, si bien no constituyen medidas de seguridad en sí, los responsables del tratamiento de datos están obligados a desarrollar "Políticas de Tratamiento" de datos personales y velar porque los encargados del tratamiento también las cumplan. Las Políticas de Tratamiento deben desarrollarse conforme lo dispuesto en el art. 13 del Dec. 1377. Arts. 4, inc. g), 17, inc. d), Ley 1581 y Arts. 13, 19 y 26, Dec. 1377. A su vez Compilados en los arts. 2.2.2.25.3.1, 2.2.2.25.3.7 y 2.2.2.25.6.1 del Dec. 1074, respectivamente.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Ejemplo: rectificación, actualización o supresión). Identificar y explicar.	Sí	Los titulares de los datos personales poseen los siguientes derechos: (i) Conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento. (ii) Solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento la obtención de la autorización. (iii) Ser informado por el responsable del tratamiento o el encargado del tratamiento. (iv) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen. (v) Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. (vi) Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento. Adicionalmente, la Ley 1581 en su art. 7, hace referencia a los derechos de los niños, niñas y adolescentes con relación al tratamiento de datos, determinando que queda proscrito el tratamiento de datos personales de estos, salvo aquellos datos que sean de naturaleza pública y cuando dicho tratamiento cumpla con determinados requisitos. Arts. 7 y 8, Ley 1581 y Art. 12, Dec. 1377. A su vez, Compilado en el art. 2.2.2.25.2.9, del Dec. 1074.
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	Los titulares o sus causahabientes podrán ejercer los derechos que estos poseen en materia de protección de datos, conforme se establece en los arts. 14 y 15 de la Ley 1581 y art. 20 y 21 del Dec. 1377. Para ello podrán interponer consultas o reclamos ante el responsable y/o encargado. En caso de no atenderse las mismas en los términos de ley, podrán interponerse quejas ante la Superintendencia de Industria y Comercio y finalmente recurrir a la acción de tutela ante un juez de la República. Arts. 14 y 15, Ley 1581 y Arts. 20 y 21 Dec. 1377. A su vez, compilados en los arts. 2.2.2.25.4.1 y 2.2.2.25.4.2 del Dec. 1074, respectivamente.
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	N/A	La normativa en materia de protección de datos no regula el instituto de la cesión de datos personales. Únicamente hace referencia a la transferencia y transmisión nacional o internacional de datos personales.
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros (data processing)? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	Sí	La normativa en materia de datos personales contempla la figura del "encargado del tratamiento". Esta podrá ser cualquier persona natural o jurídica, pública o privada que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento. Si bien no existe un procedimiento específicamente regulado para esta figura, se detallan los deberes que estos deben cumplir se encuentran detallados en el art. 18 de la Ley 1581. Art. 3, inc. d) y 18, Ley 1581. A su vez en art. 2.2.2.25.5.1 y 2.2.2.25.5.2 del Dec. 1075

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Conservación de datos	¿Hay obligación de retener/conservar los datos recolectados o procesados por un tiempo determinado? En dicho caso, ¿cuál es el plazo?	No	Únicamente existe tal obligación cuando así se requiera para el cumplimiento de una obligación legal o contractual. Art. 11 Dec. 1377. A su vez compilado en el art. 2.2.2.25.2.8, del Dec. 1074.
Eliminación de datos	¿Existe una obligación de eliminar los datos recolectados o procesados? En dicho caso, ¿en qué supuestos y cuál es el plazo?	Sí	Tanto los responsables como los encargados podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento. Una vez cumplida la o las finalidades del tratamiento y sin perjuicio de normas legales que dispongan lo contrario, el responsable y el encargado deberán proceder a la supresión de los datos personales en su posesión. Art. 11 Dec. 1377. A su vez, compilado en el art. 2.2.2.25.2.8, del Dec. 1074.
Privacy Impact Asessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (Privacy Impact Assessment)?	No	Por el momento, es la Superintendencia de Industria y Comercio ("SIC") quien ha sugerido en sus Guías sobre el tratamiento de datos personales que cuando se prevea un alto riesgo de afectación del derecho a la protección de datos personales de los Titulares, se efectúe una evaluación de impacto en la privacidad (Privacy Impact Assessment - PIA por sus siglas en inglés), con el fin de poner en funcionamiento un sistema efectivo de manejo de riesgos y controles internos, para garantizar que los datos se tratarán debidamente y conforme con la regulación existente. La SIC indica que dicha evaluación debería incluir, como mínimo, lo siguiente: (i) Una descripción detallada de las operaciones de Tratamiento de Datos Personales que involucra el proyecto de la Compañía y (ii) Una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los datos personales. La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos, son elementos cardinales del Principio de Responsabilidad Demostrada.
Incidentes	¿Hay obligación de reportar un incidente de seguridad u algún incumplimiento a las previsiones legales?	Sí	Constituye una obligación tanto para los responsables como los encargados del tratamiento de datos personales, independientemente de que el responsable esté o no obligado al registro de sus bases de datos personales ante el Registro Nacional de Bases de Datos ("RNBD") administrado por la Superintendencia de Industria y Comercio ("SIC"). Cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares, se deberá informar a la Superintendencia de Industria y Comercio en un término máximo de 15 días hábiles siguientes al haber conocido el hecho. Art. 17 inc. n) y 18, inc. k), Ley 1581.
Sanciones	¿Existen sanciones frente al incumplimiento de dicha obligación? En caso de existir, identificarlas e indicar el monto de las sanciones o penalidad aplicable correspondiente.	No	No existe sanción frente al incumplimiento de la obligación de reportar un incumplimiento. Sin embargo, al constituir un deber de carácter obligatorio, podría entenderse como un incumplimiento de las disposiciones de la normativa vigente, dando lugar a que la SIC imponga las sanciones establecidas los artículos 22 y 23 de la Ley 1581. Art. 22 y 23, Ley 1581
Acciones legales	¿Existe alguna acción legal de protección de datos personales? ¿quién tiene derecho para ejercerla/ solicitarla?	Sí	La Constitución Política consagra la figura del Habeas Data en el art. 15, así como también el derecho a la información establecido en el art. 20, como derecho fundamental. Por lo tanto, es posible interponer la acción de tutela para hacer valer estos derechos o incluso acciones civiles en caso de generarse perjuicios por el tratamiento indebido de datos personales. Igualmente existen acciones penales que buscan proteger este derecho. Arts. 15 y 20, Constitución Política y Art. 16, Ley 1266. Adicionalmente, arts. 16, 22, 23 y 24 de la Ley 1581.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Delegado o responsable de la protección de datos personales	¿Existe la figura del delegado de protección de datos (DPO) o similar? En dicho caso, ¿su designación es obligatoria? ¿debe ser designado localmente?	Sí	La SIC, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos contemplados en la normativa de protección de datos personales. La designación de tal figura es obligatoria. A través del Decreto Nº 4886/113, art. 16 se establecen las funciones del Despacho del Superintendente Delegado para la Protección de Datos Personales (artículo modificado por el artículo 6 del Decreto 092 de 2022). Art. 19, Ley 1581 y Art. 16, Decreto Nº 4886/113. A su vez, 2.2.2.25.3.1 y 2.2.2.25.4.4 del Dec. 1074.
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	La Superintendencia de Industria y Comercio puede, ante el incumplimiento de la legislación en materia de protección de datos, adelantar las investigaciones de oficio o a pedido de parte interesada, a los fines de hacer efectivo el derecho de habeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de estos. Art. 21, Ley 1581.
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (ej. GDPR)? ¿Qué diferencias relevantes encuentra?		En principio se cumplen las disposiciones del GDPR. Una de las principales diferencias es que en Colombia los responsables obligados a registrar las bases de datos personales son las sociedades y entidades sin ánimo de lucro que tengan activos totales superiores a 100.000 Unidades de Valor Tributario (UVT) y las personas jurídicas de naturaleza pública.
Otras obligaciones	¿Existen otras consideraciones/ requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	Sí	La normativa y jurisprudencia nacional destacan el principio de responsabilidad demostrada o accountability, según el cual los responsables del tratamiento deben estar en capacidad de probar en todo momento las acciones efectivas, eficaces y oportunas que han tomado para proteger los datos personales que le han sido confiado y garantizar el debido tratamiento. Estas acciones podrán ser tomadas en cuenta por la Superintendencia de Industria y Comercio al momento de una investigación, para graduar la sanción.

Costa Rica

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Normativa	¿Existe en el país una ley de protección de datos personales? En ese caso, identificar normativa aplicable.	Sí	El derecho a la intimidad se encuentra protegido en Costa Rica por el artículo 24 de la Constitución Política en el que se indica que los ciudadanos tienen derecho a que su intimidad sea protegida por el Estado. Específicamente, los Datos Personales se encuentran regulados a través de la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales Nº 8968 vigente desde el 05 de setiembre de 2011 (en adelante conocida como la "Ley 8968"), y el Reglamento a la Ley de Protección de Datos Nº 37554-JP vigente desde el 05 de marzo de 2013
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su Sitio Web.	Sí	El artículo 15 de la Ley 8968 establece como autoridad encargada a la Agencia de Protección de Datos de los habitantes (Prodhab), el cual es un órgano de desconcentración máxima adscrtio al Ministerio de Justicia y Paz. http://www.prodhab.go.cr/
Ámbito de aplicación	¿Cuál es el ámbito de aplicación de la norma? Es decir, ¿su aplicación es estrictamente territorial, o aplica el concepto de extraterritorialidad?	Sí	La Ley 8968 y su Reglamento son de orden público y su aplicación se extiende a todas las bases de datos automatizadas, de organismos públicos o privados, dentro del territorio costarricense. (Artículo 2 de la ley y artículo 3 del Reglamento).
Recolección de datos	¿Cuáles son los requisitos o procesos legales exigidos para la recolección de datos personales? (por ejemplo, consentimiento del titular de los datos, proporcionar información sobre la finalidad del uso de los datos y derechos de su titular, entre otros.	Sí	La Ley Nº 8968 tiene como principio básico fundamental la autodeterminación informativa. Por tanto, cuando se soliciten datos de carácter personal es necesario informar de previo a las personas titulares o a sus representantes, de modo expreso, preciso e inequívoco, y obtener el consentimiento voluntario, expreso e informado, ya sea por medios físicos o digitales. (Artículos 4 y 5 de la ley y artículos 4,5, y 12 del Reglamento)
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	La ley 8968 define los datos personales como cualquier dato relativo a una persona física identificada o identificable.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	Según el artículo 9 de la Ley 8968, las categorías especiales son las siguientes: ▸ **Datos sensibles:** información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros. ▸ **Datos personales de acceso restringido:** los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública. ▸ **Datos personales de acceso irrestricto:** los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados. ***Datos referentes al comportamiento crediticio.** Los datos referentes al comportamiento crediticio se regirán por las normas que regulan el Sistema Financiero Nacional, de modo que permitan garantizar un grado de riesgo aceptable por parte de las entidades financieras, sin impedir el pleno ejercicio del derecho a la autodeterminación informativa ni exceder los límites de esta ley.
Situación de las sociedades y otras personas jurídicas	¿Alcanza la protección de la normativa en materia de datos personales, de las personas jurídicas o de existencial ideal?	No	N/A
Consentimiento del titular de los datos	¿Se requiere la obtención previa del consentimiento del titular de los datos cuando se recaba su información? En tal caso, ¿existen condiciones para la obtención del consentimiento del titular de los datos? (por ejemplo, información previa que deba proporcionarse al titular de los datos).	Sí	La normativa prohíbe la recolección de datos sin el consentimiento informado de la persona titular o su representante. Por tanto, cuando se recopilen datos personales se deberá obtener el consentimiento libre, específico, informado, inequívoco e individualizado de la persona titular o su representante por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo. Tratándose de consentimiento obtenido en línea, el responsable deberá poner a disposición del titular, un procedimiento para el otorgamiento del consentimiento conforme a la Ley. (Artículo 5 de la Ley 8968 y artículos 4 y 5 del Reglamento)
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	La Ley 8968 establece que no será necesario el consentimiento expreso del titular de los datos, cuando: a. Exista orden fundamentada, dictada por autoridad judicial competente o acuerdo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo. b. Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general. c. Los datos deban ser entregados por disposición constitucional o legal. (Artículo 5.2 de la ley y artículo 5 del Reglamento)

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Contenido y alcance de la información a ser validada por el titular de los datos	¿Cuál es el contenido que debe incluir el consentimiento? (Por ejemplo, uso o destino de los datos, transferencia internacional de los datos, etc.).	Sí	Específicamente, el artículo 5.1 de la ley establece la obligación de incluir dentro del consentimiento informado la siguiente información: a. De la existencia de una base de datos de carácter personal. b. De los fines que se persiguen con la recolección de estos datos. c. De los destinatarios de la información, así como de quiénes podrán consultarla. d. Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección de los datos. e. Del tratamiento que se dará a los datos solicitados. f. De las consecuencias de la negativa a suministrar los datos. g. De la posibilidad de ejercer los derechos que le asisten. h. De la identidad y dirección del responsable de la base de datos.
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales? ¿Hay requisitos aplicables en relación a la transferencia internacional de datos? (Ejemplo: cláusulas modelos, autorización por parte de la autoridad de control, entre otros).	Sí	La Ley 8968 y su Reglamento (artículo 14 de la ley y 40 del Reglamento), establecen como regla general que los responsables de las bases de datos solo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en esta ley, salvo disposición legal en contrario. Asimismo, el artículo 43 del Reglamento de la Ley de Protección de Datos establece como requisito legal para la transferencia de datos que el responsable de la base de datos, a través de un contrato, corrobore que el receptor de la información cumpla con las mismas obligaciones a las que él se encuentra sujeto. La normativa no señala ningún requisito aplicable sobre transferencia internacional de datos.
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	Sí	En la normativa costarricense las BCR son definidas como "Protocolos de Actuación", y se establece como un sistema de autorregulación para todas aquellas personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, el almacenamiento y el uso de datos personales. De acuerdo con el artículo 32 del Reglamento, los Protocolos de Actuación deberán especificar lo siguiente: a. Elaborar políticas y manuales de privacidad obligatorios y exigibles al interior de la organización del responsable; b. Poner en práctica un manual de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales; c. Establecer un procedimiento de control interno para el cumplimiento de las políticas de privacidad; d. Instaurar procedimientos ágiles, expeditos y gratuitos para recibir y responder dudas y quejas de los titulares de los datos personales o sus representantes, así como para acceder, rectificar, modificar, bloquear o suprimir la información contenida en la base de datos y revocar su consentimiento. e. Crear medidas y procedimientos técnicos que permitan mantener un historial de los datos personales durante su tratamiento. f. Constituir un mecanismo en el cual el responsable transmitente, le comunica al responsable receptor, las condiciones en las que el titular consintió la recolección, la transferencia y el tratamiento de sus datos. En caso de que el responsable de la base de datos realice una transferencia o cesión de datos personales, el Protocolo de Actuación deberá ser inscrito ante la Prodhab. (Artículo 12 de la Ley 8968 y artículos 32 y 41)

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Datos sensibles	¿Qué se entiende por dato sensible? ¿Cómo es el tratamiento de los datos sensibles, de corresponder?	Sí	La ley define en su artículo 3 inciso e) los datos sensibles como aquella información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros. Sobre el tratamiento de los datos sensibles el, el artículo 9.1 de la ley establece que ninguna persona estará obligada a suministrar datos sensibles, y prohíbe el tratamiento de los mismo. No obstante, establece las siguientes excepciones a dicha prohibición: a. Cuando el tratamiento de datos sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que la persona interesada esté física o jurídicamente incapacitada para dar su consentimiento. b. El tratamiento de los datos sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo, por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de las personas interesadas. c. El tratamiento se refiera a datos que la persona interesada haya hecho públicos voluntariamente o sean necesarios para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial. d. El tratamiento de los datos resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un funcionario o funcionaria del área de la salud, sujeto al secreto profesional o propio de su función, o por otra persona sujeta, asimismo, a una obligación equivalente de secreto.
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (ej. ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, tratamiento y/o uso de la misma? ¿Existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	Sí	De acuerdo con el artículo 21 de la ley, toda base de datos, pública o privada, administrada con fines de distribución, difusión o comercialización, debe inscribirse en el registro que al efecto habilite la Prodhab. La inscripción no implica la transferencia de los datos hacia la autoridad. Asimismo, el responsable de la base deberá inscribir cualquier otra información que la Prodbhab solicite, así como los protocolos de actuación que se mencionado en el artículo 12 de la ley, y al cual se hace referencia en el espacio sobre BCR.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	Sí	Las medidas mínimas de seguridad deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada. (Artículo 10 de la Ley 8968). El reglamento (artículos 36 y 37) describe ampliamente las acciones mínimas requeridas y recomendadas por parte de la Prodhab para garantizar la seguridad de los datos: a) Elaborar una descripción detallada del tipo de datos personales tratados o almacenados; b) Crear y mantener actualizado un inventario de la infraestructura tecnológica, incluyendo los equipos y programas de cómputo y sus licencias; c) Señalar el tipo de sistema, programa, método o proceso utilizado en el tratamiento o almacenamiento de los datos; igualmente, indicarse el nombre y la versión de la base de datos utilizada cuando proceda. d) Contar con un análisis de riesgos, que consiste en identificar peligros y estimar los riesgos que podrían afectar los datos personales; e) Establecer las medidas de seguridad aplicables a los datos personales, e identificar aquellas implementadas de manera efectiva; f) Calcular el riesgo residual existente basado en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales; g) Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivados del resultado del cálculo del riesgo residual. Asimismo, se recomienda actualizar las medidas de seguridad al menos una vez al año. Respecto a las bases de datos que deben registrarse, si las mismas no cuentan con las acciones mencionadas y no reúnen las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas; no serán inscritas por parte de la autoridad.
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Ejemplo: rectificación, actualización o supresión). Identificar y explicar.	Sí	Siempre se deberá establecer e implementar procesos internos para garantizar los siguientes derechos a los propietarios de datos: ▸ Derecho de Acceso a la información. ▸ Derecho a rectificación. ▸ Derecho a revocar o cancelar el consentimiento para el uso, procesamiento o recolección de información personal. ▸ Derecho a suprimir o cancelar la información personal brindada. ▸ Derecho al olvido. (Artículo 7 de la Ley y artículos 7, 11, 21, 23, y 25 del Reglamento)
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	El responsable, deberá poner a disposición del titular, los medios y formas simplificados de comunicación electrónica u otros que considere pertinentes para facilitar a los titulares el ejercicio de sus derechos. Toda solicitud para el ejercicio de los derechos personales del titular deberá ser atendida de manera gratuita y ser resuelta en el plazo de cinco (5) días hábiles, contados a partir del día siguiente en que la misma haya sido recibida por el responsable. (Artículo 7 de la Ley y artículos del 13 al 20 del Reglamento)

