LA FIGURA DEL PROFESIONAL DE PRIVACIDAD EN LATINOAMÉRICA.

ESTADO ACTUAL Y PRINCIPALES DESAFÍOS PARA SU ADECUADA OPERACIÓN

GREGORIO BARCO VEGA

inai

Equipo Editorial

Sergio Octavio Contreras Padilla, Kenya Soraya Martínez Ponce, Griselda Rubalcava Hernández, María Fernanda de León Canizalez y María Alicia Barrera Aviña
Diseño editorial y portada: Diego González Hernández

Primera versión digital, noviembre 2023
ISBN: 978-607-59601-9-7
Hecho en México / *Made in Mexico*
Ejemplar de descarga gratuita

Índice

Acerca del autor 5
Abreviaturas 7
Presentación 9
Introducción 13
Planteamiento del problema 17
Sobre la Figura del Profesional de Privacidad 25
Origen 26
Necesidad 31
Perfil del Profesional de Privacidad 33
Funciones y responsabilidades 36
Posición 40
Certificación 42
Cifras relevantes
***A.** Sobre el número de Profesionales de Privacidad* 47
***B.** Datos del Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Federal 2021* 49
***C.** Datos de los Censos Económicos 2019 y del DENUE 2022* 54
Regulación de la Figura del Profesional de Privacidad en Latinoamérica 59
Contexto 60
Regulación de la Figura del Profesional de Privacidad en Latinoamérica
Argentina 63
Brasil 66
Chile 68
Colombia 69
Costa Rica 72
Cuba 73
Ecuador 73
México (sector privado) 76
México (sector público) 81
Nicaragua 87
Panamá 87

Paraguay 90
Perú 90
República Dominicana 90
Uruguay 90
Principales desafíos para la adecuada operación de la Figura del Profesional de Privacidad en Latinoamérica 95
Regulación 96
Preparación y capacitación 97
Concienciación 97
Esquemas de certificación 100
Conclusiones 103
Referencias 111
Referencias bibliohemerográficas 112
Guías y documentos de autoridades especializadas 112
Normatividad empleada:
Normatividad nacional 114
Normatividad europea 114
Normatividad vigente en Latinoamérica:
Argentina 115
Brasil 115
Chile 115
Colombia 115
Costa Rica 115
Ecuador 115
Nicaragua 115
Panamá 115
Paraguay 116
Perú 116
Uruguay 116
Normatividad soft law empleada 116
Criterios jurisprudenciales 116
Documentos publicados en internet 116
Anexo 119

Acerca del autor

Gregorio Barco Vega

Licenciado en Derecho con mención honorífica por la Universidad Nacional Autónoma de México (UNAM) y Maestro en Derecho por la misma universidad. Experto Universitario y Especialista en Reglamento General de Protección de Datos por la Universidad Nacional de Educación a Distancia (UNED), España.

Profesor del Diplomado de Derecho Digital, Tecnología e Innovación del Instituto Tecnológico Autónomo de México (ITAM) desde 2017, profesor invitado en diversas instituciones de educación superior y conferencista en instituciones académicas y foros especializados.

Miembro del Ilustre y Nacional Colegio de Abogados de México (INCAM).

Autor, coautor y colaborador de diversas publicaciones especializadas como el GPS de Protección de Datos Personales para el Sector Privado (Tirant Lo Blanch, 2020) y el Diccionario de Protección de Dates Personales (INAI, 2019).

Abogado Sénior en Davara Abogados, Firma especializada en Derecho Digital, Tecnología e Innovación, donde realiza actividades de asesoramiento legal, consultoría, auditoría, litigio, investigación y capacitación en protección de datos personales y dirige el área de Investigación, Desarrollo e Innovación (I+D+i) de la Firma.

Abreviaturas

AEPD: Agencia Española de Protección de Datos

APDP: Autoridad de Protección de Datos Personales

CEPD: Comité Europeo de Protección de Datos

DPO: Data Protection Officer

DPD: Delegado de Protección de Datos

CPEUM: Constitución Política de los Estados Unidos Mexicanos

EPDP: Estándares de Protección de Datos Personales para los Estados Iberoamericanos

GTA29: Grupo de Trabajo del Artículo 29 en materia de protección de datos

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos

LFPDPPP: Ley Federal de Protección de Datos Personales en Posesión de los Particulares

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

LGPDPSP: Lineamientos Generales de Protección de Datos Personales para el Sector Público

OPD: Oficial de Protección de Datos Personales

RGPD: Reglamento General de Protección de Datos

RIPD: Red Iberoamericana de Protección de Datos

RLFPDPPP: Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

RPD: Responsable de la Protección de Datos

SEPD: Supervisor Europeo de Protección de Datos

UE: Unión Europea

Presentación

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) continúa su proceso de divulgación e investigación mediante la difusión de obras editoriales que contribuyan entre la sociedad al conocimiento de sus dos derechos fundamentales: el acceso a la información pública y la protección de datos personales.

A través de su Programa Editorial es que se presenta la obra titulada "La Figura del Profesional de Privacidad en Latinoamérica. Estados actuales y principales desafíos para su adecuada operación", la cual constituye una visión centralizada sobre la utilidad social de los derechos humanos que el instituto garantiza.

La obra expuesta pone a la discusión una imagen que se encuentra aún en un estado de maduración en el marco normativo de países de América Latina, se trata de la figura del Profesional de Privacidad o Profesional de Protección de Datos. Concepto que es utilizado por el autor para referirse a la función de la persona física que posee la responsabilidad respecto a temas en materia de protección de datos personales dentro de una organización pública o privada.

De esta forma, Gregorio Barco Vega, parte de una exigencia contundente que es la de precisar, mediante una investigación, el origen, las funciones, así como la necesidad del Estado en tener a un profesional que posea la capacidad y, a su vez, sea competente en el estudio que el cargo demanda.

El análisis también va encaminado a la comparativa por regiones, donde se exponen países de América Latina como lo son Argentina, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana y Uruguay, en los que se presenta en el ordenamiento vigente de leyes de cada país sobre las normas que se han emitido en materia de protección de datos, al igual que sus modificaciones o reglamentos existentes.

Derivado de la identificación individual sobre el funcionamiento legal de la figura del Profesional de Privacidad, que cabe decir, es de reciente incorporación en el ámbito nacional e internacional, el autor logra corroborar la ausencia de profesionales que se encuentren calificados por una Autoridad de Protección de Datos Personales en el cumplimiento de la norma.

Tal y como se expresa en la obra presentada, el autor hace hincapié en una ausencia de Profesionales de Privacidad que se encuentren certificados por un ordenamiento de ley que corroboré dicha capacidad. A manera que, el lector podrá leer en dichas páginas la problemática que se discute al no contar con profesionales, razón que basta con ser suficiente para llegar a tener efectos negativos en el derecho humanos a la protección de datos.

En lo que respecta, un caso sobresaliente del cual Barco Vega precisa es el estado actual de México, puesto que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en su papel crucial para la democracia, se ha valido del ejercicio pleno en el cumplimiento de dichas tareas como lo es la publicación de las "Recomendaciones para la Designación de la Persona o Departamento de Datos Personales" en lo que respecta al sector privado.

En este orden de ideas, pese a que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece en el sector público que se podrá designar a un oficial de protección de datos que cumpla las demandas, sigue habiendo modificaciones en la ley, como la del pasado 25 de febrero de 2022 donde los Lineamientos Generales de Protección de Datos Personales para el Sector Público y al Estatuto Orgánico del INAI obtuvieron modificaciones con el fin de establecer un esquema de certificación como Oficial de Protección de Datos Personales.

Como resultado de las mencionadas modificaciones, así como otras tantas que el autor menciona entre páginas, se puede intuir que en posibles fechas futuras el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) presente un esquema de certificación de la que se ha venido hablando. De ser el tema, México llegaría a convertirse en el primer país en América Latina en contar con el nivel estándar de certificación para aquellos profesionales que aspiren a convertirse en Profesionales de Privacidad u Oficiales de Protección de Datos, esquema que actualmente se encuentra vigente en países de la unión europea como lo son España y Francia.

La visión del autor consta de un desafío que países en América Latina tienen en común que es la de identificar de ma-

nera legal una figura propia en el ámbito de la privacidad. Derecho que sobra decir, se tiene que adaptar a una sociedad que se encuentra en constante cambio y, a la cual, las leyes deben estar a la disposición de lo que la ciudadanía disponga.

De esta forma, el INAI y su Comité Editorial refrendan el compromiso con la sociedad y ponen a su disposición, estimadas y estimados lectores, la obra "La Figura del Profesional de Privacidad en Latinoamérica. Estados actuales y principales desafíos para su adecuada operación", que confiamos será de interés para sectores académicos y expertos en protección de datos personales.

No obstante, a lo largo de las páginas, encontrará que la narrativa con la que se encuentra escrito el texto logra un lenguaje amigable derivado de una estrategia para que cualquier ciudadano se pueda acerca a temas relacionados en materia de transparencia y protección de datos.

Confiamos que la obra expuesta contribuirá en su acervo en vista de su lograda materialización en temas de importancia en común para la sociedad, como lo son las libertades informativas y su alcance en distintas regiones a lo largo América Latina.

Comité Editorial del INAI

Introducción

Escribir sobre la regulación vigente y propuestas para la adecuada operación de la Figura del Profesional de Privacidad en Latinoamérica no es una empresa sencilla. Ya desde el título de esta obra el lector podrá advertir la complejidad del objetivo de referirse a múltiples regulaciones y a un desafío común: identificar el funcionamiento legal y práctico de la Figura del Profesional de Privacidad en Latinoamérica.

Al encontrar diversas denominaciones normativas sobre el término, se ha elegido por su practicidad y ágil lectura la denominación "Profesional de Privacidad" (no obstante, como el lector advertirá en esta obra la denominación más propicia pudiera resultar la de "Profesional de Protección de Datos") para referirse al rol de la persona física que en el interior de una organización pública o privada sujeta al cumplimiento de la normatividad de protección de datos, entre otras, tiene la responsabilidad de asesorar al responsable respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.[1] Denominación que, como el lector apreciará, de acuerdo con el entorno normativo del que se trate, puede asimilarse con la del Oficial de Protección de Datos Personales (OPDP), el Delegado de Protección de Datos (DPD también conocido en inglés, *Data Protection Officer*) o la persona responsable de privacidad en una determinada organización.[2]

Para comprender el estado de maduración de la adopción de la Figura del Profesional de Privacidad en América Latina y los desafíos que enfrenta su adecuada operación se realiza un breve estudio sobre su origen, necesidad, funciones e importancia práctica acompañado de ciertos datos que denotan la necesidad de su promoción en la región y otras latitudes.

El estudio normativo sobre la Figura del Profesional de Privacidad resulta un componente fundamental de este documento, pues, será a partir del análisis de las distintas disposiciones legales vigentes en la región que se identificará la necesidad legal de su adopción y, en consecuencia, la de formar, preparar y capacitar a profesionales de distintos ámbitos para que desarrollen las funciones de un Profesional de Privacidad tanto en organizaciones públicas como privadas, así como su regulación y la existencia de esquemas de certificación en la materia.

Una vez identificada la regulación vigente que ordena la instauración de la Figura del Profesional de Privacidad en las organizaciones se analizan los retos que, a juicio del autor, existen para la adecuada operación de esta en las jurisdicciones analizadas, y particularmente en el caso de México.

La metodología de investigación utilizada para la elaboración de esta obra incluye la revisión de la literatura sobre la Figura del DPD y el análisis de instrumentos legales, jurisprudenciales, guías y directrices emitidas por autoridades de control y órganos consultivos, así como la aplicación de los métodos deductivo, inductivo y analítico.

Notas al pie

Al respecto los EPDP señalan:
39.4. El oficial de protección de datos personales tendrá, al menos, las siguientes funciones:
1. Asesorar al responsable respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.
2. Coordinar al interior de la organización del responsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.
Supervisar al interior de la organización del responsable el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

[2] Para efectos prácticos en esta obra se emplearán de forma indistinta las expresiones “DPO”, “DPD” para referirse al Profesional de Privacidad en cualquier de sus manifestaciones.

Planteamiento del problema

El derecho a la protección de datos personales[1], como su propia denominación lo indica, es "un derecho inherente al ser humano directamente engarzado con la dignidad y la libertad de la persona, cuya distinción frente a otro tipo de derechos coetáneos como la intimidad y la privacidad, radica no solamente en una delimitación conceptual, sino en una demarcación ontológica de la cual se derivan el contenido y alcance de este derecho humano que concede a la persona un amplio espectro de protección sobre su información personal".[2] Además, "el derecho a la protección de datos personales es ambivalente, por un lado, representa un derecho humano y por el otro una obligación de los particulares y/o administraciones públicas que dan tratamiento[3] a los datos personales". [4]

En suma, cuando hablamos del derecho a la protección de datos personales decimos que se trata de "el derecho humano que protege a la persona física identificada o identificable frente al tratamiento ilícito de sus datos personales, otorgándole -en la medida de lo posible dado el actual estado de la técnica- la facultad de decidir y controlar de manera libre e informada las condiciones y características del tratamiento de sus datos personales, permitiéndole además el ejercicio de determinados derechos y medios de tutela jurídicos para garantía y eficacia práctica de estos últimos."[5]

Notas al pie

1. En relación con la definición del derecho a la protección de datos personales en México, recomendamos consultar: Davara F. de Marcos, Isabel, *Protección de datos personales*, en Derechos del Pueblo Mexicano, México a través de sus constituciones, México, Miguel Ángel Porrúa, 2016, pp. 567-581.
2. Vid, Barco Vega, Gregorio, *El derecho humano a la protección de datos personales en México*, Actas del III Coloquio Internacional de Investigadores en Derecho, España, Revista Jurídica de la Universidad de León, núm. 3, 2016, p. 145, Disponible en https://centros.unileon.es/derecho/files/2018/02/Revista-Juridica-ULE-num-3.pdf
3. En este sentido, vale la pena señalar que este concepto normativamente es definido por la LFDPPPP como "la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio". Asimismo, la citada norma precisa que, el uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.
Recomendamos consultar la voz "Tratamiento" del Diccionario de Protección de Datos Personales publicado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) disponible en Isabel Davara F. de Marcos (Coord.), México, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2020, disponible en http://inicio.inai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf
4. Barco, Gregorio, op.cit, p. 145, nota 4.
5. Vid, definición de "Protección de datos personales" escrita por Isabel Davara, Alexis Cervantes y Gregorio Barco en Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Isabel Davara F. de Marcos (Coord.), Diccionario de Protección de Datos Personales, México, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2020, p. 687, disponible en http://inicio.inai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf

En la actualidad la protección de la persona frente al tratamiento ilícito de sus datos es más que necesaria, pues, los numerosos tratamientos de datos que ocurren si no se gestionan de forma adecuada pueden materializarse en riesgos y afectaciones para los derechos y libertades fundamentales de las personas. De ahí la necesidad de contar con una normativa especializada que imponga límites a los particulares y al gobierno frente a la ingente y descontrolada recolección de datos. Por ejemplo, en el panorama jurídico mexicano, "el derecho a la protección de datos personales es más que una simple prerrogativa de la que gozan las personas, es un derecho humano (denominación derivada del artículo 1 constitucional)"[6][7] reconocido de manera específica en el párrafo segundo del artículo décimo sexto constitucional[8] "otorgando a las personas la más amplia protección legal sobre sus datos personales con independencia del tipo de tratamiento al que pudieran ser sometidos sus datos personales, ya sea por un sujeto de derecho público o de derecho privado".[9]

No obstante, en la práctica, la protección de los datos personales se ha vuelto una tarea cada vez más compleja e importante para las personas y las organizaciones públicas y privadas que llevan a cabo el tratamiento de datos personales. Por un lado, el tratamiento de datos personales deviene en una actividad imprescindible para el cumplimiento de diversos fines perseguidos por parte de sujetos de naturaleza pública y privada. De ahí que, incluso, se piense que los datos pueden ser considerados como un recurso, al igual que el petróleo (hay quien a dicho que los datos son el nuevo petróleo)[10] y se asuma que

Notas al pie

6. Ibidem, p. 688.
Al respecto, el último párrafo del artículo 1 constitucional señala:
(...)
7. Queda prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas.
8. Artículo 16.
(…)
Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.
(…)
9. Vid, Davara Isabel et al., op.cit, p. 693, nota 7.
10. Kiran Bhageshpur, *Data Is The New Oil -- And That's A Good Thing*, Forbes, 2019, disponible en https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/#29aa27157304

estos pueden comercializarse a partir de un acuerdo de voluntades. Sin embargo, cierto es que en la práctica la Ley impone límites bastante concretos al uso y recolección de datos, situación que en la práctica puede inhibir o restringir determinados negocios cuando estos no pasan *el test* de legalidad.

Como lo ha señalado Giovanni Buttarelli, designado Supervisor Europeo de Protección de Datos (SEPD) en 2014, en el manifiesto de privacidad con miras a 2030 "datos significa poder".[11] En palabras de este ombudsman de "los datos personales, el poder de los datos personales implica la capacidad de recopilar información sobre las personas, hacer inferencias a partir de esa información y, a su vez, obtener valor de esta, ya sea en forma de ganancia comercial o la capacidad de moldear y coaccionar el comportamiento humano".[12] Frente a la poderosa capacidad de las empresas presentes en el mundo digital para recopilar y usar datos personales deviene imprescindible dotar a las personas de garantías de protección.

Cuando nos enfrentamos a esta realidad, resulta imprescindible considerar además el contexto en el que ocurre el tratamiento de los datos pues, el día de hoy las condiciones en las que este se gesta son sofisticadas e impredecibles como resultado de la omnipresencia del internet y la incursión de tecnologías emergentes como la inteligencia artificial ("IA")[13], el aprendizaje de máquinas o *machine learning, el Big Data*[14], el Internet de las Cosas ("IoT" por sus siglas en inglés) por sus siglas en inglés) entre otras.

Por ello, "la normatividad de protección datos personales en México y otras jurisdicciones por supuesto, se centra en proteger al

Notas al pie

11. International Association of Privacy Professionals (IAPP), Privacy 2030, A vision for Europe, noviembre de 2019, disponible en https://iapp.org/media/pdf/resource_center/giovanni_manifesto.pdf
12. Ídem
13. El concepto de IA fue mencionado por primera vez en 1956 por John McCarthy durante una conferencia sobre la inteligencia de las computadoras con la participación de diversos científicos, como M. Minsky, C. Shannon, A. Newell, y H. Simon. Frecuentemente, se relaciona con la habilidad de tomar una buena decisión incluso cuando existe inseguridad, vaguedad o demasiada información que manejar. No obstante, a la fecha, como sucede con muchos conceptos, no existe un consenso sobre cuál debe ser su alcance y contenido.
14. Recomendamos consultar la voz "Big Data" del Diccionario de Protección de Datos Personales publicado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), México, 2020, disponible en http://inicio.inai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf

individuo contra el tratamiento ilícito de sus datos personales" [15] y a otorgarle control sobre el uso y destino de estos. Esto significa que los tratamientos de datos que existen en la actualidad ya sean realizados por un particular o las administraciones públicas no pueden permanecer ajenas al cumplimiento de determinadas prescripciones jurídicas que sustentan la tutela del derecho humano a la protección de datos personales en México y en cualquier otra jurisdicción que contemple dicha protección legal.

Sin embargo, dado que las normas no avanzan al mismo tiempo que la tecnología, garantizar esta protección entraña más que un adecuado conocimiento de la Ley implica la adopción de un enfoque de "cumplimiento proactivo y demostrable" que permita proteger los derechos de las personas a la par que se permite el flujo de datos y las actividades comerciales. Esto pareciera sencillo pero en la práctica es una actividad sumamente compleja que debe ir acompañada de diversos elementos, un conocimiento claro de la normatividad aplicable, de los tratamientos existentes en la organización, las capacidades de la organización, las tendencias en la industria o el sector de actividad de la organización, las mejores prácticas internacionales y por supuesto, una identificación apriorística de los riesgos que un determinado tratamiento puede suponer para los derechos y libertades fundamentales de las personas.[16] Dichas actividades y muchas otras son el centro de la actividad del Profesional de Privacidad en las organizaciones.

