Protección de Datos Personales en América Latina

Guía de Consulta Rápida

EY Law
Latinoamérica

The better the question. The better the answer.
The better the world works.

Shape the future
with confidence

ÍNDICE

INTRODUCCIÓN

En un contexto donde la innovación tecnológica redefine constantemente la forma en que vivimos, trabajamos y nos relacionamos, la gestión responsable de los datos personales se ha convertido en uno de los mayores desafíos de nuestro tiempo. La expansión del entorno digital y el crecimiento exponencial del uso de la inteligencia artificial, la automatización y el análisis masivo de datos están transformando la dinámica económica, política y social a nivel global.

En EY, comprendemos que la confianza digital es hoy un pilar estratégico para las organizaciones. Por eso, desde EY Law nos complace presentar la quinta edición de la Guía de Consulta Rápida en Protección de Datos Personales en América Latina, una herramienta práctica pensada para acompañar a las empresas en la gestión de sus obligaciones legales y en la consolidación de una cultura de privacidad sólida y sostenible.

Los datos personales se han convertido en el motor de la economía digital, impulsando la innovación, la competitividad y la toma de decisiones. Sin embargo, este potencial debe ir acompañado de un compromiso firme con la transparencia, la seguridad y el respeto por los derechos y las libertades de las personas. En un entorno donde los ciberataques, las brechas de seguridad y los tratamientos inadecuados de información representan riesgos crecientes, las compañías deben fortalecer sus políticas y procedimientos para lograr un manejo ético y conforme a la normativa vigente. Por ello, esta guía busca ofrecer una visión clara, comparada y actualizada de los marcos regulatorios en la región, brindando respuestas concretas a las preguntas más frecuentes y orientaciones prácticas que faciliten la toma de decisiones informadas.

Esta nueva edición incorpora las principales novedades legislativas y regulatorias de los últimos años, reflejando el esfuerzo de los países latinoamericanos por armonizar sus normativas con los estándares internacionales más exigentes. Además, esta quinta edición también incorpora nuevas jurisdicciones, ampliando la cobertura regional con las distintas oficinas de EY Law. El trabajo ha sido desarrollado por nuestro equipo regional de especialistas en privacidad y ciberseguridad, en coordinación con las firmas miembro de EY en Latinoamérica, combinando conocimiento local con una perspectiva global.

Finalmente, recordamos que la información contenida en esta publicación se encuentra actualizada a la fecha de su emisión. Por tal motivo, siempre es importante verificar la vigencia de las disposiciones aplicables antes de su implementación, dado que el marco normativo continúa evolucionando de manera dinámica.

Con esta quinta edición, reafirmamos nuestro compromiso de acompañar a las organizaciones en su camino hacia una gestión responsable y estratégica de los datos personales, fortaleciendo una cultura robusta de privacidad y gobernanza de datos. Esperamos que este material pueda resultar de utilidad y quedamos siempre abiertos a acompañarlos en caso de requerir la asistencia de nuestros especialistas en la materia.

EY Law Latinoamérica

ARGENTINA

Tema	Concepto	Sí / 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 Nº 25.326, es decir, la Ley de Protección de Datos Personales ("LPDP"). Ese marco normativo se complementa con otras normas tales como: ▸ Constitución de la Nación Argentina en su artículo 43, tercer párrafo. ▸ Decreto Nº 1.558/2001, con sus modificaciones, reglamentario de la Ley de Protección de Datos Personales Nº 25.326. ▸ Ley Nº 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 Nº 27.275: Derecho de Acceso a la Información Pública, y el Decreto 780/2024 que la reglamenta. ▸ Disposición E 60/2016, particularmente regulando los requisitos de transferencias internacionales de datos personales. ▸ Resolución Nº 159/2018: Lineamientos y contenidos básicos de normas corporativas vinculantes). ▸ Resolución Nº 47/2018: Medidas de seguridad recomendadas para el tratamiento y conservación de datos personales por medios informáticos y no informáticos. ▸ Resolución Nº 4/2019: Criterios orientadores e indicadores de buenas prácticas en la aplicación de la Ley Nº 25.326, cuyo anexo refiere a (i) Sistemas de videovigilancia; (ii) Disociación de datos; (iii) Datos Biométricos, y (iv) Consentimiento. ▸ Ley Nº 26.951: Creación del Registro Nacional "No Llame". ▸ Protocolo Adicional 108+. Ratificado por la Ley Nº 27.699. ▸ Resolución Nº 255/2022: Criterios orientadores e indicadores de buenas prácticas en la aplicación de la Ley Nº 25.326 respecto de los datos genéticos. ▸ Disposición Nº 2/2023: Recomendaciones para una Inteligencia Artificial Fiable. ▸ Ley Nº 26.548: Banco Nacional de Datos Genéticos. ▸ Resolución AAIP Nº 161/2023: Creación del Programa de Transparencia y Protección de Datos Personales en el Uso de la IA. ▸ Resolución AAIP Nº 198/2023: Aprobación de Cláusulas Contractuales Modelo. ▸ Resolución Nº AAIP 126/2024: Actualización, sistematización y unificación normativa y del Registro Nacional "No Llame". ▸ Ley Nº 27.759: Modifica la ley Nº 26.879 para ampliar el Registro Nacional de Datos Genéticos a la búsqueda de personas extraviadas y a otros delitos, además de incorporar los derechos de los titulares de datos y hacer aplicable el Convenio 108+. ▸ Resolución AAIP Nº 145/2025, establece un Programa de Fortalecimiento de Protección de Datos Personales en la Administración Pública Nacional.
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. La normativa argentina no recepta el concepto de aplicación extraterritorial.
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 con las circunstancias. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: 1. La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios. 2. 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. 3. 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. 4. Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de estos. 5. La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
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	La normativa argentina contempla las siguientes categorías de datos personales: ▸ **Datos sensibles:** Son aquellos 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 (artículo 2 LPDP). Solo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares (artículo 7 LPDP). ▸ **Datos relacionados con la salud:** Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquellos, respetando los principios del secreto profesional (artículo 8 LPDP). ▸ **Datos informatizados:** Son aquellos datos personales sometidos al tratamiento o procesamiento electrónico o automatizado (artículo 2 LPDP). Además, 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. 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 periodo de hasta dos años (artículo 25 LPDP). ▸ **Datos penales o contravencionales:** Datos relativos a los antecedentes penales y/o contravencionales, que solo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes (artículo 7 LPDP). ▸ **Datos crediticios:** No están definidos por la LPDP, aunque se entienden incluidos dentro de la definición datos personales. Sin perjuicio de ello, el artículo 26 de la LPDP establece que, en la prestación de servicios de información crediticia, solo pueden tratarse datos personales de carácter pecuniario relevantes para la evaluación de la solvencia económica y el crédito de una persona. Dichos datos, deben obtenerse de fuentes accesibles al público, o derivados de informes proporcionados por la parte interesada, o con su consentimiento. Además, la prestación de servicios de información crediticia no requerirá el consentimiento previo del interesado para los fines de la cesión de datos, o la posterior transmisión de los mismos, siempre que dichos datos estén relacionados con las actividades comerciales o crediticias de los destinatarios. Además, si bien no existen referencias respecto a otros tipos de datos sensibles dentro de la LPDP, se puede mencionar que la AAIP ha publicado diferentes pautas y recomendaciones que aclaran ciertos conceptos y términos como los **"datos de ubicación"**. Así, una directriz de la AAIP establece que existen principios fundamentales relacionados con el uso de herramientas de geolocalización y seguimiento, ya sea que dichas herramientas sean utilizadas por el sector público, el sector privado, o ambos en colaboración. Toda la información relativa a la ubicación de una persona o sus movimientos se considera como datos personales y está regulada por la LPDP. Por lo tanto, el responsable deberá basarse en una base legal de conformidad con el Artículo 5 de la LPDP para la recopilación y el procesamiento de este tipo de información. Además, los "datos de ubicación" se definen como la información recopilada por una red o servicio en el que se encontraba o se encuentra el teléfono u otro dispositivo del usuario. La ubicación de los datos puede ser recopilada por GPS, operadores de teléfonos móviles, redes wifi, bluetooth o una combinación de señales.
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.

Tema	Concepto	Sí / 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	La obtención del consentimiento debe ser **previa**, **libre**, **expresa** e **informada**. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: 1. La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios. 2. 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. 3. El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles. 4. Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos. 5. La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	Cabe destacar que no será necesario el consentimiento cuando: 1. Los datos se obtengan de fuentes de acceso público irrestricto. 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 listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio. 4. Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento. 5. 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 el apartado 'recolección de datos' más arriba (artículo 6 LPDP).
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales?, ¿hay requisitos aplicables en relación con la transferencia internacional de datos? (Por 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 N°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. La 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 han 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. Asimismo, la **Resolución N° 198/2023**, publicada el 19 de octubre de 2023, aprueba las cláusulas contractuales modelo para transferencias internacionales de datos y la Guía de Implementación de la Red Iberoamericana de Protección de Datos (RIPD). Las cláusulas contractuales modelo para las transferencias internacionales de datos fueron desarrolladas por la RIPD como una alternativa económicamente viable para que las empresas u organismos no tengan que negociar acuerdos individuales.

Tema	Concepto	Sí / 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 solo 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 (Por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el 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, de conformidad a los requisitos de información establecidos en el artículo 21 de la LPDP. 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, expresadas en el artículo 29 de la LPDP. Con relación a las registraciones como responsable del tratamiento, así como de cada base de datos que debe registrarse, a partir de la publicación de la Resolución AAIP 38/2024 se actualizó el modelo de cartel utilizado en casos de recolección de imágenes digitales. Este cartel desempeña un papel crucial al cumplir con el requisito de información previa al titular del dato, conforme a las condiciones de licitud establecidas, principalmente para quienes son responsables de bases de datos de videovigilancia (generalmente utilizadas para fines de seguridad).
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	Sí	Conforme el artículo 9 LPDP, el responsable o usuario del archivo de datos, debe adoptar aquellas medidas técnicas y organizativas que: 1. Resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado. 2. Permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Asimismo, queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad adecuadas.
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Por ejemplo, rectificación, actualización o supresión) Identificar y explicar.	Sí	La LPDP establece que el titular de los datos personales tiene los siguientes derechos: ‣ Derecho de información y su contenido (artículo 13). ‣ Derecho de acceso (artículo 14). ‣ Derecho a actualización y/o rectificación (artículo 16). ‣ Derecho de supresión (artículo 16). Por otro lado, la LPDP también refiere a la posibilidad de realizar una denuncia ante la AAIP ante la falta de respuesta o información incompleta al ejercer sus derechos. En dicha línea, el artículo 33 de la LPDP prevé la acción de protección de los datos personales o de habeas data, la cual procederá: a) Para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquellos. b) En los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido por la ley, para exigir su rectificación, supresión, confidencialidad o actualización.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	Las acciones de los titulares de los datos se pueden ejercer de la siguiente manera: ▸ **Derecho de información y su contenido**. 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. ▸ **Derecho de acceso del titular de datos personales**. 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 a terceros. ▸ **Derecho a actualización, rectificación y supresión**. 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. ▸ **Acción de protección de los datos personales o de habeas data:** La legitimación, formas de procedimiento, requisitos y demás información para el ejercicio de la referida acción, están previstos dentro del Capítulo VII 'Acción de protección de los datos personales' de la LPDP.
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	Sí	Los datos personales objeto de tratamiento solo 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. No obstante, no se requiere el consentimiento del interesado cuando: 1. Así lo disponga una ley. 2. En los supuestos previstos en el artículo 5 º inciso 2 de la LPDP en el cual se listan los supuestos en donde no se requiere el consentimiento. 3. Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias. 4. Los datos compartidos sean de carácter personal relacionados con la salud, y sea necesario por razones de salud pública o de emergencia, o para la realización de encuestas epidemiológicas, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados. 5. Se haya aplicado un procedimiento de disociación de la información, de modo que las personas a las que se refiere la información no sean identificables. Cabe destacar que el cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y este 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	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.

Tema	Concepto	Sí / 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	Como regla general, la LPDP establece que los datos personales deben conservarse únicamente por el tiempo necesario para cumplir con los fines para los cuales hubiesen sido recolectados. Por otra parte, la LPDP prevé un periodo de retención determinado para ciertas categorías o documentos, tales como: ▸ **Servicios informatizados:** una vez cumplidas las obligaciones contractuales correspondientes, los datos personales tratados deben ser destruidos, excepto en caso de que exista una autorización expresa dada por la persona por cuenta de la cual se prestan dichos servicios, en razón de la posibilidad de que los datos se utilicen para futuros servicios, en cuyo caso los datos pueden almacenarse en las debidas condiciones de seguridad durante un periodo máximo de hasta dos años (artículo 25 LPDP). ▸ **Información crediticia:** solo se pueden archivar, registrar o comunicar los datos personales relevantes para evaluar la solvencia económica y financiera de las partes interesadas en los últimos cinco años. Dicho plazo se reducirá hasta dos años cuando el deudor liquide o liquide la obligación de cualquier otra forma, y este hecho se hará constar en el informe. ▸ **Datos personales registrados con fines policiales:** se cancelarán cuando no se consideren necesarios para las investigaciones que dieron lugar a su almacenamiento (artículo 23 LPDP).
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 LPDP establece que los datos personales deberán eliminarse cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. Los datos deben ser suprimidos sin necesidad de ninguna solicitud adicional realizada por el interesado (artículo 4, párrafo 7 de la LPDP). Cabe destacar que, si se contrata a un tercero para que preste servicios informáticos de procesamiento de datos, los datos deben destruirse cuando se complete el trabajo, excepto cuando se acuerde lo contrario (artículo 25, párrafo 2). Asimismo, los datos deberán eliminarse en caso de que el titular de los datos lo solicite. Por su parte, cuando la LPDP prevé periodos de retención determinados para ciertas categorías, como en el caso de los datos de crédito/financieros y los datos informáticos/computarizados, dichos datos deben eliminarse al vencimiento de los respectivos periodos indicados.
Privacy Impact Assessment	¿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 a las empresas y organismos públicos sobre los conceptos, contextos y metodologías en una evaluación de impacto en la protección de datos (EIPD). Cabe destacar que, la referida 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. Asimismo, la guía proporciona algunos factores que deben evaluarse para determinar si se debe o no llevar a cabo una EIDP. Cuando concurren uno o varios de estos factores, se puede inferir que el proyecto o actividad bajo análisis implica riesgos significativos para los derechos de las personas. En tales casos, el responsable de los datos deberá llevar a cabo una EIPD para cumplir con la normativa vigente.
Incidentes	¿Hay obligación de reportar un incidente de seguridad o algún incumplimiento a las previsiones legales?	No	Si bien no existe un requerimiento local normativo vigente, en el año 2022, Argentina sancionó la Ley Nº 27.699, mediante la cual Argentina se adhiere al 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, dentro de las 72 horas siguientes a la toma de conocimiento de dicho incidente, al menos a la autoridad de control competente (AAIP), respecto de aquellas violaciones a los datos que puedan interferir gravemente con los derechos y las libertades fundamentales de los titulares de datos.

Tema	Concepto	Sí / 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 LPDP prevé diferentes tipos de sanciones, conforme se identifican a continuación. ▸ Sanciones administrativas (artículo 31): las cuales pueden consistir en: - Apercibimiento. - Suspensión del archivo, registro o banco de datos. - Multas: las multas pueden variar dependiendo de la gravedad de la infracción (por ejemplo, infracciones leves, graves y muy graves). Según la Resolución AAIP 126/2024, las multas pueden oscilar entre mil pesos argentinos ($ 1.000) y cien mil pesos argentinos ($ 100.000). - Clausura del archivo, registro o banco de datos. - Cancelación del archivo, registro o banco de datos. Estas sanciones se graduarán en función de la gravedad y extensión de las infracciones y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso. Asimismo, la AAIP publica en su página *web* oficial la lista de las principales empresas sancionadas, lo que también desencadena un daño reputacional a considerar, junto con las correspondientes resoluciones de la AAIP que contienen los detalles de la infracción sancionada. ▸ Sanciones penales (artículo 32): se prevé la posibilidad de que sean aplicadas aquellas sanciones que incluye el Código Penal Nacional en las Secciones 117 bis y 157 bis. Ello implica que los tribunales penales pueden ordenar sanciones penales tales como penas de prisión de un mes a tres años dependiendo de las infracciones específicas relacionadas con la protección de datos. Ambas penas también incluyen una pena complementaria de inhabilitación cuando el infractor es un funcionario público. Cabe destacar que el Código Penal argentino contempla los siguientes delitos relacionados con los datos personales (sin incluir en su definición la modalidad a través la cual se lleven a cabo): a. Inserción intencional de información falsa en una base de datos personales. b. Revelación intencional a un tercero de información falsa en una base de datos personales. c. Irrupción a sabiendas e ilícitamente, o violando la confidencialidad de los datos y los sistemas de seguridad de los datos, de cualquier forma, en una base de datos personales (acceso no autorizado). d. Divulgación de información confidencial en una base de datos personal que deba mantenerse en secreto por disposición legal. ▸ Sanciones civiles: los artículos 33 y ss. de la LPDP regulan la acción de habeas data, a la que también se refiere la Constitución Nacional (artículo 43, tercer párrafo de la CN), la cual permite la reclamación civil para la reparación de los daños causados por una infracción a la LPDP.

Tema	Concepto	Sí / 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 legislación contempla la acción de protección de los datos personales o de habeas data, la cual procederá: 1. Para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquellos. 2. En los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización. Cabe mencionar que esta acción 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 estas designen al efecto. Además de la acción de habeas data, el titular de los datos puede promover una demanda civil de carácter general por daños. No obstante, como en cualquier reclamo indemnizatorio, el éxito de la acción dependerá de que el demandante acredite cuatro requisitos esenciales: (i) la ilicitud de la conducta que origina el daño; (ii) la existencia de un daño real y efectivo; (iii) la relación de causalidad entre la conducta y el perjuicio; y (iv) la presencia de negligencia, conducta ilícita o, en su caso, responsabilidad objetiva.
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 sus objetivos. En esta línea, la AAIP cuenta con facultad para realizar investigaciones e imponer las sanciones administrativas ante violaciones a la normativa vigente, así como también puede constituirse en querellante en las acciones penales que se promovieran por violaciones a la LPDP. Las inspecciones se realizan para: 1. Tomar conocimiento de las actividades del responsable de la base de datos, los datos personales que administra, los medios y la forma en que lo hace. 2. Verificar que el responsable de la base de datos adopte las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales. 3. Evaluar el grado de cumplimiento a lo prescripto por la LPDP. 4. Realizar observaciones.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?	Sí	El artículo 21 de la Ley Nº 25.326 establece los requisitos obligatorios para mantener registros de procesamiento de datos. Específicamente, indica que todo archivo, registro, base o banco de datos públicos y privados destinados a proporcionar informes deben inscribirse en un registro habilitado por el organismo de control. Los controladores de datos están obligados a incluir la siguiente información en sus registros: 1. Nombre y domicilio del responsable del archivo o base de datos. 2. Características y finalidad del archivo. 3. Naturaleza de los datos personales contenidos en cada archivo. 4. Métodos de recolección y actualización de los datos. 5. Destino de los datos y las personas o entidades a las que pueden ser transmitidos. 6. Modo de interrelacionar la información registrada. 7. Medidas de seguridad adoptadas para proteger los datos, incluyendo la categoría de personas con acceso a la información. 8. Tiempo de conservación de los datos. 9. Condiciones y procedimientos mediante los cuales las personas pueden acceder, rectificar o actualizar sus datos. Además, la ley establece que ningún usuario podrá poseer datos personales que no estén previamente declarados en el registro. El incumplimiento de estos requisitos puede resultar en 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 (Por ejemplo, GDPR), ¿qué diferencias relevantes encuentra?	No	La normativa argentina no contempla todos los requisitos receptados por la normativa internacional. No obstante, han sido presentados ante el Poder Legislativo Nacional diversos proyectos de modificación de la LPDP en los últimos años, los cuales se adecúan a los estándares internacionales y presenta grandes similitudes con el GDPR.
Otras obligaciones	¿Existen otras consideraciones/requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	Si	El Registro Nacional "No Llame" es una iniciativa diseñada para ayudar a las personas que prefieren no recibir llamadas publicitarias. La AAIP renovó el sistema de inscripción para que las consultas y las denuncias sean más sencillas y accesibles. Ahora, todo se puede gestionar de forma online y gratuita a través de la página *web* nollame.aaip.gob.ar. Los titulares de líneas de teléfono ya sean fijas o móviles, pueden registrar su número fácilmente utilizando su DNI y el número de trámite. Hay un límite de hasta cinco líneas que se pueden inscribir. Una vez que el registro esté confirmado, si el usuario sigue recibiendo llamadas de empresas de publicidad o marketing, puede presentar una denuncia a cualquier hora del día completando un formulario en el sitio *web*. La administración de este registro está a cargo de la AAIP, que también se encarga de las acciones administrativas en caso de incumplimiento. Este registro es aplicable en toda Argentina y garantiza el derecho a no recibir llamadas comerciales, facilitando así el ejercicio del "derecho de bloqueo" que establece la Ley Nº 25.326. La iniciativa abarca diversos servicios de telefonía, incluyendo tanto líneas fijas como móviles, así como tecnologías futuras como la mensajería instantánea. Aunque no se envía una confirmación de inscripción, los usuarios pueden verificar su estado en cualquier momento. Los números inscritos aparecen de inmediato en los listados, aunque las empresas tienen un plazo de hasta 30 días para dejar de llamar. Si alguna persona decide cancelar su inscripción, puede hacerlo en cualquier momento a través de la misma página *web*. Aunque la inscripción reduce significativamente las llamadas publicitarias, no elimina todas, ya que ciertas llamadas, como las de campañas de bien público o emergencias, están exentas. También se permite que las empresas que mantienen una relación contractual con el usuario puedan contactarlo en relación con los productos o servicios adquiridos.

BOLIVIA

Tema	Concepto	Sí / 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 de personas en Bolivia está garantizada por la Constitución Política del Estado (CPE) (Arts. 21, 25, 130 y 131) y se complementa con diversas disposiciones normativas que regulan sectores específicos y respaldan el reconocimiento de la protección de datos. Es importante señalar que Bolivia es uno de los pocos países de la región que aún no cuenta con una ley específica de protección de datos. Sin embargo, actualmente existen proyectos de ley en discusión que buscan establecer un marco normativo completo en esta materia. En este contexto, el marco normativo vigente, se compone de la siguiente manera: ▸ CPE (2009) (Art. 21 "Derecho a la privacidad, intimidad", Art. 25 I. derecho "al secreto de las comunicaciones privadas en todas sus formas", II. Inviolabilidad de "las manifestaciones privadas contenidas en cualquier soporte", III. Derecho de inviolabilidad de las "conversaciones o comunicaciones privadas", Art. 130 "derecho a la eliminación o rectificación de los datos registrados por cualquier medio (...)", Art. 131 "Acción de Privacidad"). ▸ Código Civil Boliviano: Art. 12. "Protección del Nombre", Art. 16 "Derecho a la imagen", Art. 17 "Derecho al honor", Art. 18 "Derecho a la intimidad" y Art. 19 "Inviolabilidad de las comunicaciones y papeles privados". ▸ Ley Nº164 "Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación", el Decreto Supremo Nº1793 para "Desarrollo de Tecnologías de Información y Comunicación" y el Decreto Supremo Nº1391 para el "Reglamento General" a la Ley Nº164. ▸ Ley Nº393 "Ley de Servicios Financieros" (solo información financiera). ▸ Ley Nº453 "Ley General de los Derechos de las Usuarias y los Usuarios y de las Consumidoras y Consumidores". ▸ Ley Nº004 "Marcelo Quiroga Santa Cruz". Adicionalmente, cabe mencionar que los derechos fundamentales como la intimidad, privacidad y la honra, que constituyen la base de los derechos alcanzados por protección de datos personales, fueron inicialmente reconocidos por el Código Civil (1975). Posteriormente, la CPE (2009) abordó estos derechos incorporando la Acción de Privacidad y reconociendo los derechos ARCO (acceso, rectificación, cancelación y oposición), así como el principio de autodeterminación informativa. Por su parte, la Ley Nº164 de Telecomunicaciones, establece de manera directa el derecho de los usuarios a la protección de sus datos personales en el ámbito de los servicios de telecomunicaciones.
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su sitio *web*.	Sí	En Bolivia, no existe una autoridad única y especializada en materia de protección de datos personales. Sin embargo, diversas entidades públicas ejercen competencias sectoriales relacionadas con el tratamiento y protección de datos personales, según el tipo de información y el ámbito en el que se maneje. A continuación, se detallan dichas autoridades: 1. Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transporte (ATT): La ATT es la entidad responsable de aprobar los procedimientos y medidas que los operadores de TICs (Tecnologías de Información y Comunicación), deben implementar para salvaguardar la inviolabilidad y secreto de las comunicaciones, así como la protección de los datos personales (IV. Art. 176 del Decreto Supremo Nº1391). Su sitio *web* oficial: **https://www.att.gob.bo** 2. Autoridad de Supervisión al Sistema Financiero (ASFI): La ASFI es la entidad responsable de supervisar el cumplimiento de las normas que garantizan la reserva y confidencialidad de la información vinculada a los servicios financieros, incluyendo datos sobre operaciones y clientes. Dichas disposiciones se encuentran contenidas en la Ley Nº393, "Ley de Servicios Financieros", en sus Artículos 472 y siguientes, que reconocen el derecho de los usuarios financieros a la protección de su información, la cual solo puede ser revelada en los casos expresamente establecidos por la normativa vigente. Su Sitio *web* oficial: **https://www.asfi.gob.bo** 3. Viceministerio de Defensa de los Derechos del Usuario y Consumidor: Esta entidad es responsable de proteger los derechos de los consumidores en el marco de la Ley Nº453 "Ley General de los Derechos de las Usuarias y los Usuarios y de las Consumidoras y Consumidores", incluyendo aspectos relacionados con el uso de datos personales en relaciones de consumo. Su Sitio *web* oficial: **https://vdduc.justicia.gob.bo**
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 CPE establece que las leyes bolivianas se aplican a todas las personas naturales o jurídicas en el territorio boliviano (Art. 14. V.). Asimismo, la Ley Nº 164 (Art. 4) establece que el ámbito de aplicación es territorial para todas las personas naturales o jurídicas, públicas o privadas, nacionales o extranjeras, que realicen actividades o presten servicios relacionados con TICs, siempre que estos se originen, transiten o concluyan dentro del territorio boliviano.