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	Sí	Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo. Por otro lado, El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros (data processing)? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	Sí	El artículo 29 del Reglamento de la Ley 8968 define la contratación o subcontratación de servicios como aquella transacción mediante el cual el responsable de la base de datos contrata a un tercero (intermediario tecnológico o un proveedor de servicios), para que este sea el encargado de realizar el tratamiento de los datos personales. El encargado tendrá las siguientes obligaciones: a. Tratar únicamente los datos personales conforme a las instrucciones del responsable; b. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable; c. Implementar las medidas de seguridad y cumplir con los protocolos mínimos de actuación conforme a la Ley, el presente Reglamento y las demás disposiciones aplicables; d. Guardar confidencialidad respecto de los datos personales tratados; e. Abstenerse de transferir o difundir los datos personales, salvo instrucciones expresas por parte del responsable. f. Suprimir los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. No obstante lo anterior, la ley señala de manera clara, que quien contrate los servicios mantiene la responsabilidad por el tratamiento de datos personales. Por tanto, el responsable deberá verificar que el tercero cumpla con las medidas de seguridad mínimas que garanticen la integridad y seguridad de los datos personales. La intervención por parte del encargado se limitará de manera estricta a lo establecido en el contrato celebrado con el responsable, y sus indicaciones.
Conservación de datos	¿Hay obligación de retener/conservar los datos recolectados o procesados por un tiempo determinado? En dicho caso, ¿cuál es el plazo?	No	N/A

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Eliminación de datos	¿Existe una obligación de eliminar los datos recolectados o procesados? En dicho caso, ¿en qué supuestos y cuál es el plazo?	Sí	La Ley 8968 establece que El responsable de la base de datos deberá eliminar los datos que hayan dejado de ser pertinentes o necesarios, en razón de la finalidad para la cual fueron recibidos y registrados; así como que la conservación de los datos personales no deberá exceder el plazo de diez (10) años, desde la fecha de terminación del objeto de tratamiento del dato. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados de su titular No obstante, el reglamento establece las siguientes excepciones para variar el plazo de conservación: ▸ Disposición normativa especial que establezca otro plazo; ▸ Por acuerdo entre partes que establezca un plazo distinto, ▸ Que exista una relación continuada entre las partes; ▸ Interés público para conservar el dato. (Artículos 6 y 30 de la Ley y artículo 11 del Reglamento)
Privacy Impact Asessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (Privacy Impact Assessment)?	Sí	El artículo 36 inciso d) del Reglamento, establece como obligación contar con un análisis de riesgos, que permita identificar peligros y estimar los riesgos que podrían afectar los datos personales que se encuentra registrados en la base del responsable.
Incidentes	¿Hay obligación de reportar un incidente de seguridad o algún incumplimiento o las previsiones legales?	Sí	Ante una vulneración de la seguridad de la base de datos, el responsable, tiene la obligación de informar sobre cualquier irregularidad (por ejemplo: pérdida, destrucción, extravío, entre otras), tanto a los titulares de los datos, como a la autoridad. Para informar a los titulares tendrá un plazo de cinco días hábiles a partir del momento en que ocurrió el evento, a fin de que los titulares de estos datos personales afectados puedan tomar las medidas correspondientes. (Artículo 38 del Reglamento) La información mínima que debe incluir el aviso es la siguiente (Artículo 39 del reglamento): a. La naturaleza del incidente; b. Los datos personales comprometidos; c. Las acciones correctivas realizadas de forma inmediata; d. Los medios o el lugar, donde puede obtener más información al respecto.
Sanciones	¿Existen sanciones frente al incumplimiento de dicha obligación? En caso de existir, identificarlas e indicar el monto de las sanciones o penalidad aplicable correspondiente.	No	Sin embargo, si el titular de los datos se ve afectado por el incidente o por el incumplimiento, la Ley 8968 establece tres tipos de faltas (leves, graves y gravísimas). Las sanciones por incumplimiento de disposiciones legales son las siguientes: ▸ Faltas leves: Sanción entre $1,000 y $5,000 ▸ Faltas Graves: Sanción entre $5,000 y $20,000 ▸ Faltas Gravísimas: Sanción entre $15,000 y $30,000, y la suspensión para el funcionamiento del fichero de uno a seis meses.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Acciones legales	¿Existe alguna acción legal de protección de datos personales? ¿quién tiene derecho para ejercerla/ solicitarla?	Sí	Cualquier persona que ostente un derecho subjetivo o un interés legítimo puede denunciar, ante la Prodhab (autoridad), que una base de datos pública o privada actúa en contravención de las reglas o los principios básicos para la protección de los datos y la autodeterminación informativa establecidas en esta ley. En adición a lo anterior, cualquier persona que pudiera verse afectada por un incidente de seguridad o incumplimiento a la normativa vigente en protección de datos, podría demandar civilmente al responsable por los daños que le fueran causados (siempre que el responsable se encuentre domiciliado en Costa Rica)
Delegado o responsable de la protección de datos personales	¿Existe la figura del delegado de protección de datos (DPO) o similar? En dicho caso, ¿su designación es obligatoria? ¿debe ser designado localmente?	No	N/A
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	De oficio o a instancia de parte, la Prodhab podrá iniciar un procedimiento tendiente a demostrar si una base de datos regulada por esta ley está siendo empleada de conformidad con sus principios.
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (ej. GDPR)? ¿Qué diferencias relevantes encuentra?	No	La normativa costarricense no contempla todos los requisitos de la normativa internacional (GDPR). Sobre las diferencias relevantes podemos mencionar el ámbito de aplicación de la Ley Nº 8968 y su Reglamento, el cual deja en indefensión a los titulares de los datos ante un incumplimiento cometido por una persona física o jurídica internacional. Asimismo, no se contempla el derecho de portabilidad de los datos, ni la figura de Delegado de Protección de Datos. Por último, la autoridad no cuenta con el presupuesto ni el recurso humano suficiente para cumplir con sus obligaciones, por lo que el control sobre las bases de datos en el país es realmente limitado. En el 2021, y a partir de situaciones país que han generado el interés público en el tema de protección de datos, distintos sectores se encuentran en la redacción y presentación ante el Congreso, de diversos proyectos de ley para reformar la legislación sobre protección de datos en Costa Rica.
Otras obligaciones	¿Existen otras consideraciones/ requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	Sí	Sobre la aceptación de las Políticas de Privacidad y Consentimiento Informado en sitios web de comercio electrónico, la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, Nro. 7472, y su Reglamento, establecen que el comerciante debe garantizar que el consumidor acepte dichas políticas de manera libre e inequívoca, y no de manera preseleccionada.

Ecuador

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Normativa	¿Existe en el país una ley de protección de datos personales? En ese caso, identificar normativa aplicable.	Sí	La protección de datos personales está regulada por la Ley Orgánica de Protección de Datos Personales ("LOPDP"). Este cuerpo normativo entró en vigencia el 26 de mayo de 2021.
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su Sitio Web.	Sí	La LOPDP menciona a una Autoridad de Protección de Datos Personales y/o jueces competentes. Dicha autoridad todavía no ha sido creada; sin embargo, se prevé su existencia a partir de la expedición del Reglamento a la Ley, cuya fecha de aprobación no ha sido determinada.
Ámbito de aplicación	¿Cuál es el ámbito de aplicación de la norma? Es decir, ¿su aplicación es estrictamente territorial, o aplica el concepto de extraterritorialidad?	Sí	Sin perjuicio de la normativa establecida en los instrumentos internacionales ratificados por Ecuador, las disposiciones legales establecidas en la LOPDP disponen aplicación territorial cuando: 1. El tratamiento de datos personales se realice dentro del territorio nacional ecuatoriano 2. El responsable o encargado del tratamiento se encuentre domiciliado dentro del territorio nacional ecuatoriano 3. El responsable o encargado no domiciliado en Ecuador trate datos de titulares residentes en Ecuador, cuando las actividades del tratamiento se relacionen con: 1) oferta de bienes o servicios a titulares; o 2) del control de su comportamiento siempre cuando este tenga lugar en el territorio nacional ecuatoriano 4. Al responsable o encargado le aplique la legislación nacional en virtud de un contrato o regulaciones de derecho internacional público, a pesar de no estar domiciliado dentro del Ecuador.
Recolección de datos	¿Cuáles son los requisitos o procesos legales exigidos para la recolección de datos personales? (por ejemplo, consentimiento del titular de los datos, proporcionar información sobre la finalidad del uso de los datos y derechos de su titular, entre otros).	Sí	El tratamiento de datos personales será legítimo y licito cuando se cumpla con alguna de las siguientes condiciones: 1. Por existencia del consentimiento del titular para el tratamiento de sus datos personales 2. Que sea realizado por el responsable en cumplimiento de una obligación legal u orden judicial 3. Que el tratamiento se sustente en un interés público 4. Para la ejecución de medidas precontractuales a petición del titular 5. Para proteger intereses vitales (vida, salud, integridad) 6. Para tratamiento de datos personales que consten en bases de datos de acceso público 7. Para satisfacer un interés legítimo del responsable o un tercero, cuando no prevalezca el interés o derechos del titular Únicamente se podrán tratar los datos que sean estrictamente necesarios para la realización de la finalidad. De igual manera, el tratamiento debe ser transparente frente el titular.
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	La LOPDP define como dato personal al dato que identifica o hace identificable a una persona natural, directa o indirectamente.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	**Datos sensibles:** Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales. **Datos relativos a la salud:** datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud. **Datos personales crediticios:** Datos que integran el comportamiento de personas naturales para analizar su capacidad de pago y financiera. **Dato biométrico:** Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros. **Dato genético:** Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo.
Situación de las sociedades y otras personas jurídicas	¿Alcanza la protección de la normativa en materia de datos personales, de las personas jurídicas o de existencial ideal?	No	La LOPDP protege únicamente a personas naturales; dejando de lado a las personas jurídicas o de existencia ideal.
Consentimiento del titular de los datos	¿Se requiere la obtención previa del consentimiento del titular de los datos cuando se recaba su información? En tal caso, ¿existen condiciones para la obtención del consentimiento del titular de los datos? (por ejemplo, información previa que deba proporcionarse al titular de los datos.	Sí	La obtención del consentimiento debe ser previo, libre, expreso, inequívoco, específico e informado. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara. Se deberá obtener el consentimiento para cada una de las finalidades del tratamiento.
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	No será necesario el consentimiento cuando: 1. Los datos han sido recogidos de fuentes accesibles al público. 2. Deban proporcionarse a Autoridades Administrativas o Judiciales. 3. El tratamiento responda libre y legítimamente a una relación jurídica con el responsable del tratamiento y el titular, en la medida que se limite a la finalidad de la justifique 4. La comunicación se produzca entre Administraciones Públicas, y tenga por objeto el tratamiento posterior con fines históricos, estadísticos o científicos, siempre y cuando los datos sean debidamente disociados 5. Sean datos de carácter de personal relativos a la salud para solucionar una urgencia que implique intereses vitales y el titular se encuentre impedido de otorgar su consentimiento 6. Se traten datos relativos a la salud para realizar estudios epidemiológicos de interés público, siendo un tratamiento de preferencia anonimizado 7. El tratamiento de datos de salud cuando sea necesario por razones de interés público esencial, debiendo ser proporcional al objeto perseguido 8. El tratamiento sea necesario por razones de interés público en el ámbito de salud pública, o para garantizar niveles de calidad y seguridad sanitaria

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Contenido y alcance de la información a ser validada por el titular de los datos	¿Cuál es el contenido que debe incluir el consentimiento? (Por ejemplo, uso o destino de los datos, transferencia internacional de los datos, etc.).	Sí	El consentimiento será válido, cuando la manifestación de la voluntad sea: 1) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento; 2) Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento; 3) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia, 4) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular 5) Revocable, de manera que se permita su anulación en cualquier momento, sin que sea necesaria una justificación. Sin embargo, el tratamiento realizado antes de revocar el consentimiento es lícito.
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales? ¿Hay requisitos aplicables en relación a la transferencia internacional de datos? (Ejemplo: cláusulas modelos, autorización por parte de la autoridad de control, entre otros).	Sí	Transferencia nacional Los datos personales podrán transferirse o comunicarse a terceros para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario, cuando la transferencia se encuentre configurada dentro de una de las causales de legitimidad, y se cuente, además, con el consentimiento del titular. Se entiende que el consentimiento es informado cuando para la transferencia o comunicación de datos personales el Responsable del tratamiento ha entregado información suficiente al titular que le permita conocer la finalidad a que se destinarán sus datos y el tipo de actividad del tercero a quien se pretende transferir o comunicar dichos datos. Transferencia internacional Será posible cuando se respeten las siguientes consideraciones: 1. Se podrán transferir datos personales, organizaciones y personas jurídicas en general que brinden niveles adecuados de protección 2. En el caso de que se realice una transferencia internacional de datos a un país, organización o territorio económico internacional que no haya sido calificado por la ADPDP de tener un nivel adecuado de protección, se deberá emitir un instrumento jurídico de carácter vinculante, que garantice : 1) el cumplimiento de principios, derechos y obligaciones en el tratamiento de datos personales en un estándar igual o mayor a la normativa ecuatoriana; 2) disponibilidad permanente de acciones administrativas o judiciales; y 3) derecho a solicitar reparación integral de ser el caso. 3.Para los demás casos, se deberá obtener la autorización de la APDP, registrando la información sobre transferencias internacionales en el Registro Nacional de Protección de Datos Personales por parte del responsable.
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	Sí	Los responsables o encargados del tratamiento de datos personales podrán presentar a la Autoridad de Protección de Datos Personales, normas corporativas vinculantes, específicas y aplicadas al ámbito de su actividad
Datos sensibles	¿Qué se entiende por dato sensible? ¿Cómo es el tratamiento de los datos sensibles, de corresponder?	Sí	**Los datos sensibles son aquellos relativos a etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación. Atenten o puedan atentar contra los derechos humanos o la dignidad e integridad de las personas. La Autoridad de Protección de Datos Personales podrá determinar otras categorías de datos sensibles.**

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Datos sensibles	¿Qué se entiende por dato sensible? ¿Cómo es el tratamiento de los datos sensibles, de corresponder?	Sí	La LOPDP permite el tratamiento de datos personales sensibles cuando concurra alguna de las siguientes circunstancias: 1. El titular otorgue su consentimiento explícito 2. El tratamiento sea necesario para el cumplimiento de obligaciones y ejercicio de derechos en el ámbito de derecho laboral y/o seguridad y protección social 3. El tratamiento sea necesario para proteger intereses vitales del titular cuando este no esté capacitado para dar su consentimiento 4. El tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos 5. El tratamiento se lo realiza por orden de autoridad judicial 6. El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (ej. ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, tratamiento y/o uso de la misma? ¿Existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	Sí	El responsable del tratamiento de datos personales deberá reportar y mantener actualizada la información ante la Autoridad de Protección de Datos Personales, sobre lo siguiente: 1. Identificación de la base datos o tratamiento 2. Domicilio legal y contacto del responsable y encargado 3. Características y finalidad del tratamiento 4. Naturaleza de los datos personales tratados 5. Características y finalidades del tratamiento 6. Naturaleza de los datos personales tratados 7. Domicilio y contacto de los destinatarios de datos personales 8. Modo de interrelacionar información registrada 9. Medios utilizados para implementar la LODPD 10. Requisitos y herramientas implementadas para garantizar la seguridad y protección de datos personales 11. Tiempo de conservación de datos
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	Sí	El responsable o encargado deberá implementar un proceso de evaluación continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, que podrán incluir: 1. Anonimización, seudonomización o cifrado de datos personales 2. Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios 3. Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, y jurídica 4. Estándares internacionales para implementar sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la APDP