Notas al pie

15. Davara Abogados, *Cómo garantizar la protección de los datos personales, Guía Auxiliar para diagnosticar y cumplir con la legislación en la materia al interior de una organización*, México, Revista IDC Asesor Jurídico y Fiscal, septiembre de 2017, p.1.

16. Por ejemplo, en este sentido el considerando 75) del RGPD indica:

...

75) Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

...

El rol del Profesional de Privacidad no es para nada banal. Asumir el cargo de Profesional de Privacidad o DPO en una determinada organización es una responsabilidad mayúscula, pues, la adecuada gestión de las funciones del DPO tendrán consecuencias concretas tanto en la gestión del negocio como en los derechos humanos de las personas. De ahí que la persona designada como DPO deba ser un profesional con determinadas cualificaciones profesionales objetivamente verificadas y que habrán de comprobarse en el quehacer cotidiano de este. El Profesional de Privacidad tiene un rol de importancia innegable en la organización y también un compromiso ético con las personas que son titulares de los datos personales que serán materia de tratamiento.

Por tanto, la premisa que se sostiene en esta obra es que en un contexto como el actual, cada organización involucrada en el tratamiento de datos personales debiera tener un Profesional de Privacidad, incluso en aquellos casos en los que la normatividad no precisa tal requisito de forma expresa, pues, la asignación de una persona a las actividades de Profesional de Privacidad tendrá un efecto colateral en el entorno normativo, la defensa del Estado de Derecho y, por supuesto, en la tutela derecho a la protección de datos personales. La incursión de esta figura en aquellos casos en los que la Ley no prevé su implementación incluso puede considerarse como un elemento aleccionador en las organizaciones para la defensa del derecho a la protección de datos y como se mencionó previamente para demostrar el cumplimiento de la Ley de forma proactiva y continúa.

Finalmente, cabe señalar que la garantía de los derechos humanos, incluido el de protección de datos, debe regirse por el principio de progresividad, en el entendido de que el disfrute de los derechos siempre debe mejorar y, por tanto, resulta exigible a todas las autoridades del Estado mexicano, en el ámbito de su competencia, incrementar el grado de tutela en la promoción, respeto, protección y garantía de los derechos humanos. [17]

Notas al pie

17. Vid, tesis de jurisprudencia 2a./J. 35/2019 (10a.) con rubro PRINCIPIO DE PROGRESIVIDAD DE LOS DERECHOS HUMANOS. SU NATURALEZA Y FUNCIÓN EN EL ESTADO MEXICANO, publicada en la Gaceta del Semanario Judicial de la Federación, Libro 63, Febrero de 2019, Tomo I, página 980.

De esta suerte es que, debe considerarse que la visualización del derecho a la protección de datos personales bajo el tamiz de la progresividad implica concretamente la necesidad de promover la Figura del Profesional de Privacidad en las organizaciones tanto públicas como privadas del país, pues la adecuada gestión de tratamientos y la preparación de profesionales especialmente capacitados en esta materia permitirá coadyuvar a la tutela del derecho humano a la protección de datos en México. Por supuesto, este razonamiento, como se explicará en la obra, resultará aplicable también a otras jurisdicciones en las que este derecho tiene el carácter de derecho humano o derecho fundamental.

A pesar de que existe una necesidad práctica y legal de contar con numerosos Profesionales de Privacidad en diversos países de la región, en las diversas jurisdicciones que cuentan con leyes de protección de datos la cantidad de Profesionales de Privacidad que existen no ha sido cuantificada y tampoco se conoce la cantidad de especialistas requeridos para cumplir con las obligaciones previstas en las leyes aplicables. De lo que no cabe duda es que en la región esta figura, debido a la reciente incursión de normas basadas en el esquema europeo donde se ha establecido ya este requerimiento de manera formal, se encuentra en una etapa inicial y no ha madurado lo suficiente como lo ha hecho en el entorno europeo. No obstante, se puede advertir que, dado que existen normativas especializadas en protección de datos que ordenan contar con un Profesional de Privacidad en cada organización, y a la fecha, no existen mecanismos objetivos de evaluación, selección y capacitación de dichos, es innegable que la cantidad de Profesionales de Privacidad existente también es escasa.

Además, existe otro problema que es la difícil determinación del número de Profesionales de Privacidad requeridos por país y en la región en general, pues a la fecha no existe un censo oficial por país y muchos menos regional sobre la cantidad de Profesionales de Privacidad existentes en cada país y aquellos que se requieren. Dicho contexto es preocupante, en particular, en aquellas jurisdicciones en las que existe un requerimiento normativo expreso de contar con dicha figura.

En la región existe un déficit de Profesionales de Privacidad. Mientras que las leyes ordenan instaurar un Profesional de Priva-

cidad, la existencia de dichos perfiles es limitadísima pues se requiere en muchos casos, crear dicha posición, asignar recursos, capacitar al personal y por supuesto, designar a la persona que asumirá dicho cargo.

En síntesis, en esta obra sostenemos la tesis de que en México y Latinoamérica existe un déficit de Profesionales de Privacidad, una ausencia de datos sobre la cantidad de profesionistas requeridos y aquellos presentes en cada jurisdicción. Dicha situación sin duda tiene efectos en la garantía del derecho a la protección de datos, pues si no existen profesionales encargados de vigilar el cumplimiento de la normativa y apoyar en su interpretación y aplicación a las organizaciones la tutela del derecho a la protección de datos personales puede verse comprometida.

Sobre la Figura del Profesional de Privacidad

En este capítulo se realizará una breve descripción sobre la Figura del Profesional de Privacidad con el propósito de comprender el estado de maduración de la adopción de dicha posición en América Latina y los desafíos que enfrenta su adecuada operación.

De este modo se realiza una sucinta descripción sobre el origen, necesidad, funciones y responsabilidades, perfil, posición y certificación acompañando ciertos datos que denotan la necesidad de su promoción en la región. La delimitación conceptual sobre la Figura del Profesional de Privacidad se sustentará en el régimen europeo de protección de datos, los EPDP y las previsiones legales existentes en México por ser el caso de inmediata aplicación. Este apartado será la base del entendimiento de la Figura del Profesional de Privacidad en México y Latinoamérica.

Origen

La Figura del Profesional de Privacidad es de reciente incorporación en las normativas de protección de datos personales. Esta tiene origen en la Ley Alemana de Protección de Datos desde hace tiempo ordena su designación.[1] Incluso en países europeos en los que de forma previa a la emisión del Reglamento General de Protección de Datos ("RGPD")[2] su designación ya estaba prevista en países como Austria, Noruega[3] y Francia, bien en este último era algo facultativo.[4]

Notas al pie

1. Los términos alemanes son, respectivamente: behördliche- y betrieblicheDatenschutzbeauftragter. Para obtener un breve resumen de su papel y funciones según la ley alemana consulte, por ejemplo: https://www.wbs-law.de/eng/practice-areas/internet-law/it-law/data-protection-officer/
2. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE), Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679
3. Al respecto, la Encuesta al Delegado de Protección de Datos Sobre las condiciones laborales de los Delegados de Protección de Datos y el cumplimiento de la legislación de protección de datos en las empresas noruegas publicada en septiembre 2021 por la autoridad noruega de protección de datos (Datatilsynet en noruego), señala que "el sistema de Oficial de Protección de Datos (DPO) existe en Noruega desde 2001, pero con la implementación del RGPD, el contenido de esta función se ha ampliado significativamente."
4. Vid, "The DPO Handbook, Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, (Regulation (EU) 2016/679), elaborado por the EU-funded "T4DATA" programme, (Grant Agreement number: 769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01), Disponible en https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf

Fue en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante "Directiva 95/46/CE")[5] bajo la denominación de "encargado de la protección de datos" que se previó por vez primera la figura de la persona encargada de la protección de datos y que podemos entender como una versión primigenia de lo que hoy es el Profesional de Privacidad. Al respecto, el considerando 54 de la Directiva aludida precisó:

> *"(54) Considerando que, a la vista de todos los tratamientos llevados a cabo en la sociedad, el número de los que presentan tales riesgos particulares debería ser muy limitado; que los Estados miembros deben prever, para dichos tratamientos, un examen previo a su realización por parte de la autoridad de control o del encargado de la protección de datos en cooperación con aquélla; que, tras dicho control previo, la autoridad de control, en virtud de lo que disponga su Derecho nacional, podrá emitir un dictamen o autorizar el tratamiento de datos; que este examen previo podrá realizarse también en el curso de la elaboración de una medida legislativa aprobada por el Parlamento nacional o de una medida basada en dicha medida legislativa, que defina la naturaleza del tratamiento y precise las garantías adecuadas;"*

Sin embargo, la Directiva 95/46/CE no exigía de forma expresa a ninguna organización la designación de lo que hoy se denomina Delegado de Protección de Datos (DPD) en el RGPD.

Es decir, la Directiva 95/46/CE aunque no ordenaba designar un DPD reconoció su existencia en la legislación y la práctica de los Estados miembros en su artículo 18[6], al permitir que los Estados miembros eximieran a los responsables del tratamiento de la obligación de notificar las operaciones de trata-

Notas al pie

5. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=ES

6. Artículo 18
Obligación de notificación a la autoridad de control

miento a la autoridad de control competente, si la legislación del Estado miembro exigía que el responsable del tratamiento designara un encargado de protección de los datos personales con las siguientes atribuciones:

- Hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la Directiva.

- Llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información enumerada en el apartado 2 del artículo 21 de la Directiva señalada[7], garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados.

De igual manera, la Directiva 95/46/CE hacía referencia a la figura del encargado de protección de los datos personales en su artículo 20 referente a los controles previos, atribuyendo a este la función de realizar comprobaciones sobre tratamientos de alto riesgo y notificarlas a la autoridad de control competente.[8]

Notas al pie

1. Los Estados miembros dispondrán que el responsable del tratamiento o, en su caso, su representante, efectúe una notificación a la autoridad de control contemplada en el artículo 28, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos, total o parcialmente automatizados, destinados a la consecución de un fin o de varios fines conexos.
2. Los Estados miembros podrán disponer la simplificación o la omisión de la notificación solo en los siguientes casos y con las siguientes condiciones:
- cuando para las categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados habida cuenta de los datos a que se refiere el tratamiento, los Estados miembros precisen los fines de los tratamientos, los datos o categorías de datos tratados, la categoría o categorías de los interesados, los destinatarios o categorías de destinatarios a los que se comuniquen los datos y el período de conservación de los datos y/o
- cuando el responsable del tratamiento designe, con arreglo al Derecho nacional al que está sujeto, un encargado de protección de los datos personales que tenga por cometido, en particular:
- hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la presente Directiva,
- llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información enumerada en el apartado 2 del artículo 21, garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados.

7. Artículo 21
Publicidad de los tratamientos
1. Los Estados miembros adoptarán las medidas necesarias para garantizar la publicidad de los tratamientos.
2. Los Estados miembros establecerán que la autoridad de control lleve un registro de los tratamientos notificados con arreglo al artículo 18.
En el registro se harán constar, como mínimo, las informaciones a las que se refieren las letras a) a e) del apartado 1 del artículo 19.
El registro podrá ser consultado por cualquier persona.
3. Los Estados miembros dispondrán, en lo que respecta a los tratamientos no sometidos a notificación, que los responsables del tratamiento u otro órgano designado por los Estados miembros comuniquen, en la forma adecuada, a toda persona que lo solicite, al menos las informaciones a que se refieren las letras a) a e) del apartado 1 del artículo 19.
Los Estados miembros podrán establecer que esta disposición no se aplique a los tratamientos cuyo fin único sea llevar un registro, que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo.

8. Artículo 20

El Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (en adelante "Reglamento 45/2001)[9], exigía en su artículo 24 que cada institución u organismo de la UE designara al menos un Responsable de la Protección de Datos ("RPD") con las siguientes funciones:

- Garantizar que los responsables del tratamiento y los interesados sean informados de sus derechos y obligaciones de conformidad con el presente Reglamento;
- Responder a las solicitudes del SEPD y, en el marco de sus

Notas al pie

Controles previos
1. Los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados y velarán por que sean examinados antes del comienzo del tratamiento.
2. Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos quien, en caso de duda, deberá consultar a la autoridad de control.
3. Los Estados miembros podrán también llevar a cabo dicha comprobación en el marco de la elaboración de una norma aprobada por el Parlamento o basada en la misma norma, que defina el carácter del tratamiento y establezca las oportunas garantías.
9. Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32001R0045&qid=1669543394844&from=EN
10. SECCIÓN 8: RESPONSABLE DE LA PROTECCIÓN DE DATOS
Artículo 24
Nombramiento y funciones del responsable de la protección de datos
1. Cada institución y cada organismo comunitario nombrarán al menos a una persona para que actúe como responsable de la protección de datos encargado de:
a) garantizar que los responsables del tratamiento y los interesados sean informados de sus derechos y obligaciones de conformidad con el presente Reglamento;
b) responder a las solicitudes del Supervisor Europeo de Protección de Datos y, en el marco de sus competencias, cooperar con el Supervisor Europeo de Protección de Datos a petición de éste o por iniciativa propia;
c) garantizar de forma independiente la aplicación interna de las disposiciones del presente Reglamento;
d) llevar el registro de aquellas operaciones de tratamiento realizadas por el responsable del tratamiento, el cual contendrá la información a que se refiere el apartado 2 del artículo 25;
e) notificar al Supervisor Europeo de Protección de Datos las operaciones de tratamiento que pudieran presentar riesgos específicos con arreglo al artículo 27.
Dicha persona deberá velar por que el tratamiento no tenga efectos adversos sobre los derechos y las libertades de los interesados.
2. El responsable de la protección de datos será seleccionado en razón de sus cualidades personales y profesionales y, en particular, de su experiencia en la protección de datos.
3. La elección del responsable de la protección de datos no deberá poder derivar en un conflicto de intereses entre su función de responsable y otras obligaciones profesionales, en particular en relación con la aplicación de las disposiciones del presente Reglamento.
4. El responsable de la protección de datos será nombrado por un mandato de entre dos y cinco años. Su mandato podrá ser renovado; no obstante, la duración total de su mandato no podrá ser superior a diez años. El responsable de la protección de datos solo podrá ser destituido de su función de responsable de la protección de datos por la institución u organismo comunitario que le haya nombrado, previo consentimiento del Supervisor Europeo de Protección de Datos, en caso de que deje de cumplir las condiciones requeridas para el ejercicio de sus funciones.
5. Tras haber nombrado al responsable de la protección de datos, la institución o el organismo que le haya designado comunicará su nombre al Supervisor Europeo de Protección de Datos.
6. La institución u organismo comunitario que le haya designado asignará al responsable de la protección de datos el personal y los recursos necesarios para la ejecución de sus funciones.
7. El responsable de la protección de datos no aceptará instrucciones de nadie respecto del ejercicio de sus funciones.
8. Cada institución u organismo comunitario adoptará normas complementarias respecto al responsable de la protección de datos, con arreglo a lo dispuesto en el anexo. Tales normas se referirán, en concreto, a las tareas, obligaciones y competencias del responsable de la protección de datos

competencias, cooperar con el SEPD a petición de este o por iniciativa propia;

- Garantizar de forma independiente la aplicación interna de las disposiciones del Reglamento 45/2001;
- Llevar el registro de aquellas operaciones de tratamiento realizadas por el responsable del tratamiento, el cual contendrá la información a que se refiere el apartado 2 del artículo 25 del Reglamento 45/2001;
- Notificar al SEPD las operaciones de tratamiento que pudieran presentar riesgos específicos con arreglo al artículo 27.
- Velar por que el tratamiento no tenga efectos adversos sobre los derechos y las libertades de los interesados.

En esa misma línea, el apartado segundo del artículo 24 del Reglamento 45/2001 señalaba que "el responsable de la protección de datos será seleccionado en razón de sus cualidades personales y profesionales y, en particular, de su experiencia en la protección de datos".[11] Mientras que el párrafo 7 hacía referencia a su independencia.[12] Las normas sobre los RPD de las instituciones de la UE previstas en el Reglamento 45/2001 tienen un alto grado de similitud con aquellas previstas en el actual RGPD y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (en adelante "Directiva 2016/680").[13]

Notas al pie

11. SECCIÓN 8
RESPONSABLE DE LA PROTECCIÓN DE DATOS Artículo 24
Nombramiento y funciones del responsable de la protección de datos
...
2. El responsable de la protección de datos será seleccionado en razón de sus cualidades personales y profesionales y, en particular, de su experiencia en la protección de datos.
...

12. Para mayor información sobre la figura del RPD adoptada en Europa conforme al Reglamento 45/2011 se puede consultar el Reporte titulado *Monitoring compliance of EU institutions and bodies with Article 24 of Regulation (EC) 45/2001, Report on the Status of Data Protection Officers* elaborado por el Supervisor Europeo de Protección de Datos elaborado en diciembre de 2012 y que se encuentra en https://edps.europa.eu/data-protection/our-work/publications/reports/report-status-data-protection-officers-dpos_en

De esta suerte se puede advertir que el concepto de Profesional de Privacidad o DPD en el entorno europeo no es nuevo. No obstante, aunque la Directiva 95/46/CE no determinaba la obligatoriedad de designar un DPD a ninguna organización, "en la práctica, como señala el Grupo de Trabajo sobre Protección de Datos del Artículo 29 (ahora Comité Europeo de Protección de Datos o "CEPD"), tal designación se desarrolló en varios Estados miembros a lo largo de los años".[14]

Al respecto el órgano consultivo en materia de protección de datos en la UE de forma previa a la adopción del RGPD ya señalaba que el DPD "es la piedra angular de la rendición de cuentas y que el nombramiento de un DPD puede facilitar el cumplimiento y, además, convertirse en una ventaja competitiva para las empresas."[15]

Necesidad

¿Por qué son necesarios los Profesionales de Privacidad? Este es el planteamiento principal que se hacen múltiples organizaciones obligadas a observar la normatividad de protección de datos. La respuesta no es sencilla y tampoco puede tener un carácter unívoco. Sin embargo, del contenido de los ya derogados Directiva 95/46/CE y Reglamento 45/2001 se advierte que la incursión de esta figura se consideraba necesaria para hacer aplicar la normativa de protección de datos existente en ese entonces.

Notas al pie

13. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, Disponible en https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32016L0680

14. El GTA 29 ha señalado al respecto: ..." El concepto de DPD no es nuevo. Aunque la Directiva 95/46/CE3 no exigía a ninguna organización el nombramiento de un DPD, la práctica de tal designación se ha desarrollado, no obstante, en varios Estados miembros a lo largo de los años." Vid, Grupo de Trabajo sobre Protección de Datos del Artículo 29, "Directrices sobre los delegados de protección de datos (DPD)", Adoptadas el 13 de diciembre de 2016, Revisadas por última vez y adoptadas el 5 de abril de 2017, p.4, disponibles en https://www.aepd.es/es/documento/wp243rev01-es.pdf

15. Citado en Grupo de Trabajo sobre Protección de Datos del Artículo 29, "Directrices sobre los delegados de protección de datos (DPD)", Adoptadas el 13 de diciembre de 2016, Revisadas por última vez y adoptadas el 5 de abril de 2017, nota 4, p.4, disponible en https://www.aepd.es/es/documento/wp243rev01-es.pdf

Respecto de su necesidad podemos advertir en el considerando (97) del RGPD arroja información importante al señalar lo siguiente:

> *"(97) Al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial, si el tratamiento lo realiza en el sector privado un responsable cuyas actividades principales consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados, o si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. En el sector privado, las actividades principales de un responsable están relacionadas con sus actividades primarias y no están relacionadas con el tratamiento de datos personales como actividades auxiliares. El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente."*

Por su parte, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos ("EPDP") establecen en su considerando 23 lo siguiente:

> *"(23) Reconociendo la importancia de la adopción de medidas preventivas que permitan al responsable responder proactivamente ante los posibles problemas relacionados con el derecho a la protección de datos personales como son la adopción de esquemas de autorregulación vinculante o sistemas de certificación en la materia; la designación de un oficial de protección de datos personales; la elaboración de evaluaciones de impacto a la protección de datos personales y la privacidad por defecto y por diseño, entre otras, lo cual resulta esencial en el ámbito de las tecnologías de la información y las telecomunicaciones;"*

De acuerdo con lo anterior, se puede sostener que la incursión del DPD en una organización es necesaria con el objetivo de vigilar el cumplimiento de la normatividad de protección de datos en las organizaciones, así como responder proactivamente sobre su cumplimiento.