Tema	Concepto	Sí / 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	Ley Nº 164 (Art.54) reconoce el derecho de los usuarios a la protección de datos personales, prohibiendo la divulgación sin autorización previa del titular. En ese sentido, el Decreto Supremo Nº 1793 (Art. 56), establece que toda recolección y tratamiento técnico de datos personales debe realizarse con el consentimiento previo, expreso e informado del titular. Este consentimiento constituye un requisito esencial para garantizar la legalidad del tratamiento de datos. En ese marco, el consentimiento debe ser otorgado de forma libre y específica, y debe estar basado en información clara sobre la finalidad del tratamiento. El titular debe ser informado sobre el uso que se dará a sus datos, el responsable del tratamiento, los posibles destinatarios, así como los derechos que le asisten, como el acceso, la rectificación, la actualización o la supresión de sus datos personales. En línea a ello, el Decreto Supremo Nº 1391 (Art. 176) determina que los operadores y proveedores de servicios deben obtener el consentimiento previo, expreso y por escrito del titular para recolectar y tratar sus datos personales, salvo en casos excepcionales. Asimismo, se disponen las siguientes obligaciones y restricciones: 1. Confidencialidad del personal: El personal de los operadores y proveedores está obligado a guardar secreto sobre la existencia y contenido de las comunicaciones, así como a proteger los datos personales y la intimidad de los usuarios. 2. Medidas de protección: Los operadores deben adoptar las medidas más idóneas para garantizar la confidencialidad y seguridad de los datos personales de los usuarios. 3. Responsabilidad en caso de vulneraciones: Los operadores deben colaborar en la identificación de presuntos responsables de vulneraciones a la inviolabilidad de las comunicaciones, protección de datos personales y privacidad de los usuarios, especialmente si estas ocurren dentro de sus instalaciones. 4. Supervisión: La ATT es responsable de aprobar los procedimientos y medidas que los operadores implementen para salvaguardar la inviolabilidad y secreto de las comunicaciones, así como la protección de los datos personales. 5. Restricciones comerciales: Se prohíbe a los operadores permitir el acceso a registros o bases de datos de usuarios con fines comerciales o publicitarios, salvo que exista una autorización previa, expresa y escrita del usuario que desee recibir dicha publicidad.
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	El Decreto Supremo Nº 1793, (Art. 3, inciso IV.a), define a los datos personales, como "toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable". En esa línea, este concepto abarca cualquier tipo de información que, por sí sola o en conjunto con otros datos, permita identificar de forma directa o indirecta a una persona, por ejemplo, nombre, datos de localización, número de identificación y/o características propias de identidad física, económica, cultural, etc.
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	No	No.
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	Sí, La CPE reconoce el derecho a la privacidad, pero su aplicación a personas jurídicas es enunciativa, lo que restringe el ejercicio efectivo de estos derechos en ausencia de una regulación más desarrollada. Adicionalmente, la Ley Nº 164, incluye en su definición de usuarios, a las personas naturales y colectivas, por lo que se entendería que toda la normativa abarca a ambas figuras (Art. 6, numeral 40).

Tema	Concepto	Sí / 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)		Actualmente, en Bolivia, en el sector de telecomunicaciones, el Decreto Supremo Nº 1793 (Art. 56, inciso b), dispone que el consentimiento debe ser: ▸ Previo: otorgado antes de la recolección de los datos. ▸ Expreso: manifestado de forma clara, sin presunciones. ▸ Informado: el titular debe recibir información suficiente sobre el tratamiento de sus datos. El mismo cuerpo normativo establece que, para que el consentimiento sea válido, el titular debe ser informado de manera clara sobre: ▸ La finalidad del tratamiento de los datos. ▸ El uso previsto de la información. ▸ La identidad del responsable del tratamiento. ▸ Los derechos que le asisten como titular (acceso, rectificación, supresión, entre otros).
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	El Decreto Supremo Nº 1391 (II. Art. 176) contempla excepciones al consentimiento previo, expreso por escrito del titular para el tratamiento de datos personales en los siguientes casos: ▸ Orden judicial específica. ▸ En casos que la información sea necesaria para la emisión de guías telefónicas, facturas, detalle de llamadas al titular acreditado, o para la atención de reclamaciones, provisión de servicios de información y asistencia establecidos por el presente Reglamento, o para el cumplimiento de las obligaciones relacionadas con la interconexión de redes y servicios de apoyo. La Ley Nº 004 "Marcelo Quiroga Santa Cruz" (Art.19, I) dispone que no se puede invocar secreto o confidencialidad en materia comercial, tributaria o económica frente a requerimientos de la UIF (Unidad de Investigación Financiera). La información será obtenida sin necesidad de orden judicial ni trámite previo.
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	De acuerdo con el Decreto Supremo Nº 1391 (Art.56), el consentimiento para el tratamiento de datos personales debe ser previo, expreso e informado, y debe incluir como mínimo: ▸ La finalidad específica del tratamiento de los datos. ▸ El uso previsto de la información. ▸ La identidad del responsable del tratamiento. ▸ Los derechos del titular (como acceso, rectificación, supresión, etc.). En cuanto a la transferencia internacional de datos personales, Bolivia no cuenta con una regulación específica sobre esta materia.
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales?, ¿hay requisitos aplicables en relación con la transferencia internacional de datos? (Por ejemplo, cláusulas modelos, autorización por parte de la autoridad de control, entre otros)	No	Bolivia no cuenta con requisitos ni restricciones específicas para la transferencia internacional de datos personales.
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?	No	En Bolivia, la normativa vigente no contempla una definición textual de los datos sensibles. Sin embargo, la Ley Nº 164 y su reglamento incluyen definiciones relacionadas con elementos que pueden componer datos sensibles, como la información personal vinculada a la intimidad y privacidad.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (Por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el uso de la misma?, ¿existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	No	No.
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?		La Ley Nº 164 (Art. 26, inciso II, numerales 2 y 6), establece que los contratos suscritos por operadores y proveedores de servicios en telecomunicaciones deben incluir en sus contratos, mecanismos idóneos para la información y protección de los derechos de los usuarios, así como la protección de los datos personales. Complementariamente, el Decreto Supremo Nº 1391 (Art. 176), dispone que: ▸ El personal de operadores y proveedores en el sector de las telecomunicaciones, están obligados a proteger los datos personales e intimidad de los usuarios. ▸ La obligación de adoptar medidas técnicas idóneas para preservar la confidencialidad y protección de los datos personales. ▸ La ATT es la entidad responsable de aprobar los procedimientos y medidas utilizadas por los operadores para salvaguardar la inviolabilidad de las comunicaciones y la protección de datos De manera adicional, el Decreto Supremo Nº 1793, (Art. 8), establece que las entidades públicas deberán promover a seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados. En el sector financiero, la Ley Nº 393, (Art. 350), dispone que los burós de información deben implementar medidas de seguridad efectivas para evitar el uso indebido de los datos recopilados, así como cualquier acción que cause daño a los titulares o que beneficie indebidamente a la entidad. Adicionalmente se debe considerar que el Código Tributario (Ley Nº 2492), establece como una obligación para los funcionarios de la Administración Tributaria, el preservar la confidencialidad de la información a la cual tengan acceso (Art.67).
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Por ejemplo, rectificación, actualización o supresión) Identificar y explicar.	Sí	De acuerdo con lo establecido en la CPE, se reconocen derechos del titular de datos, como el Derecho a acceder a la información (Art.21, Numeral 6), a la rectificación, a objetar u obtener la eliminación o actualización de datos (Art.130), entre otros. La Ley Nº 164 (Art.54) reconoce expresamente el derecho a la privacidad, inviolabilidad de las comunicaciones (Art.56), y el Decreto Supremo Nº 1793 dispone la posibilidad de acceder, corregir o suprimir los datos personales incluidos en guías públicas.
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	En conformidad con el Decreto Supremo Nº 1793 (Art. 56), los titulares de datos personales pueden ejercer sus derechos como el acceso, rectificación, actualización o supresión por vía administrativa, mediante la presentación de una solicitud directa ante la entidad responsable del tratamiento de los datos. El responsable del tratamiento está obligado a responder de forma oportuna y adecuada, garantizando el ejercicio efectivo de los derechos del titular. En caso de negativa, silencio o respuesta insatisfactoria, el titular puede recurrir a mecanismos constitucionales, como la Acción de Protección de Privacidad, prevista en el Artículo 130 de la CPE.
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	No	No.
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros (*data processing*)? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	No	No.

Tema	Concepto	Sí / 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	Sí. En Bolivia existen obligaciones legales de conservación de datos, dependiendo del tipo de información. ▸ ▸Datos comerciales: El Código de Comercio (Art. 52) exige conservar libros y documentos comerciales por al menos 5 años desde el cierre del ejercicio o del último asiento. ▸ Datos tributarios: El Código Tributario (Ley N°2492) establece un plazo de prescripción de 10 años, por lo que se toma ese tiempo para conservar documentación que respalde obligaciones fiscales. ▸ Datos financieros: La Ley N°393 dispone que, las entidades de intermediación financiera deberán mantener una copia de respaldo de información y documentación que soporte sus operaciones, durante el plazo de 10 años (Art.470).
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	No.
Privacy Impact Assessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (*Privacy Impact Assessment*)?	No	No.
Incidentes	¿Hay obligación de reportar un incidente de seguridad o algún incumplimiento a las previsiones legales?	No	No.
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	legislación boliviana actualmente no contempla sanciones específicas por el incumplimiento de obligaciones en materia de protección de datos personales. Sin embargo, dado que derechos como la intimidad, privacidad, honra e imagen están reconocidos en la CPE (Art. 21.2 y Art. 130) y en el Código Civil (Art. 18 y 19), los afectados pueden ejercer acciones por la vía civil, en caso de que el tratamiento indebido de datos personales les haya causado perjuicio. Asimismo, en ciertos casos, el uso indebido de datos informáticos puede derivar en responsabilidad penal conforme al Código Penal (arts.363 bis, 363 ter) que contempla además otros delitos relacionados con la manipulación, alteración o acceso no autorizado de datos informáticos.
Acciones legales	¿Existe alguna acción legal de protección de datos personales?, ¿quién tiene derecho para ejercerla/solicitarla?	Sí	La Acción de Protección de privacidad contemplada en la CPE (Arts. 130 y 131) podrá ser ejercida por toda persona natural o jurídica que considere que sus datos personales han sido registrados de manera indebida o ilegal en archivos o bancos de datos públicos o privados, y que dicha información afecte sus derechos fundamentales a la intimidad, privacidad personal o familiar, imagen, honra o reputación.
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	No.
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	En Bolivia, actualmente no se ha identificado que la ATT, en el sector de telecomunicaciones, cuente con facultades normativas específicas para realizar investigaciones de oficio ante un incumplimiento en materia de protección de datos personales. En el sector financiero, la ASFI cuenta con facultades (Art. 493 de la Ley Nº 393), para investigar a los burós de información. Esta norma también establece la obligación de dichos burós de garantizar la veracidad, confidencialidad y seguridad de los datos personales que manejan. A tal efecto, el Reglamento de Gestión de Seguridad de la Información de ASFI (Art. 1. Sección 9), regula la gestión de incidentes de seguridad de la información, permitiendo a ASFI supervisar e intervenir ante vulneraciones.
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?	No	No.

Tema	Concepto	Sí / 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 (Por ejemplo, GDPR), ¿qué diferencias relevantes encuentra?		Bolivia no contempla muchos de los requisitos establecidos por el GDPR, ni cuenta con una ley específica, de protección de datos personales. Si bien es cierto que Bolivia reconoce en su normativa los derechos ARCO (acceso, rectificación), estos son apenas aproximaciones. Bolivia aún no cuenta con la mayoría de las disposiciones enmarcadas en el GDPR, como ser ▸ ▸ Ausencia de una autoridad de control independiente: El GDPR establece autoridades nacionales con facultades de supervisión, investigación y sanción. Sin embargo, Bolivia no cuenta con una entidad especializada en protección de datos. ▸ Falta de sanciones específicas por vulneración y manejo indebido de datos personales. ▸ Derechos avanzados no reconocidos: El GDPR incluye derechos como la portabilidad de datos, la limitación del tratamiento, el derecho a no ser objeto de decisiones automatizadas, y el derecho al olvido, que no están contemplados en la normativa boliviana actual. ▸ La normativa en Bolivia no contempla transferencias internaciones conforme los establece el GDPR. ▸ La normativa local no contempla evaluaciones de impacto y privacidad desde el diseño de tratamiento de datos.
Otras obligaciones	¿Existen otras consideraciones/ requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	No	No.


BRASIL

Tema	Concepto	Sí / 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 se regula en: ▸ Ley General de Protección de Datos de Brasil ("LGPD"), Ley Federal N°13.709/2018, modificada por las Leyes N° 13.853/2019 y 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 N° 1/2021, N° 2/2022, N° 4/2023, N° 15/2024 y N° 19/2024.
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	El 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: 1. La operación de procesamiento se realice en el territorio nacional. 2. El propósito de la actividad de procesamiento es ofrecer o suministrar bienes o servicios o procesar datos de personas ubicadas en el territorio nacional. 3. Los datos personales tratados han sido recabados en el territorio nacional.

Tema	Concepto	Sí / 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	El tratamiento de los datos personales se realizará de buena fe y estará sujeto a los siguientes principios (Artículo 6): ▸ Finalidad. ▸ Idoneidad. ▸ Necesidad. ▸ Acceso gratuito. ▸ Calidad de los datos. ▸ Transparencia. ▸ Seguridad. ▸ Prevención. ▸ No discriminación. ▸ 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 17). Además, el artículo 7 de la LGPD: el tratamiento de los datos personales solo podrá llevarse a cabo cuando exista al menos una de las siguientes hipótesis autorizantes: 1. Mediante el consentimiento del titular. 2. Para el cumplimiento de la obligación legal o reglamentaria por parte del controlador. 3. 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 los dispuesto en el Capítulo IV de la Ley. 4. Para la realización de estudios por parte del organismo de investigación, garantizando, siempre que sea posible, la anonimización de los datos personales. 5. 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. 6. Para el ejercicio regular de derechos en procedimientos judiciales, administrativos o arbitrales, estos últimos conforme a la Ley Nº9.307 de septiembre de 1996 (Ley de Arbitraje). 7. Para la protección de la vida o la seguridad física del titular o de un tercero. 8. Para la protección de la salud, en un procedimiento realizado por profesionales de la salud o por entidades de salud. 9. Para la protección de la salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridad sanitaria. 10. 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 para la protección del crédito, incluso en lo que respecta a las disposiciones de la legislación pertinente. Además, el artículo 11 de la LGPD indica diferentes hipótesis que autorizan el tratamiento de datos sensibles, como: 1. A través del consentimiento del titular de los datos o de su tutor o responsable legal; y sin el consentimiento, en los casos en que sea esencial para: a. El cumplimiento de una obligación legal o reglamentaria por parte del controlador. b. El tratamiento compartido de datos necesario para la ejecución, por parte de la administración pública, de políticas públicas previstas en 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 derechos, incluso en contratos y en procedimientos judiciales, administrativos y arbitrales, este último conforme a la Ley Nº 9.307 del 23 de septiembre de 1996 (Ley de Arbitraje). e. La protección de la vida o seguridad física del titular de los datos o de terceros. f. La protección de la salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridades sanitarias; o garantizar la prevención de fraudes y la seguridad del titular de los datos, en los procesos de identificación y autenticación de registros en sistemas electrónicos, protegiendo los derechos mencionados en el artículo 9 de la ley, salvo en los casos en que prevalezcan los derechos y libertades fundamentales del titular de los datos que requieran la protección de los datos personales.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	De acuerdo con la LGPD, los datos personales consisten en la información relacionada a 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 otras dos categorías de datos en el 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 con 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 con el 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 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	El consentimiento previo del titular de los datos es una de las hipótesis de autorización para el tratamiento de datos personales previstas en los artículos 7 y 11 de la LGPD. Si la base legal más adecuada (hipótesis de autorización) 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	Sí / No / NA (No aplica)	Observaciones / comentarios
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	Se renuncia al requisito de consentimiento para los datos manifiestamente hechos públicos por el interesado, salvaguardando los derechos y los principios previstos en la Ley (artículo 7, punto 4). Además, el artículo 7 de la LGPD trae otras nueve hipótesis de autorización para el tratamiento de datos que prescinde del consentimiento: 1. Para el cumplimiento de la obligación legal o reglamentaria por parte del responsable del tratamiento. 2. 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 la ley. 3. Para la realización de estudios por parte del organismo de investigación, garantizando, siempre que sea posible, la anonimización de los datos personales. 4. 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. 5. Para el ejercicio regular de derechos en procedimientos judiciales, administrativos o arbitrales, estos últimos conforme a la Ley Nº 9.307 del 23 de septiembre de 1996 (Ley de Arbitraje). 6. Para la protección de la vida o la seguridad física del titular o de un tercero. 7. Para la protección de la salud, en un procedimiento realizado por profesionales de la salud o por entidades de salud. 8. Para la protección de la salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridad sanitaria. 9. 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 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: 1. Cuando el titular o su tutor legal consienta, de manera específica y destacada, para fines específicos. 2. 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 Nº9.307 del 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. g. La protección de la salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridad sanitaria; 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 la ley y salvo en el caso de que prevalezcan los derechos y libertades fundamentales del titular que requieran la protección de datos personales.

Tema	Concepto	Sí / 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	De acuerdo con el artículo 5, XII de la LGPD, el consentimiento debe otorgarse de forma libre, informada e inequívoca, mediante la cual el titular de los datos acepta el tratamiento de sus datos personales para un propósito específico. Además, la LGPD otorga al titular de los datos el derecho a acceder a la información sobre el tratamiento de sus datos personales (artículo 9), y para garantizar que se cumplan estas especificidades, es esencial incluir al menos la siguiente información: 1. La finalidad específica del tratamiento. 2. El tipo y la duración del tratamiento, observándose el secreto comercial e industrial. 3. Identificación del responsable del tratamiento. 4. Información de contacto del responsable del tratamiento. 5. Información sobre el uso compartido de los datos por parte del responsable del tratamiento y la finalidad. 6. Responsabilidades de los agentes que llevarán a cabo el tratamiento, y os derechos del interesado, con mención explícita de los derechos (artículo 9). Además, la LGPD proporciona algunas directrices sobre el consentimiento, tales como: ▸ **Sección 7, § 5:** el responsable del tratamiento que haya obtenido el consentimiento y necesite comunicar o compartir datos personales con otros responsables debe obtener un consentimiento específico del titular de los datos para este fin, excepto en los casos en los que no se requiera consentimiento. ▸ **Sección 8, caput y § 1 y 2:** el consentimiento debe proporcionarse por escrito o por otro medio que demuestre la expresión de voluntad del titular de los datos. Si el consentimiento se proporciona por escrito, debe constar en una cláusula distinta de las demás cláusulas contractuales, y la carga de la prueba de que el consentimiento fue obtenido de acuerdo con la LGPD recae en el responsable del tratamiento. ▸ **Sección 8, § 3:** se prohíbe el tratamiento de datos personales cuando haya un defecto en el consentimiento. ▸ **Sección 8, § 4:** el consentimiento deberá referirse a finalidades específicas, siendo nulas las autorizaciones genéricas para el tratamiento de datos personales. ▸ **Sección 8, § 5:** el consentimiento puede ser revocado en cualquier momento mediante una declaración expresa del titular de los datos, a través de un procedimiento libre y facilitado, ratificando los tratamientos realizados bajo el consentimiento previamente otorgado, mientras no haya una solicitud de eliminación. ▸ **Sección 8, § 6:** en caso de un cambio en el propósito, forma y duración del tratamiento, identificación del responsable de tratamiento y/o información sobre el uso compartido de los datos, el responsable debe informar al titular de los datos, destacando específicamente el contenido de los cambios. El titular, en los casos en que se requiera su consentimiento, puede revocarlo si no está de acuerdo con el cambio.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales?, ¿hay requisitos aplicables con relación a la transferencia internacional de datos? (Por ejemplo, cláusulas modelos, autorización por parte de la autoridad de control, entre otros)	Sí	La transferencia internacional de datos personales solo está permitida de acuerdo con las disposiciones establecidas en el artículo 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: 1. Para países u organismos internacionales que proporcionen el grado de protección de datos personales adecuado a lo dispuesto en la ley. 2. 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. 3. 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. 4. Cuando la transferencia sea necesaria para la protección de la vida o la seguridad física del titular o de un tercero. 5. Cuando la autoridad nacional autorice la transferencia. 6. Cuando la transferencia resulte en un compromiso asumido en un acuerdo de cooperación internacional. 7. Cuando la transferencia sea necesaria para la ejecución de políticas públicas o atribuciones legales del servicio público, dándose publicidad de conformidad con el inciso I del caput del art. 23 de la ley. 8. 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 cuando sea necesario para atender las hipótesis previstas en los incisos II, V y VI del art. 7 de la ley. Para regular cada una de las posibilidades previstas por la LGPD, la ANPD publicó la Resolución CD/ANPD Nº 19/2024, la cual refuerza las disposiciones mencionadas anteriormente e introduce el contenido de las cláusulas contractuales estándar, así como el Reglamento de Transferencia Internacional de Datos. Este reglamento resalta información importante, como los criterios que se utilizarán para evaluar el nivel de protección de datos personales de un país extranjero o una organización internacional, incluyendo cláusulas contractuales estándar o específicas, medidas de transparencia, disposiciones sobre normas corporativas globales para la transferencia internacional de datos, así como cualquier procedimiento de aprobación y modificaciones tanto a las cláusulas como a las normas. Es importante destacar que, las cláusulas contractuales estándar proporcionadas por la ANPD a través del anexo II de la resolución deben ser adoptadas. En caso de utilizar otras cláusulas específicas, debido a circunstancias fácticas o legales excepcionales debidamente comprobadas por el controlador, estas deben ser sometidas a la aprobación de la ANPD de acuerdo con los términos de los artículos 21 al 24 y 29 al 30 de la resolución.
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	Sí	Tanto la LGPD como la Resolución CD/ANPD Nº 19/2024 contemplan normas corporativas vinculantes, las cuales deben ser aprobadas por la ANPD de acuerdo con el artículo 35 de la LGPD y el artículo 28 de la resolución.

Tema	Concepto	Sí / 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. El tratamiento de datos personales sensibles solo podrá producirse en los siguientes casos: 1. Cuando el titular o su tutor legal consienta, de manera específica y destacada, para fines específicos. 2. 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, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o por autoridad sanitaria, o 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 aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el uso de la misma?, ¿existe 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).
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Por ejemplo, rectificación, actualización o supresión).		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, con relación a sus datos personales 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).

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	Los derechos serán ejercidos a petición expresa del titular de los datos al agente de tratamiento (artículo 18, § 3), y una solicitud en relación con sus datos contra el responsable del tratamiento ante la autoridad de supervisión (artículo 18, § 1) tras una solicitud al responsable del tratamiento.
Cesión de datos personales	¿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: a. La portabilidad de datos cuando sea solicitada por el titular. b. Las operaciones financieras y administrativas derivadas de la utilización y prestación de los servicios referidos. ▸ **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: a. En el caso de renuncia al consentimiento previsto en la ley. b. 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 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.
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).

Tema	Concepto	Sí / 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	Aunque es posible encontrar periodos 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: a. Comprobación de que la finalidad fue alcanzada o de que los datos ya no son necesarios o pertinentes para alcanzar el fin específico buscado. b. Expiración del plazo de procesamiento. c. 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 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 con el alcance y los límites técnicos de las actividades, y su conservación será autorizada para los siguientes fines: a. Cumplimiento de una obligación legal o reglamentaria por parte del responsable del tratamiento. b. Estudios por parte de un organismo de investigación garantizando, siempre que sea posible, la anonimización de los datos personales. c. Cesión a terceros, previo cumplimiento de los requisitos de procesamiento de datos establecidos en la ley, o 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.
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.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Incidentes	¿Hay obligación de reportar un incidente de seguridad o algún incumplimiento a las previsiones 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 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). Además, la ANPD publicó la Resolución CD/ANPD Nº 15/2024 que introduce el reglamento sobre la Notificación de Incidentes de Seguridad, indicando que esta comunicación debe realizarse cuando el incidente pueda implicar un riesgo o daño significativo para los titulares de los datos (artículo 4), y establece los criterios para determinar la existencia de este riesgo, los cuales son: ▸ **Sección 5:** el incidente de seguridad puede implicar un riesgo o daño significativo para los titulares de los datos cuando pueda afectar de manera considerable los intereses y derechos fundamentales de los titulares y, acumulativamente, involucre al menos uno de los siguientes criterios: I. Datos personales sensibles; II. Datos de niños, adolescentes o ancianos; III. Datos financieros; IV. Datos de autenticación en sistemas; V. Datos protegidos por secreto legal, judicial o profesional; o VI. Datos a gran escala. Además, la notificación de un incidente de seguridad a la ANPD debe ser realizada por el responsable del tratamiento dentro de los tres días hábiles, salvo que exista un plazo de comunicación diferente establecido por una legislación específica (sección 6). Este plazo comenzará a contarse desde que el responsable del tratamiento tome conocimiento de que el incidente afectó datos personales (artículo 6, § 1), y debe contener la siguiente información (artículo 6, § 2): I. La descripción de la naturaleza y categoría de los datos personales afectados. II. El número de titulares de los datos afectados, especificando, cuando sea aplicable, el número de niños, adolescentes o ancianos. III. Las medidas técnicas y de seguridad utilizadas para proteger los datos personales, adoptadas antes y después del incidente, observando los secretos comerciales e industriales. IV. Los riesgos relacionados con el incidente, identificando los posibles impactos en los titulares de los datos. V. Las razones de la demora, en caso de que la notificación no se haya hecho dentro del plazo estipulado. VI. Las medidas que se han tomado o se tomarán para revertir o mitigar los efectos del incidente en los titulares de los datos. VII. La fecha de ocurrencia del incidente, cuando sea posible determinarla, y de la toma de conocimiento por parte del responsable del tratamiento. VIII. Los datos del oficial o la persona que representa al responsable del tratamiento. IX. La identificación del responsable del tratamiento y, si corresponde, una declaración de que es un agente de tratamiento a pequeña escala. X. La identificación del operador, cuando sea aplicable. XI. La descripción del incidente, incluida su causa principal, si se puede identificar; y XII. el número total de titulares de los datos cuyos datos se procesan en las actividades afectadas por el incidente.