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Ejemplo: rectificación, actualización o supresión). Identificar y explicar.	Sí	El titular de los datos tiene los siguientes derechos: ▸ Derecho de Información ▸ Derecho de Acceso ▸ Derecho de Rectificación y Actualización ▸ Derecho de Eliminación ▸ Derecho de Oposición ▸ Derecho de Portabilidad ▸ Derecho a suspensión de tratamiento ▸ Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas. ▸ Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas ▸ Derecho de consulta ▸ Derecho a la educación digital
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	Quejas directas y reclamos administrativos En el caso de que el responsable del tratamiento no conteste a la queja en el término establecido o ésta fuere negativa, el titular podrá presentar el correspondiente reclamo administrativo ante la Autoridad de Protección de Datos Personales. Sin perjuicio de lo antes expuesto, el titular podrá presentar acciones civiles, penales y constitucionales a las que se crea asistido.
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?		Consentimiento expreso del titular.
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros (data processing)? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	Sí	El tratamiento de datos personales realizado por terceros deberá estar regulado por un contrato, en el cual se establezca de manera clara y precisa que tratará sus datos conforme las instrucciones del responsable y no utilizará los datos para finalidades diferentes a las estipuladas en el contrato. El tercero no podrá transferir o comunicar los datos personales para su conservación. El tercero será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales.
Conservación de datos	¿Hay obligación de retener/conservar los datos recolectados o procesados por un tiempo determinado? En dicho caso, ¿cuál es el plazo?	No	Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento. Para garantizar que los datos personales no se conserven más tiempo del necesario, el responsable del tratamiento establecerá plazos para su supresión o revisión periódica. La conservación ampliada de tratamiento de datos personales únicamente se realizará con fines de archivo en interés público, fines de investigación científica, histórica o estadística, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales, oportunas y necesarias.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Eliminación de datos	¿Existe una obligación de eliminar los datos recolectados o procesados? En dicho caso, ¿en qué supuestos y cuál es el plazo?	Sí	El titular tiene derecho a que el responsable del tratamiento suprima sus datos personales, cuando: 1) El tratamiento no cumpla con los principios legales; 2) El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad; 3) Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados; 4) Haya vencido el plazo de conservación de los datos personales; 5) El tratamiento afecte derechos fundamentales o libertades individuales; 6) Revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, sin necesidad de que medie justificación alguna; o, 7) Exista obligación legal. El responsable del tratamiento de datos personales implementará métodos y técnicas orientadas a eliminar, hacer ilegible, o dejar irreconocibles de forma definitiva y segura los datos personales. Esta obligación la deberá cumplir en el plazo de 15 días de recibida la solicitud por parte del titular y será gratuito.
Privacy Impact Asessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (Privacy Impact Assessment)?	Sí	El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera.
Incidentes	¿Hay obligación de reportar un incidente de seguridad u algún incumplimiento o las previsiones legales?	Sí	El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la APDP y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible y máximo 5 días término desde tener constancia de la vulneración. Si no se cumple en este término, deberá indicarse los motivos de la dilación. El encargado deberá notificar al responsable cualquier vulneración de la seguridad tan pronto sea posible, y a más tardar dentro del término de 3 días a partir de la fecha en la que tenga conocimiento de ella. De igual manera, el responsable deberá notificar sin dilación la vulneración al titular cuando esta conlleve un riesgo a sus derechos fundamentales y libertades, dentro del término de 3 días contados a partir de la fecha en la que tuvo conocimiento de la vulneración.
Sanciones	¿Existen sanciones frente al incumplimiento de dicha obligación? En caso de existir, identificarlas e indicar el monto de las sanciones o penalidad aplicable correspondiente.	Sí	Infracciones Leves: Servidores o funcionarios del sector público: sanciones con una multa de uno (1) a diez (10) salarios básicos unificados del trabajador en general, sin perjuicio de la responsabilidad extracontractual del Estado. Infracciones Graves: Servidores o funcionarios del sector público: sanciones con una multa de diez (10) a veinte (20) salarios básicos unificados del trabajador en general. Sector privado: multa de entre el 0.7% y el 1% calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Acciones legales	¿Existe alguna acción legal de protección de datos personales? ¿quién tiene derecho para ejercerla/ solicitarla?	Sí	El titular de los datos personales podrá, en cualquier momento. de forma gratuita y por medios físicos o digitales puestos a su disposición por parte del responsable del tratamiento de los datos personales presentar requerimientos, peticiones, quejas o reclamaciones directamente al responsable del tratamiento de sus datos Acciones administrativas, sin perjuicio, el titular podrá presentar acciones civiles, penales o constitucionales de las que se crea asistido.
Delegado o responsable de la protección de datos personales	¿Existe la figura del delegado de protección de datos (DPO) o similar? En dicho caso, ¿su designación es obligatoria? ¿debe ser designado localmente?	Sí	La ley define al DPO como una persona natural encargada de informar al responsable o encargado del tratamiento sobre sus obligaciones legales, supervisar el cumplimiento normativo referente a la protección de datos personales, y cooperar con la APDP, sirviendo como un punto de contacto entre esta y la entidad responsable del tratamiento de datos La ley no establece un requisito para designar un oficial de protección de datos. Sin embargo, se designará cuando: 1. El tratamiento se lleve a cabo por quienes conforman el sector público. 2. Cuando se requiera un control permanente y sistematizado 3. Refiera a datos relacionado con la seguridad nacional 4. Se refiera a tratamientos de gran volumen de categorías especiales de datos La Autoridad de Protección de Datos Personales podrá definir nuevas condiciones en las que deba designarse un delegado de protección de datos personales
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	La Autoridad de Protección de Datos Personales podrá iniciar, de oficio o a petición del titular, actuaciones previas con el fin de conocer las circunstancias de] caso concreto o la conveniencia o no de iniciar un procedimiento administrativo.
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (ej. GDPR)? ¿Qué diferencias relevantes encuentra?	Sí	La Ley Orgánica de Protección de Datos Personales contempla todos los requisitos receptados por la normativa internacional adoptando los Estándares de Protección (GDPR, Datos Personales para los Estados Iberoamericanos y el Proyecto de Ley Modelo sobre Protección de Datos Personales emitidos por la OEA).
Otras obligaciones	¿Existen otras consideraciones/ requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	Sí	A partir de mayo de 2023 inicia el régimen sancionatorio Actualmente, la Asamblea Nacional está discutiendo el Reglamento a la ley; sin embargo, no se tiene claridad respecto a la fecha de promulgación del documento Hasta la fecha, no se ha creado la figura de Autoridad Nacional de Protección de Datos Personales y tampoco se ha instaurado el Registro Nacional de Protección de Datos Personales. Sin embargo, la Ley está vigente y, por tanto, su cumplimiento será considerado como responsabilidad proactiva

México

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Normativa	¿Existe en el país una ley de protección de datos personales? En ese caso, identificar normativa aplicable.	Sí	México cuenta con las siguientes normativas en la materia, aplicables a personas físicas o morales privadas: ‣ Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010) ("LFPDPPP"). ‣ Reglamento Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2011) ("Reglamento de la LFPDPPP"). ‣ Lineamientos del Aviso de Privacidad (2013) ("LAV"). ‣ Parámetros para el Correcto Desarrollo de los Esquemas de Autorregulación Vinculante (2013) ("PAPDP"). ‣ Reglas de Operación del Registro de Esquemas de Autorregulación Vinculante (2015) ("ROREAV") Cabe mencionar que México también cuenta con normatividad relativa a la protección de datos personales en posesión del sector público, y en específico la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017) ("LGPDPPSO"), cuyo análisis no se encuentra incluido en este documento.
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su Sitio Web.	Sí	La autoridad de aplicación es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ("INAI"). http://inicio.ifai.org.mx/SitePages/ifai.aspx
Ámbito de aplicación	¿Cuál es el ámbito de aplicación de la norma? Es decir, ¿su aplicación es estrictamente territorial, o aplica el concepto de extraterritorialidad?	Sí	La normativa será aplicable, conforme se establece en los arts. 2, 3 inc. ix) de la LFPDPPP y arts. 3, 4 y 49 del Reglamento de la LFPDPPP, a todo particular, sea persona física o moral de carácter privado, que lleve a cabo el tratamiento de datos personales, en los siguientes supuestos: (i) A todo tratamiento que sea efectuado en un establecimiento de un responsable ubicado en territorio mexicano; (ii) A todo tratamiento efectuado por un encargado con independencia de su ubicación, a nombre de un responsable establecido en territorio mexicano; (iii) Cuando el responsable no esté establecido en territorio mexicano pero le resulte aplicable la legislación mexicana, derivado de la celebración de un contrato o en términos del derecho internacional; y (iv) Cuando el responsable no esté establecido en territorio mexicano y utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento. Lo anterior, en el entendido de que todo tratamiento de datos personales que obren en soportes físicos o electrónicos, que hagan posible el acceso a los datos personales con arreglo a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización estará sujeto a la regulación, incluso el tratamiento de datos que sea efectuado por un encargado, sea una persona física o moral, que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Recolección de datos	¿Cuáles son los requisitos o procesos legales exigidos para la recolección de datos personales? (por ejemplo, consentimiento del titular de los datos, proporcionar información sobre la finalidad del uso de los datos y derechos de su titular, entre otros.	Sí	Todo aquel sujeto responsable de la recolección de datos tendrá obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del "aviso de privacidad". El mencionado aviso podrá ser un documento físico, electrónico o en cualquier otro formato generado por el responsable y debe ser puesto a disposición del titular, previo al tratamiento de sus datos personales. El aviso de privacidad deberá cumplir con las disposiciones establecidas en los arts. 3 sección I, 15, 16 y 17 de la LFPDPPP, los LAV. En la misma línea, los LAV tienen como base el concepto del principio de la información. Adicionalmente, cabe destacar que todo tratamiento de datos personales estará sujeto al consentimiento de su titular, ya sea tácito o expreso según corresponda, salvo las excepciones previstas por la LFPDPPP.
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	Se entiende como datos personales a cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información. Art. 3, inc. V, LFPDPPP.
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	La normativa mexicana categoriza a los datos en tres: ▸ **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información. ▸ **Datos patrimoniales o financieros.** ▸ **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual. Para el tratamiento de datos patrimoniales o financieros y sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca. Tratándose de datos sensibles, solamente podrán crearse bases de datos sensibles cuando la constitución de la misma obedezca a un mandato legal, sea justificable en términos del artículo 4 de la LFPDPPP o cuando el responsable lo requiera para finalidades legitimas, concretas y acordes con las actividades o fines explícitos que persiga. Art. 3, inc. v) y vi), 8, 9, 13, Y 16 LFPDPPP y Art. 15 inc. II y III, 56 y 62 del Reglamento de la LFPDPPP.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Situación de las sociedades y otras personas jurídicas	¿Alcanza la protección de la normativa en materia de datos personales, de las personas jurídicas o de existencial ideal?	No	
Consentimiento del titular de los datos	¿Se requiere la obtención previa del consentimiento del titular de los datos cuando se recaba su información? En tal caso, ¿existen condiciones para la obtención del consentimiento del titular de los datos? (por ejemplo, información previa que deba proporcionarse al titular de los datos.	Sí	Si, el consentimiento es requerido y deberá ser conforme se establece en los arts. 3, inc. iv), 6, 8, 9 y 12 de la LFPDPPP y el arts. 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 y 21 del Reglamento de la LFPDPPP (libre, específico e informado, además de inequívoco en caso de requerirse el consentimiento expreso). Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas (ver la siguiente pregunta). Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable. El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición. El consentimiento para el tratamiento de datos personales no será necesario cuando: (i) este previsto en una ley; (ii) los datos figuren en fuentes de acceso público; (iii) los datos personales se sometan a un proceso de disociación; (iv) tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; (v) exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes; (vi) sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento en los términos que establece la legislación aplicable, y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente; o (vii) se dicte resolución de autoridad competente. Arts. 3, inc. iv), 6, 8, y 9 LFPDPPP Arts. 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 y 21 Reglamento de la LFPDPPP.
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales cuando se presente cualquiera de las excepciones previstas en los arts. 10 y 37 de la LFPDPPP, y Art. 17 del Reglamento de la LFPDPPP.
Contenido y alcance de la información a ser validada por el titular de los datos	¿Cuál es el contenido que debe incluir el consentimiento? (Por ejemplo, uso o destino de los datos, transferencia internacional de los datos, etc.).	Sí	El consentimiento per sé no debe tener un contenido específico (puede darse tácitamente, a través de una simple firma autógrafa u otros mecanismos electrónicos), ya que el aviso de privacidad sobre el que se otorga el consentimiento es el que debe cumplir con los requisitos que establece la ley, a efecto de que el consentimiento otorgado tenga validez. Los requisitos con que debe cumplir el aviso de privacidad se describen en el rubro "Recolección de Datos"

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales? ¿Hay requisitos aplicables en relación a la transferencia internacional de datos? (Ejemplo: cláusulas modelos, autorización por parte de la autoridad de control, entre otros).	Sí	Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones mencionadas en el art. 37 de la LFPDPPP. Estas deberán ser informadas al titular mediante el aviso de privacidad y limitarse a la finalidad que las justifique. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos. En cuanto a las transferencias internacionales de datos, deberán hacerse conforme a lo establecido en los arts. 67, 68, 69, 70, 74, 75, 76 del Reglamento de la LFPDPPP. Arts. 36 y 37, LFPDPPP; Arts. 67, 68, 69, 70, 71, 73, 74, 75, 76, Reglamento de la LFPDPPP. En ese sentido, cabe destacar que la comunicación de datos personales entre el responsable y un encargado, dentro o fuera del territorio mexicano, no es calificada como una "transferencia", sino como una remisión, en términos del art. 2 inc. IX. del Reglamento de la LFPDPPP. Las remisiones nacionales e internacionales de datos personales entre un responsable y un encargado no requerirán ser informadas al titular ni contar con su consentimiento. El encargado es la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Art. 2 y 53 del Reglamento de la LFPDPPP.
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	Sí	Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por la LFPDPPP. Dichos esquemas deberán contener mecanismos para medir su eficacia en la protección de los datos, consecuencias y medidas correctivas eficaces en caso de incumplimiento. Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buena práctica profesional, políticas de privacidad, sellos de confianza u otros mecanismos y contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares. Cuando un responsable adopte y cumpla un esquema de autorregulación, dicha circunstancia será tomada en consideración para determinar la atenuación de la sanción que corresponda, en caso de verificarse algún incumplimiento a lo dispuesto por la LFPDPPP y el Reglamento de la LFPDPPP, por parte del INAI. Asimismo, el INAI podrá determinar otros incentivos para la adopción de esquemas de autorregulación, así como mecanismos que faciliten procesos administrativos ante el mismo. En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar el cumplimiento de las disposiciones previstas en la LFPDPPP, en el Reglamento de LFPDPPP y toda aquella normativa que resulte aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante y estén en línea con lo establecido por la normativa aplicable. Art. 44 de la LFPDPPP y Arts. 70 y 79 a 86 del Reglamento de la LFPDPPP.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Datos sensibles	¿Qué se entiende por dato sensible? ¿Cómo es el tratamiento de los datos sensibles, de corresponder?	Sí	Por dato sensible se entiende a todo aquel que se refiera a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual. En cuanto a su tratamiento, deberá realizarse conforme a las disposiciones establecidas en los arts. 9, 13 y 16 de la LFPDPPP, arts. 15 y 56 del Reglamento de la LFPDPPP. Arts. 9, 13, 16 y 64 inc. iv) LFPDPPP; Arts. 15, 56 y 62 Reglamento de la LFPDPPP.
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (ej. ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, tratamiento y/o uso de la misma? ¿Existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	No	No existe la obligación de registrar una base de datos ante la autoridad de aplicación.
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	Sí	El responsable y, en su caso, el encargado, deberán establecer y mantener las medidas de seguridad administrativas, como la segregación de permisos basados en roles y responsabilidades -siempre otorgando el menor privilegio-, físicas, tales como la implementación de tecnología capaz de asegurar que los datos se mantengan disponibles, íntegros y confidenciales y, en su caso, técnicas, como la implementación de controles que permitan identificar y rastrear algún cambio no autorizado realizado por los usuarios o el almacenamiento cifrado para la protección de los datos personales, con independencia del sistema de tratamiento. El art. 2, incs. v), vi) y vii) del Reglamento de la LFPDPPP explica en qué consisten dichas medidas. Asimismo, el responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de los datos en todo momento y hasta después de finalizar sus relaciones con el titular o con el responsable, según sea el caso. Las medidas de seguridad se deberán implementar a partir de un análisis de riesgos sobre los datos personales que traten y sobre un análisis de brecha sobre las medidas de seguridad existentes. El responsable debe considerar acciones con el objetivo de establecer y mantener la seguridad de los datos personales, incluyendo sin limitar: ‣ Contar con un inventario de datos personales y de repositorios (físicos y electrónicos) ‣ Tener la trazabilidad de los datos personales en todo el ciclo de vida (obtención, almacenamiento, uso, transferencias, bloqueo y eliminación) de los mismos en las distintas actividades de tratamiento. ‣ Definir planes y programas de capacitación y concientización al personal que efectué el tratamiento de los datos personales. ‣ Establecer una relación de las medidas de seguridad con las que cuente el responsable para asegurar la protección de los datos personales. El responsable deberá actualizar las medidas de seguridad para su mejora continua, o en caso de alguna modificación sustancial en el tratamiento o vulneración/afectación de datos personales El Reglamento de la LFPDPPP desarrolla el marco normativo para las medidas de seguridad en sus arts. 57, 59, 60, 61 y 62. Arts. 19 y 21, LFPDPPP; Arts. 2 incs. v), vi) y vii), 48 inc. ix), 57, 59, 60, 61 y 62, Reglamento de la LFPDPPP.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Ejemplo: rectificación, actualización o supresión). Identificar y explicar.	Sí	Los derechos de los titulares, conforme surge de la normativa mexicana son el derecho de acceso, rectificación, cancelación y oposición ("Derechos ARCO"). El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Arts. 3, inc. iii), 22, 23, 24, 25, 31 y 33, LFPDPPP; Arts. 2 inc. ii) y 87, Reglamento de la LFPDPPP.
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	Los derechos ARCO deberán ejercerse conforme lo dispuesto en los arts. 22, 23, 24, 25, 26, 28, 29, 31, 32, 33 y 35 de la LFPDPPP. Los arts. 87, 88, 89, 90, 92, 93, 94, 95, 96, 97, 98 y 101, 102, 103, 104, 105, 106 y 109 del Reglamento de la LFPDPPP. Arts. 22, 23, 24, 25, 26, 28, 29, 31, 32, 33 y 35 de la LFPDPPP; Arts. 89, 90, 92, 93, 95, 96, 97, 98, 101, 102, 103, 104, 105, 106 y 109 del Reglamento de la LFPDPPP.
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	N/A	La normativa en materia de protección de datos no regula el instituto de la cesión de datos personales. Únicamente hace referencia a la transferencia nacional o internacional de datos personales, así como a la remisión.
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros (data processing)? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	Sí	▸ El encargado es la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Este deberá cumplir con las obligaciones establecidas en el art. 50 del Reglamento LFPDPPPP. ▸ Cuando un tercero, a solicitud de un responsable, trate datos personales, este deberá velar por el cumplimiento de los principios de protección de datos personales, debiendo adoptar las medidas necesarias para su aplicación. Estos principios son: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. ▸ El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la LFPDPPP, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica ▸ El tercero que intervenga en cualquier fase del tratamiento de datos personales deberá guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable. ▸ En caso de rectificación o cancelación concedida, el responsable deberá hacer dar conocimiento al tercero de dicha solicitud para que proceda a efectuarla también. ▸ En caso de transferencia de datos, sea esta nacional o internacional, se le deberá comunicar al tercero el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento para que este asuma las mismas obligaciones que le correspondan al responsable que transfirió los datos. Arts. 6, 14, 25 y 36 LFPDPPP, Arts. 49, 50 y 51, Reglamento LFPDPPP.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Conservación de datos	¿Hay obligación de retener/conservar los datos recolectados o procesados por un tiempo determinado? En dicho caso, ¿cuál es el plazo?	Sí	Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron el tratamiento, y deberán atender las disposiciones aplicables a la materia de que se trate, y tomar en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Una vez cumplida la o las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo contrario, el responsable deberá proceder a la cancelación de los datos en su posesión previo bloqueo de los mismos, para su posterior supresión. El titular tendrá en todo momento el derecho a cancelar sus datos personales. La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia. Una vez cancelado el dato se dará aviso a su titular. Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también. Art. 11, LFPDPPP; y arts. 37, 38 y 39 del Reglamento de la LFPDPPP.
Eliminación de datos	¿Existe una obligación de eliminar los datos recolectados o procesados? En dicho caso, ¿en qué supuestos y cuál es el plazo?	Sí	Una vez que los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados. Además, el titular tendrá en todo momento el derecho a cancelar sus datos personales. Ver apartado anterior. Art. 11 LFPDPPP; y arts. 37, 38 y 39 del Reglamento de la LFPDPPP.
Privacy Impact Assessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (Privacy Impact Assessment)?	Sí	El Reglamento de la LFPDPPP si bien no impone como obligación realizar evaluaciones de impacto, aconseja a los responsables contar con un análisis de riesgo de datos personales, como medida para la seguridad de datos personales. Asimismo, dicho reglamento cuenta con un Capítulo "De la Autorregulación Vinculante" (Capítulo VI), mediante el cual alienta tanto a las personas físicas como morales, a adquirir esquemas de autorregulación, los cuales complementan lo dispuesto en las disposiciones en la materia e intentan promover el compromiso de los responsables, aconsejando la implementación de evaluaciones de riesgo, entre otras. Arts. 57, 59, 60, 61, inc. iii) y 80 inc. viii), Reglamento de la LFPDPPP Art. 10 PAPDP.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Incidentes	¿Hay obligación de reportar un incidente de seguridad u algún incumplimiento a las previsiones legales?	Sí	El responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos. Dicha obligación deberá hacerse conforme a los arts. 20 LFPDPPP, arts. 58,63, 64, 65 y 66 del Reglamento de la LFPDPPP.
Sanciones	¿Existen sanciones frente al incumplimiento de dicha obligación? En caso de existir, identificarlas e indicar el monto de las sanciones o penalidad aplicable correspondiente.	No	La normativa no dispone sanciones especificas ante el incumplimiento de la obligación de reportar un incumplimiento. No obstante, el art. 58 del Reglamento de LFPDPPP, dispone que el INAI podrá tomar en consideración el cumplimiento de sus recomendaciones para determinar una potencial atenuación de la sanción que corresponda. En los arts. 63, 64 y 65 del Reglamento LFPDPPP se establecen otras disposiciones relevantes respecto a las vulneraciones de seguridad. En esta línea, la LFPDPPP en sus arts. 64, 66, 67, 68 y 69 detalla el tipo de sanciones que recaerán cuando se comentan incumplimientos en materia de datos personales. Art. 64, 66, 67, 68 y 69 de la LFPDPPP; Arts. 58, 63, 64 y 65 Reglamento de la LFPDPPP.
Acciones legales	¿Existe alguna acción legal de protección de datos personales? ¿quién tiene derecho para ejercerla/ solicitarla?	No	No existe una acción legal especifica que proteja tal derecho. Sin embargo, los titulares pueden ejercer en todo momento los denominados "Derechos ARCO".
Delegado o responsable de la protección de datos personales	¿Existe la figura del delegado de protección de datos (DPO) o similar? En dicho caso, ¿su designación es obligatoria? ¿debe ser designado localmente?	No	El artículo 30 de la LFPDPPP establece que todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos. Asimismo, fomentará la protección de datos personales al interior de la organización.
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	El Instituto Federal de Acceso a la Información y Protección de Datos podrá iniciar el "Procedimiento de Verificación" de oficio o a pedido de parte. La verificación de oficio procederá cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos o se presuma fundada y motivadamente la existencia de violaciones a lo dispuesto en la normativa vigente en materia de protección de datos. Cualquier persona podrá denunciar ante el Instituto las presuntas violaciones a las disposiciones previstas en la LFPDPPP y demás ordenamientos aplicables, siempre que no se ubiquen en los supuestos de procedencia del procedimiento de protección de derechos. En este caso, el Pleno del Instituto determinará, de manera fundada y motivada, la procedencia de iniciar la verificación correspondiente. El derecho a presentar una denuncia precluye en el término de un año contado a partir del día siguiente en que se realicen los hechos u omisiones materia de la misma. Cuando los hechos u omisiones sean de tracto sucesivo, el término empezará a contar a partir del día hábil siguiente al último hecho realizado. A través del procedimiento, el Instituto tendrá acceso a la información y documentación que considere necesarias, de acuerdo a la resolución que lo motive. Los servidores públicos federales estarán obligados a guardar confidencialidad sobre la información que conozcan derivada de la verificación correspondiente. Arts. 59 y 60, LFPDPPP; Arts. 128 y 129, Reglamento de la LFPDPPP.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (ej. GDPR)? ¿Qué diferencias relevantes encuentra?	No	Temas que no contempla la legislación mexicana: ▸ Aplicación extraterritorial de las leyes mexicanas cuando se traten datos personales de mexicanos. ▸ Más supuestos o maneras de dar tratamiento a datos personales sin contar con el consentimiento de los titulares. ▸ Requisitos específicos sobre la elaboración de perfiles y las decisiones basadas en el tratamiento automatizado (artículos 4.4 y 22 del RGPD).
Otras obligaciones	¿Existen otras consideraciones/ requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?		Consideraciones relevantes cuando las finalidades del tratamiento de los datos personales vayan a incluir el envío de publicidad y/u otras finalidades relacionadas con marketing (Art. 30 del Reglamento de la LFPDPPP y Arts. 24, 36 y 40 de los LAV). Requisitos especiales en materia de publicidad y marketing (ArT. 30 del Reglamento de la LFPDPPP).