Perfil del Profesional de Privacidad

Conforme a lo previsto por el artículo 37, apartado 5 del RGPD, el DPD "será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39". Por su parte, el considerando 97 dispone que “el nivel de conocimientos especializados necesario se debe determinar en función de las operaciones de tratamiento de datos que se realicen y de la protección exigida para los datos personales tratados”.[16]

El RGPD no especifica las “cualidades profesionales” requeridas y el “conocimiento experto de la ley y las prácticas de protección de datos” del DPD. No obstante, organizaciones como el CIPL (Centre for Information Policy Leadership) recomiendan que la designación de DPD se base en los requisitos y necesidades específicos de una organización en términos de las habilidades y cualidades requeridas para cumplir el rol de DPD. [17]

A manera de ejemplo, vale la pena señalar que el Esquema de Certificación de Delegados de Protección de Datos de la Agen-

Notas al pie

16. (97) Al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial, si el tratamiento lo realiza en el sector privado un responsable cuyas actividades principales consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados, o si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. En el sector privado, las actividades principales de un responsable están relacionadas con sus actividades primarias y no están relacionadas con el tratamiento de datos personales como actividades auxiliares. El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente.

cia Española de Protección de Datos ("AEPD")[18] señala que "el DPD debe reunir conocimientos especializados del Derecho y la práctica en materia de protección de datos". De acuerdo con el citado esquema "se han identificado, en consecuencia, aquellos conocimientos, habilidades y destrezas necesarias que tiene que poseer la persona a certificar para llevar a cabo cada una de las funciones propias de la posición de DPD."[19]

Igualmente, el citado esquema indica que el DPD debe ser capaz de:

a) recabar información para determinar las actividades de tratamiento,
b) analizar y comprobar la conformidad de las actividades de tratamiento, e
c) informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
d) recabar información para supervisar el registro de las operaciones de tratamiento.
e) asesorar en la aplicación del principio de la protección de datos por diseño y por defecto.
f) asesorar sobre:

a. si se debe llevar a cabo o no una evaluación de impacto de la protección de datos qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa, qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados en el caso de alguna vulneración.

Notas al pie

17. Centre for Information Policy Leadership (CIPL), "Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation", CIPL GDPR Interpretation and Implementation Project, noviembre de 2016, Disponible en https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf
18. Agencia Española de Protección de Datos, Esquema de Certificación de Delegados de Protección de Datos, Redactado por el Área de Certificación de la Agencia Española de Protección de Datos 23 de diciembre 2019. Versión 1.4, p.13, Disponible en https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf
19. Idem

b. si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y

c. si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con la normatividad.

g) priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos.

h) asesorar al responsable del tratamiento sobre:

a. qué metodología emplear al llevar a cabo una evaluación de impacto de la protección de datos, qué áreas deben someterse a capacitaciones y auditoría de protección de datos interna o externa,

b. qué actividades de formación internas proporcionar al personal o los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.[20]

ISMS Forum indica que, "además del conocimiento especializado en materia de protección de datos, resulta crucial las habilidades o *soft skills* del DPD".[21] De acuerdo con el Libro Blanco del DPO publicado por ISMS Forum España[22] "estas habilidades metacompetencias tienen el denominador común de ser habilidades "transversales" e imprescindibles en cualquier DPD"[23] y que estas pueden ser de varios tipos:

- "**Introspectivas**: aprender a gestionar emociones, cambiar creencias limitadoras, identificar fortalezas y puntos de mejora, incrementar la auto-conciencia y el sentido de auto-eficacia.
- **Diagnósticas y de acción:** planteamiento y resolución de problemas, examen de los recursos disponibles, creatividad, capa-

Notas al pie

20. Ídem
21. ISMS Forum España, "El libro Blanco del DPO", p. 52, Disponible en https://www.ismsforum.es/ficheros/descargas/el-libro-blanco-del-dpo---isms-forum-y-data.pdf
22. Ídem
23. Ídem

cidad para afrontar situaciones nuevas y cambios profundos, flexibilidad, iniciativa, planificación, gestión del tiempo, etc.

- **Relacionales:** empatía, escucha activa, asertividad, comunicación eficaz, gestión de conflictos, negociación y consenso, gestión y trabajo en equipo y liderazgo." [24]

En el caso de México, los Lineamientos Generales de Protección de Datos Personales para el Sector Público ("LGPDPSP") al hacer referencia a la figura del Oficial de Protección de Datos ("OPD") señalan que este "deberá ser designado en atención a sus conocimientos, cualidades profesionales, experiencia en la materia, y en su caso a la o las certificaciones con que cuente en materia de protección de datos personales". [25]

El INAI en sus Recomendaciones para la Designación de la Persona o Departamento de Datos Personales señala "la persona que tenga a su cargo o bajo su responsabilidad la función de protección de datos personales en posesión de la organización del responsable deberá poseer experiencia en materia de protección de datos personales, tener jerarquía o posición indicada dentro de la organización, contar con recursos suficientes, contar con conocimiento en la materia, visión y liderazgo para implementar la política de privacidad a lo largo de la organización y habilidades de organización y comunicación". [26]

Funciones y responsabilidades

El RGPD establece en el primer apartado de su artículo 39 como funciones mínimas del DPD las siguientes:

Notas al pie

24. ISMS Forum España, *El libro Blanco del DPO*, Disponible en https://www.ismsforum.es/ficheros/descargas/el-libro-blanco-del-dpo---isms-forum-y-data.pdf

25. **Designación del oficial de protección de datos personales**
Artículo 121. Para aquellos responsables que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos relevantes o intensivos de datos personales a que se refieren los articulos 74 y, en su caso, 75 de la Ley General, podrán designar a un oficial de protección de datos personales, el cual formará parte de la Unidad de Transparencia.
La persona designada como oficial de protección de datos deberá contar con la jerarquia o posición dentro de la organización del responsable que le permita implementar políticas transversales en esta materia.
El oficial de protección de datos personales deberá ser designado atendiendo a sus conocimientos, cualidades profesionales, experiencia en la materia, y, en su caso, a la o las certificaciones con que cuente en materia de protección de datos personales.

26. INAI, Recomendaciones para la Designación de la Persona o Departamento de Datos Personales, Disponibles en https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/RecomendacionesDesignar.pdf

- "Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
- Cooperar con la autoridad de control;
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto." [27]

A manera ejemplificativa, vale la pena señalar que el Esquema de Certificación de Delegados de Protección de Datos de la AEPD indica que las funciones genéricas del DPD se pueden concretar en tareas de asesoramiento y supervisión, entre otras en las siguientes áreas:

- "Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.

Notas al pie

27. El Tribunal de Justicia de la Unión Europea en la sentencia del asunto C 453/21de fecha 9 de febrero de 2023 al referirse al posible conflicto de interés con motivo del ejercicio de funciones del DPD resolvió lo siguiente:

2) El artículo 38, apartado 6, del Reglamento 2016/679 debe interpretarse en el sentido de que puede existir un «conflicto de intereses», en el sentido de esta disposición, cuando se encomienden a un delegado de protección de datos otras funciones o cometidos que llevarían a este a determinar los fines y los medios del tratamiento de datos personales en el seno del responsable del tratamiento o de su encargado, lo que incumbe determinar en cada caso al juez nacional sobre la base de todas las circunstancias pertinentes, en particular de la estructura organizativa del responsable del tratamiento o de su encargado y a la luz de toda la normativa aplicable, incluidas las eventuales políticas de estos últimos.

Vid, Tribunal de Justicia de la Unión Europea, asunto C 453/21, 9 de febrero de 2023, , Disponible en https://curia.europa.eu/juris/document/document.jsf?text=&docid=270323&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=3046073

- Determinación de la existencia de normativa sectorial que pueda estipular condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de procedimientos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
- Identificación de los instrumentos para las transferencias internacionales de datos adecuados a las necesidades y características de la organización, y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditoría de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento.
- Análisis de riesgos de los tratamientos realizados.
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Realización de evaluaciones de impacto sobre la protección de datos.
- Relaciones con las autoridades de supervisión.

• Implantación de programas de formación y sensibilización del personal en materia de protección de datos.” [28]

Los EPDP en su numeral 39.4 precisan que el OPD tendrá funciones de asesoría, coordinación y supervisión al establecer lo siguiente:

> *“39.4. El oficial de protección de datos personales tendrá, al menos, las siguientes funciones:*
> *1. Asesorar al responsable respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.*
> *2. Coordinar, al interior de la organización del responsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.*
> *3. Supervisar al interior de la organización del responsable el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.”*

En relación con la designación del DPD en México, la normatividad del sector privado en su artículo 30 indica que “la persona designada por el responsable tendrá a su cargo la atención de los derechos de los titulares y fomentará la protección de datos personales en la organización.” [29]

Por otra parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (“LGPDPPSO”) indica en su artículo 85 que en el caso de que se designe un OPD, las funciones originalmente atribuidas a la Unidad de Transparencia serán realizadas por el OPD [30] y consistirán en:

• Notas al pie

29. Agencia Española de Protección de Datos, *Esquema de Certificación de Delegados de Protección de Datos*, Redactado por el Área de Certificación de la Agencia Española de Protección de Datos, pp. 14-15,
23 de diciembre 2019. Versión 1.4, p.13, Disponible en https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf
29. Artículo 30.- 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 a que se refiere la presente Ley. Asimismo fomentará la protección de datos personales al interior de la organización.

- "Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales.
- Gestionar las solicitudes para el ejercicio de los derechos ARCO.
- Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados.
- Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, de acuerdo con las normativas aplicables.
- Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.
- Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO.
- Asesorar a las áreas adscritas al responsable en materia de protección de datos personales."

Posición

En lo que concierne a la posición del Profesional de Privacidad el artículo 38 del RGPD prevé que en su párrafo primero la obligación del encargado y del responsable de que el DPD "participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales".[31] Asimismo, el párrafo segundo de dicho fundamento legal precisa que "el responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados".

Notas al pie

30. Artículo 85.

Los responsables que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos de datos personales relevantes o intensivos, podrán designar a un oficial de protección de datos personales, especializado en la materia, quien realizará las atribuciones mencionadas en este artículo y formará parte de la Unidad de Transparencia.

31. Artículo 38

La independencia del DPD se prevé en el párrafo 3 del artículo 38 del RGPD que obliga al responsable y al encargado a garantizar que el DPD "no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones, por lo que se señala que no podrá ser destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones y habrá de rendir cuentas directamente al más alto nivel jerárquico del responsable o encargado."[32]

Los EPDP en su numeral 39.3 coinciden con las disposiciones del RGPD al señalar lo siguiente:

> *"39.3. El responsable estará obligado a respaldar al oficial de protección de datos personales en el desempeño de sus funciones, facilitándole los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados y la actualización de éstos."*

En México, los LGPDPSP indican en su artículo 121, además de lo señalado en el artículo 85 de la LGPDPPSO, que "la persona designada como OPD deberá contar con la jerarquía o posición dentro de la organización del responsable que le permita implementar políticas transversales en esta materia". Así, se de-

Notas al pie

Posición del delegado de protección de datos
1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

32. El Tribunal de Justicia de la Unión Europea en la sentencia del asunto C 534/20 de fecha 22 de junio de 2022 al referirse a la posibilidad de que el responsable o encargado pueda despedir a un DP resolvió que:

"... el artículo 38, apartado 3, segunda frase, del RGPD debe interpretarse en el sentido de que no se opone a una normativa nacional que establece que un responsable o un encargado del tratamiento solo puede despedir a un delegado de protección de datos que forme parte de su plantilla por causa grave, aun cuando el despido no esté relacionado con el ejercicio de las funciones de dicho delegado, siempre que esa normativa no ponga en peligro la consecución de los objetivos del RGPD."

Vid, sentencia C 534/20 del 22 de junio de 2022, Disponible en https://curia.europa.eu/juris/document/document.jsf?text=&docid=261462&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=5284834
Además, en la sentencia del asunto C 453/21 el Tribunal reiteró el criterio anterior al resolver lo siguiente:

1) El artículo 38, apartado 3, segunda frase, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), debe interpretarse en el sentido de que no se opone a una normativa nacional que establece que un responsable o un encargado del tratamiento solo puede destituir a un delegado de protección de datos que forme parte de su plantilla por causa grave, aun cuando la destitución no esté relacionada con el desempeño de las funciones de dicho delegado, siempre que esa normativa no ponga en peligro la consecución de los objetivos de ese Reglamento.

Vid, Tribunal de Justicia de la Unión Europea, asunto C 453/21, 9 de febrero de 2023, Disponible en https://curia.europa.eu/juris/document/document.jsf?text=&docid=270323&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=3046073

talla que el OPD “deberá ser designado en atención a sus conocimientos, cualidades profesionales, experiencia en la materia, y en su caso a la o las certificaciones con que cuente en materia de protección de datos personales”.

Certificación

La Organización Internacional de Normalización (ISO) proporciona una definición de certificación entendida como un procedimiento mediante el cual "un organismo da garantía por escrito (certificado) de que el producto, servicio o sistema en cuestión cumple unos requisitos específicos". [33]

La Norma ISO/IEC ISO/IEC 17024 indica que el proceso de certificación hace referencia a “las actividades por las que un organismo de certificación determina que una persona cumple los requisitos de certificación, que incluyen la solicitud, la evaluación, la decisión de certificación, la renovación de la certificación y el uso de certificados y logotipos/marcas”.[34]

Por otro lado, la Norma EN-ISO/IEC 17000:2004 - Evaluación de la conformidad. Vocabulario y principios generales (a la que se refiere la norma ISO17065), la certificación se define como: "atestación[35] de un tercero... en relación a productos, procesos y servicios".[36]

Así, el Comité Europeo de Protección de Datos (CEPD) aclara que, “en el contexto de la certificación tal y como establecen los artículos 42 y 43 del RGPD, la certificación se entiende como la atestación de un tercero en relación a las operaciones de tratamiento de datos por parte de responsables y encargados del tratamiento.” [37]

Notas al pie

33. Citado por el Comité Europeo de Protección de Datos (CEPD) en las Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento, Versión 3.0, 4 de junio de 2019, Disponibles en https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_es.pdf

34. 3 Términos y definiciones
Para los fines de este documento, se aplican los términos y definiciones incluidos en la Norma ISO/IEC 17000 además de los siguientes.
3.1
proceso de certificación
las actividades por las que un organismo de certificación determina que una persona cumple los requisitos de certificación (3.3), que incluyen la solicitud, la evaluación, la decisión de certificación, la renovación de la certificación y el uso de certificados (3.5) y logotipos/marcas

35. La atestación es la «emisión de una declaración, con base en una decisión tomada después de la revisión, de que se ha demostrado que se cumplen los requisitos especificados». (Sección 5.2, ISO 17000:2004).

36. Disponible en https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-2:v2:es

En la práctica, como lo señala la AEPD "la certificación de personas es una herramienta adecuada y válida para la evaluación objetiva e imparcial de la competencia de un individuo para realizar una actividad determinada".[38] De acuerdo con el CIPL "la posesión de dicha certificación debe ser considerada como un activo por las instituciones/organismos de la UE al seleccionar su DPO".[39]

De la misma forma, como enfatiza el CEPD "los mecanismos de certificación pueden mejorar la transparencia para los interesados, pero también las relaciones entre empresas, por ejemplo, entre responsables del tratamiento[40] y encargados del tratamiento así como permitir a los interesados evaluar el nivel de protección de datos de los productos y servicios correspondientes".[41]

El 13 de mayo de 2022 Luxemburgo se convirtió en el primer país en introducir un mecanismo de certificación según los criterios del RGPD.[42] La Comisión Nacional de Protección de Datos (National Data Protection Commission en inglés) adoptó el mecanismo de certificación GDPR-CARPA.[43] Dicho mecanismo de certificación "certifica las operaciones de tratamiento específicas de una organización a fin de demostrar que sus actividades de procesamiento de datos cumplen con el RGPD".[44]

Notas al pie

37. Vid, Comité Europeo de Protección de Datos (CEPD) en las Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento, Versión 3.0, 4 de junio de 2019, p.9, Disponibles en https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_es.pdf

38. Agencia Española de Protección de Datos, Esquema de Certificación de Delegados de Protección de Datos, Redactado por el Área de Certificación de la Agencia Española de Protección de Datos
23 de diciembre 2019. Versión 1.4, p.4, disponible en https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf

39. Centre for Information Policy Leadership (CIPL), "Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation", CIPL GDPR Interpretation and Implementation Project, noviembre de 2016, Disponible en https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf

40. Comité Europeo de Protección de Datos (CEPD), Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento, Versión 3.0, 4 de junio de 2019, Disponibles en https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_es.pdf

41. El considerando (100) del RGPD señala:
(100) A fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes.

En octubre de 2022 el CEPD aprobó a *Europrivacy*[45] como Sello Europeo de Protección de Datos para la certificación de tratamientos de datos conforme a lo previsto por el párrafo quinto del artículo 42 del RGPD. Según información de la organización responsable "Europrivacy permite a las empresas evaluar y certificar formalmente el cumplimiento de su tratamiento de datos".[46] Bajo este esquema "los certificados de Europrivacy serán reconocidos formalmente en todos los Estados miembros de la UE y serán considerados por las autoridades de control de la protección de datos en caso de litigio".[47]

Además de los mecanismos anteriores, en Europa se han desarrollado diversos esquemas de certificación para DPO siendo uno de los más conocidos el Esquema de Certificación de Delegados de Protección de Datos[48] de la AEPD antes comentado[49] y el esquema de certificación de conocimientos y habilidades del DPO emitido por la *Commission nationale de l'informatique et des libertés (CNIL)* que es la autoridad francesa de protección de datos.[50]

Lo anterior, derivado de las previsiones del RGPD[51],en concreto de su artículo 42 cuyo párrafo primero señala que "los Estados miembros, las autoridades de control, el CEPD y la Comisión Europea promoverán, en particular a nivel de la UE, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimien-

Notas al pie

42. Hasta la fecha, la CNPD es la única autoridad de control europea que ha desarrollado un mecanismo de certificación del RGPD. Como entidad que ha desarrollado estos criterios de certificación, la CNPD es propietaria del mecanismo de certificación.
43. Para mayor información se puede consultar el sitio https://cnpd.public.lu/fr/professionnels/Certification.html
44. Información recuperada de la nota publicada por el CEPD con título "The CNPD adopts the certification mechanism GDPR-CARPA" y que se encuentra disponible en https://edpb.europa.eu/news/national-news/2022/cnpd-adopts-certification-mechanism-gdpr-carpa_en
45. Para mayor información se puede consultar el sitio https://europrivacy.com
46. Europrivacy nota de prensa "Europrivacy - El sello europeo de protección de datos RGPD aprobado por la UE, una nueva era para el cumplimiento con las normativas de privacidad y la protección de datos", 12 de octubre de 2022, Disponible en https://www.europrivacy.org/es/news/2022-10-14/europrivacy-gdpr-european-data-protection-seal-approved-eu-new-era-privacy-and-data
47. Ídem
48. De acuerdo con su descripción en el sitio web de la AEPD "Este esquema sigue los criterios internacionales de certificación de personas conforme a la norma ISO 17024 y las entidades de certificación acreditadas por ENAC otorgaran al profesional un certificado que implica un reconocimiento de que tiene las competencias adecuadas para el desarrollo de sus funciones de conformidad con el RGPD siempre y cuando con carácter previo cumpla con unos requisitos y supere un examen. Esta certificación de Delegados de Protección de Datos es voluntaria". Infomración disponible en https://www.aepd.es/es/preguntas-frecuentes/4-responsable-encargado-y-dpd/2-certificacion-de-dpd/FAQ-0418-que-es-la-certificacion-de-dpd
49. Agencia Española de Protección de Datos, Esquema de Certificación de Delegados de Protección de Datos, Redactado por el Área de Certificación de la Agencia Española de Protección de Datos, 23 de diciembre 2019. Versión 1.4, disponible en https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf

to de lo dispuesto en el RGPD en las operaciones de tratamiento de los responsables y los encargados".[52]

No obstante, en la práctica también es posible distinguir distintos mecanismos de certificación emitidos por otras organizaciones distintas de una autoridad de control como es el caso de las certificaciones de la International *Association of Privacy Professionals* ("IAPP" por sus siglas en inglés) que pudiera recibir una persona que desarrolla las funciones de DPO en una organización, entre ellas, la certificación "*Certified Information Privacy Professional*" (CIPP),[53] la certificación "*Certified Information Privacy Manager*" (CIPM),[54] la certificación "*Certified Information Privacy Technologists*" (CIPT)[55] y por supuesto la Certified Information Privacy Professional/Europe (CIPP/E Certification).[56]

A modo de ejemplo, se pueden mencionar como otras certificaciones relevantes para un DPO en el mundo las siguientes:

Notas al pie

50. De acuerdo con el documento "Practical Guide GDPR/Data Protection Officers emitido por la autoridad francesa de protección de datos (CNIL por sus siglas en francés) desde 2018, la CNIL ha aprobado organizaciones que emiten una certificación de habilidades de DPO sobre la base de su sistema de referencia y mantiene una lista de dichas organizaciones. Dichas organizaciones ofrecen una prueba, en forma de prueba de opción múltiple de al menos cien preguntas relacionadas con la regulación, la responsabilidad y la seguridad. Vid, CNIL, Certification scheme of DPO skills and knowledge, Disponible en https://www.cnil.fr/sites/default/files/atoms/files/cnil_certification-scheme-dpo-skills-and-knowledge.pdf

51. La certificación forma parte del Capítulo IV del RGPD relativo a obligaciones y responsabilidades del Responsable y encargado del tratamiento. Los artículos 42 y 43 establecen los objetivos, las garantías y las funciones de los actores junto con los principios generales para los procesos de certificación y acreditación.