Tema	Concepto	Sí / 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 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 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 (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. 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 periodo, hasta la regularización de la actividad de tratamiento por parte del responsable del tratamiento (incluido en la Ley Nº 13.853, 2019); XI. 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); XII. Prohibición parcial o total del ejercicio de actividades relacionadas con el tratamiento de datos (incluido en la Ley Nº 13.853, 2019).
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 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. Además, la ANPD publicó la Resolución CD/ANPD Nº 18/2024 que introduce el reglamento sobre el rol del DPO, indicando el requisito de formalización en el nombramiento del DPO (artículo 3), así como la divulgación de la identidad e información del DPO (artículos 8 y 9), las características que deben observarse para el cargo (artículos 12 a 14) y las actividades a realizar (artículos 15 a 17). Se destaca que el encargado puede ser tanto una persona física como jurídica (artículo 12), pero debe ser capaz de comunicarse con los titulares de los datos y con la ANPD, de manera clara y precisa, y en portugués (artículo 13). Asimismo, el encargado debe actuar con ética, integridad y autonomía técnica, evitando situaciones que puedan constituir un conflicto de intereses (artículo 18), y también puede ocupar múltiples cargos y desempeñar sus actividades para más de un agente de tratamiento de datos, siempre que pueda cumplir plenamente con sus responsabilidades relacionadas con cada agente de tratamiento de datos y no exista conflicto de intereses (artículo 19).
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 Nº01/2021 prevé que la ANPD puede actuar de oficio en las tareas de control (Artículo 16).

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?	Sí	El artículo 37 de la LGPD establece que el responsable del tratamiento y el operador deben mantener un registro de las operaciones de tratamiento de datos personales que realicen, especialmente cuando se basen en un interés legítimo. De este modo, se entiende que estos registros deben mantenerse siempre, aunque la ley no especifica los detalles de la información que debe contener dicho registro.
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (Por ejemplo, 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	Sí / 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). Sin embargo, en diciembre de 2024 se publicó la Ley Nº 21.719 que Regula la Protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales la cual modifica sustancialmente la LPDP y entrará en vigor el 1 de diciembre de 2026 (la "Nueva Ley de Datos Personales"). 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 inciso 4º, 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*.	Sí	En la actualidad, dado que no hay una autoridad dedicada específicamente a supervisar asuntos relacionados con la protección de datos personales, 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: **Inicio - SERNAC: Portal institucional.** Sin embargo, la Nueva Ley de Datos Personales contempla la creación de la Agencia de Protección de Datos Personales, la cual corresponderá a una corporación autónoma de derecho público, de carácter técnico, descentralizado, con personalidad jurídica y patrimonio propio. La Agencia de Protección de Datos Personales tendrá por objeto velar por la efectiva protección de los derechos que garantizan la vida privada de las personas y sus datos personales, de conformidad a lo establecido en la Nueva Ley de Datos Personales, y fiscalizar el cumplimiento de sus disposiciones. Este organismo no ha sido creado, por lo que no cuenta aún con sitio *web*.
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?	No	El ámbito de aplicación de la LPDP es territorial. No se prevé su aplicación fuera del país. La Nueva Ley de Datos Personales será aplicable al tratamiento de datos personales que se realice bajo cualquiera de las siguientes circunstancias: (i) Cuando el responsable o mandatario esté establecido o constituido en Chile. (ii) Cuando el mandatario, con independencia de su lugar de establecimiento o constitución, realice las operaciones de tratamiento de datos personales a nombre de un responsable establecido o constituido en Chile. (iii) Cuando el responsable o mandatario no se encuentren establecidos en Chile, pero sus operaciones de tratamiento de datos personales estén destinadas a ofrecer bienes o servicios a titulares que se encuentren en Chile, independientemente de si a estos se les requiere un pago, o a monitorear el comportamiento de titulares que se encuentran en Chile, incluyendo su análisis, rastreo, perfilamiento o predicción de comportamiento. (iv) El tratamiento de datos personales que sea realizado por un responsable que, sin estar establecido en Chile, le resulte aplicable la legislación chilena a causa de un contrato o del derecho internacional.
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 con el 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. De acuerdo con el artículo 12 de la Nueva Ley, es lícito el tratamiento de los datos personales que le conciernen al titular, cuando otorgue su consentimiento para ello. Su consentimiento debe ser libre, informado y específico en cuanto a su finalidad o finalidades y debe manifestarse, además, en forma previa y de manera inequívoca, mediante una declaración verbal, escrita o expresada a través de un medio electrónico equivalente, o mediante un acto afirmativo que dé cuenta con claridad de la voluntad del titular.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	La LPDP, en su artículo 2, define el concepto de dato personal como cualquier información concerniente a personas naturales, identificadas o identificables. La Nueva Ley de Datos Personales, en su artículo 2, letra f, define el concepto de dato personal como "cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Para determinar si una persona es identificable deberán considerarse todos los medios y factores objetivos que razonablemente se podrían usar para dicha identificación en el momento del tratamiento".
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 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. La Nueva Ley de Datos Personales reconoce las siguientes categorías definidas en el artículo 2: ▸ **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 personales sensibles:** aquellos 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, que revelen el origen étnico o racial, la afiliación política, sindical o gremial, situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.
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 definición de "dato personal" entregada por la LPDP y la Nueva Ley de Datos Personales, en el artículo 2, 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 con el artículo 4 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. De acuerdo con el artículo 12 de la Nueva Ley de Datos Personales, es lícito el tratamiento de los datos personales que le conciernen al titular, cuando otorgue su consentimiento para ello. Su consentimiento debe ser libre, informado y específico en cuanto a su finalidad o finalidades y debe manifestarse, además, en forma previa y de manera inequívoca, mediante una declaración verbal, escrita o expresada a través de un medio electrónico equivalente, o mediante un acto afirmativo que dé cuenta con claridad de la voluntad del titular.

Tema	Concepto	Sí / 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 contempladas en la LPDP 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: 1. Cuando el tratamiento se encuentre autorizado por la ley. 2. 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. 3. 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. La Nueva Ley de Datos Personales contiene las excepciones al consentimiento del titular en el artículo 13, el cual señala que será lícito el tratamiento de datos personales, sin el consentimiento del titular, en los siguientes casos: 1. Cuando el tratamiento esté referido a datos socioeconómicos, relativos a obligaciones de carácter económico, financiero, bancario o comercial y se realice de conformidad con las normas del Título III de la ley, que regula la utilización de datos relativos a este tipo de datos. 2. Cuando el tratamiento sea necesario para la ejecución o el cumplimiento de una obligación legal o lo disponga la ley. 3. Cuando el tratamiento de datos sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, o para la ejecución de medidas precontractuales adoptadas a solicitud del titular. 4. Cuando el tratamiento sea necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que con ello no se afecten los derechos y libertades del titular. En todo caso, el titular podrá exigir siempre ser informado sobre el tratamiento que lo afecta y cuál es el interés legítimo en base al cual se efectúa dicho tratamiento. 5. Cuando el tratamiento de datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia u organismos públicos. El responsable deberá acreditar la licitud del tratamiento de datos.
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. De acuerdo con el artículo 12 de la Nueva Ley de Datos Personales, es lícito el tratamiento de los datos personales que le conciernen al titular, cuando otorgue su consentimiento para ello. Su consentimiento debe ser libre, informado y específico en cuanto a su finalidad o finalidades y debe manifestarse, además, en forma previa y de manera inequívoca, mediante una declaración verbal, escrita o expresada a través de un medio electrónico equivalente, o mediante un acto afirmativo que dé cuenta con claridad de la voluntad del titular.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales?, ¿hay requisitos aplicables con relación a la transferencia internacional de datos? (Por ejemplo: cláusulas modelos, autorización por parte de la autoridad de control, entre otros)	Sí	Si bien en la LPDP 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 esta 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 5, admite la posibilidad de una transmisión automatizada de datos. La Nueva Ley de Datos Personales regula la **cesión de datos personales** en el artículo 15, señalando que los datos personales podrán ser cedidos con el consentimiento del titular y para el cumplimiento de los fines del tratamiento (y en otras circunstancias específicas, como el interés legítimo del cedente o cesionario). En caso de que el consentimiento otorgado por el titular al momento de realizarse la recolección de los datos personales no haya considerado la cesión de los mismos, este debe recabarse antes que se produzca, considerándose para todos los efectos legales como una nueva operación de tratamiento. Por su parte, las transferencias internacionales se regulan en el artículo 27 y siguientes, en los cuales se señala que serán lícitas estas operaciones cuando se cumplan ciertas condiciones, como que el destinatario esté sujeto al ordenamiento jurídico de un país que proporcione niveles adecuados de protección (esto último lo regula el artículo 28). También se incluyen circunstancias en que se permite una transferencia de datos específica cuando no existan las garantías adecuadas, como cuando se deban transferir datos para dar cumplimiento a obligaciones adquiridas en tratados o convenios internacionales que hayan sido ratificados por el Estado chileno y se encuentren vigentes (entre otras).
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	Sí	No está regulado en la LPDP. El artículo 28 de la Nueva Ley de Datos Personales que regula las reglas de determinación de países adecuados para la transferencia internacional de datos indica que serán lícitas las transferencias internacionales de datos cuando estas queden amparadas por cláusulas contractuales, normas corporativas vinculantes (BCR), u otros instrumentos jurídicos suscritos entre el responsable que efectúa la transferencia y el responsable o tercero mandatario que la reciba, y en ellas se establezcan garantías adecuadas. Además, señala que cuando la transferencia se efectúe entre sociedades o entidades que pertenezcan a un mismo grupo empresarial, siempre que todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales, las transferencias podrán quedar amparadas en normas corporativas vinculantes (BCR) previamente aprobadas por la Agencia de Protección de Datos Personales.

Tema	Concepto	Sí / 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 se encuentran definidos en el artículo 2 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. ▸ 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. De acuerdo con el artículo 2 de la Nueva Ley de Datos Personales, serán datos personales sensibles aquellos que se refieren a: ▸ Las características físicas o morales de las personas. ▸ A hechos o circunstancias de su vida privada o intimidad. ▸ Que revelen el origen étnico o racial, la afiliación política, sindical o gremial, situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas. ▸ Los datos relativos a la salud, al perfil biológico humano, los datos biométricos. ▸ La información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural. Según el artículo 16, el tratamiento de los datos personales sensibles solo puede realizarse cuando el titular a quien conciernen estos datos manifiesta su consentimiento en forma expresa, otorgado a través de una declaración escrita, verbal o por un medio tecnológico equivalente. También se contemplan ciertas excepciones al consentimiento, como que el dato se haya hecho público o cuando resulte indispensable para salvaguardar la vida, salud o integridad física o psíquica del titular o de otra persona, entre otros casos.
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el 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 estas sean privadas. En cuanto a organismos públicos, el artículo 22 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. La Nueva Ley de Datos Personales no contempla obligaciones de un registro de bases de datos y tampoco se contempla la obligación de entregar un informe periódico a la autoridad.

Tema	Concepto	Sí / 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 11 que el responsable del tratamiento debe cuidar los datos con la debida diligencia. A su vez, el artículo 7 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. Dentro de las obligaciones del responsable de datos, contenidas en el artículo 14 y siguientes de la Nueva Ley de Datos Personales, se incluyen: ▸ Deber de secreto o confidencialidad: el responsable de datos está obligado a mantener secreto o confidencialidad acerca de los datos personales que conciernan a un titular, salvo cuando el titular los hubiere hecho manifiestamente públicos. Este deber subsiste aún después de concluida la relación con el titular. ▸ Deber de protección desde el diseño y por defecto: el responsable debe aplicar medidas técnicas y organizativas adecuadas desde el diseño con anterioridad y durante el tratamiento de los datos personales. Las medidas a aplicar deberán tener en consideración el estado de la técnica; los costos de implementación; la naturaleza, ámbito, contexto y fines del tratamiento de datos, así como los riesgos asociados a dicha actividad. ▸ Deber de adoptar medidas de seguridad: el responsable de datos debe adoptar las medidas necesarias para resguardar el cumplimiento del principio de seguridad, considerando el estado actual de la técnica y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados. Las medidas aplicadas por el responsable deben asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos. Asimismo, deberán evitar la alteración, destrucción, pérdida, tratamiento o acceso no autorizado. Algunas de estas podrán incluir la seudonimización y cifrado de los datos o un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Por ejemplo: rectificación, actualización o supresión) Identificar y explicar.	Sí	La LPDP reconoce explícitamente los siguientes derechos a los titulares en su artículo 12: ▸ 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. La Nueva Ley de Datos Personales reconoce los siguientes derechos de los titulares de datos personales en su artículo 4: ▸ Derecho de acceso: derecho a solicitar y obtener del responsable, confirmación acerca de si los datos personales que le conciernen están siendo tratados por él, y en tal caso, acceder a dichos datos y a la información relativa a estos (finalidades, categorías, etc.). ▸ Derecho de rectificación: derecho a solicitar y obtener del responsable, la rectificación de los datos personales que le conciernen y que están siendo tratados por él, cuando sean inexactos, desactualizados o incompletos. ▸ Derecho de supresión: derecho a solicitar y obtener del responsable la eliminación de los datos personales que le conciernen en ciertos casos como cuando los datos no resulten necesarios en relación con los fines del tratamiento para el cual fueron recogidos, cuando el titular haya revocado su consentimiento, cuando los datos hayan sido obtenidos o tratados ilícitamente o cuando se trate de datos caducos, entre otros. ▸ Derecho de oposición: derecho a oponerse ante el responsable a que se realice un tratamiento específico o determinado de los datos personales que le conciernan, en ciertos casos como cuando la base de licitud del tratamiento sea la satisfacción de intereses legítimos del responsable o si el tratamiento se realiza exclusivamente con fines de mercadotecnia o marketing directo de bienes, productos o servicios, incluida la elaboración de perfiles, entre otros. ▸ Derecho a bloqueo del tratamiento: derecho a solicitar la suspensión temporal de cualquier operación de tratamiento de datos personales cuando se formule una solicitud de rectificación, supresión u oposición de conformidad a la ley. ▸ Derecho a la portabilidad: derecho a solicitar y recibir una copia de los datos personales que le conciernen al titular, que haya facilitado al responsable, en un formato electrónico estructurado, genérico y de uso común, que permita ser operado por distintos sistemas y, a comunicarlos o transferirlos a otro responsable de datos, cuando el tratamiento se realiza en forma automatizada y esté basado en el consentimiento del titular.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
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 16 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 23 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. La Nueva Ley de Datos Personales establece en sus artículos 10 y 11 que estos derechos se hacen valer ante el responsable y, si son varios, cualquiera de ellos. El ejercicio de los derechos de rectificación, supresión y oposición siempre serán gratuitos para el titular. El derecho de acceso también se ejercerá en forma gratuita, al menos trimestralmente. Para ejercerlos, el titular deberá presentar una solicitud ante el responsable que deberá contener ciertas menciones, como su individualización, medio de contacto y los datos respecto de los cuales se hace valer el derecho. Si se trata de una rectificación, se deberá indicar la corrección a realizar y acompañar su sustento. El responsable deberá acusar recibo y pronunciase en el plazo de 30 días (prorrogables por 30 más) y en caso de denegación total o parcial de la solicitud, el responsable deberá fundar su decisión indicando la causa invocada y los antecedentes que la justifican, además de señalar al titular que dispone de un plazo de treinta días seguidos, prorrogables por el mismo plazo, para formular una reclamación ante la Agencia de Protección de Datos Personales. Si, transcurrido el plazo de 30 días, el titular no recibe respuesta, podrá recurrir directamente a la Agencia de Protección de Datos Personales.
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 con el artículo 5 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: 1. La individualización del requirente. 2. El motivo y el propósito del requerimiento. 3. El tipo de datos que se transmiten. El artículo 15 de la Nueva Ley de Datos Personales señala que los datos personales podrán ser cedidos con el consentimiento del titular y para el cumplimiento de los fines del tratamiento. También se podrán ceder los datos personales cuando la cesión sea necesaria para el cumplimiento y la ejecución de un contrato en que es parte el titular; cuando exista un interés legítimo del cedente o del cesionario y cuando lo disponga la ley. Respecto de órganos públicos, el artículo 22 indica que estos están facultados para comunicar o ceder datos personales específicos, o todo o parte de sus bases de datos o conjuntos de datos, a otros órganos públicos, exclusivamente, siempre que la comunicación o cesión de los datos resulte necesaria para el cumplimiento de sus funciones legales y ambos órganos actúen dentro del ámbito de sus competencias. La comunicación o cesión de los datos se debe realizar para un tratamiento específico y el órgano público receptor no los podrá utilizar para otros fines. La cesión de datos deberá constar por escrito o a través de cualquier medio electrónico idóneo. En ella se deberá individualizar a las partes, los datos que son objeto de la cesión, las finalidades previstas para el tratamiento y los demás antecedentes o estipulaciones que acuerden el cedente y el cesionario. Una vez perfeccionada la cesión, el cesionario adquiere la condición de responsable de datos para todos los efectos legales. El cedente, por su parte, también mantiene la calidad de responsable de datos, respecto de las operaciones de tratamiento que continúe realizando. Si se verifica una cesión de datos sin contar con el consentimiento del titular, siendo este necesario, la cesión será nula, debiendo el cesionario suprimir todos los datos recibidos, sin perjuicio de las responsabilidades legales que correspondan.

Tema	Concepto	Sí / 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	Sí se pueden prestar servicios de procesamiento de datos por cuenta de terceros. De acuerdo con el artículo 8 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. Según el artículo 15 bis de la Nueva Ley de Datos Personales, el responsable puede efectuar el tratamiento de datos en forma directa o a través de un tercero mandatario, quien deberá hacerlo en conformidad al encargo y a las instrucciones que le imparta el responsable, quedándole prohibido su tratamiento para un objeto distinto del convenido con el responsable, así como su cesión o entrega en los casos en que el responsable no lo haya autorizado de manera expresa y específicamente para cumplir con el objeto del encargo. Si el tercero mandatario o encargado trata los datos con un objeto distinto del encargo convenido o los cede o entrega sin haber sido autorizado en los términos dispuestos en el inciso anterior, se le considerará como responsable de datos para todos los efectos legales, debiendo responder personalmente por las infracciones en que incurra y solidariamente con el responsable de datos por los daños ocasionados, sin perjuicio de las responsabilidades contractuales que le correspondan frente al mandante o responsable de datos. Una vez cumplido el encargo, los datos que obran en poder del mandatario deben ser suprimidos o devueltos al responsable de datos, según corresponda.
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 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. La Nueva Ley de Datos Personales no establece un plazo particular para la retención de datos personales, pero el titular puede ejercer el derecho de supresión en caso de que los datos no resulten necesarios en relación con los fines del tratamiento para el cual fueron recogidos o se trate de datos caducos.
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 con el artículo 6 de la LPDP, los datos personales deberán ser eliminados o cancelados cuando su almacenamiento no tenga una base legal o cuando haya expirado. El **principio de proporcionalidad** recogido en el artículo 3 de la Nueva Ley de Datos Personales señala que los datos personales que se traten deben limitarse estrictamente a aquellos que resulten necesarios, adecuados y pertinentes en relación con los fines del tratamiento. **Los datos personales pueden ser conservados solo por el periodo de tiempo que sea necesario para cumplir con los fines del tratamiento, luego de lo cual deben ser suprimidos o anonimizados**, sin perjuicio de las excepciones que establezca la ley. Un periodo de tiempo mayor requiere autorización legal o consentimiento del titular.
Privacy Impact Assessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto *(Privacy Impact Assessment)*?	Sí	La LPDP no regula las evaluaciones de impacto. La evaluación de impacto está recogida en el artículo 15 ter de la Nueva Ley de Datos Personales, en el cual se señala que cuando sea probable que un tipo de tratamiento, por su naturaleza, alcance, contexto, tecnología utilizada o fines, se pueda producir un alto riesgo para los derechos de las personas titulares de los datos personales, el responsable del tratamiento deberá realizar, previo al inicio de las operaciones del tratamiento, una evaluación del impacto en protección de datos personales. Asimismo, se establecen casos en que la evaluación es obligatorias, como cuando se realiza el tratamiento masivo de datos o gran escala o el tratamiento de datos sensibles y especialmente protegidos, en las hipótesis de excepción del consentimiento.
Incidentes	¿Hay obligación de reportar un incidente de seguridad o algún incumplimiento a las previsiones legales?	Sí	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 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. El artículo 14 de la Nueva Ley de Datos Personales contiene el deber de reportar las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no autorizados a dichos datos, cuando exista un riesgo razonable para los derechos y libertades de los titulares, por los medios más expeditos posibles.

Tema	Concepto	Sí / 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.	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 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 con el artículo 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. De acuerdo con el artículo 34 de la Nueva Ley de Datos Personales, el omitir en forma deliberada la comunicación de las vulneraciones a las medidas de seguridad que puedan afectar la confidencialidad, disponibilidad o integridad de los datos personales constituye una infracción gravísima, la cual podrá ser sancionada con una multa de hasta 20.000 unidades tributarias mensuales. Por su parte, omitir las comunicaciones o los registros en los casos de vulneración de las medidas de seguridad (sin dolo), constituye una infracción grave según el artículo 34 ter y acarrea una eventual multa de hasta 10.000 unidades tributarias mensuales.
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 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. 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. De acuerdo con lo señalado en el artículo 41 y siguientes de la Nueva Ley de Datos Personales, existen distintas acciones legales que se pueden ejercer para resguardar los derechos de los titulares de datos personales: 1) **Procedimiento administrativo de tutela de derechos:** el titular de datos podrá reclamar ante la Agencia de Protección de Datos Personales cuando el responsable le haya denegado una solicitud realizada de conformidad al artículo 11 de la ley (derechos del titular), o no hubiere dado respuesta a dicha solicitud dentro del plazo legal establecido. 2) **Procedimiento administrativo por infracción de ley:** procedimiento sancionatorio instruido por la Agencia de Protección de Datos Personales ante las infracciones que cometan los responsables de datos por incumplimiento o vulneración de los principios del tratamiento de datos. 3) **Procedimiento de reclamación judicial:** las personas naturales o jurídicas interesadas que estimen que un acto administrativo que paraliza el procedimiento, o una resolución final o de término emanado de la Agencia de Protección de Datos Personales, sea ilegal, podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último.
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 Nº 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. La Nueva Ley de Datos Personales, en su artículo 49, contempla un modelo de prevención de infracciones que los responsables de datos podrán voluntariamente a modo de programa de cumplimiento. Dentro de los elementos mínimos del programa se encuentra la designación de un delegado de protección de datos personales. Su designación no es obligatoria (pero sí un requisito base de un programa de cumplimiento efectivo) y no necesariamente debe ser designado localmente, sin embargo, debe contar con la adecuada independencia y medios suficientes para ejercer sus funciones.