Panamá

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Normativa	¿Existe en el país una ley de protección de datos personales? En ese caso, identificar normativa aplicable.	Sí	Ley 81 Sobre Protección de Datos, reglamentada por el Decreto Ejecutivo 285 del 28 de mayo de 2021.
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su Sitio Web.	Sí	La Autoridad Nacional de de Transparencia y Acceso a la Informaci[on (ANTAI) https://www.antai.gob.pa/
Ámbito de aplicación	¿Cuál es el ámbito de aplicación de la norma? Es decir, ¿su aplicación es estrictamente territorial, o aplica el concepto de extraterritorialidad?	Sí	La norma permite la aplicación extraterritorial, siempre que el responsable del almacenamiento de esos datos o el custodio de estos cumpla con los estándares de protección de datos personales exigidos por la Ley o pueda demostrar que cumple con los estándares y normas de protección de datos personales iguales o superiores a los exigidos por la Ley de la República de Panamá.
Recolección de datos	¿Cuáles son los requisitos o procesos legales exigidos para la recolección de datos personales? (por ejemplo, consentimiento del titular de los datos, proporcionar información sobre la finalidad del uso de los datos y derechos de su titular, entre otros.	Sí	Todo tratamiento de datos personales estará sujeto al consentimiento previo, informado e inequívoco por un medio que permita al responsable del tratamiento probar la trazabilidad de dicho consentimiento. El consentimiento deberá manifestarse por escrito, o por cualquier otro medio electrónico que garantice la identidad del titular de los datos personales a manera que exista certeza sobre su identidad que la identifique o la haga identificable.
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	**Dato Personal:** Cualquier información concerniente a personas naturales, que las identifica o las hace identificables.
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	**Datos confidenciales.** Aquellos datos que por su naturaleza no deben ser de conocimiento público o de terceros no autorizados, incluyendo aquellos que estén protegidos por ley, por acuerdos de confidencialidad o no divulgación, a fin de salvaguardar información. En los casos de la Administración Pública, son aquellos datos cuyo tratamiento está limitado para fines de esta Administración o si se cuenta con el consentimiento expreso del titular, sin perjuicio de lo dispuesto por leyes especiales o por las normativas que las desarrollen. Los datos confidenciales siempre serán de acceso restringido. **Dato anónimo.** Aquel dato cuya identidad no puede ser establecida por medios razonables o el nexo entre este y la persona natural a la que se refiere. **Dato caduco.** Aquel dato que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiera norma expresa, por el cambio de los hechos o circunstancias que consigna. **Dato personal.** Cualquier información concerniente a personas naturales, que las identifica o las hace identificables. **Dato disociado.** Aquel dato que no puede asociarse al titular ni permitir por su estructura, contenido o grado de desagregación la identificación de la persona, sea esta natural. **Dato sensible.** Aquel que se refiera a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, a la preferencia u orientación sexual, datos genéticos o datos biométricos, entre otros, sujetos a regulación y dirigidos a identificar de manera unívoca a una persona

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Situación de las sociedades y otras personas jurídicas	¿Alcanza la protección de la normativa en materia de datos personales, de las personas jurídicas o de existencial ideal?	Sí	El alcance de esta ley es aplicable a toda persona natural o jurídica que traten datos personales.
Consentimiento del titular de los datos	¿Se requiere la obtención previa del consentimiento del titular de los datos cuando se recaba su información? En tal caso, ¿existen condiciones para la obtención del consentimiento del titular de los datos? (por ejemplo, información previa que deba proporcionarse al titular de los datos).	Sí	Para que el tratamiento de un dato personal sea lícito, deberá ser recolectado y tratado con el consentimiento previo, informado e inequívoco del titular del dato o por fundamento legal. De igual manera deberá obtenerse de una manera que permita su trazabilidad. Para el tratamiento de datos sensibles, además deberá ser irrefutable y expreso. A fin de cumplir con el principio de transparencia toda información o comunicación al titular y deberá ser en lenguaje sencillo y claro, y mantenerlo informado de todos los derechos que le amparan como titular del dato, así como la posibilidad de ejercer los derechos ARCO.
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	Se exceptúan del ámbito de esta Ley aquellos tratamientos que expresamente se encuentren regulados por leyes especiales o por las normativas que las desarrollen, además de los tratamientos de datos personales siguientes: 1. Los que realice una persona natural para actividades exclusivamente personales o domésticas. 2. Los que realicen autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. 3. Los que se efectúen para el análisis de inteligencia financiera y relativos a la seguridad nacional de conformidad con las legislaciones, tratados o convenios internacionales que regulen estas materias. 4. Cuando se trate de tratamiento de datos relacionados con organismos internacionales, en cumplimiento de lo dispuesto en los tratados y convenios vigentes ratificados por la República de Panamá. 5. Los resultantes de información obtenida mediante un procedimiento previo de disociación o anonimización, de manera que el resultado no pueda asociarse al titular de los datos personales.
Contenido y alcance de la información a ser validada por el titular de los datos	¿Cuál es el contenido que debe incluir el consentimiento? (Por ejemplo, uso o destino de los datos, transferencia internacional de los datos, etc.).	Sí	▸ Identidad y datos de contacto del responsable del tratamiento ▸ Finalidad o finalidades del tratamientoCondición legitima ▸ La condición que legitima el tratamiento ▸ Los destinatarios de los datos personales ▸ La intención de transferir datos personales a un tercer país ▸ Plazo de conservación de los datos ▸ Procedimientos para ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad. ▸ Existencia de decisiones automatizadas (incluida la elaboración de perfiles) ▸ Datos de contacto del oficial del de protección de datos personales
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales? ¿Hay requisitos aplicables en relación a la transferencia internacional de datos? (Ejemplo: cláusulas modelos, autorización por parte de la autoridad de control, entre otros).	Sí	Solo el hecho de que el responsable del almacenamiento de esos datos o el custodio de estos cumpla con los estándares de protección de datos personales exigidos por la Ley o pueda demostrar que cumple con los estándares y normas de protección de datos personales iguales o superiores a los exigidos por la Ley de la República de Panamá.
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	No	

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Datos sensibles	¿Qué se entiende por dato sensible? ¿Cómo es el tratamiento de los datos sensibles, de corresponder?	Sí	**Dato sensible: Aquel que se refiera a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, a la preferencia u orientación sexual, datos genéticos o datos biométricos, entre otros, sujetos a regulación y dirigidos a identificar de manera unívoca a una persona natural.**
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (ej. ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, tratamiento y/o uso de la misma? ¿Existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?		Solo a solicitud de la autoridad o en caso de violación o incidente de seguridad de datos.
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	Sí	Se tomará como referencia las normas o estándares nacionales e internacionales en la materia, así como también los mecanismos de autorregulación vinculantes o cualquier otro mecanismo que se determine adecuado para tales fines. Cualquier otra que determine la autoridad de control.
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Ejemplo: rectificación, actualización o supresión).	Sí	A: acceso R: rectificación C: cancelación O: oposición Portabilidad
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	Derecho de acceso: permite al titular obtener sus datos personales que se encuentren almacenados o sujetos a tratamiento en bases de datos de instituciones públicas o privadas, además de conocer el origen y la finalidad para los cuales han sido recabados. Derecho de rectificación: permite al titular solicitar la corrección de sus datos personales que sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes. Derecho de cancelación: permite al titular solicitar la eliminación de sus datos personales incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes. Derecho de oposición: permite al titular, por motivos fundados y legítimos relacionados con una situación en particular, negarse a proporcionar sus datos personales o a que sean objeto de determinado tratamiento, así como a revocar su consentimiento. Derecho de portabilidad: derecho a obtener una copia de los datos personales de manera estructurada, en un formato genérico y de uso común, que permita ser operado por distintos sistemas y/o transmitirlos a otro responsable, cuando: a. El titular haya entregado sus datos directamente al responsable. b. Sea un volumen relevante de datos, tratados de forma automatizada. c. El titular haya dado su consentimiento para el tratamiento o se requiera para la ejecución o el cumplimiento de un contrato. En todo momento, el titular de los datos personales podrá ejercer estos derechos, los cuales son irrenunciables, salvo las excepciones establecidas en leyes especiales.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	Sí	Solo con el consentimiento otorgado.
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros (data processing)? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	Sí	El responsable del tratamiento de datos personales contenidos en bases de datos establecerá los protocolos, procesos y procedimientos de gestión y transferencia segura, protegiendo los derechos de los titulares sobre sus datos bajo los preceptos de esta Ley. Lo anterior será fiscalizado y supervisado por la Autoridad Nacional de Transparencia y Acceso a la Información, con el apoyo de la Autoridad Nacional para la Innovación Gubernamental, cuando se trate de aspectos relacionados a las Tecnologías de la Información y la Comunicación (TICs). Los requerimientos mínimos que deben contener las políticas de privacidad, los protocolos, los procesos y los procedimientos de tratamiento y transferencia segura que deberá cumplir el responsable del tratamiento de datos serán emitidos por el regulador de cada sector bajo conforme a esta Ley.
Conservación de datos	¿Hay obligación de retener/conservar los datos recolectados o procesados por un tiempo determinado? En dicho caso, ¿cuál es el plazo?	Sí	Siete (7) años, salvo la autoridad competente por casos especiales solicite sean conservados por más tiempo.
Eliminación de datos	¿Existe una obligación de eliminar los datos recolectados o procesados? En dicho caso, ¿en qué supuestos y cuál es el plazo?	Sí	En ningún caso el responsable del tratamiento de datos personales y/o el custodio de la base de datos pueden transferir o comunicar los datos que se relacionen con una persona identificada o identificable, después de transcurridos siete años desde que se extinguió la obligación legal de conservarla, salvo que el titular de los datos personales expresamente solicite lo contrario.
Privacy Impact Asessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (Privacy Impact Assessment)?	Sí	
Incidentes	¿Hay obligación de reportar un incidente de seguridad u algún incumplimiento o las previsiones legales?	Sí	Ante la autoridad correspondiente en este caso ANTAI

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Sanciones	¿Existen sanciones frente al incumplimiento de dicha obligación? En caso de existir, identificarlas e indicar el monto de las sanciones o penalidad aplicable correspondiente.	Sí	La Autoridad Nacional de Transparencia y Acceso a la Información fijará los montos de las sanciones aplicables a las respectivas faltas, acordes a la gravedad de las faltas, que se establecerán desde mil balboas (B/.1,000.00) hasta diez mil balboas (B/.10, 000.00), así como reglamentará el procedimiento correspondiente. Se considera infracción leve: 1. No remitir y/o informar a la Autoridad Nacional de Transparencia y Acceso a la Información dentro de los plazos requeridos la información de lo ordenado en esta Ley, su reglamentación o cualquier otra disposición normativa. Art. 40. Se consideran infracciones graves: 1. Efectuar el tratamiento de datos personales sin haber obtenido el consentimiento de su titular, según el procedimiento indicado por esta Ley, su reglamentación o cualquier otra disposición normativa que se refiera a la presente Ley. 2. Infringir los principios y garantías establecidos en la presente Ley o en su reglamentación. 3. Infringir el compromiso de confidencialidad relacionado al tratamiento de los datos personales. 4. Restringir o entorpecer la aplicación de los derechos de acceso, rectificación, cancelación y oposición. 5. Incumplir el deber de informar al titular afectado acerca del tratamiento de sus datos personales, cuando los datos no hayan sido obtenidos del propio titular. 6. Almacenar o archivar datos personales sin contar con las adecuadas condiciones de seguridad que esta Ley o su reglamento disponga. 7. No atender la reiteración de los requerimientos u observaciones formalmente notificados, o no proporcionar la documentación o información formalmente solicitada por la Autoridad Nacional de Transparencia y Acceso a la Información. 8. Entorpecer o no cooperar con la Autoridad Nacional de Transparencia y Acceso a la Información al momento en que esta ejerza su función de inspección. Art. 41. Se consideran infracciones muy graves: 1. Recopilar de datos personales en forma dolosa. 2. No observar de las regulaciones establecidas respecto al tratamiento de los datos sensibles. 3. No suspender el tratamiento de datos personales cuando existiera un previo requerimiento de la Autoridad Nacional de Transparencia y Acceso a la Información para ello. 4. Almacenar o transferir internacionalmente datos personales, violentando lo establecido en esta Ley. 5. Reincidir en las faltas graves. Art. 42. Las sanciones que imponga la Autoridad Nacional de Transparencia y Acceso a la Información a los responsables de las bases de datos y demás sujetos alcanzados por el régimen de la presente ley y sus reglamentos, se graduarán dependiendo de la gravedad de la infracción cometida. Art. 43. Las infracciones a esta Ley serán sancionadas así: 1. Falta leve, citación ante la Autoridad Nacional de Transparencia y Acceso a la Información con relación a registros o atender faltas. 2. Faltas graves, multas según su proporcionalidad. 3. Faltas muy graves:

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Acciones legales	¿Existe alguna acción legal de protección de datos personales? ¿quién tiene derecho para ejercerla/ solicitarla?	Sí	Quien resulte afectado por la vulneración de sus datos personales.
Delegado o responsable de la protección de datos personales	¿Existe la figura del delegado de protección de datos (DPO) o similar? En dicho caso, ¿su designación es obligatoria? ¿debe ser designado localmente?	Sí	La Designación obligatoria
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (ej. GDPR)? ¿Qué diferencias relevantes encuentra?	Sí	
Otras obligaciones	¿Existen otras consideraciones/ requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?		