52. Artículo 42, Certificación

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.
2. Además de la adhesión de los responsables o encargados del tratamiento sujetos al presente Reglamento, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el apartado 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento con arreglo al artículo 3 en el marco de transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra f). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.
3. La certificación será voluntaria y estará disponible a través de un proceso transparente.
4. La certificación a que se refiere el presente artículo no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes en virtud del artículo 55 o 56.
5. La certificación en virtud del presente artículo será expedida por los organismos de certificación a que se refiere el artículo 43 o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de conformidad con el artículo 58, apartado 3, o por el Comité de conformidad con el artículo 63. Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos.
6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación dará al organismo de certificación mencionado en el artículo 43, o en su caso a la autoridad de control competente, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.
7. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación.
8. El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

IAPP, Certified Information Privacy Professional, información disponible en https://iapp.org/certify

- Profesional certificado en seguridad de sistemas de información (CISSP): desarrollado para profesionales de seguridad de la información;[57]
- Certificación de Auditor Certificado de Sistemas de Información (CISA)[58]: desarrollado para profesionales de auditoría, control y seguridad de sistemas de información (SI);
- Certificación de Gerente Certificado de Seguridad de la Información (CISM)[59]: desarrollada para personas que administran, diseñan, supervisan y/o evalúan la seguridad de la información de una empresa.

En el ámbito regional encontramos la Certificación Internacional en Protección de Datos Personales 1 APEP-ALAP[60] de la Asociación Latinoamericana de Privacidad (ALAP) y la Asociación Profesional Española de Privacidad (APEP).

En el ámbito nacional aún no existe una certificación específica para DPD emitida y reconocida por la APDP (INAI). Sin embargo, el 25 de febrero de 2022 se publicaron modificaciones a los Lineamientos Generales de Protección de Datos Personales para el Sector Público (LGPDPSP) y al Estatuto Orgánico del INAI[61] con el propósito de "establecer las bases legales para el establecimiento de un esquema de certificación de Profesionales de Privacidad para el sector público". Derivado de esto, es probable que un futuro bastante próximo el INAI emita el primer esquema de certificación en esta materia y se convierta en la primera autoridad de protección de datos de la región en contar con un esquema de esta naturaleza.

Notas al pie

53. IAPP, Certified Information Privacy Professional, información disponible en https://iapp.org/certify/cipp/
54. IAPP, Certified Information Privacy Manager, información disponible en https://iapp.org/certify/cipm/
55. IAPP, Certified Information Privacy Technologists, información disponible en https://iapp.org/certify/cipt/
56. IAPP, Certified Information Privacy Professional/Europe, información disponible en https://iapp.org/certify/cippe/
57. Más información en https://www.isc2.org/Certifications/CISSP#
58. Más información en https://www.isaca.org/credentialing/cisa
59. Más información en https://www.isaca.org/credentialing/cism
60. https://www.alap.lat/certificacion/

Finalmente, en México NYCE, según la información de su sitio web,[62] emite las siguientes certificaciones de profesionales en relación con la protección de datos personales: auditor en Protección de Datos Personales – LFPDPPP; Profesional Certificado en Protección de Datos Personales (LFPDPPP) y Oficial de Protección de Datos Personales (Sujetos Obligados) (LGPDPPSO).[63] Estas certificaciones no son administradas por el INAI y todas, con excepción de la última, a la fecha, cuentan con la acreditación de la Entidad Mexicana de Acreditación (EMA).

La información anterior deja de manifiesto que en México aún no existe un esquema de certificación específicamente modelado para la autoridad en la materia, pero existen las bases legales para su confección en el sector público, por lo que, en un futuro próximo dicho esquema tendrá carta de naturaleza en nuestro país y será una evidencia del liderazgo del país y la autoridad competente en esta materia. No obstante, también será necesario que se establezcan las bases para la creación de esquema de certificación de Profesionales de Privacidad aplicable al sector privado administrado por el INAI para garantizar la objetividad, calidad y rigurosidad del proceso.

Cifras relevantes

A. Sobre el número de Profesionales de Privacidad

Para darse una idea de la cantidad de Profesionales de Privacidad que se requieren en el mundo, principalmente a partir de la entrada en vigor del RGPD, IAPP en un estudio de noviembre de 2016 “estimó que se necesitarán al menos 28,000 DPO solo en Europa y Estados Unidos.”[64] Derivado de esto, el estudio

Notas al pie

61. ACUERDO mediante el cual se aprueba la adición de un título décimo primero a los Lineamientos Generales de Protección de Datos Personales para el Sector Público y la modificación y adición de una fracción XXV al artículo 25 y una fracción XIII al artículo 42 del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Disponible en https://dof.gob.mx/nota_detalle.php?codigo=5643872&fecha=25/02/2022&print=true

62. Para mayor información se puede consultar https://www.nyce.org.mx/certificacion-de-profesionales-como-auditores-evaluadores-implementadores-y-oficiales-de-proteccion-de-datos-personales/

63. De acuerdo con información de NYCE consultada en noviembre de 2022 esta certificación se encuentra en proceso de Acreditación por la Entidad Mexicana de Acreditación (EMA).

con datos del Eurostat[65] concluye que "se crearían hasta 75,000 puestos de DPO en respuesta al RGPD en todo el mundo".[66]

En mayo de 2019, la IAPP en otro estudió señaló que "a un año de la entrada en vigor del RGPD aproximadamente 500,000 organizaciones de los sectores público y privado tienen oficiales de protección de datos registrados en toda Europa bajo el RGPD".[67]

En países como Noruega donde la figura del DPO ha sido adoptada de forma previa a la entrada en vigor del RGPD, según datos de la "Encuesta al Delegado de Protección de Datos sobre las condiciones laborales de los Delegados de Protección de Datos y el cumplimiento de la legislación de protección de datos en las empresas noruegas" elaborada en septiembre 2021 por la autoridad noruega de protección de datos (Datatilsynet en noruego) "a finales de 2020, se habían registrado 1,341 delegados de protección de datos, que representan a 1891 empresas noruegas".[68]

Actualmente no existe una estimación oficial sobre la cantidad de Profesionales de Privacidad que se requieren en Latinoamérica y tampoco de aquellas personas que se dedican a dicha profesión. Igualmente, tampoco existen estudios o censos locales sobre cuántos profesionales de privacidad son requeridos por cada país en el que existe una normatividad vigente de protección de datos. Incluso en el ámbito internacional estos estudios son escasos. Sin embargo, como se estudiará más adelante en múltiples jurisdicciones la designación de un DPO es un mandato legal reciente, situación que se traduce en una escasa maduración de la figura y ausencia de profesionales dedicados a protección de datos y privacidad.

Notas al pie

64. International Association of Privacy Professionals (IAPP), "Study: GDPR's global reach to require at least 75,000 DPOs worldwide", 9 de noviembre de 2016, Disponible en https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/
65. https://ec.europa.eu/eurostat
66. International Association of Privacy Professionals (IAPP), "Study: GDPR's global reach to require at least 75,000 DPOs worldwide", 9 de noviembre de 2016, Disponible en https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/
67. International Association of Privacy Professionals (IAPP), "Study: An estimated 500K organizations have registered DPOs across Europe", Mayo 2019, Disponible en https://iapp.org/news/a/study-an-estimated-500k-organizations-have-registered-dpos-across-europe/
68. Vid, Datatilsynet, Encuesta al Delegado de Protección de Datos Sobre las condiciones laborales de los Delegados de Protección de Datos y el cumplimiento de la legislación de protección de datos en las empresas noruegas, septiembre, 2021, p. 3.

B. Datos del Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Federal 2021

Como decíamos, hoy en día no contamos con cifras sobre el número de Profesionales de Privacidad que existen o se requieren en México en el sector público. Empero, la identificación del número de sujetos obligados existentes en el plano de la administración pública, tanto en el ámbito federal, local y municipal, puede servir para estimar la cantidad de OPD que se pueden requerir toda vez que la LGPDPPSO[69] y sus homólogas locales indican que los sujetos obligados podrán designar a un profesional de esta naturaleza cuando "realicen tratamientos intensivos o relevantes[70] de datos personales". De ahí, dependiendo de las actividades que desarrollen los sujetos obligados y su propia naturaleza se podría inferir, si estos realizan "tratamientos intensivos o relevantes de datos personales" y en derivación, el número de OPD requeridos. Sin embargo, como se apreciará más adelante la información sobre los sujetos obligados que realizan los citados tratamientos es inexistente.

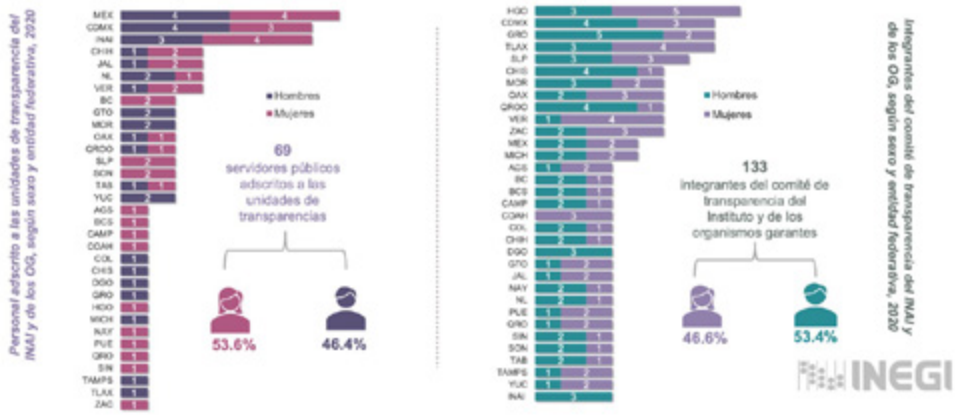
De acuerdo con datos del Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Federal 2021[71] elaborado por el Instituto Nacional de Estadística, Geografía e Informática (INEGI)[72] destacan las siguientes cifras:

El censo indica que, "al cierre de 2020, el INAI y los órganos garantes de las entidades federativas contaron con 7 y 62 servi-

Notas al pie

69. Artículo 85. Cada responsable contará con una Unidad de Transparencia, se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública, esta Ley y demás normativa aplicable, que tendrá las siguientes funciones:
I. Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;
II. Gestionar las solicitudes para el ejercicio de los derechos ARCO;
III. Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;
IV. Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;
V. Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
VI. Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO, y
VII. Asesorar a las áreas adscritas al responsable en materia de protección de datos personales.
Los responsables que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos de datos personales relevantes o intensivos, podrán designar a un oficial de protección de datos personales, especializado en la materia, quien realizará las atribuciones mencionadas en este artículo y formará parte de la Unidad de Transparencia.
Los sujetos obligados promoverán acuerdos con instituciones públicas especializadas que pudieran auxiliarles a la recepción, trámite y entrega de las respuestas a solicitudes de información, en la lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente.

doras y servidores públicos adscritos a las unidades de transparencia, respectivamente. Por su parte, el INAI reportó 3 integrantes del comité de transparencia, mientras que en los órganos garantes se reportaron 130 integrantes".[73] Esta cifra es interesante, sin embargo, el censo no indica si dichos órganos garantes contaban o no con un OPD adscrito a la unidad de transparencia.



Al cierre de 2020, el Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Federal 2021 indica que "se registraron 865 sujetos obligados en el ámbito federal, la mayoría fueron Fideicomisos y fondos públicos (45.1%); en las entidades federativas, por su parte, el total fue de 7,708, siendo la mayoría Municipios o demarcaciones territoriales de la Ciudad de México con 41.8 por ciento." [74]

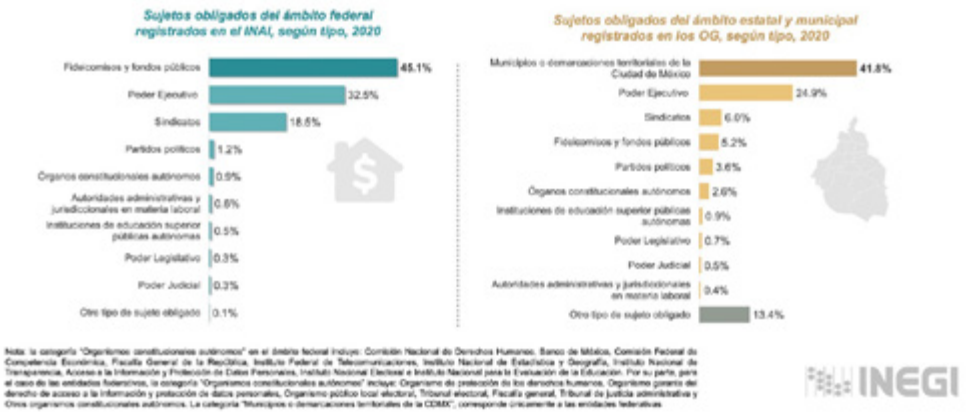
Notas al pie

70. En relación con este concepto la LGPDPPSO señala:
Artículo 75. Para efectos de esta Ley se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando:
I. Existan riesgos inherentes a los datos personales a tratar;
II. Se traten datos personales sensibles, y
III. Se efectúen o pretendan efectuar transferencias de datos personales.

71. De acuerdo con el INEGI, el Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Federal 2021 tiene como objetivo generar información estadística y geográfica sobre la gestión y desempeño del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, específicamente en las funciones de gobierno, transparencia y garantía de acceso a la información pública y protección de datos personales, con la finalidad de que esta se vincule con el quehacer gubernamental dentro del proceso de diseño, implementación, monitoreo y evaluación de las políticas públicas de alcance nacional en los referidos temas. Vid, Instituto Nacional de Estadística, Geografía e Informática (INEGI), "Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Federal 2021", Disponible en https://www.inegi.org.mx/programas/cntaippdpf/2021/

72. Instituto Nacional de Estadística, Geografía e Informática (INEGI), "Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Federal 2021", Disponible en https://www.inegi.org.mx/programas/cntaippdpf/2021/

73. Ídem



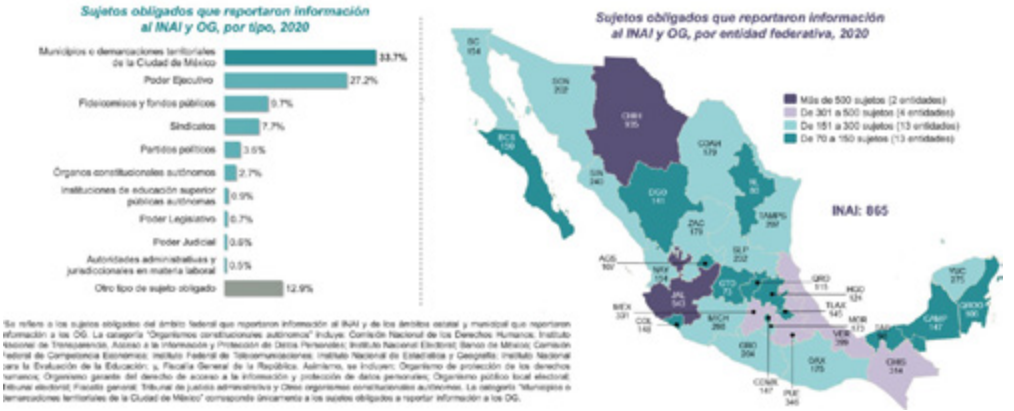
Fuente: INEGI, Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Federal 2021.

La cifra anterior resulta importante ya que aporta datos sobre la cantidad de sujetos obligados existentes en México. Sin embargo, no precisa la tipología de estos y tampoco indica información que permita inferir o determinar si estos realizan tratamientos intensivos o relevantes de datos personales.

Conforme a los datos del Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Federal 2021, "para el cierre de 2020, 7,954 sujetos obligados de los ámbitos federal, estatal y municipal reportaban información al INAI y a los órganos garantes (865 y 7,089, respectivamente). Según el censo, la mayoría de ellos fueron municipios o demarcaciones territoriales de la Ciudad de México, que representaron 33.7% del total. En tanto, concluye el censo que Chihuahua y Jalisco fueron las entidades que concentraron la mayor cantidad de sujetos obligados con 935 y 543, respectivamente".[75]

Notas al pie

74. Ídem



Fuente: INEGI, Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Federal 2021.

Las cifras anteriores sobre la cantidad de sujetos obligados que reportan acciones al INAI también son de relevancia, sin embargo, el censo no precisa la tipología de sujetos obligados que reportan al INAI y tampoco facilita información que permita inferir o determinar si estos realizan tratamientos intensivos o relevantes de datos personales. Nuevamente, los datos para la cuantificación de OPD requeridos en el sector público son ausentes.

El censo señalado también reportó que, "del total de los sujetos obligados del ámbito federal que reportaban información al INAI, durante 2020, 82.9% (717) contó con unidades de transparencia; en el caso del ámbito estatal y municipal, el porcentaje fue de 97.8% (6,933). En total, el censo indica que dichas unidades contaron con 11,757 personas adscritas, de ellas, 50.2% fueron hombres y 48.4% mujeres. De dicho personal, según el censo, los sujetos del ámbito federal registraron 3,357, mientras que en el ámbito estatal y municipal se reportaron 8,400 personas." [76]

Notas al pie

75. Ídem

Fuente: INEGI, Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Federal 2021.

Finalmente, sobre estas últimas cifras cabe señalar que, aunque reportan que, si bien, existen 11,757 personas adscritas a las unidades de transparencia de los sujetos obligados de los distintos niveles de gobierno, no se indica si dentro de dicha composición humana se hallan personas con el cargo de OPD.