Tema	Concepto	Sí / 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?	Sí	Entre las atribuciones de la Agencia de Protección de Datos Personales se encuentran: ▸ Fiscalizar el cumplimiento de las disposiciones de la ley y normas que se dicten respecto de los tratamientos de datos personales. Para ello, podrá requerir a quienes realicen tratamiento de datos personales la entrega de cualquier documento, libro o antecedente y toda la información que fuere necesaria para el cumplimiento de su función fiscalizadora. ▸ Determinar las infracciones e incumplimientos en que incurran quienes realicen tratamiento de datos personales, en sus operaciones de tratamiento de datos, respecto de los principios y obligaciones establecidos en la ley. Para tales efectos, y de manera fundada, podrá citar a declarar, entre otros, al titular, a los representantes legales, administradores, asesores y dependientes de quien trate datos personales, así como a toda persona que haya tenido participación o conocimiento respecto de algún hecho que sea relevante para resolver un procedimiento sancionatorio. Asimismo, podrá tomar las declaraciones respectivas por otros medios que aseguren su fidelidad.
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?	No	La Nueva Ley de Datos Personales no contempla la creación de registros obligatorios de procesamiento de datos personales.
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (Por ejemplo, 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. La Nueva Ley de Datos Personales que modifica la actual LDPD incorpora estándares de protección muy similares al GDPR. Alguna de sus novedades en relación con la ley vigente son 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.
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	Sí / 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 Nº 1.266/2008 (“Ley 1.266”). ▸ Decreto Nº 2.952/10 (“Dec. 2.952”), compilado en el Decreto Nro. 1.074 de 2015 (“Dec. 1.074). ▸ Decreto Nº 1727/2009 (“Dec. 1.727”), compilado en el Decreto Nro. 1.074 de 2015 (“Dec. 1.074). ▸ Ley Nº 1.273 de 2009 (“Ley 1.273”). ▸ Ley Estatutaria Nº1.581/2012 (“Ley 1.581”). ▸ Decreto Nº 1.377/2013 (“Dec. 1.377”), compilado en el Decreto Nro. 1.074 de 2015 (“Dec. 1074). ▸ Ley Nº 1.712/2014 (“Ley 1.712”). ▸ Decreto Nº 886/2014 (“Dec. 886”), compilado en el Decreto Nro. 1.074 de 2015 (“Dec. 1074). ▸ Decreto Nº1413/2017 (“Dec. 1.413”), adiciona el Decreto Nro. 1.078 de 2015 (“Dec. 1078”). ▸ Ley Nº 1.928/2018 (“Ley 1.928”). ▸ Decreto Nº 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. 1.074. ▸ Circular Única Jurídica de la Superintendencia de Industria y Comercio. Con cierta regularidad la SIC, como autoridad nacional que vela por el cumplimiento de la normativa en Datos Personales, publica guías en esta materia que, si bien no son de carácter vinculante, buscan brindar lineamientos a personas naturales y jurídicas en el debido tratamiento de los datos personales. A la fecha, la SIC ha publicado las guías que pueden ser consultadas en el siguiente *link* **Publicaciones | Superintendencia de Industria y Comercio (sic.gov.co)**: ▸ Guía de Datos Personales para la educación pública y privada (2015). ▸ Guía para la Implementación del Principio de Responsabilidad Demostrada (2016). ▸ Guía para solicitar la Declaración de Conformidad sobre las Transferencias Internacionales de Datos Personales (2016). ▸ Guía sobre el tratamiento de datos personales para fines de marketing y publicidad (2019). ▸ Guía para la Implementación del Principio de Responsabilidad Demostrada (2019). ▸ Guía sobre el Tratamiento de Datos Personales para Fines de Comercio Electrónico (2019). ▸ Guía sobre el Tratamiento de Datos Personales en la Propiedad Horizontal (2020). ▸ Guía sobre el Tratamiento de las Fotos como Datos Personales (2020). ▸ Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales (2020). ▸ Guía para la Implementación del Principio de Responsabilidad Demostrada (2021). ▸ Guía relativa a Recomendaciones para el Tratamiento de Datos Personales mediante Servicios de Computación en la Nube (2021). ▸ Guía relativa a Recomendaciones de la Red Iberoamericana de Protección de Datos (RIPD) para el Tratamiento de Datos Personales sobre la Salud en Tiempos de Pandemia (2021). ▸ Guía sobre el Tratamiento de Datos Personales en las Entidades Estatales (2021). ▸ Guía Cuida tu Identidad Digital y Protege tus Datos Personales: Riesgos sobre el Tratamiento de Datos Personales de Niños, Niñas y Adolescentes (2021). ▸ Guía Implementación – Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales (2022). ▸ Guía Oficial de Protección de Datos Personales (2023). Adicionalmente la SIC, ejerciendo su rol como máxima autoridad en materia de datos emite Circulares Externas en esta materia para ampliar y actualizar nociones jurídicas, dando alcance a lo establecido en la norma. La SIC ha emitido cuatro Circulares Externas: ▸ Circular Externa 001 del 26 de junio de 2024 mediante la cual la SIC aclara la competencia de su Delegatura para la protección de datos personales frente a la Ley 2023 de 2023, la cual establece medidas para proteger el derecho a la intimidad de los consumidores, regulando los canales, horarios y periodicidad en la que estos pueden ser contactados para gestiones de cobranza y envío de mensajes publicitarios. ▸ Circular Externa 002 del 21 de agosto de 2024 por la cual se dan lineamientos sobre el tratamiento de datos personales en sistemas de inteligencia artificial. ▸ Circular Externa 003 del 22 de agosto de 2024 por la cual se imparten instrucciones para los administradores societarios en relación con el tratamiento de datos personales. ▸ Circular Externa 001 del 18 de septiembre de 2025, por la cual se imparten instrucciones sobre el tratamiento de datos personales en la oferta de productos y la prestación de servicios de financiación, depósitos de bajo monto y otros afines que faciliten la inclusión financiera mediante el uso de tecnologías digitales (Fintech).

Tema	Concepto	Sí / 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	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 1.581.
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 2.2.2.25.2.1. al 2.2.2.25.2.5. del Decreto 1.074.
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 1.581. Bajo la Ley 1.266, se define el concepto de "dato personal" como cualquier información relacionada con, o que pueda asociarse a, una o varias personas naturales o jurídicas determinadas o determinables. Los datos personales también pueden ser considerados como datos públicos, privados o semiprivados. Los datos públicos son aquellos disponibles para el público por mandato legal o constitucional. Los datos privados o semiprivados son datos que no tienen un propósito público, son de naturaleza íntima y cuya divulgación solo concierne al titular de los datos.
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 solo 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 1.581 y Art. 3, inc. 2), Dec. 1.377.
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 con su información financiera, comercial y de cumplimiento de obligaciones dinerarias, al tenor de la Ley 1.266.

Tema	Concepto	Sí / 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	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. El responsable debe informar al titular qué información será recolectada y las finalidades del tratamiento de esos datos. Cuando existan cambios sustanciales en la finalidad del tratamiento, el responsable deberá notificar al titular y obtener su consentimiento para el tratamiento de los datos personales bajo esas nuevas finalidades. 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. 1.377.
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: 1. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial. 2. Datos de naturaleza pública. 3. Casos de urgencia médica o sanitaria. 4. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos. 5. 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. 1.074. Art. 10, Ley 1.581. Art. 2.2.2.25.5.1. Dec. 1.074.
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: 1. El tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; 2. 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; 3. Los derechos que le asisten como titular; 4. La identificación, dirección física o electrónica y teléfono del responsable del tratamiento. Art. 12, Ley 1.581 de 2012, Art. 7, Dec. 1.377 y Arts. 2.2.2.25.2.3 y 2.2.2.25.2.4 del De. 1.074.

Tema	Concepto	Sí / 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 con la transferencia internacional de datos? (Por ejemplo, cláusulas modelos, autorización por parte de la autoridad de control, entre otros).	Sí	La Ley 1.581 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: 1. Información respecto de la cual el titular haya otorgado su autorización expresa e inequívoca para la transferencia. 2. Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública. 3. Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable. 4. Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad. 5. 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. 6. Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. 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 1.581 y Art. 3, inc. 3.1, 3.2 y 3.3), Circular Externa No. 005 Bogotá D.C: **https://www.sic.gov.co/sites/default/files/normatividad/082017/Circular_Externa_005_de_2017.pdf**

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	Sí	La Ley 1.581, 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: 1. Sean jurídicamente vinculantes y se apliquen a todos los miembros que hacen parte del mismo grupo empresarial. 2. Confieran expresamente a los titulares de los datos la facultad de ejercer los derechos previstos en las normas aplicables. 3. 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 1.581 y Arts. 3, inc.4) y 5), 24 y 25, Dec. 1.377. 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. 1.074, respectivamente. Dec. 255.
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 1.581 y art. 6 del Dec. 1.377, a su vez compilado en el art. 2.2.2.25.2.3 del Dec. 1.074. Igualmente, la Superintendencia de Industria y Comercio ha señalado que (i) deben tomarse medidas de seguridad reforzada frente a estos datos sensibles; y (ii) los responsables no pueden condicionar la adquisición de bienes o la prestación de servicios, el acceso o uso de aplicaciones móviles o la creación de cuentas de usuarios, a la entrega de datos biométricos. Arts. 5 y 6, Ley 1.581 y Art. 6, Dec. 1.377, compilado en el art. 2.2.2.25.2.3 del Dec. 1.074.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el 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. 1.074. Si bien no existe obligación de presentar informes periódicos ante el" RNBD", 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. Adicionalmente, los responsables deben actualizar la información registrada en el RNBD dentro de los primeros 10 días hábiles de cada mes, cuando se hayan realizado cambios sustanciales en las bases de datos. Los cambios sustanciales son aquellos relacionados con el propósito de la base de datos, el encargado del tratamiento, la clasificación o tipos de datos personales almacenados en la base de datos, las medidas de seguridad de la información implementadas, la Política de Tratamiento de la Información, la transferencia internacional y transmisión de datos personales y, los canales de atención al titular. También deberán actualizar la información sobre reclamaciones presentadas por los titulares de los datos entre julio y diciembre del año anterior, dentro de los primeros quince (15) días hábiles de febrero de cada año. Para ello, debe tenerse en cuenta lo declarado por los titulares de los datos y los tipos de reclamaciones que están preestablecidos en el RNBD. Este informe debe ser el resultado de consolidar las reclamaciones presentadas por los responsables de los datos ante los responsables y/o encargados del tratamiento. Esta misma obligación debe cumplirse dentro de los primeros 15 días hábiles de agosto de cada año, en relación con reclamaciones presentadas entre enero y junio de ese mismo año. Finalmente, los responsables deberán reportar incidentes de seguridad dentro de los 15 días hábiles siguientes a su detección y registrar nuevas bases de datos dentro de los 2 meses siguientes a su creación. Art. 25, Ley 1.581 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. 1.074, 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. 1.377. 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. 1.074, respectivamente.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Por ejemplo, rectificación, actualización o supresión) Identificar y explicar.	Sí	Los titulares de los datos personales poseen los siguientes derechos: 1. Conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento. 2. 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. 3. Ser informado por el responsable del tratamiento o el encargado del tratamiento. 4. 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. 5. 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. 6. 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. 1.377. A su vez, Compilado en el art. 2.2.2.25.2.9, del Dec. 1.074.
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 1.581 y art. 20 y 21 del Dec. 1.377. 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. 1.377. A su vez, compilados en los arts. 2.2.2.25.4.1 y 2.2.2.25.4.2 del Dec. 1.074, 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, los cuales se encuentran detallados en el art. 18 de la Ley 1581. Art. 3, inc. d) y 18, Ley 1.581. A su vez en art. 2.2.2.25.5.1 y 2.2.2.25.5.2 del Dec. 1.075.
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. 1.377. A su vez compilado en el art. 2.2.2.25.2.8, del Dec. 1.074.
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. 1.377. A su vez, compilado en el art. 2.2.2.25.2.8, del Dec. 1.074.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Privacy Impact Assessment	¿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: 1. Una descripción detallada de las operaciones de Tratamiento de Datos Personales que involucra el proyecto de la compañía. 2. 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 o 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 1.581.
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 1.581. Art. 22 y 23, Ley 1.581.
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 1.266. Adicionalmente, arts. 16, 22, 23 y 24 de la Ley 1.581.
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 4.886/113, 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 1.581 y Art. 16, Decreto Nº 4.886/113. A su vez, 2.2.2.25.3.1 y 2.2.2.25.4.4 del Dec. 1.074.
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 1.581.
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?		No hay *per se* un requisito que obligue a los responsables y encargados a mantener registros detallados de procesamiento de los datos personales que tratan. Sin embargo, algunos responsables (sociedades y entidades sin ánimo de lucro) deben registrar las bases de datos personales que tratan cuando tengan activos totales superiores a 100.000 Unidades de Valor Tributario (UVT), así como las personas jurídicas de naturaleza pública (cf. respuesta a la pregunta número 14).

Tema	Concepto	Sí / 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 (Por ejemplo, GDPR) ?, ¿qué diferencias relevantes encuentra?	Sí	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	Sí / 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 8.968 vigente desde el 5 de septiembre de 2011 (en adelante conocida como la "Ley Nº 8.968"), y el Reglamento a la Ley de Protección de Datos Nº 37.554-JP vigente desde el 5 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 Nº 8.968 establece como autoridad encargada a la Agencia de Protección de Datos de los habitantes (Prodhab), el cual es un órgano de desconcentración máxima adscrito 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 Nº 8.968 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 8.968 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 Nº 8.968 define los datos personales como cualquier dato relativo a una persona física identificada o identificable.
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	▸ 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 Nº 8.968 y artículos 4 y 5 del Reglamento)

Tema	Concepto	Sí / 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 Ley Nº 8.968 establece que no será necesario el consentimiento expreso del titular de los datos, cuando: 1. 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. 2. Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general. 3. Los datos deban ser entregados por disposición constitucional o legal. (Artículo 5.2 de la ley y artículo 5 del Reglamento)
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: 1. De la existencia de una base de datos de carácter personal. 2. De los fines que se persiguen con la recolección de estos datos. 3. De los destinatarios de la información, así como de quiénes podrán consultarla. 4. Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección de los datos. 5. Del tratamiento que se dará a los datos solicitados. 6. De las consecuencias de la negativa a suministrar los datos. 7. De la posibilidad de ejercer los derechos que le asisten. 8. 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 con la transferencia internacional de datos? (Por ejemplo, cláusulas modelos, autorización por parte de la autoridad de control, entre otros)	Sí	La Ley Nº 8.968 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 establecen 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: 1. Elaborar políticas y manuales de privacidad obligatorios y exigibles al interior de la organización del responsable. 2. Poner en práctica un manual de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales. 3. Establecer un procedimiento de control interno para el cumplimiento de las políticas de privacidad. 4. 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. 5. Crear medidas y procedimientos técnicos que permitan mantener un historial de los datos personales durante su tratamiento. 6. 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 Nº 8.968 y artículos 32 y 41)

Tema	Concepto	Sí / 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: 1. 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. 2. 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. 3. 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. 4. 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 (por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el 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 Prodbhab solicite, así como los protocolos de actuación que se han mencionado en el artículo 12 de la ley, y al cual se hace referencia en el espacio sobre BCR.

Tema	Concepto	Sí / 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 Nº 8.968). 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: 1. Elaborar una descripción detallada del tipo de datos personales tratados o almacenados. 2. Crear y mantener actualizado un inventario de la infraestructura tecnológica, incluyendo los equipos y programas de cómputo y sus licencias. 3. 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. 4. Contar con un análisis de riesgos, que consiste en identificar peligros y estimar los riesgos que podrían afectar los datos personales. 5. Establecer las medidas de seguridad aplicables a los datos personales, e identificar aquellas implementadas de manera efectiva. 6. Calcular el riesgo residual existente basado en la diferencia de las medidas de seguridad existentes y aquellas faltantes que resultan necesarias para la protección de los datos personales. 7. 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? (Por 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 las formas simplificadas 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).
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	Sí	Los datos personales objeto de tratamiento solo 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 este 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	Sí / 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 artículo 29 del Reglamento de la Ley Nº 8.968, define la contratación o subcontratación de servicios como aquella transacción mediante la cual el responsable de la base de datos contrata a un tercero (intermediario tecnológico o un proveedor de servicios), para que sea el encargado de realizar el tratamiento de los datos personales. El encargado tendrá las siguientes obligaciones: 1. Tratar únicamente los datos personales conforme a las instrucciones del responsable. 2. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. 3. 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. 4. Guardar confidencialidad respecto de los datos personales tratados. 5. Abstenerse de transferir o difundir los datos personales, salvo instrucciones expresas por parte del responsable. 6. 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
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 Nº 8.968 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 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: 1. Disposición normativa especial que establezca otro plazo. 2. Por acuerdo entre partes que establezca un plazo distinto. 3. Que exista una relación continuada entre las partes. 4. Interés público para conservar el dato. (Artículos 6 y 30 de la Ley y artículo 11 del Reglamento)
Privacy Impact Assessment	¿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 a 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): 1. La naturaleza del incidente. 2. Los datos personales comprometidos. 3. Las acciones correctivas realizadas de forma inmediata. 4. Los medios o el lugar, donde puede obtener más información al respecto.

Tema	Concepto	Sí / 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.	No	Sin embargo, si el titular de los datos se ve afectado por el incidente o por el incumplimiento, el artículo 28 de la Ley Nº 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.
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.
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?	No	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 (Por ejemplo, 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 8.968 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, Nº 7.472, 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	Sí / 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 vigor el 26 de mayo de 2021. Complementariamente, esta normativa cuenta con su Reglamento General y con normativa secundaria emitidas por la Autoridad de Protección de Datos Personales (APDP).
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, Fabrizio Peralta Díaz, como el primer titular de la Autoridad de Protección de Datos (Superintendencia de Protección de Datos Personales) desde el 23 de abril de 2024, quien ejercerá sus funciones por un periodo de 5 años. El enlace para acceder al sitio *web* de dicha entidad es el siguiente: **https://spdp.gob.ec/**
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. La normativa ecuatoriana en materia de protección de datos establece un ámbito de aplicación **extraterritorial** en los siguientes casos: 1. El responsable o encargado no domiciliado en Ecuador trate datos de titulares residentes en Ecuador, cuando las actividades del tratamiento se relacionen con: a. La oferta de bienes o servicios a titulares. b. El control de su comportamiento siempre cuando este tenga lugar en el territorio nacional ecuatoriano. 2. 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 lícito 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 al 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.
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.

Tema	Concepto	Sí / 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	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.
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: ▸ **Libre,** es decir, cuando se encuentre exenta de vicios del consentimiento. ▸ **Específica**, en cuanto a la determinación concreta de los medios y fines del tratamiento. ▸ **Informada**, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia. ▸ **Inequívoca**, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular. ▸ **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.

Tema	Concepto	Sí / 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 con la transferencia internacional de datos? (Por 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: a. Se podrán transferir datos personales, organizaciones y personas jurídicas en general que brinden niveles adecuados de protección. b. 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 APDP de tener un nivel adecuado de protección, se deberá emitir un instrumento jurídico de carácter vinculante, que garantice: i. El cumplimiento de principios, derechos y obligaciones en el tratamiento de datos personales en un estándar igual o mayor a la normativa ecuatoriana. ii. La disponibilidad permanente de acciones administrativas o judiciales. iii. El derecho a solicitar reparación integral de ser el caso. c. 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. De oficio o a petición de parte, la APDP, mediante resolución motivada, determinará los países, las organizaciones o personas jurídicas que cuentan con adecuados niveles de protección para transferencia de datos personales.
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	Sí	Los responsables o encargados del tratamiento de datos personales podrán presentar a la APDP, normas corporativas vinculantes, específicas y aplicadas al ámbito de su actividad. Todo grupo empresarial, o unión de empresas dedicadas a una actividad económica conjunta, tendrá la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de datos a terceros países, siempre que tales normas corporativas incorporen todos los principios de tratamiento de datos personales y derechos aplicables y garantías de seguridad adecuadas para la transferencia de datos de personales.
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. 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 las obligaciones y el 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.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (Por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el 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 de 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. Identificación; 8. Domicilio y contacto de los destinatarios de datos personales, incluyendo a encargados y terceros. 9. Modo de interrelacionar información registrada. 10. Medios utilizados para implementar la LODPD y normativa conexa. 11. Requisitos y herramientas implementadas para garantizar la seguridad y protección de datos personales. 12. 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 y el acceso a datos personales de forma rápida en caso de incidentes. 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.
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Por 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	Requerimientos, peticiones, quejas directas y reclamos administrativos. En el caso de que el responsable del tratamiento no conteste a la queja en el término establecido o esta 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.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	Sí	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 los estipulados en el contrato. El tercero no podrá transferir o comunicar los datos personales para su conservación. Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable bajo la supervisión de la APDP. 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.
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. 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 Assessment	¿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 las libertades del titular o cuando la APDP lo requiera. Las evaluaciones de impacto del tratamiento de datos son obligatorias en los casos establecidos en la Ley y deben realizarse de forma previa al inicio del tratamiento de datos personales. Los responsables deben utilizar los criterios establecidos en el Reglamento para determinar en qué casos se está en presencia de una evaluación sistemática y exhaustiva de aspectos personales, de un tratamiento a gran escala de categorías especiales de datos, de datos relativos a condenas e infracciones penales o, de una observación sistemática a gran escala de una zona de acceso público. En caso de duda, el responsable puede dirigir una consulta a la APDP con la finalidad de que determine la obligatoriedad de la evaluación de impacto. La APDP debe contestar dicha consulta en el término máximo de cinco días contados desde la recepción de la consulta.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Incidentes	¿Hay obligación de reportar un incidente de seguridad o algún incumplimiento a 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 cinco 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 dos 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 tres 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 a 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 10 a 20 salarios básicos unificados del trabajador en general, sin perjuicio de la responsabilidad extracontractual del Estado. En relación con el 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. La APDP establecerá la multa aplicable en función del principio de proporcionalidad, considerando la intencionalidad, reiteración de la infracción o la naturaleza del perjuicio ocasionado.
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 un DPO cuando: 1. El tratamiento se lleve a cabo por quienes conforman el sector público. 2. 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. El DPO podrá ser contratado por el responsable del tratamiento de datos personales, bajo la figura de relación de dependencia, manteniendo total independencia entre sus funciones, o a través de un contrato de prestación de servicios. Para desempeñar sus funciones, debe cumplir y aprobar el contenido mínimo de formación del programa profesionalizante de DPO oficializado por la APDP. Los grupos empresariales pueden designar a un único DPO.
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 del caso concreto o la conveniencia o no de iniciar un procedimiento administrativo.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?	Sí	El responsable del tratamiento que cuente con cien o más trabajadores, llevará un registro de todas las actividades de tratamiento de datos personales que sean de su competencia. El registro se llevará por escrito o electrónicamente. Los responsables pondrán a disposición de la Autoridad de Protección de Datos Personales los registros de actividades cuando esta lo solicite. La obligación de registro de actividades también la tendrán los responsables de tratamiento que, teniendo menos de 100 trabajadores, cumplan alguna de las siguientes condiciones: 1. El tratamiento que realice pueda entrañar un riesgo para los derechos y las libertades de los titulares, de acuerdo con el análisis de riesgos, amenazas y vulnerabilidades, de conformidad con lo dispuesto en la ley; 2. No se trate de un tratamiento ocasional. 3. Incluya categorías especiales de datos personales.
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (Por ejemplo, GDPR)?, ¿qué diferencias relevantes encuentra?	Sí	La LOPDP 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 inició el régimen sancionatorio. Mediante Decreto 904 se emitió el Reglamento General de la Ley Orgánica de Protección de Datos Personales publicado mediante tercer suplemento del Registro Oficial No. 435 con fecha 13 de noviembre de 2023. Desde el 1 de noviembre y hasta el 31 de diciembre de 2025, las personas jurídicas de derecho público y privado que cumplan con las condiciones establecidas en la LPDP, su reglamento general y la normativa conexa que emita la APDP, deberán nombrar y registrar a su DPO de manera física o electrónica. El incumpliendo o el registro extemporáneo del DPO dará lugar a imposición de sanciones.

GUATEMALA

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Normativa	¿Existe en el país una ley de protección de datos personales? En ese caso, identificar normativa aplicable.	No	Actualmente, en Guatemala no existe una ley específica e integral de protección de datos personales. Sin embargo, hay normativa aplicable que aborda aspectos de la privacidad y el tratamiento de datos. Constitución Política de la República de Guatemala, artículo 24 que dispone la inviolabilidad de correspondencia, documentos y libros de toda persona. Artículo 24.- Inviolabilidad de correspondencia, documentos y libros. La correspondencia de toda persona, sus documentos y libros son inviolables. Solo podrán revisarse o incautarse, en virtud de resolución firme dictada por juez competente y con las formalidades legales. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna. Los libros, documentos y archivos que se relacionan con el pago de impuestos, tasa, arbitrios y contribuciones, podrán ser revisados por la autoridad competente de conformidad con la ley. Es punible revelar el monto de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro dato referente a las contabilidades revisadas a personas individuales o jurídicas, con excepción de los balances generales, cuya publicación ordene la ley. Los documentos o informaciones obtenidas con violación de este artículo no producen fe ni hacen prueba en juicio. Pacto Internacional de Derechos Civiles y Políticos, Artículo 17 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. Convención Americana sobre Derechos Humanos (Pacto de San José) Artículo 11. Protección de la Honra y de la Dignidad 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. LA CONVENCIÓN SOBRE LOS DERECHOS DE LAS PERSONAS CON DISCAPACIDAD, artículo 22. Respeto a la privacidad. Las personas con discapacidad tienen derecho a su vida privada. Por eso, los países, protegerán sus datos personales y los datos sobre su salud. Decreto 57-2008 del Congreso de la República, Ley de Acceso a la Información Pública. Aunque su objeto principal es garantizar el acceso a la información pública, contiene disposiciones importantes en materia de protección de datos personales. Algunos de los artículos relevantes son: Artículo 30: Establece que la información suministrada por particulares a la administración pública bajo "garantía de confidencia" queda excluida de la regla general de publicidad. Artículo 31: Prohíbe expresamente la comercialización por cualquier medio de datos sensibles o datos personales sensibles sin la autorización del titular. Artículo 32: Establece las excepciones al consentimiento del titular para proporcionar los datos personales. Código penal: Artículo 217.- Violación de correspondencia y papeles privados. Quien, de propósito o para descubrir los secretos de otro, abriere correspondencia, pliego cerrado o despachos telegráfico, telefónico o de otra naturaleza, que no le estén dirigidos o quien, sin abrirlos, se impusiere de su contenido, será sancionado con multa de 100 a 1,000 quetzales. Artículo 218.- Sustracción, desvío o supresión de correspondencia. Quien, indebidamente, se apoderare de correspondencia, pliego o despachos, a que se refiere el artículo anterior o de otro papel privado, aunque no estén cerrados o quien los suprimiere o desviare de su destino, será sancionado con multa de 100 a 1,000 quetzales. Artículo 219.- Intercepción o reproducción de comunicaciones. Quien, valiéndose de medios fraudulentos interceptare, copiare o grabare comunicaciones televisadas, radiales, telegráficas, telefónicas u otras semejantes o de igual naturaleza, o las impida o interrumpa, será sancionado con multa de 100 a 1,000 quetzales. Artículo 220. Agravación específica. Las sanciones señaladas para los hechos delictuosos definidos en los tres artículos que preceden, serán de prisión de seis meses a tres años, en los siguientes casos: 1º. Si el autor se aprovechare de su calidad de gerente, director, administrador o empleado de la dependencia, empresa o entidad respectiva. 2º. Si se tratare de asuntos oficiales. 3º. Si la información obtenida, el autor la hiciere pública, por cualquier medio. 4º. Si el autor fuere funcionario o empleado público Artículo 221.- Excepciones. Lo preceptuado en los artículos 217, 218 y 219 de este capítulo, no es aplicable a los padres respecto a sus hijos menores de edad, ni a los tutores o protutores respecto a las personas que tengan bajo su custodia o guarda. Artículo 222.- Publicidad indebida. Quien, hallándose legítimamente en posesión de correspondencia, de papeles o de grabaciones, fotografías no destinadas a la publicidad, los hiciere públicos, sin la debida autorización, aunque le hubieren sido dirigidos, cuando el hecho cause o pudiere causar perjuicio, será sancionado con multa de doscientos a dos mil quetzales. Artículo 223.- Revelación de secreto profesional. Quien, sin justa causa, revelare o empleare en provecho propio o ajeno un secreto del que se ha enterado por razón de su estado, oficio, empleo, profesión o arte, sin que con ello ocasionare o pudiere ocasionar perjuicio, será sancionado con prisión de seis meses a dos años o multa de 100 a 1,000 quetzales. Artículo 61. Publicación de la sentencia. La publicación de la sentencia es pena accesoria a la principal que se imponga por los delitos contra el honor y contra la libertad e indemnidad sexual, regulados en el Código Penal y otras normas específicas de la materia. En los casos de delitos contra el honor, a petición del ofendido o de sus herederos, el juez, a su prudente arbitrio, ordenará la publicación de la sentencia en uno o dos periódicos de mayor circulación en la República, a costa del condenado o de los solicitantes subsidiariamente, cuando estime que la publicidad pueda contribuir a reparar el daño moral causado por el delito. En ningún caso, podrá ordenarse la publicación de la sentencia cuando afecte a menores o a terceros. En los casos de delitos contra la libertad e indemnidad sexual, la sentencia se publicará en las páginas electrónicas oficiales del Ministerio Público y Organismo Judicial, sin hacer público los datos personales de la víctima. En ningún caso, podrá ordenarse la publicación de la sentencia cuando el condenado sea menor de edad. Asimismo, también se usa como parte de los referentes en esta materia el Reglamento General de Privacidad de Datos Europeo, la Ley Modelo Interamericana sobre gestión documental y los Principios sobre privacidad y protección de datos personales emitidos por la OEA.