Paraguay

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Normativa	¿Existe en el país una ley de protección de datos personales? En ese caso, identificar normativa aplicable.	Sí	La protección de datos personales en Paraguay está regulada por varias disposiciones normativas de forma directa o transversal. La Ley Nº 6.534/2.020 de "Protección de Datos Personales Crediticios", fue promulgada recientemente el 27 de octubre del 2020, derogando la Ley Nº 1.682/2.001 y sus modificaciones, y estableciendo un nuevo régimen de protección de datos e información personal en Paraguay. Este marco normativo se complementa principalmente con otras normas tales como: ‣ Constitución de la República del Paraguay (1992). (Art. 33 "Derecho a la Intimidad", Art. 36 "Derecho de la Inviolabilidad del Patrimonio Documental y la Información Privada", Art. 45 "De los Derechos y Garantías o enunciados", Art. 135 Habeas Data) ‣ Ley Nº 4.868/2.013 de "Comercio Electrónico"; ‣ Ley Nº 6822/2.021 "De los Servicios de Confianza para las Transacciones Electrónicas, del Documento Electrónico y los Documentos Transmisibles Electrónicos (promulgada en diciembre del 2021)" ‣ Ley Nº 861/1996 "General de Bancos, Financieras y otras entidades de Crédito" ‣ Ley Nº 5.830/2.017 "Que prohíbe la publicidad no autorizada por los usuarios titulares de telefonía móvil" ‣ Ley de Nº 5.282/2.014 "Del libre acceso al ciudadano a la Información Pública y Transparencia Gubernamental. Es dable mencionar que de acuerdo con el artículo 1, la Ley Nº 6.534/20 tiene por objeto garantizar la protección de datos crediticios de toda persona, cualquiera sea su nacionalidad, residencia o domicilio. También regula la actividad de recolección y el acceso a datos de información crediticia, así como la constitución, organización, funcionamiento, derechos, obligaciones y extinción de las empresas que se dediquen a la obtención y provisión de información crediticia, con el fin de preservar los derechos fundamentales, la intimidad, la autodeterminación informativa, la libertad, la seguridad y el trato justo de las personas, conforme a la Constitución, sus disposiciones e instrumentos internacionales en la materia que fueran ratificados. La Ley Nº 6.534/20 pone más énfasis en tratar los aspectos vinculados a la información crediticia de toda persona, cualquiera sea su nacionalidad, residencia o domicilio, en entidades bancarias, financieras, burós de créditos. Destacamos igualmente que la ley también contempla la definición de Datos Personales y Datos Personales Sensibles, con todas las particularidades a tener en cuenta para su tratamiento. La Constitución de la República contiene disposiciones específicas como el Art. 33 "Derecho a la Intimidad", Art. 36 "Derecho de la Inviolabilidad del Patrimonio Documental y la Información Privada", Art. 45 "De los Derechos y Garantías o enunciados", Art. 135 "Habeas Data" y otros, que forman parte de las disposiciones específicas complementarias vinculadas a la protección de datos personales en el país. Vale recalcar que la enunciación de los derechos y garantías contenidos en la Constitución no debe entenderse como negación de otros que, siendo inherentes a la personalidad humana, no figuren expresamente en ella. La falta de ley reglamentaria no podrá ser invocada para negar ni para menoscabar algún derecho o garantía, según la propia Constitución en su Art. 45. En mayo del 2021, se ha presentado el proyecto de ley denominado "Ley de Protección de Datos Personales en Paraguay" el cual está en pleno estudio por parte del Congreso y cuyas disposiciones prevén ocuparse finalmente del tratamiento integral de datos personales.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su Sitio Web.	Sí	En el marco de la Ley Nº 6.534/20 se designa al Banco Central del Paraguay (BCP): https://www.bcp.gov.py/ y la Secretaría de Defensa del Usuario y Consumidor (SEDECO): http://www.sedeco.gov.py/ como los órganos de control y autoridades de aplicación de sus disposiciones.
Ámbito de aplicación	¿Cuál es el ámbito de aplicación de la norma? Es decir, ¿su aplicación es estrictamente territorial, o aplica el concepto de extraterritorialidad?	Sí	La Ley Nº 6.534/20 determina que es de aplicación obligatoria al tratamiento de datos personales en registros públicos o privados recopilados o almacenados en territorio paraguayo.
Recolección de datos	¿Cuáles son los requisitos o procesos legales exigidos para la recolección de datos personales? (por ejemplo, consentimiento del titular de los datos, proporcionar información sobre la finalidad del uso de los datos y derechos de su titular, entre otros.	Sí, parcialmente en lo referente a datos crediticios	La Ley Nº 6.534/20 garantiza a toda persona el derecho de ser informado en forma expresa y clara sobre la finalidad que se le dará sus datos requeridos y así poder manifestar expresamente su consentimiento para la obtención y uso de ellos. El consentimiento debe otorgarse de manera libre, específica, inequívoca e informada, mediante una declaración o una clara acción afirmativa para el tratamiento de los datos personales. Deberá constar de manera escrita, electrónica, digital u otro mecanismo fehaciente. Es decir, el consentimiento debe darse en las condiciones que no admitan dudas de su otorgamiento. Se entiende por "tratamiento", cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados, realizadas sobre datos personales, relacionadas de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, cesión, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales. Igualmente, el derecho de la autodeterminación informativa reconocido en la ley establece que el titular de los datos debe conocer el uso que se haga de los mismos o su finalidad y a requerir su acceso, rectificación, cancelación y oposición (el ejercicio de los denominados "Derechos ARCO").
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	La Ley Nº 6.534/20 define a datos personales como la "Información de cualquier tipo, referida a personas jurídicas o personas físicas determinadas o determinables". Se entiende por determinable la persona que pueda ser identificada mediante algún identificador o por uno o varios elementos característicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Los derechos y garantías de protección de datos personales serán extendidos a personas jurídicas en cuanto le sean aplicables. En el contexto crediticio se entiende como aquella información, positiva y negativa, relacionada con el historial crediticio de personas físicas y jurídicas, acerca de actividades crediticias, comerciales y otras de naturaleza análoga, que sirva para identificar correcta e inequívocamente a la persona, su domicilio, actividad comercial, determinar su nivel de endeudamiento, de cumplimiento de sus obligaciones y, en general, de riesgos crediticios en un determinado momento.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	En el marco de la Ley Nº 6.534/20, se establecen las siguientes categorías de datos: Datos sensibles: Aquellos que se refieran a la esfera íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular. Son considerados sensibles los datos personales que puedan revelar aspectos como el origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física. Información crediticia: Aquella información, positiva y negativa, relacionada con el historial crediticio de personas físicas y jurídicas, acerca de actividades crediticias, comerciales y otras de naturaleza análoga, que sirva para identificar correcta e inequívocamente a la persona, su domicilio, actividad comercial, determinar su nivel de endeudamiento, el cumplimiento de sus obligaciones y en general, de riesgos crediticios en un determinado momento.
Situación de las sociedades y otras personas jurídicas	¿Alcanza la protección de la normativa en materia de datos personales, de las personas jurídicas o de existencial ideal?	Sí	Ley Nº 6.534/20 alcanza a los datos relativos a personas de existencia ideal o jurídicas, determinadas o determinables.
Consentimiento del titular de los datos	¿Se requiere la obtención previa del consentimiento del titular de los datos cuando se recaba su información? En tal caso, ¿existen condiciones para la obtención del consentimiento del titular de los datos? (por ejemplo, información previa que deba proporcionarse al titular de los datos).	Sí parcialmente en lo referente a datos crediticios	En el marco de la Ley Nº 6.534/20, el titular debe conocer la finalidad que se le dará a sus datos para así otorgar o no su consentimiento en cuanto a su tratamiento. Como se ha mencionado, el consentimiento debe ser otorgado de forma libre, específica, inequívoca e informada, mediante una declaración o una clara acción afirmativa. Podrá ser revocado de forma expresa en las mismas condiciones y a título gratuito. Este acto no generará efecto retroactivo. Reiteramos, que las disposiciones específicas incluidas en la Constitución como el Art. 33 "Derecho a la Intimidad", Art. 36 "Derecho de la Inviolabilidad del Patrimonio Documental y la Información Privada" y otros análogos, que recaen sobre la información y datos de una persona, deben ser tenidos en cuenta al momento de recabar información. Como se ha resaltado, la enunciación de los derechos y garantías contenidos en la Constitución no debe entenderse como negación de otros que, siendo inherentes a la personalidad humana, no figuren expresamente en ella. La falta de ley reglamentaria no podrá ser invocada para negar ni para menoscabar algún derecho o garantía.
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	No será necesario el consentimiento cuando los datos se obtengan de fuentes de acceso público; o cuando requieran ser revelados por autoridad competente mediando orden judicial o se recaben para el ejercicio de funciones propias del Estado. La Ley Nº 6.534/2020, dispone expresamente que las personas responsables y encargadas del tratamiento de información crediticia de terceros, y quienes intervengan en cualquier fase de su recolección, procesamiento, almacenamiento, uso o circulación deben mantener su secreto, salvo orden de autoridad competente.
Contenido y alcance de la información a ser validada por el titular de los datos	¿Cuál es el contenido que debe incluir el consentimiento? (Por ejemplo, uso o destino de los datos, transferencia internacional de los datos, etc.).	Sí	Ver la respuesta en Recolección de datos.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales? ¿Hay requisitos aplicables en relación a la transferencia internacional de datos? (Ejemplo: cláusulas modelos, autorización por parte de la autoridad de control, entre otros).	Sí	La Ley Nº 6.534/20 dispone que la transferencia de datos personales será posible siempre que medie consentimiento y exista una clara manifestación sobre los fines y usos de los datos. En consecuencia, está prohibido transferir datos personales a otras personas o empresas en contravención de las reglas establecidas en las disposiciones vigentes. La ley dispone la prohibición de transferir datos personales de cualquier tipo a países u organismos internacionales o supranacionales que no proporcionen las garantías reconocidas, requisitos o excepciones establecidos en la Ley ni aporten los niveles de protección adecuados. Estas situaciones son infracciones a la luz de la norma y derivan en la aplicación de sanciones por parte de las autoridades competentes. Actualmente, no se cuenta con una lista de jurisdicciones que no cumplan los requisitos citados arriba. No se contemplan referencias en cuando a modelos de contratos para ser empleados en transferencias internacionales de datos a países no adecuados, tanto en caso de cesiones de datos como en los supuestos de prestación de servicios.
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	No	No.
Datos sensibles	¿Qué se entiende por dato sensible? ¿Cómo es el tratamiento de los datos sensibles, de corresponder?	Sí	De conformidad a la Ley Nº 6.534/20, se entiende por datos sensibles a los datos personales que revelan: ‣ Origen racial y étnico; ‣ Opiniones políticas; ‣ Convicciones religiosas, filosóficas o morales; ‣ Afiliación sindical; ‣ Información referente a la salud o a la vida sexual; ‣ Datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física; Se prohíbe dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables.
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (ej. ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, tratamiento y/o uso de la misma? ¿Existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	No	A la fecha, no existe por ley un Registro de Base de Datos en Paraguay.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	Sí, parcialmente en lo referente a datos crediticios.	En cuanto a la seguridad de los datos, la Ley Nº 6.534/20 dispone que el Responsable del Tratamiento de los datos personales crediticios deberá garantizar la adopción e implementación de medidas técnicas, organizativas y de seguridad necesarias para salvaguardar el acceso y la integridad de los datos personales a fin de evitar su alteración, pérdida, consulta, comercialización o acceso no autorizado. Así mismo, existe una obligación expresa para los Burós de Información Crediticia de manejar la información con altos estándares de ética, confidencialidad y seguridad. La recolección, almacenamiento y transmisión de datos personales de terceros por medio de mecanismos inseguros o que de alguna forma no garanticen la seguridad e inalterabilidad de los datos; así como la notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales, son infracciones establecidas a la ley. Existe protección constitucional de conformidad a los Art. 33 "Derecho a la Intimidad", Art. 36 "Derecho de la Inviolabilidad del Patrimonio Documental y la Información Privada" y otros análogos, contemplados en la Constitución y que ya fueron mencionados previamente.
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Ejemplo: rectificación, actualización o supresión). Identificar y explicar.	Sí	En el marco de la Ley Nº 6.534/20, el titular de los datos tiene los siguientes derechos: ‣ Derecho de acceso; ‣ Derecho a actualización y/o rectificación; ‣ Derecho de supresión; ‣ Derecho de oposición; ‣ Derecho de portabilidad; ‣ Derecho al olvido. Adicionalmente, nos remitimos a la figura del Habeas Data de la Constitución que garantiza que toda persona puede solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	De conformidad a la Ley Nº 6.534/20, cualquier persona podría solicitar la rectificación o supresión de sus datos personales en poder de cualquier persona o empresa, extendiendo este derecho más allá de la garantía de Habeas Data (CN. Art. 135), que asegura a toda persona el derecho a solicitar judicialmente la actualización, rectificación o destrucción de datos personales erróneos sobre la misma o que afecten ilegítimamente sus derechos que obren en registros oficiales o privados de carácter público (de acceso público, como los Burós de Información Crediticia). El titular de los datos o su representante legal podrá solicitar, en cualquier momento al Responsable del Tratamiento, el acceso, la actualización, la rectificación, la supresión, la oposición y portabilidad de los datos personales que le conciernen. Los responsables del manejo de la información deben establecer medios y procedimientos sencillos, rápidos, accesibles y gratuitos para que el titular pueda ejercer sus derechos. La acción de amparo es otra herramienta legal de conformidad a la Constitución Nacional [protegiendo el Art. 33 o Art. 36 y otros]. Este procedimiento, no está taxativamente contemplado en el marco legal de referencia, pero sería viable de conformidad al Art. 45 de la Constitución. La acción colectiva [class action] no está contemplada en la legislación del Paraguay, por lo que la acción colectiva de titulares de datos no tiene aún procedimiento judicial determinado. También sería potencialmente viable la presentación de una acción de inconstitucionalidad contra cualquier resolución judicial o norma jurídica que atente contra los principios y garantías reconocidos a toda persona.
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	Sí, parcialmente en lo referente a datos crediticios.	En el marco de la Ley Nº 6.534/20, el tratamiento y la cesión de datos personales sería posible, siempre y cuando concurra el consentimiento de su titular y exista una notificación fehaciente sobre la finalidad de los datos. La ley define al Encargado de Tratamiento de datos como la persona física o jurídica, autoridad u otro organismo que trate datos personales por cuenta del Responsable del Tratamiento, este último, es la persona física o jurídica, autoridad u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento de los datos.
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros (data processing)? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	Sí	En el marco de la Ley Nº 6.534/20, será posible siempre y cuando exista consentimiento, y no se apliquen o utilicen con un fin distinto al que figure en el contrato. Favor remitirse a los comentarios sobre Responsable y Encargado del Tratamiento de Datos.
Conservación de datos	¿Hay obligación de retener/conservar los datos recolectados o procesados por un tiempo determinado? En dicho caso, ¿cuál es el plazo?	Si	En el marco de la Ley Nº 6.534/20, se establece el derecho al olvido de los datos crediticios. Los datos sobre una persona o empresa que obre en un registro pueden ser conservados hasta por 5 (cinco) años, contados desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que establezca otro plazo o si las partes pactan un plazo menor. Si la información debe conservarse más allá del plazo máximo, los datos personales del titular deben desasociarse de la misma.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Eliminación de datos	¿Existe una obligación de eliminar los datos recolectados o procesados? En dicho caso, ¿en qué supuestos y cuál es el plazo?	Sí, parcialmente en lo referente a datos crediticios.	Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. Por otro lado, los datos deberán eliminarse en caso de que el titular del dato lo solicite o cuando hubiesen caducado. Igualmente, el hecho de negarse injustificadamente a eliminar o rectificar Datos Personales o Información Crediticia de una persona que así lo haya solicitado por medio claro e inequívoco constituye una infracción a la luz de la normativa vigente estando facultada tanto el BCP como la SEDECO a implementar sanciones. Reiteramos que, en el marco de las garantías reconocidas en la Constitución, toda persona podría solicitar a través del Habeas Data o el Amparo la destrucción de sus datos cuando se encuentre afectada ilegítimamente en sus derechos.
Privacy Impact Asessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (Privacy Impact Assessment)?	No	No se prevé en la ley.
Incidentes	¿Hay obligación de reportar un incidente de seguridad u algún incumplimiento a las previsiones legales?	Si	En el marco de la Ley 6.534/20, el responsable del tratamiento de los datos personales crediticios deberá garantizar la adopción e implementación de medidas técnicas, organizativas y de seguridad necesarias para salvaguardar el acceso y la integridad de los datos personales, a fin de evitar su alteración, pérdida, consulta, comercialización o acceso no autorizado.
Sanciones	¿Existen sanciones frente al incumplimiento de dicha obligación? En caso de existir, identificarlas e indicar el monto de las sanciones o penalidad aplicable correspondiente.	Sí	En el marco de la Ley Nº 6.534/20, tanto el BCP o la SEDECO pueden imponer las siguientes sanciones a los responsables de infracciones a la Ley. Las sanciones van desde apercibimientos, multas, suspensiones, cierres temporales, hasta inhabilitaciones. a) Multa de hasta 15.000 jornales mínimos (aproximadamente US$ 178.500), duplicándose en caso de reincidencia (30.000 jornales mínimos, equivalente a aprox. US$ 357.000); pudiendo elevarse a 50.000 jornales mínimos (aproximadamente US$ 595.000) en casos de personas o empresas que tengan una facturación anual superior a Gs. 6.000.000.000 (aproximadamente US$ 853.000); b) Suspensión de las actividades relacionadas con el tratamiento de datos hasta por seis meses, indicándose las medidas correctivas que deben adoptarse; c) Inhabilitación para desempeñar un empleo, cargo o comisión dentro del sistema financiero, crediticio y en Burós de Información Crediticia de entre seis meses y cinco años; d) Cierre temporal de las operaciones relacionadas con el tratamiento de datos una vez transcurrido el término de suspensión sin que se hubieren adoptado las medidas correctivas ordenadas por la autoridad de control; e) Cierre inmediato y definitivo de la operación que involucre el tratamiento de Datos Sensibles. Las sanciones administrativas, que pueden ser graduadas por la autoridad de aplicación competente según su gravedad, son independientes de las medidas correctivas o cautelares que dicten dichas autoridades para salvaguardar el interés público protegido por la Ley Nº 6.534/20. Las sanciones pueden ser recurridas ante la justicia contencioso-administrativa.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Acciones legales	¿Existe alguna acción legal de protección de datos personales? ¿quién tiene derecho para ejercerla/ solicitarla?	Sí	La acción de protección de los datos personales podrá ser ejercida por el afectado por sí o por intermedio de apoderado. En el caso de personas fallecidas, el ejercicio de los derechos establecidos corresponderá a sus herederos o legatarios.
Delegado o responsable de la protección de datos personales	¿Existe la figura del delegado de protección de datos (DPO) o similar? En dicho caso, ¿su designación es obligatoria? ¿debe ser designado localmente?	No	La normativa no establece la figura de un delegado oficial de protección de datos. Favor remitirse a los comentarios sobre Responsable y Encargado del tratamiento de datos personales.
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	El BCP y la SEDECO tienen amplias facultades de conformidad a la Ley Nº 6.534/20 y deben coordinar esfuerzos para que la misma se cumpla.
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (ej. GDPR)? ¿Qué diferencias relevantes encuentra?	No	La normativa paraguaya no contempla todos los requisitos contemplados por la normativa internacional.
Otras obligaciones	¿Existen otras consideraciones/ requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	N/A	