En síntesis, aunque existe información sobre el número de sujetos obligados, unidades de transparencia y personas adscritas a estas en los distintos niveles de gobierno, a la fecha, no se encuentra presente una estimación sobre los sujetos obligados que realizan tratamientos intensivos o relevantes de datos personales ni información relacionada con el número de personas que fungen como OPD en el sector público. Derivado de esto, sería lógico afirmar que toda vez que no existe registro de los OPD en el sector público, evidentemente su designación no es una práctica frecuente, y, en consecuencia, hay un déficit de estos, pues como decíamos, existe un claro requerimiento normativo de su designación y la información disponible no indica que dicha figura opere en las organizaciones de forma generalizada.

Dicho lo anterior, tomando en cuenta el alcance y características del censo citado, sería recomendable que en su composición se consideraran aspectos como el número de sujetos

Notas al pie

76. Ídem

obligados que realizan tratamientos intensivos o relevantes de datos personales en México y el número de personas que fungen como OPD en los sujetos obligados registrados. Dicha información sería de gran utilidad para la sociedad mexicana con ánimo de entender el estado de maduración de dicha figura, el número de OPD requeridos, así como para la creación de mecanismos de certificación para dichos profesionales.

C. Datos de los Censos Económicos 2019 y del DENUE 2022

El documento titulado "Las empresas en los Estados Unidos Mexicanos, Censos Económicos 2019" elaborado por el INEGI[77] muestra un panorama sobre la manera en que están organizados los establecimientos del país en las distintas actividades que conforman la economía nacional. De acuerdo con los datos de los censos se puede apreciar una magnitud de la cantidad de empresas que existen en México, y que, al realizar tratamientos de datos personales (en general todas las empresas deben tener empleados para funcionar y como resultado de ello es lógico asumir que deberán tratar datos personales de estos) están obligadas a cumplir con la normatividad de protección de datos, pues no existe una excepción para no hacerlo, si bien, la normativa excluye de su aplicación los tratamientos domésticos y aquellos realizados por las Sociedades de Información Crediticia.[78]

Con todo lo anterior, la LFPDPPP aplicable al sector privado no refiere de forma expresa la designación de un OPD con las características que dicha figura tiene en otras latitudes como Europa, pero si refiere que las organizaciones deben designar una persona responsable de privacidad o departamento que atienda los derechos de los titulares y fomente la cultura de protección de datos en la organización.[79]

Notas al pie

77. INEGI, "Las empresas en los Estados Unidos Mexicanos: Censos Económicos 2019", 2020, Disponible en https://www.inegi.org.mx/contenidos/productos/prod_serv/contenidos/espanol/bvinegi/productos/nueva_estruc/702825198817.pdf

En la práctica, la designación del OPD en las empresas puede asimilarse con el cumplimiento de dicha obligación, y como decíamos líneas arriba será una medida de demostrar responsabilidad en la observancia de la normatividad de protección de datos vigente.

De esta forma, la presunción que se realiza es que todas las empresas con personal humano deberán contar con una persona responsable o departamento de datos personales para cumplir con las obligaciones de la LFPDPPP y como buena práctica podrían oficializar el nombramiento de un OPD.

Los datos de los Censos Económicos 2019 indican que "la conformación del sector empresarial y paraestatal incluye un total de 4,800,157 establecimientos captados en 2018 de los cuales 4,616,864 son empresas distribuidas en: 4,581,663 empresas uniestablecimiento; 35,201 empresas multiestablecimiento de las cuales 17,682 empresas efectúan una misma actividad y 25,622 empresas tienen todos sus establecimientos en la misma entidad federativa." [80]

Sector privado y paraestatal
Categorización de empresas 2018

Cuadro 3

Total de empresas	**4 616 864**
Empresas uniestablecimiento (con un establecimiento)	4 581 663
Empresas multiestablecimiento (con dos o más establecimientos)	35 201
Empresas especializadas	17 682
Empresas mixtas	17 519
Empresas nacionales	9 579
Empresas locales	25 622

Fuente: Censos Económicos 2019.

Notas al pie

78. Artículo 2.- Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:
I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y
II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

79. Artículo 30.- 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 a que se refiere la presente Ley. Asimismo fomentará la protección de datos personales al interior de la organización.

80. INEGI, "Las empresas en los Estados Unidos Mexicanos: Censos Económicos 2019", 2020, pp. 14-15, Disponible en https://www.inegi.org.mx/contenidos/productos/prod_serv/contenidos/espanol/bvinegi/productos/nueva_estruc/702825198817.pdf

De acuerdo con los censos, la cobertura sectorial de los resultados por empresa comprende las categorías de la columna "sector de actividad" y el número de empresas conformadas es el que se identifica en la última columna sobre número de empresas conformadas:

Estructura del Sector privado y paraestatal por empresas, 2018 Cuadro 4

Sector de actividad	Unidades económicas publicadas en tabulados por establecimiento (a)	Unidades económicas publicadas en tabulados por empresa (b)	Diferencia (c) (c = b - a)	Número de empresas conformadas
Total nacional	**4 800 157**	**4 800 157**	**0**	**4 616 864**
Pesca y acuicultura	24 372	24 377	5	24 350
Minería	3 123	3 116	- 7	2 991
Electricidad, agua y gas	2 961	2 961	0	2 961
Construcción	19 501	19 502	1	19 450
Manufacturas	579 828	586 991	7 163	571 828
Comercio al por mayor	155 545	153 787	- 1 758	132 683
Comercio al por menor	2 092 770	2 087 585	- 5 185	1 977 271
Transportes, correos y almacenamiento	22 245	22 216	- 29	20 567
Información en medios masivos	8 828	8 844	16	7 499
Servicios financieros y de seguros	26 593	26 613	20	17 636
Servicios inmobiliarios y de alquiler de bienes	68 010	67 971	- 39	66 324
Servicios profesionales, científicos y técnicos	100 098	100 069	- 29	98 843
Corporativos	366	401	35	333
Apoyo a los negocios y manejo de desechos	76 059	76 231	172	72 403
Servicios educativos	53 524	53 584	60	50 992
Servicios de salud y de asistencia social	196 089	196 046	- 43	193 213
Servicios de esparcimiento culturales y deportivos	51 352	51 321	- 31	50 503
Hoteles y restaurantes	637 124	636 872	- 252	627 454
Otros servicios excepto gobierno	681 769	681 670	- 99	679 563

Fuente: Censos Económicos 2019.

Los datos de los Censos Económicos 2019[81] además arrojaron los siguientes datos:

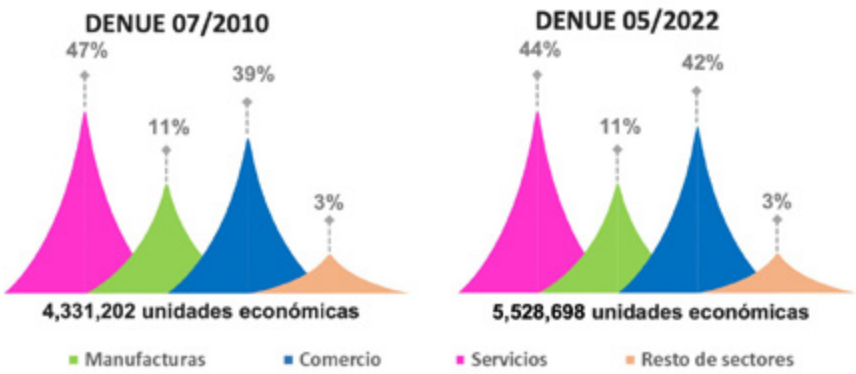
- "En 2019 había en México 6.3 millones de establecimientos, con 36 millones de personas ocupadas en ellos.
- En nuestro país 94.9% de los establecimientos son tamaño micro; 4.9% son pequeños y medianos (PYMES) y 0.2% son grandes.
- El 62.6% del total de los establecimientos son informales.
- Se censaron 6,373,169 establecimientos, en donde trabajan 36,038,272 personas."

Notas al pie

81. INEGI, COMUNICADO DE PRENSA NÚM. 305/20 16 DE JULIO DE 2020, https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2020/OtrTemEcon/CenEconResDef2019_Nal.pdf

Por otro lado, el Directorio Estadístico Nacional de Unidades Económicas (DENUE)[82] Interactivo correspondiente a mayo de 2022 proporciona los datos de 5,528,698 negocios, entre los que predominan los del sector terciario, es decir, los que realizan actividades de comercio y servicios.[83]

Gráfica 1
NEGOCIOS POR GRAN SECTOR DE ACTIVIDAD ECONÓMICA EN EL DENUE INTERACTIVO
(Distribución porcentual)



Fuente: INEGI, Directorio Estadístico Nacional de Unidades Económicas 2022.

Así, de acuerdo con las cifras anteriores se puede advertir que "en México existe un número amplio de establecimientos (6.3 millones), de los cuales 4.9% son medianas empresas y solo 0.2% son grandes empresas."[84] Indudablemente las medidas y grandes empresas son sujetos que tratan datos y estarán obligados a cumplir con la LFPDPPP.

En esta tesitura podemos presumir que si las medidas y grandes empresas que realizan tratamientos de datos personales designaran un DPO se requerirían cerca de 313,560 Profesionales de Privacidad para cumplir con las funciones ordenadas

Notas al pie

82. De acuerdo con el INEGI, el DENUE proporciona información actualizada con base en el Estudio sobre la Demografía de los Negocios (EDN) 2021, realizado por el INEGI. Este ofrece a los usuarios un marco de comparación entre los hallazgos del EDN 2020 y los del EDN 2021 con relación a los resultados de los Censos Económicos 2019 en el contexto de la contingencia sanitaria. También mide el impacto en los negocios micro, pequeños y medianos (MiPyME) del país y apoya la evaluación de las políticas públicas y privadas implementadas para impulsar la recuperación económica de este sector de los negocios. Fuente: INEGI, COMUNICADO DE PRENSA NÚM. 299/22 26 DE MAYO DE 2022, Disponible en https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/denue/denue2022.pdf

83. INEGI, COMUNICADO DE PRENSA NÚM. 299/22 26 DE MAYO DE 2022, Disponible en https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/denue/denue2022.pdf

por el artículo 30 de la LFPDPPP y diversas obligaciones señaladas en la misma.

De la misma forma que ocurre con el sector público, a la fecha no existe un censo formal sobre el número de DPO requeridos y/o existentes. No obstante, se pueden encontrar algunos datos interesantes en la industria.

Por ejemplo, en 2017 el "Estudio de Privacidad en México 2016 realizado por PwC"[85] estimó que "12% de las empresas mexicanas no habían iniciado labores relacionadas con la privacidad y protección de datos sensibles".[86]

En esa misma línea, PwC señala que, "en México hay 341 mil profesionales de ciberseguridad, según el (ISC), y 53% de los ejecutivos busca que sus nuevas contrataciones tengan habilidades digitales de inteligencia de seguridad (49%), así como en gestión y análisis de datos (45%)".[87] En la práctica es común que los profesionales de ciberseguridad en las organizaciones del sector privado asuman las funciones de privacidad y protección de datos personales en las empresas, sin embargo, no es la regla general, y tampoco disponemos de datos para determinar cuántos de estos realizan tales funciones, por lo que no es posible determinar cuántos Profesionales de Privacidad existen en el sector privado en México de forma particular.

En síntesis, se puede estimar que, en México se requieren al menos 313,560 Profesionales de Privacidad en las organizaciones del sector privado y que su designación no es potestativa ya que la LFPDPPP ordena contar con una figura de este tipo.

Notas al pie

84. Ídem
85. Información extraída de PricewaterhouseCoopers, ASUG, Estudio de la privacidad en México 2016: más allá de los compromisos, 2017, Disponible en https://asug.mx/wp-content/uploads/2017/06/20170602-pg-flyer-estudio-privacidad-asug.pdf
86. Ídem
87. PricewaterhouseCoopers, Entrada "Más del 50% de las empresas mexicanas asegura que su industria podría sufrir incidentes de ciberseguridad", 11 de noviembre de 2020, Disponible en https://www.pwc.com/mx/es/prensa/archivo/2020/20201111-dti-vf1.pdf

Regulación de la Figura del Profesional de Privacidad en Latinoamérica

Contexto

Actualmente, diversos países de la región han emitido normas específicas en materia de protección de datos basándose en el estándar RGDP. Por ejemplo, la Ley General de Protección de Datos de Brasil, la Ley 81 de Panamá y su Reglamento y la Ley Orgánica de Protección de Datos Personales en Ecuador. Asimismo, están en proceso de discusión algunas modificaciones a ordenamientos existentes como en el caso de Argentina, Chile, Costa Rica y Paraguay para adecuarse al estándar más alto que es el europeo. Con todo ello, la Figura del Profesional de Privacidad, cualquiera que sea su denominación, reporta y reportará más peso en las organizaciones que tratan datos personales, ya sean públicas o privadas.[1]

Así, en este apartado se realizará un análisis de la recepción de la Figura del Profesional de Privacidad en las leyes de protección de datos personales de la región con el propósito de determinar en qué casos y bajo qué condiciones es obligatorio designar un DPO u OPD.

De esta forma, en el análisis individualizado por país se considerarán los siguientes ordenamientos vigentes:

Leyes de protección de datos en Latinoamérica

País	Normatividad de Protección de Datos	Fecha de publicación
Argentina	Ley 25.326	30 de octubre de 2000
	Decreto 1558/2001	3 de diciembre de 2001

Notas al pie

1. La influencia de RGPD en la región es fuerte, y es el estándar elegido para adecuar las normas internas. No obstante, existen otras importantes referencias como los Estándares de Protección de Datos para los Estados Iberoamericanos y las Directrices de Privacidad de la OCDE (2013) que sirven para realizar este proceso de adecuación en aquellos Estados en los que aún no existe una normatividad homogénea y comprensiva.

Brasil	Ley General de Protección de Datos (Ley N° 13.709/2018)	14 de agosto de 2018
	Resolución CD/ANPD Nº 2	27 de enero de 2022
Chile	Ley No. 19.628 sobre Protección a la Vida Privada	18 de agosto de 1999
Colombia	Ley Estatutaria No. 1581	17 de octubre de 2012
	Decreto 1377 de 2013 que Reglamenta parcialmente la Ley 1581 de 2012	27 de junio de 2013
Costa Rica	Decreto 620 de 2020	2 de mayo de 2020
	Ley No. 7975	18 de enero de 2000
	Ley No. 8968	5 de septiembre de 2011
	Decreto Ejecutivo No. 37554-JP del 30 de octubre del 2012	30 de octubre del 2012
Ecuador	Ley Orgánica de Protección Datos Personales	26 de mayo de 2021
México (sector privado)	Ley Federal de Protección de Datos Personales en Posesión de Particulares	5 de julio de 2010
	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares	21 de diciembre de 2011

México (sector público	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	26 de enero de 2017
	Lineamientos Generales de Protección de Datos Personales para el Sector Público	26 de enero de 2018
Nicaragua	Ley de Protección de Datos Personales	29 de marzo de 2012
Panamá	Ley 81 de 2019 sobre Protección de Datos Personales	29 de marzo de 2019
	Reglamento de la Ley 81	28 de mayo de 2021
Paraguay	Ley No. 1682	16 de enero de 2001
	Ley 1969	3 de septiembre de 2002
Perú	Ley No. 29733 de Protección de Datos Personales	3 de julio de 2011
	Reglamento de la ley 29733	22 de marzo de 2013
República Dominicana	Ley No. 172-13	15 de diciembre de 2013
Uruguay	Ley 18.331 de Protección de Datos Personales y Acción de Habeas Data	11 de agosto de 2018
	Ley No. 19.030	7 de enero de 2013
	Ley N° 19670	25 de octubre de 2018
	Decreto N° 64/020	21 de febrero de 2020
	Decreto 414/009	31 de agosto de 2009

Fuente: Elaboración propia.

Al final de la obra se incluye una tabla de resumen sobre los resultados del análisis realizado en la región.

Figura del Profesional de Privacidad en Latinoamérica

Argentina

La actual Ley 25.326 y su decreto de desarrollo 1558/2001 no establecen la obligación de designar un Profesional de Privacidad ni regulan su funcionamiento. A la fecha, tampoco existe un esquema de certificación para Profesionales de Privacidad administrado y/o reconocido por la autoridad de control competente.

Sin embargo, en febrero de 2023, después de un amplio proceso de consulta pública[2] la Agencia de Acceso a la Información Pública presentó un Nuevo Proyecto de Ley de Protección de Datos Personalescon[3] el propósito de actualizar la Ley 25.326.

Como aspectos relevantes sobre la Figura del Profesional de Privacidad, el proyecto de ley referido introduce novedades interesantes:

- El artículo 2 incorpora la definición de Delegado de protección de datos e indica que este es la: "persona humana o jurídica encargada de informar, instruir y asesorar al Responsable o al Encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar y supervisar el cumplimiento normativo, y de cooperar con la Autoridad de aplicación, y servir como punto de contacto entre ésta y el Responsable o Encargado del tratamiento de datos."
- El artículo 44 del Nuevo Proyecto de Ley de Protección de Datos Personales indica que los responsables y encargados deberán designar un DPD en los siguientes casos:

Notas al pie

2. De acuerdo con la Agencia de Acceso a la Información Pública a lo largo del proceso de consulta pública se recibieron **173 opiniones, aportes y comentarios** presentados por **123 participantes** correspondientes a la ciudadanía en general, organizaciones de la sociedad civil, universidades e investigadores, sector privado y sector público nacional e internacional. Vid, Agencia de Acceso a la Información Pública, Nuevo Proyecto de Ley de Protección de Datos Personales, Disponible en https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales
3. El Nuevo Proyecto de Ley de Protección de Datos Personales se puede consultar en la siguiente dirección: https://www.argentina.gob.ar/sites/default/files/proyecto_de_ley_de_proteccion_de_datos_personales_-_febrero_2023.pdf

- » “Si se trata de una autoridad u organismo público;
- » Las actividades del Responsable o Encargado del tratamiento de datos personales requieran un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades, conforme a lo que se establezca en esta ley, su reglamentación, o en la normativa que dicte al respecto la Autoridad de aplicación.”

• Con respecto al DPD el artículo 44 referido también establece las siguientes reglas relativas a la designación del DPD:

- » Los Responsables y Encargados del tratamiento que no se encuentren obligados a designar un DPD pueden hacerlo de manera voluntaria o por orden expresa de la Autoridad de aplicación.
- » Las autoridades u organismos públicos con dependencias subordinadas pueden designar un único DPD, teniendo en consideración su tamaño y estructura organizativa.
- » Un grupo económico puede nombrar un único DPD siempre que esté en contacto permanente con cada una de las empresas que lo conforman.

• Sobre el perfil y funciones del DPD el artículo 44 establece los requisitos siguientes:

- » “La designación del DPD debe recaer en una persona que reúna los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones.
- » Las funciones del DPD pueden ser desempeñadas por un empleado del Responsable o Encargado del tratamiento o en el marco de un contrato de prestación de servicios.
- » El DPD puede ejercer otras funciones siempre que no den lugar a conflictos de intereses.
- » El Responsable o Encargado del tratamiento está obligado a respaldar al DPD en el desempeño de sus funciones, y a facilitarle los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados y la actualización de éstos”.

- **El DPD debe ejercer sus funciones de manera autónoma y libre de interferencias, sin recibir instrucciones, y solo debe responder ante el más alto nivel jerárquico de la organización.**
- **El DPD no puede ser destituido ni sancionado por desempeñar sus funciones.**

• El artículo 45 del Nuevo Proyecto de Ley de Protección de Datos Personales señala que el DPD tendrá las siguientes funciones:

- **"Informar y asesorar a los Responsables y Encargados del tratamiento, así como a sus empleados, de las obligaciones a su cargo;**
- **Promover y participar en el diseño y aplicación de una política de tratamiento de datos personales;**
- **Supervisar el cumplimiento de la presente ley y de la política de protección de datos;**
- **Asignar responsabilidades, concientizar, formar al personal y realizar las auditorías correspondientes;**
- **Ofrecer el asesoramiento que se le solicite para hacer una evaluación de impacto relativa a la protección de datos, cuando entrañe un alto riesgo de afectación para los derechos de los Titulares, y supervisar luego su aplicación;**
- **Cooperar y actuar como referente ante la Autoridad de aplicación para cualquier consulta sobre el tratamiento de datos efectuado por el Responsable o Encargado del tratamiento."**

En síntesis, en Argentina no existe una obligación de designar un Profesional de Privacidad en las organizaciones ni se cuenta con un esquema de certificación sobre el tema. No obstante, el Nuevo Proyecto de Ley de Protección de Datos Personales si considera tal requerimiento para las organizaciones públicas y privadas.