Tema	Concepto	Sí / 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*.	N/A	No tenemos una dependencia específica, sería todos los órganos del Estado.
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	Territorial
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	Los principios que se espera que se aseguren en la protección de datos personales son: consentimiento, legitimidad, finalidad, exactitud, confidencialidad, responsabilidad en el tratamiento de datos y garantizar al titular el acceso a sus datos, rectificar, cancelar datos excesivos, oponerse o limitar el tratamiento. Lo anterior fundado principalmente en las buenas prácticas en materia de privacidad de datos y artículos del Decreto 57-2008, Ley de Acceso a la Información Pública artículo 13, 31, 32, 33, 34, 35 - 45
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Si	Conforme al art. 9 del Decreto 57-2008, Ley de Acceso a la Información Pública, la normativa guatemalteca entiende por dato personal toda "información concerniente a personas naturales identificadas o identificables".
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Si	Conforme a la normativa guatemalteca, específicamente el Decreto 57-2008, existen dos categorías principales de datos: 1.Datos personales: Los relativos a cualquier información concerniente a personas naturales identificadas o identificables. 2. Datos sensibles o datos personales sensibles: Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, el origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencia o vida sexual, situación moral y familiar u otras cuestiones íntimas de similar naturaleza.
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	¿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)
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Si	Según el Decreto 57-2008, Ley de Acceso a la Información Pública, existen excepciones a la necesidad de obtener el consentimiento del titular de los datos. Estas excepciones, que no requieren la autorización previa del individuo, son: Datos de registros públicos: No se requiere consentimiento cuando la información ya está contenida en registros públicos o es de acceso irrestricto. Fines estadísticos, científicos o de interés general: La información personal puede ser utilizada con fines estadísticos, científicos o de interés general, siempre que no sea posible asociar los datos con la persona a la que se refieren. Transferencia entre entidades públicas: La información puede ser transferida entre dependencias del Estado siempre y cuando se utilice para el ejercicio de sus facultades propias. Orden judicial: El consentimiento no es necesario cuando la entrega de los datos es ordenada por un juez, especialmente en casos de investigación criminal o para la procuración y administración de justicia. Cualquier otra establecida en ley. En esencia, la normativa guatemalteca permite la recolección y el uso de datos sin consentimiento si la información ya es pública, si los datos no son identificables, o si se utilizan para funciones estatales específicas, la justicia o el interés público legítimo.

Tema	Concepto	Sí / 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.)		La persona debería tener claridad de qué información, para qué, quién será el encargado/responsable, por cuánto tiempo y los derechos
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales?, ¿hay requisitos aplicables en relación con la transferencia internacional de datos? (Por ejemplo, cláusulas modelos, autorización por parte de la autoridad de control, entre otros)	No	Guatemala no tiene una ley de protección de datos dedicada que detalle estos requisitos, la transferencia de datos personales está sujeta a la prohibición de comercialización sin autorización y a los principios de finalidad y confidencialidad.
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	No	No, Guatemala no cuenta con normas corporativas vinculantes (BCR).
Datos sensibles	¿Qué se entiende por dato sensible?, ¿cómo es el tratamiento de los datos sensibles, de corresponder?	Si	Según el Decreto 57-2008, se entiende por Dato sensible aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, el origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencia o vida sexual, situación moral y familiar u otras cuestiones íntimas de similar naturaleza.
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (Por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el uso de la misma?, ¿existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	No	No es obligatorio debido a la ausencia de regulación local.
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	No	No existen lineamientos debido a la falta de regulación local.
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Por ejemplo, rectificación, actualización o supresión) Identificar y explicar.	Si	En Guatemala, los derechos de los titulares de los datos se derivan principalmente del derecho constitucional de habeas data, que ha sido desarrollado a través del Decreto 57-2008. Estos derechos permiten a las personas ejercer control sobre su información personal que se encuentra en archivos y registros públicos. Habeas data según la citada ley es la garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos, fichas, registros o cualquier otra forma de registros públicos, y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación o actualización. **Derecho de Acceso:** El titular tiene el derecho de acceder y conocer la existencia y el contenido de los datos personales que se encuentren en cualquier archivo, registro o banco de datos de carácter público. **Derecho de Rectificación y Actualización:** El titular puede solicitar la rectificación o actualización de sus datos si estos son inexactos, incompletos o están desactualizados. Este derecho busca garantizar que la información personal sea veraz y pertinente. **Derecho de Supresión:** El titular puede solicitar la supresión de sus datos si la información ya no es necesaria para los fines para los que fue recolectada, si su tratamiento es contrario a la ley, o si se ha revocado el consentimiento. Es importante señalar que la Ley de Acceso a la Información Pública aplica estos derechos a los registros en poder de las entidades del Estado. La aplicación en el sector privado no está regulada de manera específica por una ley.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Si	Los titulares de los datos pueden ejercer sus derechos a través de un procedimiento formal establecido en la Ley de Acceso a la Información Pública (Decreto 57-2008), que aplica principalmente a los archivos y registros del sector público. Proceso para el sector público Presentar la solicitud: El titular de los datos debe dirigir una solicitud de información a la Unidad de Información Pública (UIP) de la entidad del Estado que se presume tiene la información personal. La solicitud puede ser verbal o escrita. Aunque no se requiere justificación, es importante especificar el derecho que se desea ejercer (acceso, rectificación o supresión) y, si es posible, identificar los datos a los que se refiere. Plazo de respuesta: La entidad pública tiene un plazo de diez días hábiles para responder a la solicitud. Este plazo puede prorrogarse por diez días adicionales en casos justificados. Proceso para el sector privado: Debido a la ausencia de una ley específica que regule al sector privado, no existe un procedimiento legal formal para ejercer estos derechos ante el sector privado por lo cual operaría el principio de libertad de acción que reza, lo que no está prohibido está permitido, teniendo el titular la oportunidad de utilizar cualquier acción que considere oportuna según cada caso para poder ejercerlos.
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?		No está regulada, pero debería de mediar consentimiento del titular para poder realizar la cesión y garantizar la integridad en la portabilidad de los mismos, así como cualquier exclusión.
Procesamiento de datos	¿Se pueden prestar servicios por cuenta de terceros (*data processing*)? En caso afirmativo, explicar procedimiento y excepciones aplicables, de corresponder.	No	Guatemala no cuenta con un marco legal específico que regule la prestación de servicios de tratamiento de datos personales por cuenta de terceros.
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	No, la normativa guatemalteca no establece una obligación de retener o conservar los datos personales por un periodo de tiempo determinado.
Eliminación de datos	¿Existe una obligación de eliminar los datos recolectados o procesados? En dicho caso, ¿en qué supuestos y cuál es el plazo?		Artículo 36. Salvaguarda de documentos. Ley de acceso a la Información Pública La información pública localizada y localizable en los archivos administrativos no podrá destruirse, alterarse, modificarse, mutilarse u ocultarse por determinación de los servidores públicos que la produzcan, procesen, administren, archiven y resguarden, salvo que los actos en ese sentido formaren parte del ejercicio de la función pública y estuvieren jurídicamente justificados. El incumplimiento de esta norma será sancionado de conformidad con la esta ley y demás leyes aplicables. Artículo 37. Archivos administrativos. Ley de acceso a la Información Pública. Con relación a la información, documentos y expedientes que formen parte de los archivos administrativos no podrán en ningún caso ser destruidos, alterados o modificados sin justificación. Los servidores públicos que incumplan el presente y el anterior artículo de esta ley podrán ser destituidos de su cargo y sujetos a lo previsto por los artículos 418 Abuso de Autoridad y 419 Incumplimiento de Deberes del Código Penal vigente. Si se trata de particulares quienes coadyuven, provoquen o inciten, directa o indirectamente a la destrucción, alteración o modificación de archivos históricos, aplicará el delito de depredación del patrimonio nacional, regulado en el Código Penal.
Privacy Impact Assessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (*Privacy Impact Assessment*)?	No	Actualmente no existen programas ni exigencias específicas debido a la falta de regulación local.
Incidentes	¿Hay obligación de reportar un incidente de seguridad o algún incumplimiento a las previsiones legales?	N/A	

Tema	Concepto	Sí / 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.	Si	Constitución Política de la República de Guatemala, artículo 155.- Responsabilidad por infracción a la ley. Cuando un dignatario, funcionario o trabajador del Estado, en el ejercicio de su cargo, infrinja la ley en perjuicio de particulares, el Estado o la institución estatal a quien sirva, será solidariamente responsable por los daños y perjuicios que se causaren. La responsabilidad civil de los funcionarios y empleados públicos podrá deducirse mientras no se hubiere consumado la prescripción, cuyo término será de veinte años. La responsabilidad criminal se extingue, en este caso, por el transcurso del doble del tiempo señalado por la ley para la prescripción de la pena. Asimismo, para conocer otras responsabilidades ver la sección 1 en lo relativo a la responsabilidad penal y además para la reparación del daño causado ver lo regulado en el código civil, Artículo 1645.- Toda persona que cause daño o perjuicio a otra, sea intencionalmente, sea por descuido o imprudencia, está obligada a repararlo, salvo que demuestre que el daño o perjuicio se produjo por culpa o negligencia inexcusable de la víctima. Artículo 1646.- El responsable de un delito doloso o culposo, está obligado a reparar a la víctima los daños o perjuicios que le haya causado. Artículo 1647.- La exención de responsabilidad penal no libera de la responsabilidad civil, a no ser que el juez así lo estimare atendiendo a las circunstancias especiales del caso.
Acciones legales	¿Existe alguna acción legal de protección de datos personales?, ¿quién tiene derecho para ejercerla/solicitarla?		Según cada caso podrían corresponder diferentes acciones y recursos, quedando a salvo lo contemplado en la Ley de Amparo, Exhibición Personal y de Constitucionalidad, Artículo 10. Procedencia del amparo. La procedencia del amparo se extiende a toda situación que sea susceptible de un riesgo, una amenaza, restricción o violación a los derechos que la Constitución y las leyes de la República de Guatemala reconocen, ya sea que dicha situación provenga de personas y entidades de derecho público o entidades de derecho privado.
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	No aplica, debido a la ausencia de regulación específica
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	N/A	Actuarán a instancia de parte
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?	N/A	No aplica, debido a la ausencia de regulación específica
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (Por ejemplo, GDPR), ¿qué diferencias relevantes encuentra?	N/A	No aplica, debido a la ausencia de regulación específica, de hecho, se usa el reglamento como referente para esta materia
Otras obligaciones	¿Existen otras consideraciones/requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	N/A	

MÉXICO

Tema	Concepto	Sí / 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 (21 de marzo de 2025) ("LFPDPPP"). La nueva LFPDPPP es sustancialmente similar a su antecesora. ▸ Reglamento de la 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"). Conforme al decimosegundo transitorio del decreto por virtud del cual se expidió la nueva LFPDPPP, las adecuaciones correspondientes a "los reglamentos y demás disposiciones aplicables" debieron haberse expedido dentro de los 90 días naturales siguientes a la entrada en vigor de la LFPDPPP. No obstante lo anterior, se continúa a la espera de las reformas a la regulación secundaria en materia de protección de datos personales en posesión de particulares y, por ende, la regulación secundaria que se menciona en los incisos anteriores continúa vigente. 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 la Secretaría de Anticorrupción y Buen Gobierno, a través de la Unidad de Protección de Datos Personales ("SABG"). **Secretaría Anticorrupción y Buen Gobierno | Gobierno | gob.mx**
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. 1, 2 inc. XII) 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: 1. A todo tratamiento que sea efectuado en un establecimiento de un responsable ubicado en territorio mexicano. 2. A todo tratamiento efectuado por un encargado con independencia de su ubicación, a nombre de un responsable establecido en territorio mexicano. 3. 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. 4. 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.
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, información con respecto a las transferencias de datos que se efectúen, en su caso, y cuáles son los derechos del titular, así como los medios para ejercerlos, 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, a partir del momento en el cual se recaben sus datos personales. El aviso de privacidad deberá cumplir con las disposiciones establecidas en los arts. 2 sección I, 14-16 de la LFPDPPP, y 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.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	Se entiende como datos personales a cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información. Art. 2, 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 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 afectan la esfera más íntima del titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. 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 3 de la LFPDPPP o cuando el responsable lo requiera para finalidades legitimas, concretas y acordes con las actividades o fines explícitos que persiga. Art. 2, inc. v) y vi), 7, 8, 12 y 15 LFPDPPP y Art. 15 inc. II y III, 56 y 62 del Reglamento de la LFPDPPP.
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	Si bien la definición de "datos personales" prevista en la LFPDPPP no especifica que sea información concerniente a una persona física, consideramos que actualmente no hay elementos suficientes en la legislación aplicable ni en criterios judiciales para concluir que la protección es extensiva a personas jurídicas.

Tema	Concepto	Sí / 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	Sí, el consentimiento es requerido y deberá ser conforme se establece en los arts. 2, inc. iv), 5, 7, 8 y 11 de la LFPDPPP y los arts. 9, 11-21 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: 1. Una disposición jurídica así lo disponga; 2. Los datos personales figuren en fuentes de acceso público. 3. Los datos personales se sometan a un proceso de disociación. 4. Se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable. 5. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes. 6. Sean indispensables para efectuar un tratamiento de atención médica, la prevención, el diagnóstico, la prestación de asistencia sanitaria, los 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. 7. Exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente. El titular de los datos personales podrá revocar en cualquier momento el consentimiento para el tratamiento de sus datos personales, para lo que el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello. Arts. 2, inciso iv), 5, 7, y 8 LFPDPPP. Arts. 9, 11-21, 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. 9 y 36 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 se 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	Sí / 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 con la transferencia internacional de datos? (Por ejemplo, cláusulas modelos, autorización por parte de la autoridad de control, entre otros)	Sí	Toda transferencia de datos personales, sea esta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones mencionadas en el art. 36 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. 67-70, 74-76 del Reglamento de la LFPDPPP. Arts. 35 y 36, LFPDPPP; Arts. 67-71, 73-76, 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, 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 SABG. Asimismo, el SABG 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. 37 de la LFPDPPP y Arts. 70 y 79-86 del Reglamento de la LFPDPPP.

Tema	Concepto	Sí / 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 afecta la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. 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. ▸ 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. 8, 12, 15 y 59 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 (Por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el 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. ▸ **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, incisos. 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 implementar controles o mecanismos que tengan por objeto que todas las personas que intervengan en el tratamiento de los datos guarden la confidencialidad de estos. Las medidas de seguridad se deberán implementar a partir de un análisis de riesgos sobre los datos personales que traten, tomando en cuenta la sensibilidad de los datos personales, su valor cuantitativo o cualitativo, así como el desarrollo tecnológico, 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 efectúe 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. Arts. 18 y 20, LFPDPPP; Arts. 2 incisos. v), vi) y vii), 48 inc. ix), 57, 59-62, Reglamento de la LFPDPPP.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Por 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. 2, inc. iii), 21-24, 30 y 32, 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. 21-25, 27, 28, 30-32 y 34 de la LFPDPPP. Los arts. 87-90, 92-98 y 101-106 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, 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 estos, 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. 5, 13, 24 y 35 LFPDPPP, Arts. 49, 50 y 51, Reglamento LFPDPPP.
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 aquellos 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. 10, LFPDPPP; y arts. 37-39 del Reglamento de la LFPDPPP.

Tema	Concepto	Sí / 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	Una vez que los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones legales aplicables, deberán ser suprimidos previo bloqueo, en su caso, y una vez que concluya el plazo de conservación de los mismos. Además, el titular tendrá en todo momento el derecho a cancelar sus datos personales, en cuyo caso se dará aviso al titular de la cancelación efectiva de los mismos. Ver apartado anterior. Art. 10 y 24 LFPDPPP; y arts. 37-39 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, 59-61, inc. iii) y 80 inc. viii), Reglamento de la LFPDPPP Art. 10 PAPDP.
Incidentes	¿Hay obligación de reportar un incidente de seguridad o 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. 19 LFPDPPP, arts. 58,63-66 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 específicas ante el incumplimiento de la obligación de reportar un incumplimiento. No obstante, el art. 58 del Reglamento de LFPDPPP, dispone que la autoridad podrá tomar en consideración el cumplimiento de sus recomendaciones para determinar una potencial atenuación de la sanción que corresponda. En los arts. 63-65 del Reglamento LFPDPPP se establecen otras disposiciones relevantes respecto a las vulneraciones de seguridad. En esta línea, la LFPDPPP en sus arts. 59, 61-64 detalla el tipo de sanciones que recaerán cuando se comentan incumplimientos en materia de datos personales.
Acciones legales	¿Existe alguna acción legal de protección de datos personales?, ¿quién tiene derecho para ejercerla/solicitarla?	No	No existe una acción legal específica que proteja tal derecho. Sin embargo, los titulares pueden ejercer en todo momento los denominados "Derechos ARCO", asimismo, la ley prevé un procedimiento de protección de datos personales que debe llevarse a cabo ante la SABG. Capítulo VIII de la LFPDPPP y Capítulo VIII del Reglamento de la LFPDPPP.
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 29 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.
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	La SABG 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 la SABG 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. A través del procedimiento, la SABG tendrá acceso a la información y documentación que considere necesarias, de acuerdo con la resolución que lo motive. Los servidores públicos estarán obligados a guardar confidencialidad sobre la información que conozcan derivada de la verificación correspondiente. Arts. 54, 55 y 56 de la LFPDPPP; Arts. 128 y 129, Reglamento de la LFPDPPP.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?		A fin de garantizar el debido tratamiento de los datos personales, el responsable deberá adoptar ciertas medidas -privilegiando los intereses del titular y la expectativa razonable de privacidad-. Entre las medidas que podrá adoptar el responsable se encuentra la implementación de procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento. En este sentido, es importante recalcar que, a fin de establecer y mantener la seguridad de los datos personales, el responsable deberá, entre otras cosas, contar con un inventario de datos personales y de los sistemas de tratamiento/repositorios (físicos y electrónicos). Art. 48 del Reglamento de la LFPDPPP.
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (Por ejemplo, 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 (Artículo 30 del Reglamento de la LFPDPPP y Artículos 24, 36 y 40 de los LAV). ▸ Requisitos especiales en materia de publicidad y marketing (Artículo 30 del Reglamento de la LFPDPPP), y en relación con el uso de cookies (Artículo 14 del Reglamento de la LFPDPPP y Artículos 3 y 31 de los LAV).

PANAMÁ

Tema	Concepto	Sí / 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 Nº81 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 Transparencia y Acceso a la Información (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 las normas de protección de datos personales iguales o superiores a los exigidos por la Ley de la República de Panamá.
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	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. Para que el consentimiento se considere informado implica que el responsable del tratamiento informe al titular de los datos personales sobre la identidad y datos de contacto del responsable del tratamiento, las finalidades del tratamiento, la condición que legitima el tratamiento, los destinatarios o categorías de destinatarios de los datos personales, la intención del responsable del tratamiento de transferir datos personales a un tercer país, el plazo de conservación de los datos personales, información sobre los derechos de acceso, rectificación, cancelación, oposición y portabilidad y mecanismos o procedimientos para su ejercicio, la existencia de decisiones automatizadas, incluida la elaboración de perfiles y los datos de contacto del oficial de protección de datos. (art. 14 Decreto Ejecutivo 285). Cuando el tratamiento está basado en el consentimiento, se le debe informar al titular de los datos personales, sobre el derecho a revocarlo. (art. 19 Decreto Ejecutivo 285). Para cumplir con el consentimiento inequívoco, es necesario que el titular de los datos quede informado sobre las finalidades del tratamiento, en concordancia con el principio de finalidad. 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.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
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 las 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. El régimen de protección de datos personales de Panamá, a manera de categorías taxativas, únicamente se refiere a dato personal y dato sensible, no obstante, la práctica comúnmente observada, es la segmentación de las categorías según la naturaleza de los datos personales que se recaban, por ejemplo: datos de identificación, datos financieros, datos de contacto, datos demográficos, datos de empleo, datos de salud, datos de ubicación, datos de redes sociales, entre otros.
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. Asimismo, 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. La información previa a la recolección del consentimiento es la que establece el art. 14 del Decreto Ejecutivo 285. Si el consentimiento se recolecta a través de medios digitales, la obligación de información previa se cumple mediante la presentación al interesado de las políticas de privacidad. Si el consentimiento del titular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás, de forma comprensible y de fácil acceso, utilizando un lenguaje claro y sencill0 (art. 27 Ley 81 de 2019), Cuando la información sobre las políticas de privacidad se facilita a través de internet o dispositivos de pantalla reducida, es permitido que se facilite la información mediante un sistema de información dividido en capas (art. 16 del Decreto Ejecutivo 285)

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
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, los tratados o convenios internacionales que regulen estas materias. 4. Cuando se refiera al 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 tratamiento. ▸ 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.

Tema	Concepto	Sí / 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 con la transferencia internacional de datos? (Por 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. Además de lo anterior, las excepciones a lo anteriormente indicado son: 1. Cuando el titular haya otorgado su consentimiento para la transferencia. 2. Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar por el interesado o en interés de este. 3. Cuando se trate de transferencias bancarias, dinerarias y bursátiles del mercado de valores. 4. Cuando se trate de información cuya transmisión sea requerida por ello en cumplimiento de tratados internacionales ratificados por la República de Panamá. Igualmente, el tratamiento o transferencia de datos personales que ser realice a través de internet o cualquier otro medio de comunicación electrónica, digital o física, el custodio de la base de datos y el responsable del tratamiento deben cumplir con los estándares, normas, certificaciones, protocolos, medidas técnicas y de gestión informática adecuados para preservar la seguridad en sus sistemas o redes, o en la prestación de sus servicios, con el fin de garantizar los niveles de protección de los datos personales tal cual lo establece la Ley y su reglamentación. (art. 5 Ley 81 de 2019). Como parte de las restricciones, el artículo 13 de la Ley 81 de 2019 establece que los datos sensibles no pueden ser objeto de transferencias, a excepción de ciertos casos, tales como cuando el titular haya dado su autorización explícita, salvo casos que por ley no sea requerido el otorgamiento de dicha autorización. (entre otros supuestos). Siguiendo con los requisitos, el artículo 32 de la Ley 81 de 2019, establece que la transferencia de datos personales, mediante el uso de una red digital o de cualquier otro medio, deberá dejarse constancia de: 1. La individualización del requirente. 2. El motivo y el propósito del requerimiento. 3. Los datos que se requiere que sean trasferidos. 4. La notificación a los titulares de los datos personales que integran el requerimiento, el motivo y el nuevo responsable de la información, salvo consentimiento previo por parte del titular. 5. El tiempo máximo que el requirente utilizará los datos y la forma como serán destruidos una vez terminado su uso. Se exceptúan de estos requerimientos los procesos internos del responsable del tratamiento de los datos. El artículo 33 de la Ley 81 de 2019 establece las condiciones para que una transferencia de datos personales se tenga como lícita, entre las cuales tenemos que se cuente con el consentimiento del titular de los datos. Dentro del concepto de transferencia de datos (numeral 19 del artículo 4 de la Ley 81 de 2019, se incluyen las transferencias extrafronterizas. La sección cuarta de la reglamentación de la Ley, artículo 51 del Decreto Ejecutivo 285 de 2021, establece las condiciones para la transferencia extrafronteriza de datos, indicando que los datos objeto de tratamiento podrán ser transferidos a otro país siempre que se reúna alguna de las condiciones previstas, entre las cuales podemos resaltar países u organizaciones internacionales que brindan un grado de protección de datos personales equivalente o superior al previsto en la Ley 81 de 2019 y su reglamentación, el consentimiento expreso del titular de los datos, entre otras. También cabe añadir, las garantías adecuadas para la transferencia de datos personales extrafronterizas (art. 53 del Decreto Ejecutivo 285 de 2021), entre las cuales tenemos: 1. Las cláusulas contractuales suscritas entre el exportador y el destinatario que ofrezcan garantías suficientes y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares. 2. Los modelos de cláusulas contractuales que valide la autoridad de control para ser utilizadas por exportador y destinatario como garantía de la transferencia. 3. Los mecanismos de autorregulación vinculante convenidos entre el exportador y el destinatario y aprobado por la autoridad de control o reconocida por esta, siempre y cuando estos sean acordes con las disposiciones previstas en la Ley 81 de 2019 y el presente decreto. La autoridad de control podrá promulgar el listado de mecanismos de autorregulación vinculantes que se reconocen a estos efectos. 4. Si el exportador y el destinatario pertenecen al mismo grupo económico y los tratamientos queden sujetos a unas normas corporativas que les vinculen. Entre las atribuciones y facultades de fiscalización y supervisión a cargo de la Dirección de Protección de Datos Personales, se establece la realización de evaluaciones, informes y análisis de procedimientos en los que se realicen tratamientos de datos personales a todos los responsables o custodios del tratamiento de los datos para lo cual podrá solicitarles, a través del oficial de protección de datos personales, información, documentación y certificaciones de sus bases de datos, las cuales no podrán ser negadas; adoptar modelos de cláusulas contractuales que, conforme al artículo 33 de la Ley 81 de 2019, constituyan una condición de licitud de las transferencias de datos, intra y extrafronterizas. (art. 58 del Decreto Ejecutivo 285 de 2021) Es importante tener presente el contenido del art. 33 de la Ley 81 de 2019, el cual establece que debe cumplirse al menos una de las condiciones indicadas para que la transferencia de datos personales se considere lícita y el numeral 13 dispone que se realice en el marco de cláusulas contractuales que contengan mecanismos de protección de los datos personales acordes con las disposiciones previstas en la presente Ley, siempre que el titular sea parte.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	Sí	El art. 33 del Decreto Ejecutivo 285 de 2021, establece en una de sus partes que los responsables del tratamiento y los custodios de la base de datos podrán adoptar entre otras, mecanismos de autorregulación vinculantes en materia de protección de datos personales. El art. 36 del Decreto Ejecutivo 285 de 2021 que se refiere a la seguridad de los datos personales, establece que los mecanismos de autorregulación vinculantes se tomarán como referencia para establecer las medidas técnicas y organizativas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas, servicios y tratamiento de los datos personales. El artículo 40 del Decreto Ejecutivo 285 de 2021 establece el contenido del mecanismo de autorregulación vinculante, el cual debe someterse a la aprobación de la autoridad de control y una vez aprobado será publicado en Gaceta Oficial. El artículo 47 del Decreto Ejecutivo 285 de 2021, se refiere al contrato de custodio de la base de datos, y dispone entre otros aspectos que el contar con un mecanismo de autorregulación vinculante, forma parte de las garantías suficientes para aplicar medidas técnicas y organizativas apropiadas. El art. 53 del Decreto Ejecutivo 285 de 2021, con respecto a las garantías adecuadas para la transferencia de datos extrafronterizo, incluye los mecanismos de autorregulación vinculante convenidos entre el exportador y el destinatario y aprobado por la autoridad de control o reconocida por esta.
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. El artículo 5 de la Ley 81 de 2019 establece que el almacenamiento o transferencia de datos personales originados o almacenados dentro de la República de Panamá que sean confidenciales, sensibles o restringidos, que reciban un tratamiento transfronterizo, será permitido 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 esta Ley, o pueda demostrar que cumple con los estándares y normas de protección de datos personales iguales o superiores a los exigidos por esta Ley 81. El artículo 13 de la Ley 81 de 2019 dispone que los datos sensibles no pueden ser objeto de transferencia, excepto en los casos siguientes: 1. Cuando el titular haya dado su autorización explícita, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización. 2. Cuando sea necesario para salvaguardar la vida del titular y este se encuentre física o jurídicamente incapacitado. En estos casos, los acudientes, curadores o quienes tengan la tutela deben dar la autorización. 3. Cuando se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso con autorización judicial competente. 4. Cuando tenga una finalidad histórica, estadística o científica. En este caso, deberán adoptarse las medidas conducentes a disociar la identidad de los titulares. El no observar las regulaciones establecidas respecto al tratamiento de los datos sensibles se considera una infracción grave (art. 41 Ley 81 de 2019) Con respecto a las medidas técnicas y organizativas relacionadas con la seguridad de los datos personales, el artículo 36 del Decreto Ejecutivo 285 de 2021, establece que, para la determinación de las medidas, entre los factores a tomar en cuenta está la naturaleza de los datos personales tratados, en especial, si se trata de datos personales sensibles.
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (Por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el uso de la misma?, ¿existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	No	Solo a solicitud de la autoridad o en caso de violación o incidente de seguridad de datos.