Perú

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Normativa	¿Existe en el país una ley de protección de datos personales? En ese caso, identificar normativa aplicable.	Sí	El régimen de protección de datos personales se compone de las siguientes regulaciones. ‣ Constitución Política del Perú (1993), Artículo 2 Nº6. ‣ La Ley 29.733 - se conoce como 'Ley de Protección de Datos Personales' ("LPDP"). ‣ Decreto Supremo 003-2013-JUS, que reglamenta la LPDP. ("Decreto Supremo"). ‣ Resolución Directoral 019-2013-JUS/DGPDP, Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales. ‣ Resolución Directoral 080-2019-JUS/DGTAIPD, Guía del Deber de Informar. ‣ Directiva 01-2020-JUS/DGTAIPD, sobre Tratamiento de Datos Personales mediante Sistemas de Videovigilancia, aprobada por Resolución Directoral 02-2020-JUS/DGTAIPD. ‣ Decreto de Urgencia 007-2020, Ley Marco de Confianza Digital ‣ Resolución Ministerial 326-2020-JUS, Metodología para el Cálculo de Multas en Materia de Protección de Datos Personales.
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su Sitio Web.	Sí	Autoridad Nacional de Protección de Datos Personales, órgano adscrito al Ministerio de Justicia y Derechos Humanos. Portal web: https://www.gob.pe/anpd
Ámbito de aplicación	¿Cuál es el ámbito de aplicación de la norma? Es decir, ¿su aplicación es estrictamente territorial, o aplica el concepto de extraterritorialidad?	Sí	El ámbito de aplicación es territorial (artículo 3 de la LPDP), es decir, referidos al tratamiento de datos personales en el territorio nacional, sin embargo, hay cláusulas extraterritoriales en el artículo 5 del Decreto Supremo. Por ejemplo, cuando el responsable del tratamiento no está ubicado en territorio peruano pero (i) le resulta de aplicación la normativa peruana por disposición contractual o derecho internacional o (ii) cuando utilice medios o soportes ubicados en Perú.
Recolección de datos	¿Cuáles son los requisitos o procesos legales exigidos para la recolección de datos personales? (por ejemplo, consentimiento del titular de los datos, proporcionar información sobre la finalidad del uso de los datos y derechos de su titular, entre otros.	Sí	Para el tratamiento de los datos personales debe mediar el consentimiento del titular. Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. Tal como surge del artículo 13 inciso 5 de la LPDP, los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, a excepción de que la ley disponga lo contrario. Conforme a lo establecido en el artículo 12 del Decreto Supremo, el consentimiento debe ser libre, previo, informado, expreso e inequívoco. Asimismo, de acuerdo con lo previsto en el artículo 14 del Decreto Supremo, para el caso de datos sensibles (por ejemplo, relativos a la salud o ingresos económicos) el consentimiento debe ser, además, por escrito (esto incluye medios digitales con algunos mecanismos de autenticación).
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	La LPDP en su artículo 2, define como dato personal a toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados. A su vez, en el artículo 2 inciso 4 del Decreto Supremo, lo define como la información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	En adición al concepto general de datos personales, la LPDPy el Decreto Supremo reconocen dos tipos particulares de datos personales: **Datos sensibles:** datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual. (Artículo 2 inciso 5 de la LPDP) **Datos personales relacionados con la salud:** Es aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética. (artículo 2 inciso 5 del Decreto Supremo).

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Situación de las sociedades y otras personas jurídicas	¿Alcanza la protección de la normativa en materia de datos personales, de las personas jurídicas o de existencial ideal?	No	El ámbito de aplicación de la LPDP y el Decreto Supremo no alcanza a la información relativa a las personas jurídicas.
Consentimiento del titular de los datos	¿Se requiere la obtención previa del consentimiento del titular de los datos cuando se recaba su información? En tal caso, ¿existen condiciones para la obtención del consentimiento del titular de los datos? (por ejemplo, información previa que deba proporcionarse al titular de los datos).	Sí	La obtención del consentimiento debe ser de manera libre, previa, expresa e inequívoca y por último informada como surge del artículo 18 de la LPDP y artículo 12 del Decreto Supremo. De acuerdo con lo previsto en el artículo 14 del Decreto Supremo, para el caso de datos sensibles (por ejemplo, relativos a la salud o ingresos económicos) el consentimiento debe ser, además, por escrito.
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los casos establecidos en el artículo 14 de la LPDP. Por ejemplo (i) cuando el tratamiento de los datos personales se realiza para el ejercicio de las funciones de las entidades públicas; (ii) cuando los datos personales sean necesario para la preparación celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte; o (iii) cuando dicha información está contenida en fuentes accesibles (registros públicos, diarios, páginas web, etc.) para el público.
Contenido y alcance de la información a ser validada por el titular de los datos	¿Cuál es el contenido que debe incluir el consentimiento? (Por ejemplo, uso o destino de los datos, transferencia internacional de los datos, etc.).	Sí	Tal como lo establece el artículo 18 de la LPDP, el titular de los datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados, los destinatarios (de la transferencia nacional o internacional) de su información, la existencia del banco de datos personales, la identidad y el domicilio de su titular y, de ser el caso, del encargado del tratamiento de sus datos personales, el tiempo de conservación de su información y la posibilidad de ejercer sus derechos para proteger sus datos personales.
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales? ¿Hay requisitos aplicables en relación a la transferencia internacional de datos? (Ejemplo: cláusulas modelos, autorización por parte de la autoridad de control, entre otros).	Sí	Para el flujo transfronterizo de datos personales, el titular y el encargado del banco de datos personales deben realizar el flujo transfronterizo de datos personales solo si el país destinatario mantiene niveles de protección adecuados conforme a la LPDP. En caso de que el país destinatario no cuente con un nivel de protección adecuado, el emisor del flujo transfronterizo de datos personales debe garantizar que el tratamiento de los datos personales se efectúe conforme a lo dispuesto por la ley.} Asimismo, conforme con lo establecido en el artículo 25 del Decreto Supremo, para la formalización del flujo transfronterizo (transferencia internacional de datos personales) se puede utilizar cláusulas contractuales u otros instrumentos jurídicos a fin de establecer las obligaciones de ambas partes (país emisor y país receptor).
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	No	El Decreto Supremo en su artículo 21 establece, a través de la figura denominada "código de conducta", un supuesto para el caso de transferencias de datos personales dentro de grupos empresariales, sociedades subsidiarias afiliadas o vinculadas bajo el control común del mismo grupo del titular del banco de datos personales o responsable del tratamiento.
Datos sensibles	¿Qué se entiende por dato sensible? ¿Cómo es el tratamiento de los datos sensibles, de corresponder?	Sí	Los datos sensibles se definen en el numeral 5 del artículo 2 de la LPDP y en el numeral 6 del artículo 2 del Decreto Supremo. Los datos sensibles son definidos como aquellos datos referidos a datos biométricos, origen racial y étnico, ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales, afiliación sindical, la salud o vida sexual. El consentimiento debe ser otorgado por escrito, a través de su firma manuscrita, firma digital o cualquier otro mecanismo de autenticación que garantice la voluntad inequívoca del titular tal como lo indica el artículo 14 del Decreto Supremo.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (ej. ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, tratamiento y/o uso de la misma? ¿Existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	Sí	El Registro Nacional de Protección de Datos Personales es un registro de carácter administrativo y público a cargo de la Autoridad Nacional de Protección de Datos Personales, que tiene como finalidad de inscribir en forma diferenciada, a nivel nacional, los bancos de datos personales, las comunicaciones transfronterizas y las sanciones respectivas. La omisión de inscribir los bancos de datos personales en el Registro Nacional de Protección de Datos Personales, constituye una infracción leve conforme lo dispone el literal e) del numeral 1 del artículo 132 del Decreto Supremo. La inscripción de un banco de datos personales deberá estar actualizada en todo momento. Cualquier modificación que afecte el contenido de la inscripción deberá ser previamente comunicada a la Dirección de Protección de Datos Personales.
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	Sí	Los sistemas informáticos que manejen bancos de datos personales deberán incluir en su funcionamiento lo que surge del artículo 39 del Decreto supremo: 1. El control de acceso a la información de datos personales. 2. Generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos y una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros. Conforme al artículo 42 del Decreto Supremo, la documentación no automatizada (armarios o archivadores) debe encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deben permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el banco de datos personales.
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Ejemplo: rectificación, actualización o supresión). Identificar y explicar.	Sí	El titular de los datos tiene los siguientes derechos, establecidos en los artículos 18 a 24 de la LPDP: ‣ Derecho de acceso. ‣ Derecho de actualización, inclusión, rectificación y supresión. ‣ Derecho a impedir el suministro. ‣ Derecho de oposición. ‣ Derecho al tratamiento objetivo. ‣ Derecho a la tutela El Capítulo II (Disposiciones especiales) del Decreto Supremo regula el procedimiento para ejercer el "derecho a la información" (artículo 60) y los denominados "derechos ARCO": ‣ Derecho de acceso (artículo 61) ‣ Derecho de rectificación (artículo 65) ‣ Derecho de cancelación (artículo 67) ‣ Derecho de oposición (artículo 71)
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	El procedimiento para ejercer los derechos por parte de los titulares de los datos se encuentra establecido en los artículos 47 al 75 del Decreto Supremo. De acuerdo con el artículo 50 del Decreto Supremo, para ejercer cualquiera de los derechos mencionados, se debe presentar una solicitud con la información siguiente: (i) nombres y apellidos del titular de los datos personales; (ii) petición concreta, descripción clara del dato personal vinculado al ejercicio del derecho y la manifestación expresa del derecho que pretende ejercer; (iii) documentos que sustenten la petición; (iv) dirección a donde se realizarán las comunicaciones que correspondan; y, (v) fecha y firma. Si el ejercicio del derecho se efectúa por un representante, se debe acreditar su representación. El artículo 55 del Decreto Supremo establece plazos de respuesta específicos. Por ejemplo, para la solicitud sobre el derecho de información es de ocho (8) días y de las solicitudes sobre derechos de rectificación, cancelación y oposición es de diez (10) días hábiles. Por su parte, la solicitud sobre el derecho de acceso tiene un plazo de respuesta de veinte (20) días hábiles. Estos plazos podrán ser ampliados por una sola vez y por un periodo igual, siempre que las circunstancias lo justifiquen.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	Sí	Cuando los datos personales se transfieren a otra entidad, los destinatarios -quienes reciben la información- deben estar obligados a manejar dichos datos personales de acuerdo con las disposiciones de la LPDP y el Decreto Supremo. Por ejemplo, conforme con el tercer párrafo del artículo 18 de la LPDP, si con posterioridad al consentimiento brindado por el titular de los datos personales se produce la transferencia de su información por fusión, adquisición de cartera, o supuestos similares, el nuevo responsable del tratamiento debe establecer un mecanismo de información eficaz para el titular de los datos personales.
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros (data processing)? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	Sí	Según el artículo 30 de la LPDP, cuando, por cuenta de terceros, se presten servicios de tratamiento de datos personales, estos no pueden aplicarse o utilizarse con un fin distinto al que figura en el contrato o convenio celebrado ni ser transferidos a otras personas, ni aun para su conservación. Conforme con el artículo 36 del Decreto Supremo, el encargado del banco de datos personales se encuentra prohibido a transferir a terceros los datos personales objeto de la prestación de servicios de tratamiento, a menos que el titular del banco de datos personales que le encargó el tratamiento lo haya autorizado y el titular del dato personal haya brindado su consentimiento. El plazo para la conservación será de dos (2) años contado desde la finalización del último encargo realizado. De acuerdo con el artículo 37 del Decreto Supremo, el tratamiento de datos personales puede realizarse por un tercero diferente al encargado del tratamiento a través de un convenio o contrato entre estos dos (subcontratación).
Conservación de datos	¿Hay obligación de retener/conservar los datos recolectados o procesados por un tiempo determinado? En dicho caso, ¿cuál es el plazo?	No	Si bien la LPDP y el Decreto Supremo no establecen un plazo específico para retener/conservar los datos personales, el numeral 6.13 de la Directiva 01-2020-JUS/DGTAIPD, sobre Tratamiento de Datos Personales mediante Sistemas de Videovigilancia, dispone que los datos personales (imágenes) obtenidos a través de cámaras de videovigilancia deberán ser almacenados por un período mínimo de 30 días hábiles y máximo de 60 días hábiles, salvo disposición distinta en normas sectoriales.
Eliminación de datos	¿Existe una obligación de eliminar los datos recolectados o procesados? En dicho caso, ¿en qué supuestos y cuál es el plazo?	No	El único supuesto regulado sobre la obligación de eliminar los datos personales (imágenes) se encuentra contenido en el numeral 6.15 de la Directiva 01-2020-JUS/DGTAIPD, sobre Tratamiento de Datos Personales mediante Sistemas de Videovigilancia. Este numeral establece que, una vez trascurrido el plazo de conservación de la información y no habiendo requerimiento de alguna autoridad competente para entregar o visualizar el contenido de la grabación, los archivos que contienen datos personales deben ser eliminados en un plazo máximo de dos (02) días hábiles. Este plazo máximo no será aplicable cuando exista alguna finalidad o interés legítimo que justifique su conservación (numeral 6.16 de la citada Directiva). Por ejemplo, cuando el dato personal (imagen) haya sido considerado como medio probatorio en una investigación policial o procedimiento administrativo y/o judicial.
Privacy Impact Asessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (Privacy Impact Assessment)?	No	No se prevé en la LPDP ni en el Decreto Supremo.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Incidentes	¿Hay obligación de reportar un incidente de seguridad u algún incumplimiento a las previsiones legales?	Sí	El literal e) del numeral 9.1 del artículo 9 de la Ley Marco de Confianza Digital establece que los proveedores de servicios digitales están obligados a reportar y colaborar con la Autoridad Nacional de Protección de Datos Personales cuando verifiquen un incidente de seguridad digital que involucre datos personales. Si bien la LPDP y el Decreto Supremo no imponen obligación alguna para que los responsables del tratamiento o titulares de bancos de datos personales reporten incidentes de seguridad ante la Autoridad Nacional de Protección de Datos Personales, sí se recomienda, como una buena práctica, que dichos incidentes sean informados a los interesados tan pronto como se confirme la incidencia.
Sanciones	¿Existen sanciones frente al incumplimiento de dicha obligación? En caso de existir, identificarlas e indicar el monto de las sanciones o penalidad aplicable correspondiente.	Sí	El artículo 38 de la LPDP clasifica a las infracciones en leves, graves y muy graves, las cuales son tipificadas en el artículo 132 del Decreto Supremo. El artículo 39 de la LPDP establece que las infracciones leves son sancionadas desde 0,5 Unidad Impositiva Tributaria (UIT) hasta 5 UIT; las graves desde más de 5 UIT hasta 50 UIT; y, las muy graves desde más de 50 UIT hasta 100 UIT. Cabe precisar que, para el año 2022, la UIT asciende a S/ 4 600,00 equivalente a un aproximado de U$S 1 210,00. La calificación y descripción de las infracciones están contempladas en el artículo 132 del Decreto Supremo.
Acciones legales	¿Existe alguna acción legal de protección de datos personales? ¿quién tiene derecho para ejercerla/ solicitarla?	Sí	El artículo 24 de la LPDP contempla la posibilidad de que en caso se deniegue al titular de datos personales el ejercicio de sus derechos, este puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación (ámbito administrativo) o al Poder Judicial para los efectos de la correspondiente acción de hábeas data (ámbito jurisdiccional).
Delegado o responsable de la protección de datos personales	¿Existe la figura del delegado de protección de datos (DPO) o similar? En dicho caso, ¿su designación es obligatoria? ¿debe ser designado localmente?	No	Actualmente no hay obligación legal para designar un oficial de protección de datos (DPO). Sin embargo, en la Directiva de Seguridad emitida por la Autoridad Nacional de Protección de Datos Personales establece, como disposición específica de medidas de seguridad, que el titular del banco de datos personales debe designar un responsable de seguridad del banco de datos personales (que posea las capacidades y autoridad necesaria para el desarrollo de sus funciones). Cuando dicha designación no exista, se entiende que el rol de responsable de seguridad del banco de datos personales recae en el titular del banco de datos personales (es decir, el órgano de mayor jerarquía o que representa a la entidad).
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	El procedimiento de fiscalización y sancionador se inicia de oficio, por la Autoridad Nacional de Protección de Datos Personales o por denuncia de parte, ante la presunta comisión de actos contrarios a lo dispuesto en la LPDP o el Decreto Supremo. El órgano que investiga es la Dirección de Fiscalización e Instrucción. Por su parte, el órgano que inicia el procedimiento sancionador es la Dirección de Protección de Datos Personales (primera instancia administrativa). Contra las resoluciones emitidas por esta última procede recurso de apelación, el cual será resuelto por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (segunda instancia administrativa).

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (ej. GDPR)? ¿Qué diferencias relevantes encuentra?	No	Existen algunos temas que la normativa peruana actualmente no regula. Por ejemplo, a diferencia del GDPR, no contempla los derechos a la limitación del tratamiento y a la portabilidad de datos. Tampoco hace referencia a la regulación en materia de "cookies". De igual forma, no regula la figura de la corresponsabilidad del tratamiento de datos personales (esta figura se da en supuestos de acuerdos colaborativos o de asociación en participación). Finalmente, el marco legal peruano no establece un plazo mínimo ni máximo de conservación de los datos personales, así como tampoco exige que, ante la ocurrencia de un incidente de dato personal, el responsable del tratamiento o titular del banco de datos personales deba reportarlo ante la Autoridad Nacional de Protección de Datos Personales. Por otro lado, resulta pertinente mencionar que la normativa peruana, a diferencia del GDPR, sí regula la obligación de que los responsables del tratamiento deban inscribir y mantener actualizados sus bancos de datos personales ante la Autoridad Nacional de Protección de Datos Personales.
Otras obligaciones	¿Existen otras consideraciones/ requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	Sí	Conforme con el artículo 13 del Decreto Supremo, existe la obligación de publicar la Política de Privacidad (adecuada a la normativa peruana), la cual debe entenderse como una forma de cumplimiento del deber de información. Incluso esta obligación se extiende a las páginas web en caso de que los datos personales sean recogidos en línea (artículo 18 de la LPDP).