Brasil

El artículo 41 de la Ley General de Protección de Datos (LGPD) establece que el responsable del tratamiento deberá designar a un responsable del tratamiento de los datos personales.

El citado fundamento legal señala que las actividades del responsable serán:

- "Aceptar quejas y comunicaciones de los titulares, brindar aclaraciones y adoptar medidas;
- Recibir comunicaciones de la autoridad nacional y adoptar medidas
- Orientar a los empleados y contratistas de la entidad sobre las prácticas a ser adoptadas en relación con la protección de datos personales; y
- Ejercer otras atribuciones determinadas por el controlador o establecidas en normas complementarias."

Finalmente, el párrafo tercero del artículo 41 señala que la autoridad nacional podrá establecer reglas adicionales sobre la definición y atribuciones del responsable, inclusive supuestos en los que no sea obligatoria su designación, según la naturaleza y tamaño de la entidad o el volumen de las operaciones de tratamiento de datos.

El 27 de enero de 2022 la Autoridad Nacional de Protección de Datos (ANPD) emitió la Resolución CD/ANPD Nº 2 de 27 de enero de 2022 por virtud de la cual se regulan obligaciones de protección de datos para pequeñas empresas y señaló en el artículo 11 lo siguiente:

- "Las pequeñas empresas no están obligadas a indicar el responsable del tratamiento de los datos personales exigido en el artículo 41 de la ley.
- Las pequeñas empresas que no designen un responsable deberán proporcionar un canal de comunicación

con el interesado para aceptar quejas y comunicaciones de los titulares, brindar aclaraciones y adoptar medidas.
• La designación de un responsable por parte de las pequeñas empresas será considerada como políticas de buenas prácticas y de buen gobierno."

En relación con lo anterior, la autoridad ha aclarado en su guía de orientación para agentes del tratamiento emitida en abril de 2022[4] los siguientes aspectos relevantes:

• "En virtud de que la LGPD no ha determinado bajo qué circunstancias una organización debe designar a un responsable se debe asumir, como regla general, que toda organización debe nominar a una persona para asumir este rol.
• El artículo 41 de la LGPD no distingue entre instituciones públicas o privadas, por lo que es importante que ambas sean conscientes de su obligación de designar un responsable del tratamiento.
• La LGPD tampoco distingue si el responsable debe ser una persona natural o jurídica, y si debe ser un empleado de la organización o un agente externo. Considerando las buenas prácticas internacionales, el responsable puede ser un empleado de la institución o un agente externo, ya sea físico o jurídico. Se recomienda que el responsable sea señalado mediante un acto formal, como un contrato de prestación de servicios o un acto administrativo.
• Como buena práctica, se considera importante que el responsable tenga libertad en el ejercicio de sus funciones. En cuanto a sus calificaciones profesionales, estas deben definirse mediante un juicio de valor realizado por el responsable del tratamiento que los designe, considerando conocimientos en protección de datos y seguridad de la información a

Notas al pie

4. Autoridade Nacional de Proteçao de Datos, Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, versión 2, abril, 2022, Disponible en https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf

un nivel que satisfaga las necesidades de las operaciones de tratamiento de datos personales de la organización.

- La LGPD no prohíbe que el responsable sea apoyado por un equipo de protección de datos. Por el contrario, considerando las buenas prácticas, es importante que el responsable cuente con los recursos adecuados para llevar a cabo sus actividades, lo que puede incluir recursos humanos. Otros recursos que se deben considerar son el tiempo (plazos apropiados), las finanzas y la infraestructura.
- Si bien la LGPD no impide que un mismo responsable actúe en nombre de diferentes organizaciones, es importante que pueda desempeñar sus funciones de manera eficiente.
- Antes de designar a un responsable, el controlador debe considerar si podrá atender sus demandas y las de otras organizaciones concomitantemente. La responsabilidad por el tratamiento de los datos personales sigue siendo del responsable del tratamiento o del operador de los mismos, tal y como establece el artículo 42 de la LGPD."

A la fecha, tampoco existe un esquema de certificación para Profesionales de Privacidad administrado y/o reconocido por la autoridad de control competente.

Chile

La actual Ley 19628 y diversas normas de desarrollo existentes no establecen la obligación de designar un Profesional de Privacidad ni regula su funcionamiento. A la fecha, tampoco existe un esquema de certificación para Profesionales de Privacidad administrado y/o reconocido por la autoridad de control competente.

No obstante, a la fecha se encuentra en discusión un proyecto de ley para modificar la Ley 19628.

Con respecto a la Figura del Profesional de Privacidad el proyecto citado en su artículo 52 hace referencia lo que se denomina "Modelo

de prevención de infracciones" y señala que "los responsables de datos sean personas naturales o entidades o personas jurídicas, públicas o privadas, podrán adoptar modelos de prevención de infracciones que deben contener, a lo menos, los siguientes elementos:

- Designación de un encargado de prevención o delegado de protección de datos personales.
- Definición de medios y facultades del encargado de prevención."

El artículo 52 indica también que "el responsable de datos debe disponer que el encargado de prevención cuente con los medios y facultades suficientes para el desempeño de sus funciones, debiendo otorgarle los recursos materiales necesarios para realizar adecuadamente sus labores, en consideración al tamaño y capacidad económica de la entidad".

Colombia

La Ley Estatutaria No. 1581 y el Decreto 1377 no establecen de forma expresa la obligación de designar un DPO en los términos asumidos por normativas como el RGPD. Sin embargo, el Decreto 1377 en su artículo 23 establece que "todo Responsable y Encargado deberán designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 y el decreto."

No obstante, el Decreto 620 de 2020, relativo a los servicios ciudadanos digitales, en su artículo 2.2.17.5.4 establece que "todo responsable y encargado del tratamiento de datos deberá designar a una persona o área que asuma la función de protección de datos personales, quien dará trámite a las solicitudes de los Titulares para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y del capítulo 25 del Decreto 1074 de 2015; y quien deberá, además de cumplir los lineamientos de la Superintendencia de In-

dustria y Comercio (SIC), en particular, la guía para la implementación de la responsabilidad demostrada (accountability) de dicha entidad, realizar las siguientes actividades en cuanto a los datos de los usuarios de los servicios ciudadanos digitales:

> • "Velar por el respeto de los derechos de los titulares de los datos personales respecto del tratamiento de datos que realice el prestador de servicios ciudadanos digitales.
> • Informar y asesorar al prestador de servicios ciudadanos digitales en relación con las obligaciones que les competen en virtud de la regulación colombiana sobre privacidad y tratamiento de datos personales.
> • Supervisar el cumplimiento de lo dispuesto en la citada regulación y en las políticas de tratamiento de información del prestador de servicios ciudadanos digitales, así como del principio de responsabilidad demostrada.
> • Prestar el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos.
> • Atender los lineamientos y requerimientos que le haga la Delegatura de Protección de Datos Personales de la SIC o quien haga sus veces."

La Guía para la Implementación del Principio de Responsabilidad Demostrada (*Accountability*) de la SIC (Guía sobre Responsabilidad Demostrada)[5] establece que "la función del OPD o del área encargada de protección de datos en la organización es la de velar por la implementación efectiva de las políticas y procedimientos adoptados por esta para cumplir las normas, así como la implementación de buenas prácticas de gestión de datos personales dentro de la empresa".[6]

En este tenor, la Guía sobre Responsabilidad Demostrada señala que "el OPD tiene la tarea de estructurar, diseñar y administrar el programa que permita a la organización cumplir

Notas al pie

5. Superintendencia de la Industria y Comercio de Colombia (SIC), Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability), Disponible en https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf
6. Ídem
7. Ídem

las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente".[7] Dentro de las actividades del DPO la Guía indica las siguientes:

- "Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.
- Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales.
- Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.
Impulsar una cultura de protección de datos dentro de la organización.
- Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo.
- Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC.
- Obtener las declaraciones de conformidad de la SIC cuando sea requerido.
- Revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con Encargados no residentes en Colombia.
- Analizar las responsabilidades de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos personales específico para cada uno de ellos.
- Realizar un entrenamiento general en protección de datos personales para todos los empleados de la compañía.
- Realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.
- Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, call centers y gestión de proveedores, etc.).

- Medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos.
- Requerir que, dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales.
- Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal.
- Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la SIC.
- Realizar seguimiento al Programa Integral de Gestión de Datos Personales."

En consecuencia, se puede advertir que en Colombia es obligatorio designar un OPD que cumpla con funciones bastante amplias, incluyendo la atención de derechos de los Titulares.

A la fecha no existe un esquema de certificación para Profesionales de Privacidad administrado y/o reconocido por la autoridad de control competente.

Costa Rica

La Ley No. 7975, la Ley No. 8968 y el Reglamento de la Ley 8968 actualmente no prevén la obligación de designar un Profesional de Privacidad en las organizaciones. A la fecha tampoco existe un esquema de certificación para Profesionales de Privacidad administrado y/o reconocido por la autoridad de control competente.

No obstante, existe una iniciativa de reforma a la Ley No. 8968 en actual discusión. Dicha iniciativa en su artículo 34 establece la figura de la "Persona Delegada de Protección de Datos" e indica que "en el supuesto de que la Autoridad de Protección de Datos determine que una operación de tratamiento presenta altos riesgos para la integridad de los datos personales, el responsable del tratamiento deberá designar a DPD".

De acuerdo con la propuesta referida, el DPD "velará por el cumplimiento legal de la normativa atinente y deberá contar con capacidades y competencias profesionales para responder ante

las autoridades". El proyecto señala también que el rol del DPD "podrá ser asumido por una persona a lo interno de la institución u organización, o por un tercero".

Finalmente, la propuesta de modificación a la Ley 8968 indica que los requisitos para las personas delegadas, así como los criterios para definir en qué operaciones de tratamiento será necesaria su existencia se definirán mediante disposiciones reglamentarias.

Cuba

La actual Ley 149/2022 "De Protección de Datos Personales" no establece la obligación de designar un Profesional de Privacidad ni regula su funcionamiento.

A la fecha no existe un esquema de certificación para Profesionales de Privacidad administrado y/o reconocido por la autoridad de control competente.

Ecuador

La Ley Orgánica de Protección Datos Personales (LOPD) de Ecuador en su artículo 3 señala que "el DPD es la persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales (APDP), sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos".

La LOPD señala en el párrafo 13 de su artículo 47 que "es obligacion de responsable designar al DPD, en los casos que corresponda".[8] Con respecto a los supuestos en los que la designación de DPD es obligatoria el artículo 48 del referido ordenamiento prevé los siguientes:

Notas al pie

8. Art. 47.- Obligaciones del responsable y encargado del tratamiento de datos personales.- El responsable del tratamiento de datos personales está obligado a:
13) Designar al Delegado de Protección de Datos Personales, en los casos que corresponda;

- "Cuando el tratamiento se lleve a cabo por quienes conforman el sector público de acuerdo con lo establecido en el artículo 225 de la Constitución de la República;
- Cuando las actividades del responsable o encargado del tratamiento de datos personales requieran un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades del tratamiento, conforme se establezca en la LOPD, su reglamento, o en la normativa que dicte al respecto APDP;
- Cuando se refiera al tratamiento a gran escala de categorías especiales de datos, de conformidad con lo establecido en el reglamento de la LOPD; y,
- Cuando el tratamiento no se refiera a datos relacionados con la seguridad nacional y defensa del Estado que adolezcan de reserva ni fuesen secretos, de conformidad con lo establecido en la normativa especializada en la materia".

Asimismo, el último párrafo del artículo 48 señala que "la APDP podrá definir nuevas condiciones en las que deba designarse un delegado de protección de datos personales y emitirá, a dicho efecto, las directrices suficientes para su designación".

Las funciones del DPD se describen en el artículo 49 de la LOPD y son las siguientes:

- "Asesorar al responsable, al personal del responsable y al encargado del tratamiento de datos personales, sobre las disposiciones contenidas en la LOPD, su reglamento, las directrices, lineamientos y demás regulaciones emitidas por la APDP;
- Supervisar el cumplimiento de las disposiciones contenidas en la LOPD, su reglamento, las directrices, lineamientos y demás regulaciones emitidas por la APDP;
- Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, y supervisar su aplicación;
- Cooperar con la APDP y actuar como punto de contacto con dicha entidad, con relación a las cuestiones referentes al tratamiento de datos personales; y

- Las demás que llegase a establecer la APDP con ocasión de las categorías especiales de datos personales."

Con respecto a las funciones anteriores, el último párrafo del artículo 49 de la LOPD indica que, "en caso de incumplimiento de sus funciones, el delegado de protección de datos personales responderá administrativa, civil y penalmente, de conformidad con dicha ley".

En este orden de ideas, el artículo 59 de la LOPD establece que "para la ejecución de las funciones del delegado de protección de datos, el responsable y el encargado de tratamiento de datos personales, deberán observar lo siguiente:

- Garantizar que la participación del delegado de protección de datos personales, en todas las cuestiones relativas a la protección de datos personales, sea apropiada y oportuna;
- Facilitar el acceso a los datos personales de las operaciones de tratamiento, así como todos los recursos y elementos necesarios para garantizar el correcto y libre desempeño de sus funciones:
- Capacitar y actualizar en la materia al delegado de protección de datos personales, de conformidad con la normativa técnica que emita la APDP;
- No podrán destituir o sancionar al DPD por el correcto desempeño de sus funciones;
- El DPD mantendrá relación directa con el más alto nivel ejecutivo y de decisión del responsable y con el encargado;
- El titular de los datos personales podrá contactar al DPD con relación al tratamiento de sus datos personales a fin de ejercer sus derechos; y,
- El DPD estará obligado a mantener la más estricta confidencialidad respecto a la ejecución de sus funciones."

Finalmente, el último párrafo del artículo 50 sostiene que, "siempre que no exista conflicto con las responsabilidades establecidas en la LOPD, su reglamento, directrices, lineamientos y

demás regulaciones emitidas por la APDP, el DPD podrá desempeñar otras funciones dispuestas por el responsable o el encargado del tratamiento de datos personales".

Aunque la LOPD reconoce los mecanismos de certificación, a la fecha, no existe un esquema de certificación para Profesionales de Privacidad administrado y/o reconocido por la autoridad de control competente.

México (sector privado)

En México la figura del DPD no se encuentra expresamente reconocida en la LFPDPPP y su Reglamento. Sin embargo, el artículo 30 de la LFPDPPP instituye la obligación de que todo responsable del tratamiento en el sector privado designe a una persona, o departamento de datos personales para que dé trámite a las solicitudes de Derechos ARCO de los titulares y fomente la protección de datos personales al interior de la organización.[9] No obstante, la designación de un DPD puede considerarse una buena práctica que las organizaciones pueden seguir para cumplir con la obligación del artículo 30 de la Ley.

Con el propósito de orientar a los responsables en el cumplimiento de esta obligación el INAI emitió las "Recomendaciones para la Designación de la Persona o Departamento de Datos Personales".[10] Al abordar el tema de la designación de una persona responsable, el INAI sugiere tomar en cuenta lo siguiente:

- "Que las obligaciones que establece la Ley siguen estando a cargo del responsable, por lo que él estará obligado a responder sobre todo lo relacionado con el desempeño de estas funciones;
- Que en el aviso de privacidad se deberá establecer con claridad los medios para que los titulares de los datos personales ejerzan los derechos que prevé la Ley, y

Notas al pie

9. Artículo 30.- 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 a que se refiere la presente Ley. Asimismo fomentará la protección de datos personales al interior de la organización.
10. INAI, Recomendaciones para la Designación de la Persona o Departamento de Datos Personales, Disponibles en https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/RecomendacionesDesignar.pdf

• Que es indispensable que formalice la relación con el encargado mediante un contrato en el que se establezcan las obligaciones de ambos en torno a la protección de datos personales."

En cambio, si el responsable elige designar a un departamento para realizar las funciones de protección de datos personales, el INAI indica que "no se considera necesario que estas sean las únicas tareas a cargo del departamento, ni que cree uno nuevo para estos fines, sino se sugiere que las funciones de protección de datos sean asignadas a un departamento ya existente en la organización, de preferencia que tenga funciones afines a las de protección de datos".[11]

Con respecto a las funciones de la persona o departamento de datos personales las Recomendaciones del INAI agrupan las funciones en dos secciones, la primera referente a la atención de los derechos de los titulares y la segunda al fomento de la cultura de protección de datos en la organización. En la siguiente tabla se describen estas funciones.

Funciones de la persona o Departamento Responsable

Atención de Derechos de los Titulares	Fomento de la cultura de protección de datos
1. Establecer y administrar procedimientos para la recepción, tramitación, seguimiento y atención oportuna de las solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, así como para la atención de quejas o solicitudes presentadas por los titulares relacionadas con las políticas y/o prácticas de protección de datos personales desarrolladas por la organización, y	1. Diseñar y ejecutar una política y/o prácticas de protección de datos personales al interior de la organización, o bien, adecuar y mejorar las prácticas ya existentes en el marco de la Ley;

Notas al pie

11. INAI, Recomendaciones para la Designación de la Persona o Departamento de Datos Personales, pp-10-11, Disponibles en https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/RecomendacionesDesignar.pdf

Funciones de la persona o Departamento Responsable

Atención de Derechos de los Titulares	Fomento de la cultura de protección de datos
2. Monitorear los avances o cambios legislativos en materia de privacidad y protección de datos personales que pudieran impactar en los ejes rectores y acciones desarrolladas en este tema al interior de la organización, haciendo las adecuaciones necesarias.	2. Alinear esta política y/o prácticas -incluyendo sus objetivos, acciones estratégicas, líneas de acción, asignación de roles y responsabilidades generales y específicas y un procedimiento y plazos de implementación- a los procesos internos de la organización que demanden o aprovechen información personal; 3. Desarrollar un mecanismo para evaluar la eficacia y eficiencia de esta política y/o prácticas; 4. Monitorear y evaluar los procesos internos de la organización vinculados con la obtención, uso, explotación, conservación, aprovechamiento, cancelación y transferencia de datos personales, a fin de asegurar que la información sea protegida, tratada conforme a los principios de la Ley y respetada; 5. Colaborar y coordinar acciones con otras áreas de la organización como la legal, de tecnologías, sistemas, seguridad de la información, mercadotecnia, atención al cliente, recursos humanos, entre otras, a efecto de asegurar el debido cumplimiento de la política y/o prácticas de privacidad en sus procesos internos, formatos, avisos, recursos y gestiones que se lleven a cabo; 6. Asegurar que la política y/o prácticas de protección de datos personales cumplan con la Ley y demás normatividad aplicable;

Funciones de la persona o Departamento Responsable

Atención de Derechos de los Titulares	Fomento de la cultura de protección de datos
	7. Difundir y comunicar la política y/o prácticas de protección de datos personales implementadas al interior de la organización, así como capacitar a todo el personal sobre las mismas; 8. Fomentar una cultura de protección de datos personales orientada a elevar el nivel de concienciación del personal y terceros involucrados, como encargados en el tratamiento de datos personales; 9. Monitorear el cumplimiento de la política y/o prácticas de protección de datos personales de las sociedades subsidiarias o afiliadas bajo el control de común de la organización o cualquier sociedad del mismo grupo del responsable que opere y le sean aplicables estas prácticas; 10. Identificar e implementar mejores prácticas relacionadas con la protección de datos personales; 11. Promover la adopción de esquemas de autorregulación, y 12. Ser el representante de la organización en materia de protección de datos personales ante otros actores.