Tema	Concepto	Sí / 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	Se tomará como referencia las normas o los 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. Medidas técnicas taxativas tanto la Ley como la reglamentación no las establece, pero en varias de sus partes se refieren a la obligación. El artículo 5 de la Ley 81 de 2919 en una de sus partes establece que el tratamiento o transferencia de datos personales que se realice a través de Internet o cualquier otro medio de comunicación electrónica, digital o física, el custodio de la base de datos y/o el responsable por el tratamiento deberá cumplir con los estándares, normas, certificaciones, protocolos, medidas técnicas y de gestión informática adecuados para preservar la seguridad en sus sistemas o redes, o en la prestación de sus servicios, con el fin de garantizar los niveles de protección de los datos personales. Particularmente, el artículo 36 del Decreto Ejecutivo 285 de 2021, se refiere a la seguridad de los datos personales, dispone que las medidas técnicas y organizativas deben ser suficientes para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios y tratamiento de los datos personales. Para ello 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. Para determinar estas medidas, se considerarán los siguientes factores: 1. El riesgo para los derechos y libertades de los titulares, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión. 2. El estado de la tecnología. 3. Los costos para la aplicación de las medidas. 4. La naturaleza de los datos personales tratados, en especial, si se trata de datos personales sensibles. 5. El alcance, contexto y las finalidades del tratamiento. 6. Las transferencias internacionales de datos personales que se realicen o pretendan realizar. 7. El número de los titulares afectados. 8. Las posibles consecuencias que se derivarían de una violación de seguridad de los datos para los titulares. 9. Las violaciones de seguridad de los datos previas, ocurridas en el tratamiento de datos personales. Igualmente, al establecerse los mecanismos de autorregulación vinculante, también se debe establecer las medidas técnicas y organizativas dirigidas a garantizar la seguridad en el tratamiento y transferencia de los datos. (art. 40 Decreto Ejecutivo 285 de 2021) Por su parte, el art. 47 Decreto Ejecutivo 285 de 2021, el cual se refiere al contrato de custodio de la base de datos, establece que el responsable del tratamiento elegirá únicamente un custodio de la base de datos que ofrezca suficientes garantías para aplicar medidas técnicas y organizativas que garanticen la protección de los datos personales.
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Por ejemplo, rectificación, actualización o supresión) Identificar y explicar.	Sí	▸ Acceso. ▸ Rectificación. ▸ Cancelación. ▸ Oposición. ▸ Portabilidad.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
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. El capítulo II del Decreto Ejecutivo 285 de 2021, se refiere a los derechos de los titulares de los datos personales. El artículo 21 en una de sus partes dispone que el responsable del tratamiento debe establecer protocolos sencillos, accesibles y gratuitos que permitan al titular de los datos ejercer sus derechos y al responsable del tratamiento dar respuesta en tiempo y forma además de informar al titular de los datos sobre los medios a su disposición para ejercer los derechos que le correspondan. La implementación comúnmente observada es que, en cumplimiento del principio de transparencia, los mecanismos o protocolos para ejercerlos se informan a través de la política de privacidad, cláusulas contractuales y como parte del consentimiento informado a través de los medios físicos o electrónicos dispuestos para recabar la autorización para el tratamiento de datos personales.
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	Sí	Solo con el consentimiento otorgado.

Tema	Concepto	Sí / 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 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). Según la Ley 81 de 2019, una transferencia de datos consiste en dar a conocer, divulgar, comunicar, intercambiar y/o transmitir, de cualquier forma y por cualquier medio, de un punto a otro, intra o extrafronterizo, los datos a personas naturales o jurídicas distintas del titular, ya sean determinadas o indeterminadas. La transferencia de datos para la prestación de servicios por cuenta de terceros es permitida siempre que se cuente con el consentimiento del titular de los datos para la transferencia, o sea necesaria para la celebración o ejecución de un contrato celebrado por el interesado o en interés de este. Tanto el custodio de la base de datos y/o el responsable del tratamiento deberán cumplir con los estándares, normas, certificaciones, protocolos, medidas técnicas y de gestión informática adecuados para preservar la seguridad en sus sistemas o redes, o en la prestación de sus servicios, con el fin de garantizar los niveles de protección de los datos personales que establece la Ley y su reglamentación. (art. 5 Ley 81 de 2019) Los datos sensibles no pueden ser objeto de transferencia, salvo que el titular haya dado su autorización explícita (art. 13 Ley 81 de 2019) También se debe tomar en consideración el art. 32 de la Ley 81 de 2019 el cual indica que en una transferencia de datos personales a través de una red digital o de cualquier otro medio, se debe dejar constancia de: 1. La individualización del requirente. 2. El motivo y el propósito del requerimiento. 3. Los datos que se requiere que sean trasferidos. 4. La notificación a los titulares de los datos personales que integran el requerimiento, el motivo y el nuevo responsable de la información, salvo consentimiento previo por parte del titular. 5. El tiempo máximo que el requirente utilizará los datos y la forma como serán destruidos una vez terminado su uso. Se exceptúan de estos requerimientos los procesos internos del responsable del tratamiento de los datos. El artículo 35 del Decreto Ejecutivo 285 de 2021, se refiere al registro de las bases de datos y sobre el particular indica que el registro de las bases de datos transferidas a terceros deberá constar por escrito, por cualquier medio, inclusive por medios electrónicos, dejándose constancia de lo siguiente: 1. La identificación de la base de datos. 2. La identificación del responsable de la base de datos. 3. La naturaleza de los datos personales que contiene, esto es, la descripción del universo de personas que comprende la base de datos. 4. Las condiciones de legitimación aplicables. 5. La finalidad o finalidades del tratamiento. 6. Los procedimientos de obtención y tratamiento de los datos. 7. El plazo de conservación de los datos. 8. El destino de los datos y las personas naturales o jurídicas a las que pueden ser transferidos. 9. Las medidas técnicas y organizativas de seguridad adoptadas, al menos un resumen de ellas o la referencia a la política o protocolo donde se describen. 10. Los protocolos aplicables a la base de datos, tales como los referentes a la atención y respuesta del ejercicio de los derechos por los titulares de los datos. 11. La descripción técnica de la base de datos. 12. La identificación y periodo de todas las personas que han ingresado a los datos personales dentro de los quince días hábiles desde que se inicie la actividad. Sobre el particular podemos añadir que si el propósito de la transferencia al tercero es *data processing*, este es el tratamiento de datos personales que se debe precisar en lo que concierne a la finalidad o finalidades del tratamiento.

Tema	Concepto	Sí / 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	Siete años, salvo la autoridad competente por casos especiales solicite sean conservados por más tiempo. Se debe precisar. El artículo 28 de la Ley 81 de 2019 establece que 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. En atención al principio de finalidad (art. 7 del Decreto Ejecutivo 285 de 2021), en una de sus partes indica que los fines del tratamiento de los datos determinarán el plazo de conservación de estos, transcurrido el cual el responsable del tratamiento los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización. Para determinar el plazo de conservación de los datos se acudirá a las leyes aplicables en cada caso y a las responsabilidades de todo orden que deban ser atendidas por el responsable del tratamiento o custodio de la base de datos.
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. El régimen de protección de datos para Panamá contiene disposiciones aplicables a la eliminación o supresión de datos personales. En principio, eliminación o cancelación de datos personales consiste en suprimir o borrar de forma permanente los datos almacenados en bases de datos, cualquiera que sea el procedimiento empleado para ello. El artículo 8 de la Ley 81 de 2019 que se refiere a los tratamientos de datos personales que no requieren consentimiento, al final establece que el titular de los datos podrá ejercer el derecho de acceso a sus datos personales sin cargo alguno. El titular podrá, en cualquier momento, solicitar la modificación, eliminación o bloqueo de sus datos personales de las bases de datos a los que se refiere este artículo. Lo anterior se entiende, sin perjuicio de lo que dispongan leyes especiales. También con respecto a los derechos de los titulares de los datos personales, el artículo 15 de la Ley 81 de 2019, establece que, con respecto al ejercicio del derecho de cancelación, este le permite al titular solicitar la eliminación de sus datos personales incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes. Igualmente, el art. 16 de la Ley 81 de 2019 establece que, sin perjuicio de las excepciones legales, el titular tendrá, además, derecho a exigir que se eliminen sus datos personales cuando su almacenamiento carezca de fundamento legal, cuando no hayan sido expresamente autorizados o cuando estuvieran caducos. El suministro de información, la modificación, bloqueo o la eliminación de los datos personales será absolutamente gratuito y deberá proporcionarse, a solicitud del titular de los datos o quien lo represente, constancia de la base de datos actualizada en lo concerniente. Por su parte el art. 17 de la Ley 81 de 2019, dispone que los datos deberán ser modificados cuando sean erróneos, inexactos, equívocos o incompletos dentro de un término de cinco días hábiles siguientes a la solicitud de modificación, quien sea responsable de una base de datos regulada por esta Ley, podrá proceder a la eliminación, modificación o bloqueo de los datos personales sin necesidad de requerimientos del titular, cuando existan pruebas de inexactitud de dichos datos. Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación. En este caso, serán bloqueados para acceso a terceros o para evitar su uso en otros fines que no hayan sido los expresamente autorizados. En todo caso, corresponderá a la Autoridad Nacional de Transparencia y Acceso a la Información, como autoridad competente, determinar cuándo un dato es inexacto o cuándo carece de fundamento legal, sin perjuicio de lo dispuesto en leyes especiales que regulen materias específicas. El art. 48 del del Decreto Ejecutivo 285, con respecto al contenido del contrato de custodio de la base de datos, establece entre sus estipulaciones que se debe pacta la eliminación, devolución o comunicación, al responsable del tratamiento o a un nuevo custodio de la base de datos designado por el responsable del tratamiento, los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable del tratamiento, excepto que una ley exija la conservación de los datos personales. En este caso, los datos serán devueltos al responsable del tratamiento que garantizará su conservación por el tiempo establecido en la Ley 81 de 2019 o en otras leyes especiales.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Privacy Impact Assessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto *(Privacy Impact Assessment)*?	Sí	La evaluación de impacto en protección de datos está definida como la documentación del responsable del tratamiento que contiene la descripción de los procesos con datos personales que pueden generar riesgos para los derechos y deberes individuales y sociales, así como medidas, salvaguardas y mecanismos de riesgos. Atendiendo a la gravedad del riesgo que presente el tratamiento para los datos personales, así como a la novedad de la tecnología utilizada, la Autoridad de Control, podrá ordenar que se presente un informe de evaluación de impacto en protección de datos. El informe debe contener, como mínimo, una descripción de los tipos de datos recopilados, la metodología utilizada para la recopilación y garantía de seguridad de la información, y el análisis del responsable en relación con medidas, salvaguardas y mecanismos de mitigación de riesgos adoptados. La autoridad de control podrá solicitar a las entidades que publiquen los informes de evaluación de impacto en protección de datos que lleven a cabo y sugerirles la adopción de normas y buenas prácticas para el tratamiento de datos personales. La reglamentación de la Ley 81 de 2019 cuando se refiere a las evaluaciones de impacto, lo hace como una actividad no vinculante para el responsable del tratamiento o para el custodio de la base de datos, o bien, a requerimiento de la autoridad de control. La reglamentación al referirse al principio de proporcionalidad, indica que para conocer qué datos son adecuados, pertinentes y mínimos necesarios para la finalidad perseguida con el tratamiento de los datos, los responsables del tratamiento y, en su caso, los custodios de la base de datos tomarán en cuenta el estado de la tecnología, la naturaleza, ámbito, contexto y fines de tratamiento. Con este fin podrán realizar y documentar evaluaciones de impacto en protección de datos personales con el objeto de minimizar los datos objeto de tratamiento, conocer los riesgos que impliquen los tratamientos y adoptar las medidas y garantías necesarias para mitigarlos. La autoridad de control podrá definir aquellos supuestos en los que es recomendable realizar una evaluación de impacto y establecer las pautas o estándares a seguir en su desarrollo.
Incidentes	¿Hay obligación de reportar un incidente de seguridad o algún incumplimiento a las previsiones legales?	Sí	Ante la autoridad correspondiente, en este caso, ANTAI. La notificación de un incidente de seguridad se realiza a la autoridad de control y a los titulares afectados.

Tema	Concepto	Sí / 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) hasta diez mil balboas (B/.10.000), 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 las garantías establecidas 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**: a. Clausura de los registros de la base de datos, sin perjuicio de la multa correspondiente. Para ejecutar esta acción, la Autoridad Nacional de Transparencia y Acceso a la Información deberá contar con la opinión formal del Consejo de Protección de Datos Personales, sin perjuicio de los recursos que esta Ley le concede al afectado. b. Suspensión e inhabilitación de la actividad de almacenamiento y/o tratamiento de datos personales de forma temporal o permanente, sin perjuicio de la multa correspondiente.
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.

Tema	Concepto	Sí / 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	El artículo 42 del Decreto Ejecutivo 285 de 2021, establece que las entidades privadas, podrán designar un oficial de protección de datos, que podrá ser personal laboral o profesional con contrato de servicios, suscrito con el responsable del tratamiento o el custodio de la base de datos. La designación de un Oficial de Protección de Datos Personales para el sector privado no es obligatoria, no obstante, si fuera el caso, la autoridad de control la tomará en cuenta como criterio para la graduación de las sanciones.
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	Dentro de las facultades legales otorgadas a la Dirección General de Protección de Datos, está la de fiscalizar y supervisar la debida aplicación de ley por parte de los responsables del tratamiento y custodios de las bases de datos.
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?	Sí	Los responsables y/o custodios de bases de datos que transfieran datos personales almacenados en bases de datos a terceros llevarán un registro de estas y deberán estar a disposición de la Autoridad Nacional de Transparencia y Acceso a la Información en caso de que esta lo requiera para cumplir con las facultades que le otorga esta Ley. En el registro al que se refiere el párrafo anterior constará, respecto de cada una de esas bases de datos, la identificación de estas y el responsable de estas, la naturaleza de los datos personales que contienen, el fundamento jurídico de su existencia, los procedimientos de obtención y el tratamiento de los datos, el destino de los datos y las personas naturales o jurídicas a las que pueden ser transferidos, la descripción del universo de personas que comprende, las medidas de seguridad, los protocolos y la descripción técnica de la base de datos, la forma y las condiciones en que las personas pueden recibir o acceder a los datos referidos a ellas, los procedimientos a realizar para la rectificación, la actualización de los datos, el tiempo de conservación de los datos y cualquier cambio de los elementos indicados, así como la identificación y el periodo de todas las personas que han ingresado a los datos personales dentro de los 15 días hábiles desde que se inicie dicha actividad. El artículo 35 del Decreto Ejecutivo 285 de 2021, establece el contenido del registro Respecto de cada base de datos se dejará constancia en dicho registro de: 1. La identificación de la base de datos. 2. La identificación del responsable de la base de datos. 3. La naturaleza de los datos personales que contiene, esto es, la descripción del universo de personas que comprende la base de datos. 4. Las condiciones de legitimación aplicables 5. La finalidad o finalidades del tratamiento. 6. Los procedimientos de obtención y tratamiento de los datos. 7. El plazo de conservación de los datos. 8. El destino de los datos y las personas naturales o jurídicas a las que pueden ser transferidos. 9. Las medidas técnicas y organizativas de seguridad adoptadas, al menos un resumen de ellas o la referencia a la política o protocolo donde se describen. 10. Los protocolos aplicables a la base de datos, tales como los referentes a la atención y respuesta del ejercicio de los derechos por los titulares de los datos. 11. La descripción técnica de la base de datos. 12. La identificación y periodo de todas las personas que han ingresado a los datos personales dentro de los quince días hábiles desde que se inicie la actividad. Los responsables del tratamiento y/o los custodios de la base de datos mantendrán el registro actualizado, de forma que responda con veracidad a la realidad de los tratamientos que se lleven a cabo. Estará a disposición de la autoridad de control cuando esta lo requiera.
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (Por ejemplo, GDPR)?, ¿qué diferencias relevantes encuentra?	Sí	En efecto, la normativa panameña contempla mayormente los preceptos de GDPR, reconociendo los derechos ARCO.
Otras obligaciones	¿Existen otras consideraciones/requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	No	Aun cuando la figura de oficial de cumplimiento no es obligatoria, su designación será tomada en cuenta como criterio para la graduación de las sanciones.

PARAGUAY

Tema	Concepto	Sí / 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 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. 135 "Habeas data", Art. 28 "Derecho a Informarse", 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"). ▸ Ley Nº 4.868/2.013 de "Comercio Electrónico" y sus disposiciones complementarias. ▸ Ley Nº 6.822/2.021 "De los Servicios de Confianza para las Transacciones Electrónicas, del Documento Electrónico y los Documentos Transmisibles Electrónicos" y sus disposiciones complementarias. ▸ Ley Nº 861/1.996 "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". ▸ Código Penal del Paraguay Nº 1.160/1.997 y sus disposiciones complementarias. ▸ Resolución Nº 3/2.023 del Banco Central del Paraguay "Reglamento de Burós de Información Crediticia (BIC) y Protección de la Información Personal Crediticia en el marco de la Ley Nº 6.534/2.020 de Protección de Datos Personales Crediticios". Esta Resolución, establece los lineamientos y obligaciones aplicables a los BIC y a los Usuarios de Información Crediticia, además de mecanismos para el ejercicio efectivo de los derechos de los titulares de datos. ▸ Resolución SDCU Nº 1.502/2.022 "Por la cual se reglamentan los Artículos 6º, 9º y 20º de la Ley Nº 6.534/2.020 de Protección de Datos Personales Crediticios". De acuerdo con su Art. 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, el funcionamiento, los derechos, las obligaciones y la 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 al tratamiento de los datos personales crediticios y la información crediticia de toda persona por parte de los burós de información crediticia y de los usuarios de información crediticia. No obstante, también contempla la definición de datos personales y datos personales sensibles con las particularidades a tener en cuenta para su tratamiento. Las disposiciones contenidas en la Constitución de la República y la normativa mencionada previamente, forman parte de las fuentes complementarias vinculadas a la protección de datos personales en el país. Vale recalcar que, según la Constitución en su Art. 45, 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.
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 a la Secretaría de Defensa del Usuario y Consumidor (SEDECO) dependiente del Ministerio de Industria y Comercio (MIC): **http://www.sedeco.gov.py/** como los órganos de control y autoridades de aplicación de sus disposiciones. Por su parte y a modo complementario, en el marco de la Ley Nº 4.868/13, la Ley Nº 5.830/17 y la Ley Nº 6.822/21, se designa al MIC, a través de sus dependencias, como autoridad de aplicación.
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.

Tema	Concepto	Sí / 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	La Ley N° 6.534/20 garantiza a toda persona el derecho de ser informado en forma expresa y clara sobre la finalidad que se le darán a sus datos requeridos y así poder manifestar expresamente su consentimiento para la obtención y el 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. 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 la información y de los datos sobre sí misma que obren en registros oficiales o privados de carácter público o en entidades que suministren información sobre solvencia económica y situación patrimonial, conocer 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 N° 6.534/20 define 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 las garantías de protección de datos personales serán extendidos a personas jurídicas en cuanto le sean aplicables.
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	En el marco de la Ley N° 6.534/20, se establecen las siguientes categorías de datos: ▸ **Datos personales**. Información de cualquier tipo, referida a personas jurídicas o personas físicas determinadas o determinables. Se entenderá 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 las garantías de protección de datos personales serán extendidos a personas jurídicas en cuanto le sean aplicables. ▸ **Datos personales 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, las creencias o convicciones religiosas, filosóficas y morales, la afiliación sindical, las opiniones políticas, los 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. ▸ **Datos personales crediticios o 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	En el marco de la Ley N° 6.534/20, esta alcanza a los datos relativos a personas de existencia ideal o jurídicas, determinadas o determinables.

Tema	Concepto	Sí / 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	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. 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. Con relación al consentimiento informado otorgado por el consumidor final a un proveedor, la SDCU Nº 1.502/22 que reglamenta los artículos 6º, 9º y 20º de la Ley Nº 6.534/20 de Protección de Datos Personales Crediticios, establece que el consentimiento informado solo habilita al proveedor que lo obtuvo de manera directa. Siendo así, los demás proveedores deberán obtener una nueva autorización o consentimiento informado del consumidor final. En este sentido, la Resolución indica que no puede considerarse que el consentimiento otorgado por parte de un consumidor final a un proveedor lleva implícita, la autorización a terceros proveedores que no fueron parte de la primera autorización o consentimiento informado. Por otro lado y a modo enunciativo, la Ley 4.868/13 de Comercio Electrónico y sus normas reglamentarias, disponen que el Proveedor de Bienes y Servicios deberá requerir el consentimiento expreso del consumidor o usuario para obtener sus datos personales, disponer de un procedimiento sencillo y gratuito para oponerse a la utilización de datos con fines promocionales, contar con mecanismos de confirmación expresa, poner a conocimiento la finalidad y el tratamiento que se le darán a los datos personales del consumidor o usuario, entre otros. Por su parte, la Ley Nº 6.822/21 dispone que los prestadores de servicios de confianza solo pueden recolectar los datos personales directamente de la persona a quien esos datos se refieran. Estas, deben dar su consentimiento expreso e informado para tales efectos. La recolección y el procesamiento de los datos personales se realizarán solo en la medida en que los mismos sean necesarios para la prestación del servicio de confianza. Los datos personales no pueden ser procesados para otro fin distinto al acordado, sin el consentimiento expreso del titular de los datos.
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.
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales?, ¿hay requisitos aplicables en relación con la transferencia internacional de datos? (Poe 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 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 contempla, en la normativa vigente, referencias en cuanto 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. Como buena práctica, podría ser interesante considerar en este aspecto, las orientaciones de la Red Iberoamericana de Protección de Datos (RIPD), específicamente, la Guía de implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales, siendo Paraguay miembro de la Red.
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	No	No.