República Dominicana

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Normativa	¿Existe en el país una ley de protección de datos personales? En ese caso, identificar normativa aplicable.	Sí	Es la Ley Nº 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. G. O. Nº 10737 del 15 de diciembre de 2013.
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su Sitio Web.	Sí	INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL). https://www.indotel.gob.do
Ámbito de aplicación	¿Cuál es el ámbito de aplicación de la norma? Es decir, ¿su aplicación es estrictamente territorial, o aplica el concepto de extraterritorialidad?	Sí	Las normas de la ley son de orden público y de aplicación en todo el territorio nacional.
Recolección de datos	¿Cuáles son los requisitos o procesos legales exigidos para la recolección de datos personales? (por ejemplo, consentimiento del titular de los datos, proporcionar información sobre la finalidad del uso de los datos y derechos de su titular, entre otros.	Sí	Cuando se recaben datos personales que requieran del consentimiento del titular de los datos, para que se les pueda dar el tratamiento de datos o ser cedidos después de obtener dicho consentimiento, se deberá informar previamente, a por lo menos uno de los titulares de los datos, en forma expresa y clara, explicando: a) La finalidad para la que serán destinados y quiénes pueden ser sus destinatarios o clase de destinatarios. b) La existencia del archivo, registro, banco de datos o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable. c) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	N/A	**Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables**
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	**Datos especialmente protegidos:** Datos de carácter personal que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. **Datos de carácter personal:** Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. **Datos de carácter personal relacionados con la salud:** Cualquier información concerniente a la salud pasada, presente y futura, física o mental, de un individuo.
Situación de las sociedades y otras personas jurídicas	¿Alcanza la protección de la normativa en materia de datos personales, de las personas jurídicas o de existencial ideal?	No	**Artículo 4.- Numeral 4, de Ley 172-13: El régimen de protección de los datos de carácter personal no aplicará: A los tratamientos de datos referidos a personas jurídicas, ni a los archivos de datos personales que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquellas, consistentes en sus nombres y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.**

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Consentimiento del titular de los datos	¿Se requiere la obtención previa del consentimiento del titular de los datos cuando se recaba su información? En tal caso, ¿existen condiciones para la obtención del consentimiento del titular de los datos? (por ejemplo, información previa que deba proporcionarse al titular de los datos).	Sí	Tener en cuenta siguientes informaciones: **Derecho de información.** Cuando se recaben datos personales que requieran del consentimiento del titular de los datos, para que se les pueda dar el tratamiento de datos o ser cedidos después de obtener dicho consentimiento, se deberá informar previamente, a por lo menos uno de los titulares de los datos, en forma expresa y clara, explicando: a) La finalidad para la que serán destinados y quiénes pueden ser sus destinatarios o clase de destinatarios. b) La existencia del archivo, registro, banco de datos o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable. c) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos. **Consentimiento del afectado.** El tratamiento y la cesión de datos personales es ilícito cuando el titular de los datos no hubiere prestado su consentimiento libre, expreso y consciente, que deberá constar por escrito o por otro medio que permita que se le equipare, de acuerdo a las circunstancias. El referido consentimiento, prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de los datos descritos en el numeral 3 del presente artículo.
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	Según el artículo 27 de la ley 172-13, el consentimiento no será necesario para la obtención de datos cuando: 1. Se obtengan de fuentes de acceso público; 2. Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; 3. Se trate de listas para fines mercadológicos, cuyos datos se limiten a nombre, cédula de identidad y electoral, pasaporte, identificación tributaria y demás informaciones biográficas; 4. Se deriven de una relación comercial, laboral o contractual, científica o profesional con la persona física, y resulten necesarios para su desarrollo o cumplimiento; 5. Se trate de datos personales que reciban de sus clientes en relación a las operaciones que realicen las entidades de intermediación financiera reguladas por la Ley Monetaria y Financiera y de agentes económicos, de las Sociedades de Información Crediticia (SIC), y de las entidades que desarrollan herramientas de puntajes de crédito para la evaluación del riesgo de los deudores del sistema financiero y comercial nacional, de acuerdo a las condiciones establecidas en el Artículo 5, numeral 4; 6. Así lo disponga una ley; 7. Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias; 8. Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve el secreto de la identidad de los titulares de los datos mediante mecanismos de disociación adecuados; 9. Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables
Contenido y alcance de la información a ser validada por el titular de los datos	¿Cuál es el contenido que debe incluir el consentimiento? (Por ejemplo, uso o destino de los datos, transferencia internacional de los datos, etc.).	Sí	a) La finalidad para la que serán destinados y quiénes pueden ser sus destinatarios o clase de destinatarios. b) La existencia del archivo, registro, banco de datos o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable. c) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales? ¿Hay requisitos aplicables en relación a la transferencia internacional de datos? (Ejemplo: cláusulas modelos, autorización por parte de la autoridad de control, entre otros).	Sí	**Transferencia internacional de datos.** La transferencia de datos personales de cualquier tipo con países u organismos internacionales o supra nacionales, que requieran del consentimiento del titular de los datos, solamente se efectuará cuando: 1. La persona física, libre y conscientemente, decidiera autorizar por voluntad propia la transferencia de datos, o cuando las leyes lo permitan. 2. Se trate de intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado o una investigación epidemiológica, o por razones de salud o higiene pública. 3. Se trate de transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable. 4. La transferencia de datos se hubiera acordado o contemplado en el marco de tratados internacionales o convenios, y en los tratados de libre comercio de los cuales sea parte la República Dominicana. 5. La transferencia de datos tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo, la trata de personas, el narcotráfico, y demás crímenes y delitos. 6. La transferencia de datos sea necesaria para la ejecución de un contrato entre el titular de los datos y el responsable del tratamiento, o para la ejecución de medidas precontractuales. 7. La transferencia de datos legalmente exigida sea para la salvaguarda del interés público o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, o solicitada por una administración fiscal o aduanera para el cumplimiento de sus competencias. 8. La transferencia de datos se efectúe para prestar o solicitar un auxilio judicial internacional. 9. La transferencia de datos se efectúe a petición de un organismo internacional con interés legítimo desde un registro público. Se debe tener en cuenta que el artículo 28 de la ley 172-13 establece que, la Cesión de los datos personales objeto de tratamiento de datos sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario, con el previo consentimiento de por lo menos uno de los titulares de los datos
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	NA	
Datos sensibles	¿Qué se entiende por dato sensible? ¿Cómo es el tratamiento de los datos sensibles, de corresponder?	Sí	Datos personales que revelan las opiniones políticas, las convicciones religiosas, filosóficas o morales, la afiliación sindical e información referente a la salud o a la vida sexual.
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (ej. ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, tratamiento y/o uso de la misma? ¿Existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	NA	

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	Sí	**Seguridad de los datos.** El responsable del archivo de datos personales y en su caso, el encargado del tratamiento, deberán adoptar e implementar las medidas de índole técnica, organizativa y de seguridad necesarias para salvaguardar los datos de carácter personal y eviten su alteración, pérdida, tratamiento, consulta o acceso no autorizado. En consecuencia: a) Queda prohibido registrar datos personales en archivos, registros o bancos de datos que no reúnan condiciones técnicas de integridad y seguridad. b) Los aportantes de datos, las Sociedades de Información Crediticia (SIC) y los usuarios o suscriptores deben adoptar las medidas y controles técnicos necesarios para evitar la alteración, pérdida, tratamiento o acceso no autorizado de los datos sobre historial de crédito que manejen o reposen en la base de datos de las Sociedades de Información Crediticia (SIC). c) Las Sociedades de Información Crediticia (SIC) deben adoptar medidas apropiadas para proteger sus bases de datos contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informáticos
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Ejemplo: rectificación, actualización o supresión). Identificar y explicar.	Sí	**Derecho de consulta para la protección de datos.** Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de discriminación, inexactitud o error, exigir la suspensión, rectificación y la actualización de aquellos, conforme a esta ley. **Derecho de acceso.** Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por esta ley. El tratamiento de los datos e informaciones personales o de sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Solicitarán ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos. **Derechos de rectificación y cancelación.** Toda persona tiene derecho a que sean rectificados, actualizados, y, cuando corresponda, suprimidos, los datos personales de los que sea titular y que estén incluidos en un banco de datos. **Derecho a indemnización.** Los interesados que como consecuencia del incumplimiento de lo dispuesto en la presente ley, sufran daños y perjuicios, tienen el merecimiento a ser indemnizados conforme al derecho común.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	Artículo 17.- Acción de hábeas data. Sin perjuicio de los mecanismos establecidos para el ejercicio de los derechos de los interesados, éstos podrán ejercer la acción judicial de hábeas data de conformidad con la Constitución y las leyes que rigen la materia. La acción judicial de hábeas data procederá para tomar conocimiento de la existencia de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados que se deriven de una relación comercial, laboral o contractual con una entidad pública o privada; o simplemente, para tomar conocimiento de los datos personales que se presuma que existen almacenados en archivos, registros o bancos de datos públicos o privados. En los casos en que se presuma inexactitud, la desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentre prohibido en la presente ley, para exigir su rectificación, supresión o actualización. Artículo 18.- Legitimación activa. La acción de protección de los datos personales o de hábeas data será ejercida por el afectado, sus tutores, los sucesores o sus apoderados. Cuando la acción judicial sea ejercida por personas jurídicas deberá ser interpuesta por sus representantes legales o los apoderados que éstas designen a tal efecto. Artículo 19.- Legitimación pasiva. La acción judicial procederá con respecto a los responsables y usuarios de bancos de datos públicos y privados destinados a proveer informes, cuando actúen contrario a las disposiciones establecidas en la presente ley. Artículo 20.- Competencia. Será competente para conocer de esta acción el juez del domicilio del demandado, y para el caso de pluralidad de demandados, en el domicilio de uno de ellos. Artículo 21.- Procedimiento aplicable. La acción de hábeas data se tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo. El registro o el banco de datos, mientras dure el procedimiento, debe asentar o publicar en los informes que la información cuestionada está sometida a un proceso judicial o de impugnación de hábeas data.
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	Sí	Cesión. Los datos personales objeto de tratamiento de datos sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario, con el previo consentimiento de por lo menos uno de los titulares de los datos.
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros *(data processing)*? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	Sí	A través de comunicaciones, consultas, interconexiones o transferencias. Es decir, cualquier operación o conjunto de operaciones o procedimientos técnicos, automatizados o no, que dentro de una base de datos permiten recopilar, organizar, almacenar, elaborar, seleccionar, extraer, confrontar, compartir, comunicar, transmitir o cancelar datos de consumidores.
Conservación de datos	¿Hay obligación de retener/conservar los datos recolectados o procesados por un tiempo determinado? En dicho caso, ¿cuál es el plazo?	Sí	Varía según la materia. En la Ley Nº 172-13 no se establece un una obligación o plazo específico para la retención/conservación de datos, sin embargo, esta obligación pudiese nacer en un plano contractual o mediante disposición de alguna otra ley sectorial. Ej. Materia de impuestos. Donde los contribuyentes, responsables y terceros están obligados a conservar en forma ordenada, por un período de diez (10) años: los libros de contabilidad, libros y registros especiales, antecedentes, recibos o comprobantes de pago, o cualquier documento, físico o electrónico, referido a las operaciones y actividades del contribuyente.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Eliminación de datos	¿Existe una obligación de eliminar los datos recolectados o procesados? En dicho caso, ¿en qué supuestos y cuál es el plazo?	Sí	Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o, en su caso, completados por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular de los datos establecidos en la presente ley.
Privacy Impact Asessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (Privacy Impact Assessment)?	NA	
Incidentes	¿Hay obligación de reportar un incidente de seguridad u algún incumplimiento o las previsiones legales?	NA	En la Ley Nº 172-13 no se establece una obligación específica de reportar un incidente de seguridad u algún incumplimiento o las previsiones legales, sin embargo, los responsables del tratamiento de datos están obligados a conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta y uso o acceso no autorizado.
Sanciones	¿Existen sanciones frente al incumplimiento de dicha obligación? En caso de existir, identificarlas e indicar el monto de las sanciones o penalidad aplicable correspondiente.	NA	Se debe evaluar según el caso ya que en la Ley 172-13 se establece el Derecho a indemnización. Los interesados que como consecuencia del incumplimiento de lo dispuesto en la presente ley, sufran daños y perjuicios, tienen el merecimiento a ser indemnizados conforme al derecho común. Las sanciones específicas que presenta la Ley son dirigidas a las Sociedades de Información Crediticia (SIC) y su regulación.
Acciones legales	¿Existe alguna acción legal de protección de datos personales? ¿quién tiene derecho para ejercerla/ solicitarla?	Sí	Derecho de consulta para la protección de datos. Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de discriminación, inexactitud o error, exigir la suspensión, rectificación y la actualización de aquellos, conforme a esta ley.
Delegado o responsable de la protección de datos personales	¿Existe la figura del delegado de protección de datos (DPO) o similar? En dicho caso, ¿su designación es obligatoria? ¿debe ser designado localmente?	No	
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	Debe evaluarse según el caso. Ej. En materia de lavado de activos se puede proceder de oficio al tratamiento de datos personales dependiendo de la investigación que se estuviese llevando a cabo.
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (ej. GDPR)? ¿Qué diferencias relevantes encuentra?	No	Poseen diferencias relevantes en el sentido que la Ley 172-13 es una ley con un enfoque principal al tratamiento de datos personales por las entidades crediticias.
Otras obligaciones	¿Existen otras consideraciones/ requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	Sí	Consideraciones constitucionales y jurisprudenciales, según el caso.

Uruguay

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Normativa	¿Existe en el país una ley de protección de datos personales? En ese caso, identificar normativa aplicable.	Sí	En Uruguay existe una amplia reglamentación en materia de protección de datos, identificamos la más relevante: ‣ Ley Nro. 18.331" Protección de Datos Personales y acción de Habeas Data" ("Ley 18.331") ‣ Decreto Reglamentario Nro. 414/009 ("Dec. 414/900") ‣ Ley Nro. 19.670 - Artículos 37 a 40 ("Ley 19.670") ‣ Ley Nro. 19.030 ("Ley 19.30") ‣ Decreto Reglamentario Nro. 64/020 ("Dec. 64/020") ‣ Decreto Reglamentario Nro. 664/008 ("Dec. 664/008") ‣ Decreto Reglamentario Nro. 242/017 ("Dec. 242/017") ‣ Resolución de la URCDP Nro. 1.647/010 ‣ Resolución de la URCDP Nro. 23/021 ‣ Resolución de la URCDP Nº41/021. ‣ Resolución de URCDP Nº 58/021.
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su Sitio Web.	N/A	La autoridad de aplicación, se denomina Unidad Reguladora y de Control de Datos Personales ("URCDP"), la cual está dirigida por el Director Ejecutivo de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento ("AGESIC") y dos miembros designados por el Poder Ejecutivo. La URCDP es un órgano desconcentrado de la AGESIC. Link: https://www.gub.uy/unidad-reguladora-control-datos-personales/
Ámbito de aplicación	¿Cuál es el ámbito de aplicación de la norma? Es decir, ¿su aplicación es estrictamente territorial, o aplica el concepto de extraterritorialidad?	N/A	El ámbito de aplicación de la norma en principio es territorial. No obstante, en el art. 3 del Dec.414/009 hace una especial distinción de acuerdo al tratamiento de datos que se practique: (a) Tratamiento de datos efectuados por un responsable de base de datos o tratamiento establecido en territorio uruguayo, siendo éste el lugar donde ejerza su actividad, cualquiera sea su forma jurídica. (b) El responsable de la base de datos o tratamiento no esté establecido en territorio uruguayo, pero utilice en el tratamiento de datos medios situados en el país, en cuyo caso queda igualmente alcanzado por la normativa uruguaya. Quedan exceptuados de la regla precedente, los casos en que los citados medios se utilicen exclusivamente con fines de tránsito, siempre que el responsable de la base de datos o tratamiento designe un representante, con domicilio y residencia permanente en territorio nacional. Art. 3, Dec. 414/009 A partir de la entrada en vigor de la Ley 19.670, la normativa regirá también fuera de las fronteras del país en caso de que el responsable o encargado no se encuentre establecido en territorio uruguayo si se dan las siguientes situaciones: A) En caso de que las actividades del tratamiento de datos estén relacionadas con la oferta de bienes y servicios dirigidos a habitantes de Uruguay o B) En caso de que las actividades de tratamiento de datos estén relacionadas con el análisis del comportamiento de los habitantes de la República. C) Si así lo disponen las normas de derecho internacional público o un contrato. D) Si en el tratamiento se utilizan medios situados en el país, tales como redes de información y de comunicación, centros de datos e infraestructura informática en general. Por lo tanto, la Ley 18.331 amplía su ámbito de aplicación fuera del territorio de Uruguay. Art. 37, Ley 19.670 y Arts. 1 y 2, Dec. 64/020