Fuente: INAI, Recomendaciones para la Designación de la Persona o Departamento de Datos Personales

Con respecto al perfil de la persona a cargo de las funciones de protección de datos personales el INAI recomienda[12] considerar las siguientes cualificaciones:

- "**Experiencia en materia de protección de datos personales.** Se sugiere considerar los perfiles de personas que con motivo de sus funciones en la organización pueden tener experiencia en materia de privacidad. Si no es el caso, el INAI recomienda que las funciones de la persona o departamento de protección de datos personales sean afines al tema, tal es el caso de áreas de *compliance* o auditoría.
- **Jerarquía o posición indicada dentro de la organización.** El INAI recomienda que la persona o departamento de datos personales cuente con la jerarquía o posición dentro de la organización del responsable que le permita implementar políticas transversales y en todos los niveles, en materia de protección de datos personales.
- **Recursos suficientes.** Se considera fundamental que la persona o departamento de datos personales cuente con los recursos materiales, técnicos y humanos necesarios para el ejercicio de sus funciones y acciones, a efecto de dar cumplimiento a las disposiciones previstas en la Ley.
- **Contar con conocimiento en la materia.** Se considera deseable que la persona que tenga a su cargo la función de datos personales conozca sobre regulación y temas de protección de datos personales y seguridad de la información.
- Visión y liderazgo para implementar la política de privacidad a lo largo de la organización.
- Habilidades de organización y comunicación."

De acuerdo con el INAI, "las características anteriores son las que se consideran más relevantes, sin embargo, en todos los

Notas al pie

12. I INAI, Recomendaciones para la Designación de la Persona o Departamento de Datos Personales, pp-13-14, Disponibles en https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/RecomendacionesDesignar.pdf
13. INAI, Recomendaciones para la Designación de la Persona o Departamento de Datos Personales, p. 14, Disponibles en https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/RecomendacionesDesignar.pdf

casos es recomendable que la persona que realice las funciones de protección de datos personales se capacite en la materia y de manera regular actualice sus conocimientos sobre el tema".[13]

Finalmente, cabe señalar que, aunque la LFPDPPP reconoce diversos esquemas de autorregulación[14] y la posibilidad de que las organizaciones los adopten para demostrar el cumplimiento de las obligaciones previstas en la Ley, a la fecha no existe un esquema de certificación para Profesionales de Privacidad administrado y/o reconocido por la autoridad de control competente.

México (sector público)

En el sector público la LGPDPPSO establece en el penúltimo párrafo de su artículo 85 que "los sujetos obligados podrán designar a un oficial de protección de datos personales (OPD), especializado en la materia para que realice las atribuciones mencionadas en dicho artículo y forme parte de la Unidad de Transparencia cuando los responsables lleven a cabo tratamientos intensivos de datos personales".[15]

Los LGPDPSP concuerdan con la Ley aplicable al señalar en su artículo 121 que, "la persona designada como OPD deberá contar con la jerarquía o posición dentro de la organización del responsable que le permita implementar políticas transversales en esta materia. Igualmente, los LGPDPSP delimitan el perfil del OPD al prevenir que este deberá ser designado en atención a sus

Notas al pie

14. Artículo 44.- 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 presente Ley. 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, 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. Dichos esquemas serán notificados de manera simultánea a las autoridades sectoriales correspondientes y al Instituto.

15.[…]
Los responsables que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos de datos personales relevantes o intensivos, podrán designar a un oficial de protección de datos personales, especializado en la materia, quien realizará las atribuciones mencionadas en este artículo y formará parte de la Unidad de Transparencia.
[…]

conocimientos, cualidades profesionales, experiencia en la materia, y en su caso a la o las certificaciones con que cuente en materia de protección de datos personales".

En lo que concierne a las funciones del OPD, la LGPDPPSO en su artículo 85 indica que en el supuesto de que se designe al OPD este tendrá las atribuciones originalmente asignadas a la Unidad de Transparencia del responsable consistentes en:

- "Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales.
- Gestionar las solicitudes para el ejercicio de los derechos ARCO.
- Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados.
- Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, de acuerdo con las normativas aplicables.
- Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.
- Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO.
- Asesorar a las áreas adscritas al responsable en materia de protección de datos personales."

Los LGPDPSP detallan las funciones del OPD al indicar en su artículo 122 que estas serán las siguientes:

- "Asesorar al Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.
- Proponer al Comité de Transparencia políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la LGPDPPSO y los LGPDPSP.

- Implementar políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la LGPDPPSO y los LGPDPSP, previa autorización del Comité de Transparencia.
- Asesorar permanentemente a las áreas adscritas al responsable en materia de protección de datos personales.
- Las demás que determine el responsable y la normatividad que resulte aplicable.

Además, el INAI ha emitido las Recomendaciones para los sujetos obligados en la designación del oficial de protección de datos personales[16] con el propósito orientar a los sujetos obligados a identificar los elementos mínimos que le permitan realizar la designación de un OPD, cuando en el ejercicio de sus funciones sustantivas, lleven a cabo tratamientos de datos personales relevantes o intensivos."[17]

El INAI, que en las Recomendaciones aplicables al OPD al referirse al perfil de este, señala que "la persona que tenga a su cargo o bajo su responsabilidad dicha función deberá poseer experiencia en materia de protección de datos personales, tener jerarquía o posición indicada dentro de la organización, contar con recursos suficientes, contar con conocimiento en la materia, visión y liderazgo para implementar la política de privacidad a lo largo de la organización y habilidades de organización y comunicación".[18]

Finalmente, cabe señalar que, en el ámbito nacional, si bien, la ley habilita a los responsables a adoptar estándares o esquemas de mejores prácticas tanto nacionales como internacionales para demostrar el cumplimiento de las obligaciones aplicables,[19] a la fecha no existe aún una certificación específica para DPD emitida y reconocida por la APDP (INAI).

Notas al pie

16. INAI, "Recomendaciones para los sujetos obligados en la designación del oficial de protección de datos personales", Disponibles en https://home.inai.org.mx/wp-content/uploads/Recomendaciones-para-los-sujetos-obligados-en-la-designación-del-oficial-de-protección-de-datos-personales-1.pdf
17. INAI, "Recomendaciones para los sujetos obligados en la designación del oficial de protección de datos personales", p.4, Disponibles en https://home.inai.org.mx/wp-content/uploads/Recomendaciones-para-los-sujetos-obligados-en-la-designación-del-oficial-de-protección-de-datos-personales-1.pdf
18. INAI, "Recomendaciones para los sujetos obligados en la designación del oficial de protección de datos personales", p.14, Disponibles en https://home.inai.org.mx/wp-content/uploads/Recomendaciones-para-los-sujetos-obligados-en-la-designación-del-oficial-de-protección-de-datos-personales-1.pdf

Sin embargo, el 25 de febrero de 2022 se publicaron modificaciones a los LGPDPSP y al Estatuto Orgánico del INAI[20] con el propósito de establecer las bases legales para el establecimiento de un esquema de certificación de OPD para el sector público.

En este orden de ideas, las adiciones a los LGPDPSP sientan las bases para la certificación de personas en materia de protección de datos personales y en un Capítulo Único de su título Décimo Primero establecen lo siguiente:

- Se establece en el artículo 254 de los LGPDPSP que "el INAI desarrollará y gestionará con plena independencia, un esquema de certificación de personas en materia de protección de datos personales para el sector público, del cual asumirá la propiedad y será responsable de su funcionamiento".
- Se establece en el artículo 255 de los LGPDPSP que "el INAI administrará y será el responsable de establecer las condiciones y requisitos que conforman y regulan el funcionamiento del esquema de certificación conforme a la normativa secundaria que para dichos efectos emita, considerando las atribuciones otorgadas en los LGPDPSP, para realizar las funciones de certificación de personas en materia de protección de datos personales para el sector público".
- Se establece en el artículo 256 los LGPDPSP que "la certificación en materia de protección de datos personales tiene por objeto, en el marco de las mejores prácticas previstas en el artículo 72 de la LGPDPPSO, emitir certificaciones a personas físicas que acrediten los requisitos, competencias y cualificaciones definidos en los criterios del esquema de certificación que emita el INAI, con el fin de validar los conocimientos y competencias de personas en la materia de protección de datos personales para el sector público".

Notas al pie

19. Artículo 29. El responsable deberá implementar los mecanismos previstos en el artículo 30 de la presente Ley para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la presente Ley y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular e Instituto o a los Organismos garantes, según corresponda, caso en el cual deberá observar la Constitución y los Tratados Internacionales en los que el Estado mexicano sea parte; en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.

20. ACUERDO mediante el cual se aprueba la adición de un título décimo primero a los Lineamientos Generales de Protección de Datos Personales para el Sector Público y la modificación y adición de una fracción XXV al artículo 25 y una fracción XIII al artículo 42 del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Disponible en https://dof.gob.mx/nota_detalle.php?codigo=5643872&fecha=25/02/2022&print=true

- En el artículo 257 de los LGPDPSP se reconoce como actores del sistema de certificación a los siguientes:
  - **"El INAI, como propietario del esquema de certificación y organismo de certificación.**
  - **El Comité INAI conformado por diversas unidades administrativas competentes del Instituto.**
  - **Las entidades de formación reconocidas por el INAI.**
  - **Personas físicas certificadas en materia de protección de datos personales.**
  - **Equipo de operación, gestión y atención para la certificación".**
- Se establecen las siguientes atribuciones del INAI en el artículo 258 de los LGPDPSP:

» **"Realizar actividades de certificación y evaluación con plena imparcialidad e independencia;**
» **Emitir los Criterios del esquema de certificación de personas en materia de protección de datos personales;**
» **Constituir y formar parte del Comité Técnico del esquema de certificación;**
» **Adoptar un proceso público y no discriminatorio para el reconocimiento de entidades de formación;**
» **Establecer un procedimiento para la gestión de quejas y reclamaciones sobre el esquema de certificación;**
» **Aprobar los programas de formación de las entidades de formación;**
» **Emitir, otorgar, renovar, suspender y retirar la certificación de personas en materia de protección de datos personales y de las entidades de formación;**
» **Establecer y administrar el registro de certificaciones expedidas bajo el esquema de certificación;**
» **Cancelar, revocar y/o suspender las certificaciones otorgadas;**
» **Elaborar un Código de Ética para guiar la conducta de los actores del esquema de certificación;**
» **Emitir las Reglas sobre la creación, usos del logotipo, y en su caso, marca del esquema de certificación.**

» **Establecer y aplicar las sanciones que correspondan por incumplimiento a los LGPDPSP y/o criterios que emita el INAI."**

- Se establece la facultad del INAI para emitir los criterios del esquema de certificación con base en lo dispuesto por el artículo 259 de los LGPDPSP, mismos que contemplarán al menos lo siguiente:

» **"Requisitos, competencias y cualificaciones requeridas para la certificación.**
» **Funciones de los actores del esquema de certificación.**
» **Proceso, método y criterios de evaluación.**
» **Proceso de certificación de personas.**
» **Emisión, renovación y suspensión de certificados.**
» **Derechos y obligaciones de las personas certificadas.**
» **Uso del logotipo, y en su caso, marca del esquema de certificación.**
» **Gestión de quejas y reclamaciones.**
» **Seguimiento y supervisión del esquema de certificación.**
» **Registro de personas certificadas.**
» **Procedimiento de cancelación, revocación y/o suspensión de certificaciones.**
» **Procedimiento de aplicación de sanciones por incumplimiento a los criterios."**

Además, se adicionó la fracción XXV, y se recorren las subsecuentes del artículo 25 del Estatuto Orgánico del INAI para establecer las siguientes atribuciones de la Secretaría de Protección de Datos Personales:

- "Coordinar y supervisar la administración general del esquema de certificación de personas en materia de protección de datos personales para el sector público implementado por el INAI a cargo de la Dirección General de Normatividad y Consulta.
- Las demás que le confieran las disposiciones legales y administrativas aplicables, así como las que le encomiende el Pleno y el Comisionado Presidente. Para el ejercicio de sus

funciones, la Secretaría de Protección de Datos Personales se auxiliará de las Direcciones Generales de Investigación y Verificación; de Normatividad y Consulta; de Prevención y Autorregulación; y de Protección de Derechos y Sanción; así como de una Dirección de Coordinación y Seguimiento."

Igualmente, se adicionó la fracción XIII al artículo 42 del Estatuto Orgánico del INAI, para establecer en el catálogo de funciones de la Dirección General de Normatividad y Consulta la de "administrar el esquema de certificación de personas en materia de protección de datos personales para el sector público propiedad del INAI, conocer, resolver y realizar todos los trámites y procedimientos relativos a dicho esquema, así como desarrollar sus requerimientos normativos".

Dada la modificación a la normativa señalada es de esperarse que un futuro próximo el INAI presente y difunda este esquema de certificación a la sociedad dirigido específicamente a las personas que desean certificarse bajo los conocimientos de la LGPDPSP como OPD. De ser el caso, México se convertiría en el primer país de la región en contar con un esquema de certificación de personas que aspiren a ser Profesionales de Privacidad u OPD en las organizaciones como sucede actualmente en países de Europa como España y Francia. No puede dejar de señalarse que la emisión de este esquema es una práctica positiva que debiera ser replicada también para las organizaciones del sector privado.

Nicaragua

La actual Ley de Protección de Datos Personales no establece la obligación de designar un Profesional de Privacidad.

A la fecha tampoco existe un esquema de certificación para Profesionales de Privacidad administrado y/o reconocido por la autoridad de control competente.

Panamá

El Reglamento de la Ley 81 de 2019 sobre Protección de Datos Personales (Reglamento de la ley 81) define en el numeral 10. de su artículo 4 al Oficial de Protección de Datos Personales (OPD) como el funcionario designado para atender la unidad de enlace.

La obligación de designar un OPD se instituye en el numeral 9 del artículo 33 del Reglamento de la ley 81 sobre responsabilidad del tratamiento al señalar que, "el responsable y el custodio de las bases de datos podrán adoptar entre otras medidas para cumplir con el principio de responsabilidad la de designar a un OPD, que participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales".

En relación con la figura del OPD el artículo 42 del Reglamento de la ley 81 aclara que "el oficial de información, que desarrolla la ley 33 de 2013, será también para los efectos de la ley 81 de 2019 el OPD para el sector público". En este contexto, el artículo 42 indica 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".

Sobre la designación del OPD en el sector privado, el artículo 42 del Reglamento de la ley 81 aclara que "esta no es obligatoria y de ser necesario, la autoridad de control la tomará en cuenta como criterio para la graduación de las sanciones".

El perfil del OPD se describe en el artículo 43 del Reglamento de la ley 81 al indicar que "para ser OPD se requiere una experiencia profesional previa en la materia y el conocimiento del sector de actividad de la entidad pública o privada en la que ejercerá sus funciones. Asimismo, se indica que la designación del OPD se estimará válida por parte de la autoridad de control solo cuando el responsable del tratamiento o el custodio de la base de datos lo notifique formalmente y de manera expresa. Lo mismo ocurrirá en el caso de que dicha designación sea revocada".

Conforme al artículo 43 anterior, la autoridad de control tiene la facultad de "llevar un registro de los oficiales de protección de datos y organizar capacitaciones dirigidas a fortalecer sus funciones".

En lo que concierne a las funciones del OPD el artículo 44 del Reglamento de la ley 81 precisa que "este las desempeña-

rá con independencia, siendo obligación del responsable del tratamiento o del custodio de la base de datos garantizar esta independencia y evitar cualquier conflicto de interés. Para ello, el artículo 44 indica que el OPD debe tener una interlocución directa con la dirección u órgano de toma de decisión de la entidad a la que representa en esta materia y se le deberán proporcionar los medios necesarios para que pueda cumplir su misión".

El artículo 44 anterior indica que las funciones principales del OPD son las siguientes:

- "Participar en tiempo y forma en las cuestiones referidas a la protección de datos personales.
- Informar y asesorar al responsable del tratamiento o al custodio de la base de datos en las cuestiones relacionadas con el cumplimiento de la Ley 81 de 2019, del decreto o de cualquier disposición legal aplicable en cada caso.
- Supervisar el cumplimiento de la normativa. Para ello podrá examinar, a solicitud del responsable del tratamiento o del custodio de la base de datos o por iniciativa propia, tratamientos de datos personales que se estén llevando a cabo y realizar recomendaciones para la adopción de medidas correctoras necesarias cuando los tratamientos analizados no sean conformes con la normativa aplicable.
- Promover la capacitación de las personas que asuman tareas relacionadas con el tratamiento de los datos personales.
- Cooperar con la autoridad de control.
- Ser la unidad de enlace con la autoridad de control.
- Asesorar al responsable del tratamiento o al custodio de la base de datos en la respuesta a los requerimientos u observaciones formalmente notificados por la autoridad de control.
- Ser la unidad de enlace con los titulares de los datos para las cuestiones relativas al tratamiento de los datos y a sus derechos."

El artículo 45 del Reglamento de la ley 81 establece que el OPD "no tendrá la consideración de responsable del tratamiento o custodio de la base de datos por prestar sus servicios en la entidad correspondiente".

Finalmente, vale la pena destacar que, si bien, el numeral 4 del artículo 33 del Reglamento referido establece la posibilidad de que las organizaciones adopten esquemas de autorregulación, a la fecha no existe un esquema de certificación para OPD administrado por la autoridad de control competente.

Paraguay

La actual normativa de protección de datos personales vigente en Paraguay no establece la obligación de designar un Profesional de Privacidad.

A la fecha tampoco existe un esquema de certificación para Profesionales de Privacidad administrado y/o reconocido por la autoridad de control competente.

Perú

La actual normativa de protección de datos personales vigente en Perú no establece la obligación de designar un Profesional de Privacidad.

A la fecha tampoco existe un esquema de certificación para Profesionales de Privacidad administrado y/o reconocido por la autoridad de control competente.

República Dominicana

La actual Ley No. 172-13 no establece la obligación de designar un Profesional de Privacidad.

A la fecha tampoco existe un esquema de certificación para Profesionales de Privacidad administrado y/o reconocido por la autoridad de control competente.

Uruguay

De acuerdo con el contenido del artículo 40 de la Ley N° 19670 “las entidades públicas, estatales o no estatales, las privadas total o parcialmente de propiedad estatal, así como las entidades pri-

vadas que traten datos sensibles como negocio principal y las que realicen el tratamiento de grandes volúmenes de datos tienen la obligación de designar un delegado de protección de datos".

Por su parte, el Decreto 64/020 en su artículo delimita el alcance de la obligación anterior al establecer que las organizaciones deberán designar un DPD en los siguientes casos:

- "Entidades públicas, estatales o no estatales y las privadas total o parcialmente de propiedad estatal.
- Entidades privadas que traten datos sensibles como negocio principal. De conformidad con lo establecido por el artículo 4° literal E) de la Ley N° 18.331 de 11 de agosto de 2008, son datos sensibles aquellos que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e información referente a la salud o a la vida sexual.
- Entidades privadas que realicen tratamiento de grandes volúmenes de datos."[21]

Ell artículo 40 de la Ley N° 19670 y al artículo 11 del Decreto 64/020 especifican que las funciones principales del DPD son:

- "Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales.
- Supervisar el cumplimiento de la normativa sobre dicha protección en su entidad.
- Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en materia de protección de datos personales.
- Actuar como nexo entre su entidad y la Unidad Reguladora y de Control de Datos Personales."

Notas al pie

21. Se considera tratamiento de grandes volúmenes de datos cualquier actividad en la que se realice un tratamiento de datos personales de más de 35.000 personas.