Tema	Concepto	Sí / 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	De conformidad a la Ley Nº 6.534/20, se entiende por datos personales sensibles a aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para este. Son aquellos que revelan aspectos como: ▸ 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 (Por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el 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 como figura única o centralizada en el marco del tratamiento de los datos personales en general. La Ley 6534/20 no establece expresamente la obligación de presentar informes periódicos ante el BCP o SEDECO, pero ▸sí existe obligación de registro/autorización para burós ante el BCP y la obligación de suministro de información entre usuarios y burós.
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 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. Asimismo, existe una obligación expresa para los Burós de Información Crediticia de manejar la información con altos estándares de ética, confidencialidad y seguridad. La recolección, el almacenamiento y la 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 en la Ley Nº 6.534/20.
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Por 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 normativa complementaria como la ley de comercio electrónico, así como la figura del habeas data o el Derecho a Informarse contemplados en la Constitución, entre otros.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	De conformidad con la Ley Nº 6.534/20, el titular de los datos o su representante legal podrá solicitar en cualquier momento al responsable el acceso, la actualización, la rectificación, la supresión, la oposición y portabilidad de los datos personales que le conciernen. El responsable debe establecer medios y procedimientos sencillos, rápidos, accesibles y gratuitos para que el titular pueda ejercer sus derechos. Para ello, podrá interponer solicitudes o reclamos, y en caso de no ser atendidos en los términos de ley y el reglamento, recurrir ante la Oficina de Atención al Consumidor Financiero de la Superintendencia de Bancos o ante la SEDECO (según corresponda), y finalmente, acudir a la acción de tutela ante el magistrado competente. La garantía constitucional del habeas data, 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). 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. 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	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?	Sí	La Ley Nº 6.534/20, regula el derecho al olvido de los datos crediticios. Los datos sobre una persona o empresa que obre en un registro y que pudieran afectar al titular pueden ser conservados hasta por 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. Por su parte, la Resolución 3/23 del BCP, dispone que los datos personales crediticios que se consideran información positiva deberán conservarse y publicarse mínimamente por 10 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 eliminados cuando hubiesen caducado conforme con los artículos, 9 y 19 de la Ley Nº 6.534/20 de protección de datos personales crediticios y de acuerdo con la Resolución 3/23 que regula la ley en cuestión referente al derecho al olvido. Asimismo, cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. El hecho de negarse injustificadamente a eliminar o rectificar datos personales o información crediticia de una persona que así lo haya solicitado por un medio claro e inequívoco constituye una infracción a la luz de la normativa vigente, estando facultado 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 Assessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto *(Privacy Impact Assessment)*?	No	No se prevé en la ley Nº 6.534/20.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Incidentes	¿Hay obligación de reportar un incidente de seguridad o algún incumplimiento a las previsiones legales?	Sí	En el marco de la Ley Nº 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. 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 constituye infracción.
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, la autoridad de control puede imponer sanciones que van desde apercibimientos, multas, suspensiones, cierres temporales, hasta inhabilitaciones. 1. Multa de hasta 15.000 jornales mínimos (aproximadamente US$ 204.000), duplicándose en caso de reincidencia (30.000 jornales mínimos, equivalente a aprox. US$ 408.000); pudiendo elevarse a 50.000 jornales mínimos (aproximadamente US$ 680.000) en casos de personas o empresas que tengan una facturación anual superior a Gs. 6.000.000.000 (aproximadamente US$ 760.000). 2. Suspensión de las actividades relacionadas con el tratamiento de datos hasta por seis meses, indicándose las medidas correctivas que deben adoptarse. 3. 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. 4. 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. 5. Cierre inmediato y definitivo de la operación que involucre el tratamiento de Datos Sensibles. Las sanciones administrativas, pueden ser graduadas por la autoridad de aplicación competente según su gravedad, y son independientes de las medidas correctivas o cautelares que dicten las autoridades de aplicación para salvaguardar el interés público protegido por la presente Ley y la sana gestión de las sociedades dedicadas al manejo de informaciones personales y crediticias. Estas sanciones son recurribles ante la jurisdicción contencioso-administrativa. A la fecha, existen varias resoluciones administrativas de la SEDECO por las cuales se han aplicado multas, sanciones y medidas correctivas a empresas que han violado disposiciones de la Ley Protección de Datos Personales Crediticios. Por otro lado, y a modo complementario, otras disposiciones normativas como ser la ley de comercio electrónico disponen multas en caso de infracciones relacionadas con la utilización o el tratamiento de datos personales en trasgresión a la norma.
Acciones legales	¿Existe alguna acción legal de protección de datos personales?, ¿quién tiene derecho para ejercerla/solicitarla?	Sí	La acción para el ejercicio de los derechos reconocidos en materia de protección de los datos personales podrá ser ejercida por el titular o por intermedio de su representante. 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 vigente no establece explícitamente la figura de un delegado oficial de protección de datos. No obstante, las disposiciones relativas al tratamiento de datos personales crediticios y las exigencias aplicadas a los BIC y los Usuarios de Información Crediticia, son un ejemplo claro de tendencia en la eventual creación de un área de protección de datos y/o en la externalización de una asesoría en este contexto, que exige, un nivel adecuado de conocimientos en la materia acorde a la complejidad del tratamiento de datos. Favor remitirse a los comentarios sobre "Otras Obligaciones".
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	Las autoridades de aplicación tienen amplias facultades de conformidad con la Ley y sus disposiciones complementarias y deben coordinar esfuerzos para que las mismas se cumplan.
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?	No	La normativa paraguaya no lo contempla explícitamente.

Tema	Concepto	Sí / 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 (Por ejemplo, GDPR)?, ¿qué diferencias relevantes encuentra?	No	La normativa paraguaya no contempla todos los requisitos contemplados por la normativa internacional. No obstante, en mayo del 2021, se ha presentado ante el Congreso Paraguayo para su estudio el proyecto de ley denominado "Ley de Protección de Datos Personales en la República del Paraguay" y cuyas disposiciones prevén regular de forma integral el tratamiento de los datos personales. A la fecha de elaboración de la presente Guía (octubre de 2025), el proyecto fue aprobado por la Cámara de Senadores y remitido nuevamente a la Cámara de Diputados para que se pronuncie sobre las modificaciones introducidas. Se espera su pronta promulgación, lo que representará un avance significativo en la regulación y garantía de los derechos vinculados a la protección de datos personales en Paraguay.
Otras obligaciones	¿Existen otras consideraciones/requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	Sí	La Resolución 3/23 del BCP, dispone que los BIC tienen la obligación de: ▸ Establecer Departamentos de Atención a los titulares de la información que cuente con los medios y procedimientos internos necesarios para brindar una eficiente y oportuna atención ante solicitudes de actualización, rectificación, oposición, eliminación y portabilidad de datos personales crediticios, todo esto, dentro de los plazos legales. ▸ Determinar los mecanismos de comunicación y coordinación adecuados con las fuentes y usuarios de los que se recolecta la información. ▸ Presentar para su aprobación por la Superintendencia de Bancos (SIB) del BCP, el Protocolo de Actuación que establezca Códigos de Conducta de práctica profesional, parámetros para el tratamiento de datos personales crediticios que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información, Políticas de buenas prácticas de Gobierno Corporativo. ▸ En cuanto a la seguridad de la información, implementar lo dispuesto en el Manual de Gobierno y Control de Tecnologías de Información (Resolución SB SG. Nº 00124/2017). ▸ Obligaciones de reportar a la SIB. ▸ Entre otros. Asimismo, los Usuarios de Información Crediticia están obligados a: ▸ Tramitar las consultas y reclamos formulados en los términos señalados en la Res. 3/2023. ▸ Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley Nº 6.534/20 y sus reglamentaciones. ▸ Contar con el consentimiento expreso de los titulares para poder tratar sus datos, incluso, para los casos en los que ya hayan tratado sus datos antes de la vigencia de la Resolución. ▸ Informar al titular de los datos personales sobre la consulta a realizarse sobre su información crediticia. ▸ Entre otros. Está expresamente prohibido a los usuarios de información crediticia utilizar o proveer a terceros datos crediticios para la toma de decisiones laborales, acceso al empleo, promoción, traslado o despido de personal. Asimismo, queda expresamente prohibido el uso de la información crediticia para negar o restringir el acceso a la medicina prepaga, así como negar o restringir al acceso a la atención médica de urgencia a cualquier persona. Como dato adicional y como se ha indicado previamente, en el marco de regulación sobre el Comercio Electrónico, el Decreto Reglamentario Nº 1165/14 de la ley de Comercio Electrónico dispone que el proveedor de bienes y servicios por vía electrónica a distancia, debe poner a conocimiento del consumidor o usuario la finalidad y el tratamiento que se le dará a sus datos personales, conforme a la Ley vigente relativa a la materia. Asimismo, debe comunicar el destinatario de los datos suministrados y el responsable de custodiar o almacenar la información proporcionada. El proveedor de bienes y servicios empleará sistemas seguros para evitar la pérdida, alteración y el acceso de terceros no autorizados a los datos suministrados por el consumidor o usuario. En julio el 2022, el BCP ha emitido la Resolución BCP 10/2022 "Reglamento de Uso de Servicios de Computación en la Nube", el cual establece los lineamientos mínimos y las obligaciones que deberán cumplir las entidades supervisadas que opten por externalizar sus procesos y actividades de servicios computacionales en la nube. En ella, se dispone que las entidades deben cumplir con la legislación y normativa vigente referente a protección de datos personales y crediticios en los procesos de servicios de computación en la nube, a fin de asegurar una adecuada protección a los datos personales de sus clientes.

PERÚ

Tema	Concepto	Sí / 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 Nº 29733 - se conoce como "Ley de Protección de Datos Personales" ("LPDP"). ▸ Decreto Supremo 016-2024-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. ▸ Resolución Directoral 074-2022-JUS/DGTAIPD, que aprueba las Cláusulas Contractuales Modelo para la Transferencia Internacional 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 disposiciones extraterritoriales en el artículo VI 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 III, 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 LPDP y 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 la información que se derive de un acto médico, el grado de discapacidad y su información genética (Artículo III inciso 5 del Decreto Supremo).

Tema	Concepto	Sí / 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 ni a sus representantes (que actúan en nombre de dichas 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 2 del Decreto Supremo. De acuerdo con lo previsto en el artículo 8 del Decreto Supremo, para el caso de datos sensibles (por ejemplo, datos biométricos, 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: 1. Cuando el tratamiento de los datos personales se realiza para el ejercicio de las funciones de las entidades públicas. 2. Cuando los datos personales sean necesarios para la preparación celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte. 3. 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, principalmente, sobre lo siguiente: 1. La finalidad para la que sus datos personales serán tratados. 2. Los destinatarios (de la transferencia nacional o internacional) de su información. 3. La existencia del banco de datos personales. 4. La identidad y el domicilio de su titular y, de ser el caso, del encargado del tratamiento de sus datos personales. 5. El tiempo de conservación de su información. 6. 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 con la transferencia internacional de datos? (Por 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 20 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). Sobre este punto, precisamente por Resolución Directoral 074-2022-JUS/DGTAIPD, se aprobaron las Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales, cuyo texto forma parte de la *Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales* de la Red Iberoamericana de Protección de Datos. Guía de implementación de cláusulas: **https://www.gob.pe/institucion/minjus/noticias/663844-peru-aprueba-guia-de-implementacion-para-la-transferencia-internacional-de-datos-personales-en-linea-con-estandares-internacionales**
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	No	Sin perjuicio de ello, el Decreto Supremo en su artículo 59.3 establece que, a través de la figura denominada "código de conducta" supuesto voluntario (no obligatorio) para el caso de transferencias de datos personales dentro de grupos empresariales, se haga referencia a la totalidad de tratamientos llevados a cabo por los mismos. Ahora bien, el artículo 15 del Decreto Supremo establece que, para realizar las transferencias de datos personales dentro de un grupo empresarial o entre sociedades subsidiarias vinculadas, se debe obtener el consentimiento del titular de los datos, salvo que el tratamiento se ajuste a alguna excepción legal.

Tema	Concepto	Sí / 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 se definen en el numeral 5 del artículo 2 de la LPDP y en el numeral 6 del artículo III del Decreto Supremo. Los datos sensibles son definidos como aquellos datos referidos a: ▸ Datos genéticos. ▸ Datos biométricos. ▸ Datos neuronales. ▸ Datos morales o emocionales. ▸ Hechos o circunstancias de su vida afectiva o familiar. ▸ Hábitos personales que corresponden a la esfera más íntima. ▸ Origen racial y étnico. ▸ Ingresos económicos. ▸ Opiniones o convicciones políticas, religiosas, filosóficas o morales. ▸ Afiliación sindical. ▸ La salud física o mental. ▸ 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 8 del Decreto Supremo.
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (Por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el 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 numeral 4 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, incluyendo incluso la cancelación de dicho banco, deberá ser previamente puesta en conocimiento de la Dirección de Protección de Datos Personales, a través de los formatos aprobados correspondientes.
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 (plataformas, sitios *web*, aplicaciones móviles y servicios digitales en general) que manejen bancos de datos personales deberán incluir en su funcionamiento lo que surge del artículo 46 del Decreto Supremo: 1. El control de acceso a la información de datos personales. 2. Monitoreo y revisión periódica de las medidas de seguridad y los planes de capacitación del personal. 3. Generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos y una vez que estos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros. 4. Medidas de seguridad que impidan al personal no autorizado la generación de copias o la reproducción de documentos digitales que contengan datos personales. Asimismo, la Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales, aprobada por Resolución Directoral 019-2013-JUS/DGPDP, es un documento facilitador y orientador que contiene el detalle de las condiciones, los requisitos y las medidas técnicas que se deben tomar en cuenta para cumplir la LPDP y el Decreto Supremo. Por otro lado, conforme al artículo 53 del Decreto Supremo, la documentación no automatizada (armarios, archivadores o similares) 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.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Por ejemplo, rectificación, actualización o supresión. Identificar y explicar.	Sí	El titular de los datos tiene los siguientes derechos, establecidos en los artículos 18 a 25 de la LPDP: ▸ Derecho de información. ▸ 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. ▸ Derecho a ser indemnizado El Capítulo II (Disposiciones especiales) del Decreto Supremo regula el procedimiento para ejercer el "derecho a la información" (artículo 74) y los denominados "derechos ARCO": ▸ Derecho de acceso (artículo 75). ▸ Derecho de rectificación (artículo 80). ▸ Derecho de cancelación (artículo 82). ▸ Derecho de oposición (artículo 86). ▸ Derecho de portabilidad (artículo 76).
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 61 al 87 del Decreto Supremo. De acuerdo con el artículo 64 del Decreto Supremo, para ejercer cualquiera de los derechos mencionados, se debe presentar una solicitud con la siguiente información: 1. Nombres y apellidos del titular de los datos personales. 2. Petición concreta, descripción clara del dato personal vinculado al ejercicio del derecho y la manifestación expresa del derecho que pretende ejercer. 3. Documentos que sustenten la petición. 4. Dirección a donde se realizarán las comunicaciones que correspondan. 5. Fecha y firma. Si el ejercicio del derecho se efectúa por un representante, se debe acreditar su representación. El artículo 69 del Decreto Supremo establece plazos de respuesta específicos. Por ejemplo, para la solicitud sobre el derecho de información es de ocho días y de las solicitudes sobre derechos de rectificación, cancelación y oposición es de 10 días hábiles. Por su parte, la solicitud sobre el derecho de acceso y de portabilidad de datos personales tienen un plazo de respuesta de veinte (20) días hábiles. Estos plazos podrán ser ampliados por una sola vez y por un periodo igual (a excepción del derecho de información), siempre que las circunstancias lo justifiquen.
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.

Tema	Concepto	Sí / 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	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 31 del Decreto Supremo, el encargado del banco de datos personales tiene prohibido 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 32 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 periodo mínimo de 30 días hábiles y máximo de 60 días hábiles, salvo disposición distinta en normas sectoriales. En el caso de instituciones educativas el plazo máximo para conservar las imágenes captadas por sistemas de videovigilancia es de 30 días hábiles.
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	Si bien no existe un plazo mínimo ni máximo previsto en la LPDP ni en el Decreto Supremo para la conservación de los datos personales recolectados, el artículo 8 de la LPDP establece que, bajo el principio de calidad, los datos personales deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento. Ahora bien, un primer 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 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. Del mismo modo, un segundo supuesto es en el caso del encargo de tratamiento de datos, contemplada en el artículo 31 del Decreto Supremo. En este caso, el plazo máximo para la conservación será de dos (2) años contado desde la finalización del último encargo realizado.
Privacy Impact Assessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto *(Privacy Impact Assessment)*?	No	De acuerdo con el artículo 40 del Decreto Supremo, la elaboración de una Evaluación de Impacto a la Privacidad (PIA) es facultativa. El PIA es el análisis que el responsable del tratamiento puede realizar antes de procesar datos personales, especialmente en situaciones que involucren datos sensibles, grandes volúmenes de datos u otros determinados por la Autoridad, con el fin de identificar y mitigar riesgos asociados al tratamiento.
Incidentes	¿Hay obligación de reportar un incidente de seguridad o algún incumplimiento a las previsiones legales?	Sí	Según el artículo 34 del Decreto Supremo, existe la obligación de notificar un incidente de seguridad de datos personales a la Autoridad Nacional de Protección de Datos Personales dentro de las 48 horas posteriores a su conocimiento, en los casos que dicho incidente (i) genere exposición de grandes volúmenes de datos personales en cantidad o tipo de datos, (ii) pueda afectar a un gran número de personas, (iii) trate de datos sensibles o (iv) produzca un perjuicio evidente a otros derechos o libertades del titular del dato personal. Esta obligación se mantiene incluso si el incidente ha sido subsanado internamente. Además, se debe comunicar al titular de los datos afectados si el incidente impacta sus derechos, utilizando un lenguaje claro y sencillo. Además, si un incidente de seguridad de datos personales ocurre en el entorno digital, debe notificarse al Centro Nacional de Seguridad Digital para su registro, a través del formulario virtual: https://reporte.cnsd.gob.pe/home/minjus.

Tema	Concepto	Sí / 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	En términos generales, el artículo 38 de la LPDP clasifica a las infracciones en leves, graves y muy graves, las cuales son tipificadas en los artículos 132, 133 y 134, respectivamente, 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. ▸ **Graves**: son sancionadas desde más de 5 UIT hasta 50 UIT. ▸ **Muy graves**: son sancionadas desde más de 50 UIT hasta 100 UIT. Cabe precisar que, para el año 2025, la UIT asciende a S/ 5.350 equivalente a un aproximado de US$ 1.500. La calificación y descripción de las infracciones están contemplados en los artículos 132, 133 y 134 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 habeas data (ámbito jurisdiccional). Del mismo modo, el artículo 73 del Decreto Supremo complementa esta información estableciendo que en caso se deniegue de forma parcial o total el ejercicio de un derecho, se debe, además, informar al titular la posibilidad de acceder a las vías previamente mencionadas.
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	El artículo 37 del Decreto Supremo establece la obligación legal designar un oficial de protección de datos (DPO) en los supuestos siguientes: ▸ Cuando el tratamiento de datos lo realice una entidad pública. ▸ Cuando el titular o encargado del tratamiento maneje grandes volúmenes de datos personales. ▸ Cuando la posible ocurrencia de un incidente durante de tratamiento pueda afectar a muchos titulares, o pueda perjudicar derechos o libertades de los titulares. ▸ Cuando las actividades principales del negocio impliquen el tratamiento de datos sensibles. En estos casos, de acuerdo con el artículo 37.2, un grupo empresarial puede nombrar un único DPO, siempre que sea fácil contactarlo para cada empresa.
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	El procedimiento de fiscalización (artículo 95 de Decreto Supremo) y procedimiento sancionador (artículo 111 del Decreto Supremo) 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).
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?	Sí	Según el artículo 47 del Decreto Supremo, el controlador (responsable del tratamiento) debe contar con un documento de seguridad que incluya, como mínimo, procedimientos de gestión de accesos, gestión de privilegios, verificación periódica de privilegios, políticas internas para el tratamiento de datos, y un inventario de datos personales y sistemas utilizados, especificando si se trata de datos sensibles. Este documento es obligatorio para el personal con acceso a los sistemas de información y debe ser actualizado y aprobado formalmente.

Tema	Concepto	Sí / 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 (Por ejemplo, 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. 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). Asimismo, el marco legal peruano no establece un plazo mínimo ni máximo de conservación de los datos personales. No obstante, 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 7 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). Es importante destacar que, aunque la elaboración de una Evaluación de Impacto a la Privacidad (PIA) o de un Código de Conducta es facultativa, su implementación, debidamente acreditada antes del inicio de un procedimiento administrativo sancionador, se considera una atenuante de responsabilidad, de acuerdo con el artículo 125 del Decreto Supremo.

REPÚBLICA DOMINICANA

Tema	Concepto	Sí / 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. Nº10737 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: 1. La finalidad para la que serán destinados y quiénes pueden ser sus destinatarios o clase de destinatarios. 2. La existencia del archivo, registro, banco de datos o de cualquier otro tipo de que se trate y la identidad y el domicilio de su responsable. 3. 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 N °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, el teléfono y número de fax profesionales.
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 lo siguiente: ▸ **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 con 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.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
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 Nº 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 con 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 con 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	1. La finalidad para la que serán destinados y quiénes pueden ser sus destinatarios o clase de destinatarios. 2. 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. 3. La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Tema	Concepto	Sí / 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? (Por ejemplo, cláusulas modelos, autorización por parte de la autoridad de control, entre otros)	Sí	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 Nº172-13 establece que, la Cesión de los datos personales objeto de tratamiento de datos solo 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)?	N/A	
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. ▸ 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 (Por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el uso de la misma?, ¿existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	N/A	

Tema	Concepto	Sí / 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	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: 1. Queda prohibido registrar datos personales en archivos, registros o bancos de datos que no reúnan condiciones técnicas de integridad y seguridad. 2. 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 SIC. 3. Las 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? (Por 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 y las 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.
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	▸ **Artículo 17.- Acción de habeas data**. Sin perjuicio de los mecanismos establecidos para el ejercicio de los derechos de los interesados, estos podrán ejercer la acción judicial de habeas data de conformidad con la Constitución y las leyes que rigen la materia. La acción judicial de habeas 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 habeas 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 estas 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 habeas 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 habeas data.
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	Sí	Los datos personales objeto de tratamiento de datos solo 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.

Tema	Concepto	Sí / 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	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 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. Por ejemplo, en materia de impuestos los contribuyentes, responsables y terceros están obligados a conservar en forma ordenada, por un periodo de 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.
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 Assessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (*Privacy Impact Assessment*)?	N/A	
Incidentes	¿Hay obligación de reportar un incidente de seguridad o algún incumplimiento a las previsiones legales?	N/A	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.	N/A	Se debe evaluar según el caso ya que en la Ley Nº172-13 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 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. Por ejemplo, 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.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?	No	Sin embargo, la ley establece sobre la Seguridad de los datos que el responsable del archivo de datos personales y en su caso, el encargado del tratamiento ¨procesamiento¨, 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 los 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 SIC. c) Las 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.
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (Por ejemplo, GDPR)?, ¿qué diferencias relevantes encuentra?	No	Poseen diferencias relevantes en el sentido que la Ley Nº 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	Sí / 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 Nº 18.331: Protección de Datos Personales y acción de habeas data ("Ley Nº 18.331"). ▸ Decreto Reglamentario Nro. 414/009 ("Decreto Nº 414/900"). ▸ Ley Nº 19.670 - Artículos 37 a 40 ("Ley Nº 19.670"). ▸ Ley Nº 19.030 ("Ley Nº 19.030"). ▸ Ley Nº 20.212 – Artículos 74, 75, 398 y 399. ▸ Decreto Reglamentario Nº 64/020 ("Decreto Nº 64/020"). ▸ Decreto Reglamentario Nº 664/008 ("Decreto Nº 664/008"). ▸ Decreto Reglamentario Nº 242/017 ("Decreto Nº 242/017"). ▸ Resolución de la URCDP Nº 1.647/010. ▸ Resolución de la URCDP Nº 23/021. ▸ Resolución de la URCDP Nº 41/021. ▸ Resolución de URCDP Nº 58/021. ▸ Resolución de URCDP Nº 63/023. ▸ Resolución de URCDP Nº 70/023.
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su sitio *web*.	Sí	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?	Sí	El ámbito de aplicación de la norma en principio es territorial. No obstante, en el artículo 3 del Decreto Nº 414/009 hace una especial distinción de acuerdo con el tratamiento de datos que se practique: 1. Tratamiento de datos efectuados por un responsable de base de datos o tratamiento establecido en territorio uruguayo, siendo este el lugar donde ejerza su actividad, cualquiera sea su forma jurídica. 2. 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. **Artículo 3, Decreto Nº 414/009**. A partir de la entrada en vigor de la Ley Nº 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: 1. En caso de que las actividades del tratamiento de datos estén relacionadas con la oferta de bienes y servicios dirigidos a habitantes de Uruguay. 2. En caso de que las actividades de tratamiento de datos estén relacionadas con el análisis del comportamiento de los habitantes de la República. 3. Si así lo disponen las normas de derecho internacional público o un contrato. 4. 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 Nº 18.331 amplía su ámbito de aplicación fuera del territorio de Uruguay. Art. 37, Ley Nº 19.670 y Arts. 1 y 2, Decreto Nº 64/020.

Tema	Concepto	Sí / 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	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: 1. La recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones a la presente ley. 2. Los datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario. 3. 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 con 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 Nº 18.331.
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	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 Nº 18.331.
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	Conforme surge del artículo 4, incisos. D) y E) y artículo 18 de la Ley Nº 18.331 la normativa en la materia hace distinción entre datos personales y datos sensibles. La ley también realiza una distinción en relación con: ▸ 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. ▸ Datos transferidos internacionalmente. Todos estos datos son considerados "datos especialmente protegidos" por la Ley. Arts. 4 inc. D) y E),18-23 Ley Nº 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 Nº 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 artículo 13 de la Ley Nº 18.331. Arts. 9 y 13, Ley Nº 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 artículo 9 de la Ley Nº 18.331. Por su parte, el artículo 17 de la misma Ley refiere a los supuestos en los cuales no será necesario obtener el consentimiento del titular para la comunicación de los datos recabados.