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Recolección de datos	¿Cuáles son los requisitos o procesos legales exigidos para la recolección de datos personales? (por ejemplo, consentimiento del titular de los datos, proporcionar información sobre la finalidad del uso de los datos y derechos de su titular, entre otros.	N/A	La actuación de los responsables de las bases datos se deberá ajustar a ciertos principios generales, entre ellos, el de la veracidad de los datos. Dicho principio dispone una serie de requisitos para la recolección de datos: ‣ La recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones a la presente ley. ‣ Los datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario. ‣ Cuando se constate la inexactitud o falsedad de los datos, el responsable del tratamiento, en cuanto tenga conocimiento de dichas circunstancias, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados. Asimismo, deberán ser eliminados aquellos datos que hayan caducado de acuerdo a lo previsto en la presente ley. Con respecto al consentimiento, el tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse. La ley prevé ciertos casos en que no será necesario el previo consentimiento. Por otro lado, la ley también recepta el derecho de información frente a la recolección de datos, el cual establece que cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca la finalidad del tratamiento de los datos recolectados. Art. 7, 9 y 13, Ley 18.331
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	N/A	Por dato personal se entiende a la información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables. Art. 4 inc. D), Ley 18.331
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	Conforme surge del art. 4, incs. D) y E) y art. 18 de la Ley 18.331 la normativa en la materia hace distinción entre datos personales y datos sensibles. La ley también realiza una distinción en relación a datos relativos a la salud, datos relativos a las telecomunicaciones, datos relativos a bases de datos con fines de publicidad, datos relativos a la actividad comercial o crediticia y datos transferidos internacionalmente. Todos estos datos son considerados "datos especialmente protegidos" por la Ley. Arts. 4 inc. D) y E),18, 19, 20, 21, 22 y 23 Ley 18.331
Situación de las sociedades y otras personas jurídicas	¿Alcanza la protección de la normativa en materia de datos personales, de las personas jurídicas o de existencial ideal?	Sí	En la medida que corresponda, el derecho a la protección de datos personales se aplicará por extensión a las personas jurídicas. Art. 2, Ley 18.331
Consentimiento del titular de los datos	¿Se requiere la obtención previa del consentimiento del titular de los datos cuando se recaba su información? En tal caso, ¿existen condiciones para la obtención del consentimiento del titular de los datos? (por ejemplo, información previa que deba proporcionarse al titular de los datos).	Sí	El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse. El referido consentimiento prestado deberá figurar en forma expresa y destacada. Asimismo, al momento de recabarse los datos personales se deberá brindar cierta información al titular conforme lo expuesto en el art. 13 de la Ley 18.331. Arts. 9 y 13, Ley 18.331
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	El consentimiento previo no será necesario cuando se den alguno de los supuestos enumerados en el art. 9 y de la Ley 18.331. Por su parte, el Art. 17 de la misma Ley refiere a los supuestos en los cuáles no será necesario obtener el consentimiento del titular para la comunicación de los datos recabados.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Contenido y alcance de la información a ser validada por el titular de los datos	¿Cuál es el contenido que debe incluir el consentimiento? (Por ejemplo, uso o destino de los datos, transferencia internacional de los datos, etc.).	Sí	El titular que preste consentimiento para la recolección y tratamiento de sus datos deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos, y el tipo de actividad desarrollada por el responsable de la base de datos otorgamiento. En caso contrario, el consentimiento será nulo. Asimismo, la transferencia internacional de datos requerirá que el interesado haya dado su consentimiento (inequívoco) a la transferencia prevista, según indica el Art. 23, literal A de la Ley 18.331. Art. 5, Dec. 414/009
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales? ¿Hay requisitos aplicables en relación a la transferencia internacional de datos? (Ejemplo: cláusulas modelos, autorización por parte de la autoridad de control, entre otros).	Sí	La normativa se expide acerca de la transferencia internacional de datos. La misma en principio queda prohibida con países y organismos internacionales que no proporcionen los niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional de la materia. Sin embargo, la prohibición no regirá cuando se trate de los supuestos enumerados en el art. 23 de la Ley 18.331 (numerales 1 al 5 y literales A a F). Es importante tener en cuenta que la Resolución de la URCDP Nº 23/021, modifica la Resolución de la URCDP Nº 4/019, disponiendo que se consideran adecuados - y en consecuencia apropiados para las transferencias internacionales de datos - todos los países que, a juicio de la Unidad, cuenten con normas de protección adecuadas y medios para asegurar su aplicación eficaz. En particular, se consideran adecuados a los miembros de la Unión Europea y el Espacio Económico Europeo, Principado de Andorra, República Argentina, el sector privado de Canadá, , Guernsey, Isla de Man, Islas Feroe, Estado de Israel, Japón, Jersey, Nueva Zelanda, Reino Unido de Gran Bretaña e Irlanda del Norte, y Confederación Suiza. La Resolución de la URCDP Nº 23/021 fue publicada el 16 de setiembre de 2021, y eliminó a las organizaciones incluidas en el marco "Privacy Shield" de los Estados Unidos de América de los países adecuados para las transferencias internacionales de datos. Dicho cambio responde a la invalidación del "Privacy Shield" por parte del Tribunal de Justicia de la Unión Europea. En virtud de dicha resolución, las transferencias internacionales de datos realizadas a Estados Unidos de América deberán justificarse a través del consentimiento de los interesados o de algunas de las excepciones previstas en el Art. 23 de la Ley Nº 18.331. Sin perjuicio de ello, la norma estableció un plazo de adecuación para aquellos sujetos que hubieran sustentado sus transferencias en el marco del "Privacy Shield", concediendo un plazo de 6 meses a contar del 16 de setiembre de 2021, para ajustar las condiciones de las transferencias realizadas de conformidad con la normativa actual (en consecuencia, el plazo para dicho ajustaste culmina el 16 de marzo de 2022). Por último, a través de la Resolución de la URCDP 41/021 se recomendó la implementación de una serie de cláusulas en lo que respecta a las transferencias internacionales de datos personales a territorios no adecuados. A través de ellas se pretende establecer claramente las responsabilidades de las partes involucradas a los efectos de salvaguardar de forma eficaz la protección de datos de los sujetos intervinientes.
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	Sí	La normativa uruguaya en su art. 36 lo define como "Código de conducta". Arts. 35 y 36, Ley 18.331.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Datos sensibles	¿Qué se entiende por dato sensible? ¿Cómo es el tratamiento de los datos sensibles, de corresponder?	Sí	Los datos sensibles, son aquellos datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual. Estos se encuentran desarrollados en los arts. 4, inc. E) y 18 de la Ley 18.331. Las entidades públicas, estatales o no estatales, las privadas total o parcialmente de propiedad estatal, así como las entidades privadas que traten datos sensibles como negocio principal y las que realicen el tratamiento de grandes volúmenes de datos deberán designar un delegado de protección de datos. Dicho delegado tendrá funciones de asesoramiento, supervisión y control, entre otras. Art. 4 inc. E) y art. 18, Ley 18.331. Art 40, Ley 19.670.
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (ej. ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, tratamiento y/o uso de la misma? ¿Existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	Sí	Es obligatorio registrar toda base de datos pública o privada ante el Registro de la URCDP. Necesariamente la inscripción deberá contener lo dispuesto en el art. 29 de la Ley 18.331 y cumplimentar con la obligación de actualización dispuesta en el art. 20 del Dec. 414/009. Asimismo, la Resolución Nº 1.647/010, del 15 de octubre de 2010: regula el contenido y la forma de presentación de las actualizaciones de bases de datos, indicando que solo se deberá presentar la actualización trimestral de los datos de las Bases de Datos inscriptas, si se cumplen algunas de las siguientes condiciones: a) que exista una alteración cuantitativa del 20% de los datos indicados en la solicitud de registro, o b) que existan modificaciones estructurales en la Base de Datos registrada, tales como el agregado o la supresión de un campo, cambio de la finalidad u otra que altere significativamente la información declarada inicialmente en la solicitud de registro. Art. 29, Ley. 18.331; Arts. 15 y 20, Decreto Reglamentario Nº 414/009; Decreto Reglamentario Nº 664/008 y Resolución Nº 1.647/010.
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	Sí	La ley recepta el principio de seguridad de los datos mediante el cual el responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. En cuanto a medidas de seguridad, el art. 3 del Dec. 64/2020 dispone que los responsables y encargados del tratamiento, deberán adoptar las medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar la seguridad de los datos personales. Art. 10, Ley 18.331 y Art. 3, Dec. 64/020
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Ejemplo: rectificación, actualización o supresión). Identificar y explicar.	Sí	La normativa en materia de datos personales establece los siguientes derechos para los titulares de datos: ‣ Derecho a la información frente a la recolección de datos. ‣ Derecho de acceso. ‣ Derecho de rectificación, actualización, inclusión o supresión. ‣ Derecho a la impugnación de valoraciones personales. ‣ Derechos referentes a la comunicación de datos. Dichos derechos se encuentran dispuestos en los arts. 13, 14, 15, 16 y 17 de la Ley 18.331 y en los arts. 9, 10, 11, 12, 13 y 14 del Dec. 414/009.
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	En cuanto a su ejercicio, los derechos deberán ejercerse conforme lo establecido en los arts. 13, 14, 15, 16 y 17 de la Ley 18.331.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	Sí	La ley entiende por cesión de datos, como "...comunicación de acuerdo con lo establecido en el artículo 4º literal B) de la Ley que se reglamenta..." Por su parte, el art. 4 inc. B) define a la comunicación de datos como toda revelación de datos realizada a una persona distinta del titular de datos. En virtud de lo establecido en el art. 17 de la Ley 18.331 los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo. Asimismo, la norma determina una serie de hipótesis en las cuales el previo consentimiento no será necesario. Arts. 4, inc. B) y 17, Ley 18.331.
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros (data processing)? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	Sí	La Ley define, y dispone un régimen de responsabilidad – además de a los responsables – a los "encargados" del tratamiento, a saber, persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento. La ley en su art. 30 hace referencia, asimismo, a la prestación de servicios informatizados de datos personales. Arts. 4 y 30, Ley 18.331.
Conservación de datos	¿Hay obligación de retener/conservar los datos recolectados o procesados por un tiempo determinado? En dicho caso, ¿cuál es el plazo?	No	Si bien la ley no establece dicha obligación de retención, o conservación de datos, el NºDec.414/009 en su art. 37 establece un Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos.
Eliminación de datos	¿Existe una obligación de eliminar los datos recolectados o procesados? En dicho caso, ¿en qué supuestos y cuál es el plazo?	Sí	Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados. Art. 8, Ley 18.331 y Art. 39, Dec. 414/009
Privacy Impact Assessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (Privacy Impact Assessment)?	Sí	En ejercicio de una responsabilidad proactiva, se deberán adoptar ciertas medidas técnicas y organizativas entre las cuales se encuentra la evaluación de impacto a la protección de datos, a fin de garantizar un tratamiento adecuado de los datos personales y demostrar su efectiva implementación. Las evaluaciones de impacto deberán realizarse de conformidad con los estándares establecidos en los arts. 6 y 7 del Dec. 64/020. Art. 12, Ley 18.331 Arts. 6 y 7, Dec. 64/020
Incidentes	¿Hay obligación de reportar un incidente de seguridad u algún incumplimiento a las previsiones legales?	Sí	El Dec. 64/020 dispone de un Capítulo destinado a vulneraciones de seguridad. A lo largo de los arts. 3 y 4 de dicho Decreto, se detalla todo lo concerniente a ellas. Por otra parte, a partir de la Ley 19.670, cuando el responsable o encargado de una base de datos tome conocimiento de que se ha vulnerado la seguridad de dicha base, deberá informarlo de inmediato, conjuntamente con las medidas adoptadas, tanto al titular de los datos como a la URCDP, quien coordinará con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy) los pasos a seguir. Arts. 3 y 4, Dec. 64/020. Art. 38, Ley 19.670.
Sanciones	¿Existen sanciones frente al incumplimiento de dicha obligación? En caso de existir, identificarlas e indicar el monto de las sanciones o penalidad aplicable correspondiente.	Sí	La Ley 18.331 en su art. 35 establece diversas sanciones a los responsables de las bases de datos, encargados de tratamiento de datos personales y demás sujetos alcanzados por el régimen legal, en caso de que se violen las normas de la presente ley y modificatorias. Las mismas se graduarán en atención a la gravedad, reiteración o reincidencia de la infracción cometida. Por otra parte, el artículo 39 de la Ley 19.670 sustituye el antiguo artículo 12 de la Ley 18.331 de Protección de Datos Personales. La nueva redacción impone modificaciones al "principio de responsabilidad", estableciendo que tanto el responsable como el encargado de una base de datos son responsables de la violación de las disposiciones de la ley.

Tema	Concepto	Si / No / NA (No Aplica)	Observaciones / comentarios
			Asimismo, la normativa establece que responsables y encargados de bases de datos deben adoptar las medidas técnicas y organizativas que correspondan (privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, etc.) para asegurar su protección. Art. 35, Ley 18.331. Art. 39, Ley 19.670.
Acciones legales	¿Existe alguna acción legal de protección de datos personales? ¿quién tiene derecho para ejercerla/ solicitarla?	Sí	Es la acción de Habeas Data, mediante la cual, toda persona tiene derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y -en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización- a exigir su rectificación, inclusión, supresión o lo que entienda corresponder. Arts. 37, 38, 39 y 40, Ley 18.331
Delegado o responsable de la protección de datos personales	¿Existe la figura del delegado de protección de datos (DPO) o similar? En dicho caso, ¿su designación es obligatoria? ¿debe ser designado localmente?	Sí	Las entidades públicas, estatales o no estatales, las privadas total o parcialmente de propiedad estatal, así como las entidades privadas que traten datos sensibles como negocio principal y las que realicen el tratamiento de grandes volúmenes de datos (i.e. más de 35.000 personas) deberán designar un delegado de protección de datos. Las funciones de los delegados de protección de datos se encuentran descriptas en el art. 40 de la Ley 19.670. Arts. 10, 11, 12, 13, 14 y 15, Dec. 64/020
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	La URCDP, de oficio o a solicitud de cualquier interesado, posee la facultad de expedirse sobre el derecho a la protección de datos personales. Arts. 9-Bis, 34, 45, Ley 18.331
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (ej. GDPR)? ¿Qué diferencias relevantes encuentra?	Sí	Como antecedente, destacamos que Uruguay aprobó en el año 2013 el Convenio Nº 108 del Consejo de Europa – a partir de la Ley Nº 19.030 - y fue declarado por la Unión Europea como un país con nivel de protección adecuado en materia de protección de datos personales, de acuerdo con la Directiva 95/467CE. A partir de las reformas recientes en la legislación uruguaya sobre datos personales (Ley 19.670 y Dec. 64/020), es posible decir que se ha procurado una alineación de la normativa local a los estándares del GDPR.
Otras obligaciones	¿Existen otras consideraciones/ requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	Sí	Por Dec. 242/017, Uruguay reguló el tratamiento e intercambio electrónico de información personal por parte de las Instituciones públicas y privadas con competencias en materia de salud, así como el Sistema de Historia Clínica Electrónica Nacional. El art. 181 de la Ley 19.996 creó el Registro "No llame" con el objetivo de proteger a los titulares o usuarios de los servicios de telecomunicaciones de los abusos del procedimiento de contacto, publicidad, oferta, venta y regalo de bienes o servicios no solicitados a través de ellos. Mediante el decreto Nº 132/022 se reglamentó el procedimiento para el registro y la baja de los usuarios en dicha Base, así como las condiciones para el contacto a consumidores. A tales efectos, se establece como obligación de las empresas la consulta al registro previo al contacto, la conservación de la prueba de la consulta por un plazo de 4 años, y la realización de llamadas desde un número visible o indicando la empresa de call center que realiza el contacto, la marca y el motivo comercial de éste. Se exceptúa este requisito en las hipótesis en que exista un consentimiento o una relación contractual vigente con el usuario, siempre que el contacto refiera al objeto de tal vinculo. Respecto de estas llamadas consideradas como "permitidas" se dispone que se deberá recabar el consentimiento libre, expreso e informado del usuario inscripto, siendo este documentado y preservado por parte de la entidad que realice la campaña.

EY Law Latam

Contactos

Argentina

Jorge Garnier | Socio/Partner
jorge.garnier@ar.ey.com

Pablo Bisogno | Director Ejecutivo/
Associate Partner
pablo.bisogno@ar.ey.com

Laila Yu | Gerente/Manager
laila.yu@ar.ey.com

Brasil

Ligia Augusto | Socia/Partner
ligia.augusto@br.ey.com

Gustavo Poggio | Director Ejecutivo/
Associate Partner
gustavo.poggio@br.ey.com

Sandra Avella | Gerente/Manager
sandra.avella@br.ey.com

Chile

Pedro Lluch | Socio/Partner
pedro.lluch@cl.ey.com

Felipe Fernández | Director Ejecutivo/
Associate Partner
felipe.fernandez@cl.ey.com

Colombia

Ximena Zuluaga | Socia/Partner
ximena.zuluaga@co.ey.com

Ana María Castellanos | Associate Partner
ana.m.castellanos.vargas@co.ey.com

Costa Rica

Fernando Vargas Winiker | Socio/Partner
Fernando.Vargas.Winiker@cr.ey.com

María Lucía Alvarado | Gerente Senior /
Senior Manager
Maria.Alvarado@cr.ey.com

Ecuador

Fernanda Checa | Director Ejecutivo/
Associate Partner
fernanda.checa@ec.ey.com

México

Carina Barrera Cota | Socia/Partner
carina.barrera@mx.ey.com

Bárbara Fernandez Vargas | Director
Ejecutivo/Associate Partner
barbara.fernandez@mx.ey.com

Alejandro Guevara Cortéz | Gerente/Manager
alejandro.guevara@mx.ey.com

Panamá

Ana Clement | Gerente Senior/Senior Manager
ana.clement@pa.ey.com

Joan Otero | Asociada/Senior
joan.otero@pa.ey.com

Paraguay

Gustavo Colman | Socio/Partner
gustavo.colman@py.ey.com

Nabila Larroza | Gerente/Manager
nabila.larroza@py.ey.com

Perú

Maria del Pilar Sabogal | Socia/Partner
maria.sabogal@pe.ey.com

Mario Zúñiga | Director Ejecutivo/
Associate Partner
mario.zuniga@pe.ey.com

Bruno Mejía | Gerente/Manager
bruno.mejia@pe.ey.com

República Dominicana

Thania Gomez | Socia/Partner
thania.gomez@do.ey.com

Eleni González | Staff
eleni.gonzalez@do.ey.com

Uruguay

Martha Roca | Socia/Partner
martha.roca@uy.ey.com

German Gomez | Gerente/Manager
german.gomez@ey.com

EY | Construyendo un mejor mundo de negocios

EY existe para construir un mejor mundo de negocios, ayudando a crear valor a largo plazo para sus clientes, su gente y la sociedad en general, así como también para construir confianza en los mercados de capitales.

Por medio de datos y tecnología, los equipos diversos e incluyentes de EY, ubicados en más de 150 países, brindan confianza a través de la auditoría y ayudan a los clientes a crecer, transformarse y operar.

El enfoque multidisciplinario en auditoría, consultoría, legal, estrategia, impuestos y transacciones, busca que los equipos de EY puedan hacer mejores preguntas para encontrar nuevas respuestas a los asuntos complejos que actualmente enfrenta nuestro mundo.

EY se refiere a la organización global y podría referirse a una o más de las firmas miembro de Ernst & Young Global Limited, cada una de las cuales es una entidad legal independiente. Ernst & Young Global Limited, una compañía del Reino Unido limitada por garantía, no proporciona servicios a clientes. Para conocer la información sobre cómo EY recaba y utiliza los datos personales y una descripción de los derechos que tienen las personas conforme a la ley de protección de datos, ingrese a ey.com/privacy. Las firmas miembro de EY no ofrecen servicios legales en los casos en que las leyes locales lo prohíban. Para obtener mayor información acerca de nuestra organización, ingrese a ey.com.