Tema	Concepto	Sí / 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 el 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 artículo 23, literal A de la Ley Nº 18.331. Art. 5, Decreto Nº 414/009.
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales?, ¿hay requisitos aplicables en relación con la transferencia internacional de datos? (Por 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 con 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 artículo 23 de la Ley Nº 18.331 (numerales 1 al 5 y literales A al F). Es importante tener en cuenta que la Resolución de la URCDP Nº 63/023, modifica la Resolución de la URCDP Nº 23/021 y 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, la Confederación Suiza, la República de Corea, y a las transferencias a organizaciones incluidas en el "Listado del Marco de Privacidad de Datos" publicado por el Departamento de Comercio de los Estados Unidos de América. Respecto al Listado del Marco de Privacidad de Datos, este surgió en respuesta a la invalidación del "Privacy Shield" por parte del Tribunal de Justicia de la Unión Europea. Previamente, la Resolución de la URCDP Nº 23/021 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. En virtud de dicha resolución, las transferencias internacionales de datos realizadas a Estados Unidos de América debían justificarse a través del consentimiento de los interesados o de algunas de las excepciones previstas en el artículo 23 de la Ley Nº 18.331. En respuesta a la invalidación del "Privacy Shield", el Departamento de Comercio de los Estados Unidos de América preparó el "Listado del Marco de Privacidad de Datos", aprobado por la Comisión de la Unión Europea por decisión de 10 de julio de 2023. De esta forma, como ya fue mencionado, la Resolución de la URCDP Nº 63/023 permitió las transferencias de datos internacionales a las organizaciones incluidas en el nuevo "Listado del Marco de Privacidad de Datos" publicado por el Departamento de Comercio de los Estados Unidos de América y aprobado por la Comisión de la Unión Europea por decisión de 10 de julio de 2023. Luego, la Resolución de la URCDP Nº 70/023 agregó que los responsables y encargados que procuren realizar transferencias internacionales a estas organizaciones deberán presentar ante la URCDP, en el momento previo a la inscripción de la base de datos o de la transferencia, una declaración expresa en la que la organización importadora declare haber extendido la aplicación de las salvaguardas del Marco de Privacidad de Datos a los datos transferidos desde Uruguay. Si no se formula dicha declaración, la transferencia a las citadas organizaciones podrá realizarse en virtud de las cláusulas contractuales presentadas por los responsables o encargados, que sean autorizadas previamente por la URCDP, u otros fundamentos previstos legalmente. A través de la Resolución de la URCDP Nº 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. Por último, la Resolución de la URCDP Nº 70/2023 agregó ciertos requisitos adicionales que el encargado o responsable de la base de datos deberá comunicar a los titulares de los datos para los casos en que se realice una transferencia internacional de datos: 1) El destino de sus datos. 2) El rol del importador. 3) El plazo de la transferencia. 4) La base de la legitimación. 5) Las operaciones de tratamiento realizadas por el importador.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
BCR	¿Cuentan con normas corporativas vinculantes (BCR)?	Sí	La normativa uruguaya en su artículo 36 lo define como "Código de conducta". Arts. 35 y 36, Ley Nº 18.331.
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 Nº 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 Nº 18.331. Art 40, Ley Nº 19.670.
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (Por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el 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 artículo 29 de la Ley Nº18.331 y cumplimentar con la obligación de actualización dispuesta en el artículo 20 del Decreto Nº 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: 1. Que exista una alteración cuantitativa del 20% de los datos indicados en la solicitud de registro. 2. 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 Nº 18.331; Arts. 15 y 20, Decreto Nº 414/009; Decreto 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 artículo 3 del Decreto Nº 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 Nº 18.331 y Art. 3, Decreto Nº 64/020.
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Por 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. 13-17 de la Ley Nº18.331 y en los arts. 9-14 del Decreto Nº 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. 13-17 de la Ley Nº 18.331.

Tema	Concepto	Sí / 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 artículo 17 de la Ley N°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 Nº 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 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 artículo 30 hace referencia, asimismo, a la prestación de servicios informatizados de datos personales. Arts. 4 y 30, Ley Nº 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 Decreto Nº 414/009 en su artículo 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 Nº 18.331 y Art. 39, Decreto Nº 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 artículos 6 y 7 del Decreto Nº 64/020. Art. 12, Ley Nº 18.331. Arts. 6 y 7, Decreto Nº 64/020.
Incidentes	¿Hay obligación de reportar un incidente de seguridad o algún incumplimiento a las previsiones legales?	Sí	El Decreto N°64/020 dispone de un Capítulo destinado a vulneraciones de seguridad. A lo largo de los artículos 3 y 4 de dicho Decreto, se detalla todo lo concerniente a ellas. Por otra parte, a partir de la Ley N°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, junto 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. Además, el art. 80 de la Ley 20.212 creó el Registro Nacional de Incidentes de Ciberseguridad. Las entidades públicas y las entidades privadas vinculadas a servicios o sectores críticos del país deberán comunicar la ocurrencia de incidentes de ciberseguridad a AGESIC en un plazo de 24 horas de conocido y complementar la información necesaria para el registro efectivo a la brevedad. Asimismo, el art. 83 de la Ley 20.212 creó el Comité de Gestión de la Estrategia Nacional de Ciberseguridad conformado por diferentes organismos del estado, con el cometido principal de apoyar y colaborar con la AGESIC en la implantación y el monitoreo de la estrategia nacional de Ciberseguridad. Arts. 3 y 4, Decreto Nº 64/020. Art. 38, Ley Nº 19.670. Art. 80 y 82, Ley Nº 20.212.

Tema	Concepto	Sí / 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 Ley Nº 18.331 en su artículo 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 Nº 19.670 sustituye el antiguo artículo 12 de la Ley Nº 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. 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 Nº 18.331. Art. 39, Ley Nº 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 Nº 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 (por ejemplo, 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 artículo 40 de la Ley Nº 19.670. Arts. 10-15, Decreto Nº 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 Nº 18.331.
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?		La normativa no prevé registros concretamente de las actividades de procesamiento realizadas por el responsable de la base de datos o del tratamiento. De todos modos, el art. 5 del Decreto 64/020 establece que los responsables y encargados del tratamiento de datos personales deberán documentar las medidas de responsabilidad proactiva que adopten, revisar las mismas periódicamente y evaluarlas en su efectividad, para lo cual se deberá prever el estado de la técnica, el costo de su aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que aquél entrañe para los derechos de las personas. El art. 5 de dicho decreto determina que, según la naturaleza de los datos, los tratamientos que efectúen y los riesgos que impliquen, se deberán implementar medidas técnicas y organizativas apropiadas, como son la evaluación de impacto en la protección de datos personales, la privacidad desde el diseño y la privacidad por defecto, sin perjuicio de otras que pueden establecerse, a fin de garantizar un tratamiento adecuado de los datos personales y demostrar su efectiva implementación. Estas medidas deberán ser documentadas y contener, como mínimo, la forma, medios y finalidad del tratamiento, los procedimientos orientados a dar cumplimiento a las normas, la planificación de mecanismos para responder a vulneraciones de seguridad, y el rol del delegado de protección de datos cuando corresponda. Esta documentación deberá estar disponible ante la solicitud efectuada por la URCDP.

Tema	Concepto	Sí / 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 (Por ejemplo, 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 Nº19.030- 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 Nº 19.670 y Decreto Nº 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 Decreto Nº 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 artículo 181 de la Ley Nº 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 cuatro 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 este. 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.

VENEZUELA

Tema	Concepto	Sí / 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 Venezuela está regulada por diversas disposiciones normativas: ▸ Constitución de la República Bolivariana de Venezuela (1999): (Art. 28 "Derecho a informarse", Art. 60 "Derecho a la intimidad"). ▸ Ley Especial contra los Delitos Informáticos, promulgada el 30/10/2001 mediante Gaceta Oficial No. 37.313, la cual tipifica diversas conductas delictivas relacionadas con el uso de la tecnología y la información (privacidad e integridad de datos personales). ▸ Ley de Mensajes y Firmas Electrónicas, promulgada el 28/02/2001 mediante Gaceta Oficial No. 37.148, la cual tiene como objeto otorgar y reconocer la firma electrónica, el mensaje de datos y toda información inteligible en formato electrónico. ▸ Ley Orgánica del Tribunal Supremo de Justicia, promulgada el 19/01/2022 mediante Gaceta Oficial No. 6.684 (habeas data) ▸ Ley de Infogobierno, promulgada el 17/10/2013 mediante Gaceta Oficial No. 40.274 (uso de las tecnologías de la información en el Poder Público y el Poder Popular. ▸ Ley de Instituciones del Sector Bancario, promulgada el 08/12/2014 mediante Gaceta Oficial No. 40.557. ▸ Ley sobre Acceso e intercambio electrónico de datos, información y documentación entre los órganos y entes del Estado, promulgada el 15/06/ 2012 mediante Gaceta Oficial No. 39.945 ▸ Criterio Jurisprudencial: Sala Constitucional del Tribunal Supremo de Justicia en sentencia No. 1050 del 23/08/2000 (caso Ruth Capriles y otros)
Autoridad de aplicación	¿Cuál es la autoridad de aplicación? En su caso, proporcionar el enlace a su sitio *web*.	Sí	El Consejo Nacional para el Uso de las Tecnologías de Información es el máximo órgano de consulta para la planificación y asesoramiento del Poder Público en los asuntos relacionados con las tecnologías de información, junto con la Comisión Nacional de las Tecnologías de Información (CONATI) otra institución del estado venezolano encargada de establecer y ejecutar las políticas, estrategias y lineamientos en el sector de las tecnologías de información. (**https://www.conati.gob.ve**). Adicionalmente, la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) (**https://www.suscerte.gob.ve**) es la responsable del desarrollo, implementación, ejecución y seguimiento al Sistema Nacional de Seguridad de Informática del Estado venezolano (SNSI).
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	En principio su ámbito de aplicación es territorial, el Estado venezolano tiene la obligación de proteger estos derechos a todas las personas que se encuentren bajo su jurisdicción, bien sean venezolanos o extranjeros, así como también garantizar la aplicación de las leyes que se dicten para limitar el uso de la informática. Sin embargo, la Ley Especial de Delitos Informáticos establece en su Art. 3 que, cuando alguno de los delitos tipificados en dicha norma se comenta fuera del territorio venezolano y se hubiesen producido efectos del hecho punible dentro de Venezuela y el responsable no ha sido juzgado por ese hecho en la jurisdicción donde se encuentra, se aplicará el principio de extraterritorialidad.
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 de Infogobierno establece que el Poder Público debe garantizar la integridad, confidencialidad, autenticidad y disponibilidad de la información, a través del uso de certificados y firmas electrónicas emitidas dentro de la cadena de confianza de certificación electrónica del Estado venezolano.
Concepto legal de "dato personal"	¿Qué se entiende por dato personal?	Sí	Según el Art. 2 de la Ley Especial de Delitos Informáticos, la Data, son hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se le asignan o se les puede asignar un significado. Vale decir, en Venezuela, el dato personal, está protegido por los derechos constitucionales a la intimidad, el honor y a la vida privada, y sobre el cual toda persona tiene derecho a la autodeterminación informativa, es decir, controlar su recogida, uso y difusión.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Categorías de "datos personales"	¿Existen diferentes categorías de datos? Explicar cada una en caso de corresponder.	Sí	El Art.4 de la Ley sobre Acceso e intercambio electrónico de datos, información y documentación entre los órganos y entes del Estado distingue la siguiente categoría: ▸ Dato: Hecho, concepto, instrucción o caracteres, que se expresa por sí mismo, representado de una manera apropiada para que sea comunicado, transmitido o procesado por seres humanos o por medios automáticos, y al cual se le asigna o se les puede asignar un significado. ▸ Dato complementario: Dato adicional requerido por un órgano o ente para complementar un proceso o trámite que conforme a la ley tiene atribuido. ▸ Dato de autoría: Dato emanado de un órgano o ente del Estado, en su condición de autoridad competente para emitirlo o registrarlo, que resulta del cumplimiento de los 3 procesos administrativos que realiza con ocasión al ejercicio de sus atribuciones o como resultado de la tramitación de las diligencias, actuaciones o gestiones que realizan las personas ante ellos.
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 que regula estos temas posee un ámbito de protección que abarca: ▸ Toda persona física o jurídica – titular del dato. ▸ Todo el que acredite tener un vínculo de parentesco con el titular fallecido. ▸ Prevé que las personas jurídicas pueden ejercer el derecho de acceso a sus datos.
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	Según el Art. 20 de la Ley Especial de Delitos Informáticos toda persona que intencionalmente se apodere, utilice, modifique o elimine cualquier medio sin el consentimiento de su dueño, la data o información personal o sobre las cuales tenga interés legítimo será penada con prisión de dos a seis años y multa de 200 a 600 unidades tributarias. ($130 aproximadamente) Adicionalmente, la Ley de Infogobierno en su Art. 79, señala que el Poder Público y el Poder Popular no puede divulgar, ceder, traspasar, ni compartir con ninguna otra persona los datos recopilados de niñas, niños y adolescentes en relación con el cumplimiento de sus derechos y garantías sin el previo consentimiento de su representante legal e indica que dicho consentimiento siempre puede ser revocado
Excepciones al consentimiento	¿Existen excepciones al consentimiento voluntario del titular de datos? En caso afirmativo, identificar excepciones.	Sí	El Art. 86 de la Ley de Instituciones del Sector Bancario, prohíbe a las instituciones bancarias, así como a sus directores y trabajadores, suministrar a terceros cualquier información sobre las operaciones pasivas y activas con sus usuarios, a menos que medie autorización escrita de estos. También se encuentran obligados a cumplir el secreto bancario: i) El superintendente de las instituciones del Sector Bancario y los trabajadores de la Superintendencia de las Instituciones del Sector Bancario. ii) Los directores y trabajadores del Banco Central de Venezuela. iii) Los directores y trabajadores de las empresas de auditoría externa. (El secreto bancario no rige cuando la información sea requerida para fines oficiales (Art. 87) La institución bancaria está obligada a comunicar la información que requieren los organismos competentes contemplados en la Ley, que regulan la prevención de legitimación de capitales y financiamiento al terrorismo.
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.)	No.	La normativa no específica sobre el contenido que debe incluir el consentimiento.
Transferencia de datos personales	¿Existen requisitos o restricciones para la transferencia de datos personales?, ¿hay requisitos aplicables en relación con la transferencia internacional de datos? (Por ejemplo, cláusulas modelos, autorización por parte de la autoridad de control, entre otros)	Sí	Venezuela no cuenta con una regulación en materia de transferencia internacional de datos. Sin embargo, si prevé la transferencia de datos e información entre los órganos y entes del Estado, los cuales solo pueden ser utilizados para los fines solicitados (Ley sobre Acceso e intercambio electrónico de datos, información y documentación entre los órganos y entes del Estado).
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?	No	La normativa no prevé la categorización de dato sensible.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Registración de bases de datos o informes periódicos a la autoridad de control	¿Existe la obligación de registrar (Por ejemplo, ante el organismo de aplicación correspondiente) una base de datos y/o la titularidad, el tratamiento y/o el uso de la misma?, ¿existe obligación de presentar algún tipo de información o informe periódico a la autoridad de aplicación?	No	La normativa no prevé la obligación de registrar.
Seguridad de los datos	¿Existen medidas técnicas para garantizar la seguridad y confidencialidad de los datos personales? En caso afirmativo, ¿cuáles son?	Sí	El Art. 22 de la Ley de Infogobierno establece que en las actuaciones que realice el Poder Público y el Poder Popular a través de las tecnologías de información sólo se exigirán a las personas las medidas de seguridad necesarias según la naturaleza de los trámites y actuaciones a realizar. Igualmente, se requerirán los datos que sean estrictamente necesarios para tramitar los asuntos que haya solicitado, a los fines de garantizar el cumplimiento de los principios y derechos establecidos en la Constitución de la República y la ley (Principio de proporcionalidad).
Derechos de los titulares de los datos	¿Cuáles son los derechos de los titulares de los datos? (Por ejemplo, rectificación, actualización o supresión) Identificar y explicar.	Sí	La Sala Constitucional del Tribunal Supremo de Justicia en sentencia No. 1050 del 23/08/2000 (caso Ruth Capriles y otros) identifica los siguientes derechos: ▸ El derecho de conocer sobre la existencia de registros. ▸ El derecho de acceso individual a la información, la cual puede ser nominativa, o donde la persona queda vinculada a comunidades o a grupos de personas. ▸ El derecho de respuesta, lo que permite al individuo controlar la existencia y exactitud de la información recolectada sobre él. ▸ El derecho de conocer el uso y finalidad que hace de la información quien la registra. ▸ El derecho de actualización, a fin de que se corrija lo que resulta inexacto o se transformó por el transcurso del tiempo. ▸ El derecho a la rectificación del dato falso o incompleto. ▸ El derecho de destrucción de los datos erróneos o que afectan ilegítimamente los derechos de las personas.
Acciones de los titulares de los datos	¿Cómo pueden ejercerlos?	Sí	De conformidad con la Ley Orgánica del Tribunal Supremo de Justicia, los titulares de los datos pueden ejercer el habeas data mediante escrito interpuesto ante el Tribunal de Municipio con competencia en lo Contencioso Administrativo y con competencia territorial en el domicilio del solicitante. Según la doctrina venezolana existen diferentes tipos de habeas data: ▸ Habeas data informativo: con la finalidad de recabar la información y pueden ser exhibitorio dirigido a conocer qué se registró, finalista: con el objetivo de determinar para qué y para quién se realizó el registro, autoral: su propósito es inquirir acerca de quién obtuvo los datos que obran en el registro. ▸ Habeas data aditivo: se procuran agregar más datos a los que figuran en un registro respectivo. ▸ Habeas data ratificador o correctivo: su misión es la de corregir o sanear informaciones falsas, y también podría abarcar a las inexactas o imprecisas, respecto de las cuales es factible solicitar determinadas precisiones terminológicas, especialmente cuando los datos son registrados de manera ambigua o pueden dar lugar a más de una interpretación. ▸ Habeas data reservador: su fin es asegurar que un dato que se encuentra legítimamente registrado, se proporcionado solo a quienes se encuentre legalmente autorizados para ello y en las circunstancias en que ello corresponde. ▸ Habeas data cancelatorio: tiene por misión eliminar la información del registro cuando por algún motivo no debe mantenerse registrada. Finalmente, la sentencia que declare con lugar el habeas data ordenará al agraviante de forma inmediata la exhibición, supresión, rectificación, confidencialidad, inclusión, actualización o el uso correcto de los datos, según corresponda.
Cesión de datos personales	¿Cuáles son los requisitos para la cesión de datos personales?	No	No se encuentra previsto en la normativa la cesión 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.	No	No se encuentra previsto en la normativa.

Tema	Concepto	Sí / 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 datos deben conservarse por el lapso legal o contractual establecido entre el responsable o usuario del archivo o el titular de los datos. El Código de Comercio venezolano prevé en términos generales en su Art. 44 que los libros y sus comprobantes deben ser conservados durante diez años, a partir del último asiento de cada libro. La correspondencia recibida y las copias de las cartas remitidas serán clasificadas y conservadas durante diez 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?	No	La normativa no prevé la obligación de eliminar datos recolectados o procesados. Sin embargo, la Ley de Instituciones del Sector Bancario ordena a la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN) dictar una normativa prudencial mediante la cual regule, lo relacionado con la forma y oportunidad de transmisión, calidad de los datos transmitidos, exclusión o inclusión de usuarios, tiempo de permanencia en el Sistema de Información Central de Riesgos, verificación de la veracidad de la información y tramitación de reclamos.
Privacy Impact Assessment	¿Se requieren y/o son obligatorias las evaluaciones de impacto (*Privacy Impact Assessment*)?	No	La normativa no prevé ni establece la obligatoriedad las evaluaciones de impacto.
Incidentes	¿Hay obligación de reportar un incidente de seguridad o algún incumplimiento a las previsiones legales?	Sí	El Art.75 de la Ley de Infogobierno establece que el Poder Público y el Poder Popular, a través de las tecnologías de información, están obligados a notificar a las personas: ▸ Que la información será recolectada de forma automatizada; ▸ Su propósito, uso y con quién será compartida; ▸ Las opciones que tienen para ejercer su derecho de acceso, ratificación, supresión y oposición al uso de la referida información; ▸ Las medidas de seguridad empleadas para proteger dicha información, el registro y archivo, en las bases de datos de los organismos respectivos.
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 Art. 80 de la Ley de Infogobierno establece que todas aquellas personas que ejerzan una función pública, incurren en responsabilidad civil, penal y administrativa por las infracciones cometidas a la presente Ley. Las multas pueden estar comprendidas entre 50 a 500 unidades tributarias ($120).
Acciones legales	¿Existe alguna acción legal de protección de datos personales?, ¿quién tiene derecho para ejercerla/solicitarla?	Sí	Consultar la respuesta del punto No. 17. En cuanto a quienes tienen derecho a ejercer o solicitar tales acciones, se encuentran: ▸ Tutores y curadores de incapaces. ▸ Apoderados –facultad expresa. ▸ Representantes legales de la persona jurídica
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	No se prevé en el ordenamiento jurídico venezolano.
Investigaciones	¿Puede actuar y/o investigar de oficio la autoridad competente ante un incumplimiento de protección de datos personales?	Sí	El Art. 41 de la Ley de Infogobierno establece que la Comisión Nacional de las Tecnologías de Información puede de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos sancionatorios previstos en dicha Ley y normativa aplicable, en el ámbito de su competencia. Entendiéndose que puede actuar o investigar los procedimientos relacionados a la protección de datos.

Tema	Concepto	Sí / No / NA (No aplica)	Observaciones / comentarios
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?	Sí	La Ley de Infogobierno en su Art. 12 prevé que el Poder Público y el Poder Popular deben registrar ante la autoridad competente los programas informáticos que utilicen o posean; su licenciamiento, código fuente y demás información y documentación que determine la norma instruccional correspondiente. No está prevista dicha obligación aplicable a las personas naturales o jurídicas.
Similitudes con el GDPR	En su entendimiento, ¿considera que la normativa referida contempla todos los requisitos receptados por la normativa internacional en la materia (Por ejemplo, GDPR), ¿qué diferencias relevantes encuentra?	No	El ordenamiento jurídico venezolano no contempla todos los requisitos establecidos por la normativa internacional, ya que a la fecha no hay una legislación especial dedicada exclusivamente a la protección de datos personales y privacidad.
Otras obligaciones	¿Existen otras consideraciones/requisitos adicionales u obligaciones legales que se deben cumplir en materia de protección de datos?	Sí	La Ley sobre Acceso e intercambio electrónico de datos, información y documentación entre los órganos y entes del Estado dispone la obligación de Compartir los Datos, Información y Documentos por parte de los órganos y entes del Estado, tales como: ▸ Datos de autoría, y solo podrán excusarse de compartir los datos, información y documentos que manejan cuando la ley expresamente así lo limite, a fin de garantizar la protección al honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de los ciudadanos y ciudadanas. La obligación de compartir datos de autoría, información y documentos de acceso público no será exigible cuando la solicitud de estos sea impertinente, inadecuada o excesiva con relación al ámbito y fines del proceso que se desea ejecutar. (Art.43).

Contactos EY Law Latinoamérica

Argentina	Bolivia	Brasil	Chile	Colombia
Jorge Garnier Partner **jorge.garnier@ar.ey.com** Pablo Bisogno Associate Partner **pablo.bisogno@ar.ey.com** Laila Yu Manager **laila.yu@ar.ey.com** Mercedes García Senior **mercedes.garcia.gomez@ar.ey.com** Melania Gadea Staff **melania.gadea@ar.ey.com**	Sandra Vásquez Directora Ejecutiva **sandra.vasquez@bo.ey.com** Miguel A. Plaza Staff **miguel.a.plaza@bo.ey.com**	Ligia Augusto Partner **ligia.augusto@br.ey.com** Gustavo Poggio Associate Partner **gustavo.poggio@br.ey.com** Sandra Avella Manager **sandra.avella@br.ey.com**	Pedro Lluch Partner **pedro.lluch@cl.ey.com** Tomás Labbé Manager **tomas.labbe@cl.ey.com** Sofía Muñoz Senior **sofia.munoz@cl.ey.com**	Camila González Partner **camila.gonzalez@co.ey.com**
Costa Rica	**Ecuador**	**Guatemala**	**México**	**Panamá**
Antonio Ruiz Partner **antonio.ruiz@cr.ey.com** Melania Sibaja Senior **melania.sibaja@cr.ey.com**	Fernanda Checa Partner **fernanda.checa@ec.ey.com**	Antonio Ruiz Partner **antonio.ruiz@cr.ey.com** Ginny Castillo Senior Manager **ginny.castillo@gt.ey.com** Mirla Tubac Manager **mirla.tubac@gt.ey.com**	Carina Barrera Partner **carina.barrera@mx.ey.com** Bárbara Fernandez Associate Partner **barbara.fernandez@mx.ey.com** Alejandro Guevara Manager **alejandro.guevara@mx.ey.com**	Antonio Ruiz Partner **antonio.ruiz@cr.ey.com** Francisco Javier Vanegas Senior **francisco.vanegas@pa.ey.com**
Paraguay	**Perú**	**República Dominicana**	**Uruguay**	**Venezuela**
Gustavo Colman Partner **gustavo.colman@py.ey.com** Nabila Larroza Manager **nabila.larroza@py.ey.com**	Maria del Pilar Sabogal Partner **maria.sabogal@pe.ey.com** Bruno Mejía Senior Manager **bruno.mejia@pe.ey.com**	Antonio H Ruiz Rojas Partner **Antonio.Ruiz@cr.ey.com** Dionigi De Santis Manager **dionigi.de.santis@do.ey.com**	Rodrigo Barrios Partner **rodrigo.barrios@uy.ey.com** Ines Eibe Associate Partner **ines.eibe@uy.ey.com** Germán Gómez Manager **german.gomez.bonaglia@uy.ey.com**	Saul Medina Rodriguez Partner **saul.medina@ve.ey.com** Diana C. Socorro M. Senior Manager **diana.c.socorro.marquez@ve.ey.com** Marion S. Medina R Senior **marion.s.medina@ve.ey.com**

EY | Building a better working world

EY está construyendo un mejor mundo de negocios al crear nuevo valor para los clientes, las personas, la sociedad y el planeta, mientras genera confianza en los mercados de capital.

Impulsados por datos, IA y tecnología avanzada, los equipos de EY ayudan a los clientes a dar forma al futuro con confianza y desarrollar respuestas para los problemas más urgentes de hoy y mañana.

Los equipos de EY trabajan en un espectro completo de servicios en Auditoría y Finanzas, Consultoría, Fiscal-Legal, Estrategia y Transacciones. Impulsados por conocimientos sectoriales, una red globalmente conectada y multidisciplinaria, y socios de ecosistemas diversos, brindamos soluciones en más de 150 países y territorios.

All in to shape the future with confidence.

EY se refiere a la organización global y podría referirse a una o más de las firmas integrantes de Ernst & Young Global Limited, cada una de las cuales es una entidad legal independiente. Ernst & Young Global Limited, una compañía de responsabilidad limitada constituida conforme a las leyes del Reino Unido, 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 **www.ey.com/es_mx.**

© 2025 EY.
Integrante de Ernst & Young Global
Derechos Reservados