22. Unidad Reguladora y de Control de Datos Personales, Documento de Trabajo sobre Delegado de Protección de Datos Personales, Disponible en https://www.gub.uy/unidad-reguladora-control-datos-personales/sites/unidad-reguladora-control-datos-personales/files/documentos/publicaciones/Documento%20de%20trabajo%20Delegado%20de%20PDP.pdf

El Documento de Trabajo sobre Delegado de Protección de Datos Personales publicado por la Unidad Reguladora y de Control de Datos Personales[22] establece que para ejercer la función de DPD, es necesario contar con los siguientes requisitos mínimos:

- "Conocimientos especializados en Derechos Humanos, con especial énfasis en Protección de Datos Personales.
- Poseer práctica en materia de Protección de Datos Personales.
- Aptitud para la adopción e implementación de las medidas dirigidas a la Protección de Datos Personales.
- Contar con conocimiento del sector en el que desempeñará sus funciones.
- Poseer capacidad de comunicación, habilidades personales y de negociación y conocimiento de gestión de riesgos."

Asimismo, el artículo 40 de la Ley N° 19670 indica que el DPD "deberá poseer las condiciones necesarias para el correcto desempeño de sus funciones y actuará con autonomía técnica".

El Decreto 64/020 en su artículo 13 se refiere a la posición del DPD y señala que "...este deberá participar de forma adecuada en todas las cuestiones relativas a la protección de datos personales y que a fin de que desarrolle sus tareas se le deberá brindar pleno acceso a las bases de datos personales y a las operaciones de tratamiento".

El citado Decreto también indica que el DPD "actuará con autonomía técnica y no recibirá instrucciones en el desempeño de sus funciones específicas como delegado de protección de datos".

El citado artículo 13 también precisa que el DPD deberá "guardar absoluta confidencialidad de las informaciones a las que tenga acceso por su calidad y lo habilita para desempeñar otras funciones en cuanto no generen conflicto de intereses".

El artículo 14 del Decreto 64/020 establece que "la designación correspondiente deberá informarse a la Unidad Reguladora y de Control de Datos Personales en un plazo de 90 días a contar del inicio del tratamiento. El artículo 14 citado también establece la obligación de informar todo cese o renuncia del DPD a la autoridad competente".

Por su parte, el artículo 15 del Decreto 64/020 prevé la posibilidad de "designar un único DPD cuando se trate de un conjunto de entidades con cometidos o actividades afines, siempre que éste pueda cumplir cabalmente con las funciones legalmente establecidas en relación con todas y cada una de ellas". Dicha posibilidad también aplica "cuando varias entidades públicas que formen parte de la misma estructura administrativa, lo que se efectuará por resolución fundada, en especial en cuanto a la viabilidad del cabal cumplimiento antes referido".

Finalmente, el artículo 15 aludido indica que "la autoridad competente podrá requerir la designación de delegados de protección de datos adicionales a fin de proteger los derechos de los titulares de los datos en los casos previstos en la presente disposición."

A la fecha no existe un esquema de certificación para Profesionales de Privacidad administrado y/o reconocido por la autoridad de control competente.

Principales desafíos para la adecuada operación de la Figura del Profesional de Privacidad en Latinoamérica

Una vez realizado el análisis legal sobre el estado actual en los países de Latinoamérica, con respecto a la Figura del Profesional de Privacidad, en este capítulo se realiza una sucinta descripción de los que, se consideran, son los principales retos que actualmente existen en la región para la adecuada operación del Profesional de Privacidad.

Regulación

En virtud del análisis realizado en el capítulo anterior sobre la recepción legal de la figura del DPO, DPD u OPD en los distintos países de la región que actualmente cuentan con leyes vigentes de protección de datos personales se puede sostener que un primer reto para la adecuada operación de esta figura es la instauración expresa de esta obligación en las leyes correspondientes a las jurisdicciones analizadas en las que si bien, existen leyes de protección de datos, las mismas no señalan de forma expresa y/o de forma genérica al menos, la obligación de contar con un Profesional de Privacidad al interior de la organización.

Esto es, de las 14 jurisdicciones y marcos normativos analizados, se identificó que solo en 6 de ellas existe el mandato legal expreso de designar un Profesional de Privacidad bajo cualquiera de las denominaciones mencionadas en este documento. Además, se identificó que, en México, por ejemplo, dicha obligación aplica solo al sector público y en cambio, en el sector privado, si bien, el INAI ha emitido recomendaciones relevantes, en la Ley únicamente se hace referencia a una persona responsable sin que se especifique de forma concreta el perfil, funciones y responsabilidades aplicables, pues solo se expresa que la persona o departamento designado debe atender los derechos de los titulares y fomentar la cultura de protección de datos.

De esta forma, es dable sostener que un reto a considerar para que la Figura del Profesional de Privacidad opere de forma adecuada en la práctica de los países de la región es la institución de la obligación de contar con un profesional de este tipo en las leyes vigentes con el propósito de que las organizaciones, tanto públicas como privadas, procedan a

designar Profesionales de Privacidad en el interior de sus organizaciones.

Preparación y capacitación

Dado que la materia de protección de datos personales y las leyes en la materia son de reciente incorporación en los ordenamientos legales de la región, se puede apreciar que en múltiples jurisdicciones existe una necesidad constante de preparación y capacitación de personas sobre el cumplimiento de obligaciones de protección de datos, y muy en particular, sobre la obligación de designar un Profesional de Privacidad.

De acuerdo con la información del capítulo anterior de esta obra, se pudo constatar que de las 14 jurisdicciones analizadas solo en 4 de ellas la APDP ha emitido guías, directrices o documentos de orientación con respecto al cumplimiento de la obligación de designar un Profesional de Privacidad.

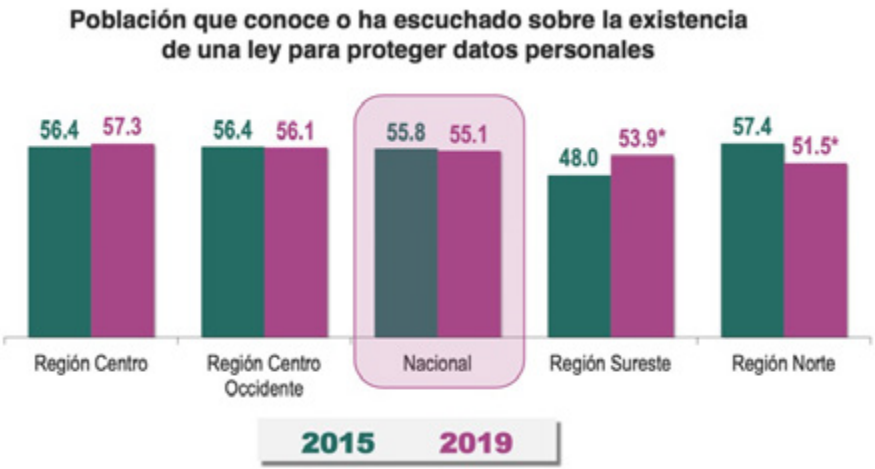
En resumen, se puede señalar que a fin de que la Figura del Profesional de Privacidad tenga una operación que resulte apropiada para demostrar el cumplimiento del principio de responsabilidad es necesario que las autoridades de control competentes de la región y los sujetos obligados fortalezcan las actividades de capacitación y preparación de personas en la materia de protección de datos personales, tanto para el sector público como el privado.

Concienciación

De la mano con el reto anterior, se puede sostener que un desafío visible para la adecuada operación de la Figura del Profesional de Privacidad son las actividades de concienciación a las organizaciones y en la sociedad en general, pues solo en la medida en la que exista mayor conciencia y conocimiento sobre el alcance e importancia de este derecho se podrá configurar un ambiente propicio para la operación de la figura.

Por ejemplo, en México, según los resultados de la Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID) 2019 elaborada por el INEGI en cola-

boración con el INAI[1] "55.1% de la población conoce o ha escuchado de la existencia de una Ley encargada de garantizar la protección de datos personales".

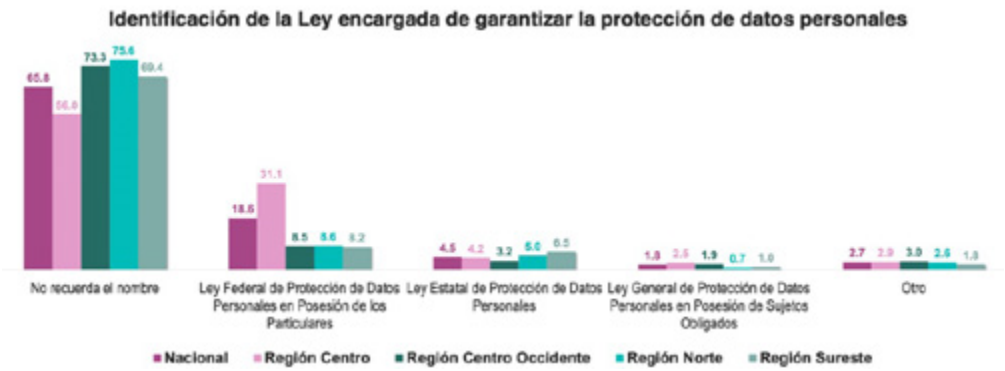


Fuente: INEGI/INAI, Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID) 2019.

En esta tesitura, según datos de la ENAID 2019, "de la población que conoce o ha escuchado una Ley encargada de garantizar la protección de datos personales, 65.8% no recordó el nombre de esta, mientras que 18.6% mencionó la LFPDPPP".[2] Según la ENAID 2019, esto "representa un 10.2% de la población total que conoce la LFPDPPP".[3]

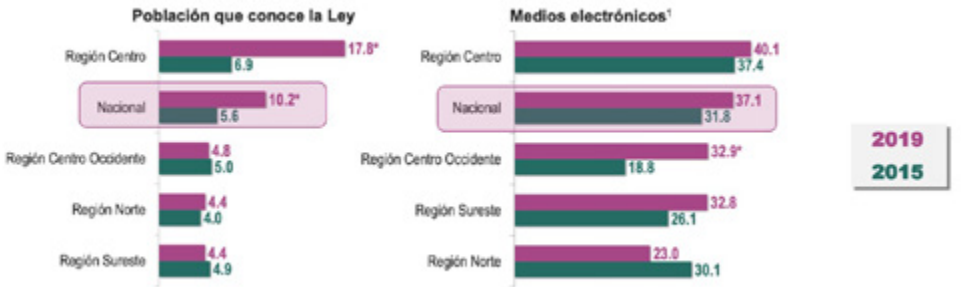
Notas al pie

1. INEGI/INAI, "Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID) 2019, Disponible en https://www.inegi.org.mx/programas/enaid/2019/#Documentacion
2. Ídem
3. Ídem



Fuente: INEGI/INAI, Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID) 2019.

La ENAID 2019 también arrojó que "solo 10.2% de la población identifica la LFPDPPP, de esta, 37.1% se enteró de la Ley a través de medios electrónicos".



Fuente: INEGI/INAI, Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID) 2019.

De acuerdo con lo anterior, si bien, se presentan cifras aplicables a México de forma concreta, se puede sostener que un reto considerable para la operación de la Figura del Profesional de Privacidad es el fomento a la cultura de protección de datos y la socialización de este derecho en general, pues a la fecha una parte importante de la población no conoce la relevancia de este derecho y del marco jurídico que lo regula. Es decir, para que la figura del Responsable de Privacidad opere de forma adecuada es necesario que las personas tengan conocimiento sobre los derechos que les asisten, órganos de tutela existentes, obligaciones de las organizaciones y, por supuesto, de que órgano o persona,

en un caso concreto es quien debe atender las solicitudes para ejercicio de derechos o quejas que se formulen.

Esquemas de certificación

Uno de los aspectos clave para evaluar y constatar las cualificaciones, aptitudes y formación de las personas que aspiran a ser un Profesional de Privacidad reconocido es la certificación, pues, como decíamos, "se trata de una herramienta para la evaluación objetiva e imparcial de la competencia de un individuo para realizar una actividad determinada"[4] y la posesión de dicha certificación se puede considerar como un activo por las organizaciones obligadas a contar con un profesional de dicha categoría.[5] Además, "los mecanismos de certificación pueden mejorar la transparencia para los interesados, pero también las relaciones entre empresas, por ejemplo, entre responsables del tratamiento y encargados del tratamiento,"[6] así como "permitir evaluar el nivel de protección de datos de los productos y servicios correspondientes".[7]

Sin embargo, de los 14 territorios analizados, actualmente en ninguno de ellos existe un esquema de certificación de protección de datos personales y/o de certificación de Profesionales de Privacidad como DPD administrado, autorizado y/o reconocido por la autoridad de control competente. En cambio, se constató que existe únicamente un país (México) en el que existe una propuesta de esquema de certificación siendo aplicable exclusivamente para el sector público, situación que se infiere de la publicación de modi-

Notas al pie

4. Agencia Española de Protección de Datos, *Esquema de Certificación de Delegados de Protección de Datos*, Redactado por el Área de Certificación de la Agencia Española de Protección de Datos,
23 de diciembre 2019. Versión 1.4, p.4, disponible en https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf

5. Centre for Information Policy Leadership (CIPL), *"Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation"*, CIPL GDPR Interpretation and Implementation Project, noviembre de 2016, Disponible en https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf

6. Comité Europeo de Protección de Datos (CEPD), Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento, Versión 3.0, 4 de junio de 2019, Disponibles en https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_es.pdf

7. El considerando (100) del RGPD señala:

...

(100) A fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes.

...

ficaciones a la normatividad aplicable, pues, a la fecha, no se han dado a conocer pormenores de este proyecto.

En relación con lo anterior, es de reconocerse que actualmente el INAI haya reformado la normatividad aplicable para establecer las bases de operación de un esquema de certificación en materia de protección de datos personales para el sector público, pues dicha acción será un diferenciador importante en el papel que juega y seguirá jugando México como un gran referente en materia de protección de datos personales en la región, pues pasará a convertirse en el primer país con un esquema de certificación de protección de datos en la región. Empero, es fundamental que esta actividad también sea analizada y considerada para el sector privado, pues actualmente la LFPDPPP prevé la posibilidad de que los responsables adopten cualquier tipo de esquema de autorregulación en materia de protección de datos personales, ya sea, en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos análogos.[8] Aquí, el INAI deberá retomar su liderazgo y fijar las bases para un esquema de certificación en el sector privado que permita fomentar la protección de datos en las organizaciones mediante la creación de una acreditación objetiva para los Profesionales de Privacidad del sector privado.

Por ello, se puede sostener que uno de los retos principales para que la Figura del Profesional de Privacidad opere de forma idónea en las jurisdicciones de la región en las que su designación es obligatoria, es la confección de esquemas de certificación de protección de datos personales que analicen, validen y acrediten de forma objetiva las competencias, perfil profesional, formación experiencia y actividades de las personas que aspiran a ocupar el cargo de Profesional de Privacidad en una determinada organización, ya sea del sector público o privado.

Notas al pie

8. Artículo 44.- 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 presente Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia en la protección de los datos, consecuencias y medidas correctivas eficaces en caso de incumplimiento.

Conclusiones

- La Figura del Profesional de Privacidad es un componente de enorme relevancia para las organizaciones tanto públicas como privadas que realizan actividades de tratamiento de datos personales. El Profesional de Privacidad se caracteriza por su especialidad técnica en el conocimiento y aplicación de la normatividad vigente de protección de datos personales. Las funciones que este profesional realiza en la práctica son complejas y variadas y, de acuerdo con cada jurisdicción, pueden entenderse como funciones de asesoramiento legal en protección de datos personales frente a todo tipo de tratamientos de datos personales, en particular respecto de aquellos considerados como intensivos o de alto riesgo, atención diligente de los derechos de los titulares, contacto con la APDP, asesoramiento especializado a otras áreas de la organización supervisión en el interior de la organización con respecto a la observancia de la normatividad vigente.
- Las actividades desarrolladas por el Profesional de Privacidad inciden de forma directa y significativa en la tutela del derecho humano a la protección de datos personales, pues la dedicación exclusiva de este individuo a las tareas relacionadas con la gestión adecuada de datos personales y su protección son las bases para la correcta aplicación de la normatividad vigente y la defensa del derecho humano a la protección de datos personales en las organizaciones.
- La promoción, concienciación, capacitación y certificación de los DPD son actividades primordiales para sentar las bases para el adecuado ejercicio de las funciones del DPD en las organizaciones tanto públicas como privadas. Mientras mayores sean los esfuerzos que se dediquen a la preparación técnica de personas especializadas en privacidad y protección de datos personales, mejores serán las condiciones para la tutela efectiva del derecho a la protección de datos personales en las organizaciones, y por supuesto, menores serán los riesgos de que las organizaciones incurran en prácticas relacionadas con el trata-

miento indebido de datos personales, pues, ante todo, la labor del DPD es la de supervisión de cumplimiento de la normatividad vigente.

- A pesar de que la Figura del Profesional de Privacidad es de reciente incorporación en el ámbito nacional e internacional, cierto es que actualmente las funciones que desarrolla el DPD se perfilan como actividades de innegable importancia para las organizaciones que tratan datos personales en cada vez más países de la región, pues el número de normativas que han pasado a reconocer dicha figura ha incrementado en los últimos años, principalmente por la consecución del modelo europeo de protección de datos personales instaurado por el RGPD.
- En México y la región no se cuentan con cifras oficiales o particulares sobre el número de profesionales de privacidad requeridos por cada país en los que existe una ley de datos personales vigente. Tampoco existe un censo o registro oficial sobre la cantidad de Profesionales de Privacidad existentes en cada jurisdicción. No obstante, es claro que mientras más son las organizaciones públicas y privadas que tratan datos personales en el país, mayor es la cantidad de Profesionales de Privacidad que se requieren para vigilar y garantizar el cumplimiento de la normatividad.
- Es ampliamente recomendable que las autoridades competentes de cada país promuevan la realización de un censo sobre Profesionales de Privacidad y/o al menos de aquellas que se dedican a temas de protección de datos y privacidad en las organizaciones a fin de abocar esfuerzos precisos para la preparación técnica, certificación y capacitación de DPD en las organizaciones públicas y privadas.
    - » **Por ejemplo, en el caso de México el INAI podría colaborar con el INEGI en complementar como un rubro del Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales el de estimaciones sobre el número de Profesionales de Privacidad en México tanto en el sector público como en el privado.**

» El INEGI y el INAI podrían colaborar en la medición de profesionales existentes en el sector privado tomando en cuenta los datos de los censos económicos y la cantidad de empresas existentes en México y que realizan tratamientos de datos personales.

• La Figura del Profesional de Privacidad es de reciente incorporación en las normativas de protección de datos personales de la región y derivado del estudio comprensivo de las normativas vigentes de protección de datos personales se determinó lo siguiente:

» De las 14 jurisdicciones y marcos normativos analizados, se identificó que solo en 6 de ellas existe el mandato legal expreso de designar un Profesional de Privacidad bajo cualquiera de las denominaciones mencionadas en este documento y con una descripción más o menos precisa de su perfil, funciones y responsabilidades.
» De las 14 jurisdicciones analizadas solo en 4 de ellas la APDP ha emitido guías, directrices o documentos de orientación con respecto al cumplimiento de la obligación de designar un Profesional de Privacidad, por lo que un gran reto para la adecuada operación de esta figura es la concienciación y capacitación técnica de los DPD, ya sea que estos se dediquen a asesorar a organizaciones públicas o privadas.
» Un desafío visible para la adecuada operación de la Figura del Profesional de Privacidad son las actividades de concienciación a las organizaciones y en la sociedad en general, ya que no existen mecanismos suficientes para la preparación técnica de este tipo de profesionales. Además, la sociedad mexicana poco conoce sobre el tema de privacidad, por ejemplo, en México, según la ENAID 2019 solo 10.2% de la población identifica la LFPDPPP.
» De los 14 territorios analizados, actualmente en ninguno de ellos existe un esquema de certificación de

protección de datos personales y/o de certificación de Profesionales de Privacidad como DPD administrado, autorizado y/o reconocido por la autoridad de control competente, a diferencia del panorama internacional donde encontramos esquemas especializados en países como España y Francia.

- Se constató que únicamente en México existe una propuesta de esquema de certificación siendo aplicable exclusivamente para el sector público, situación que se deriva de la publicación de modificaciones a la normatividad aplicable. No obstante, a la fecha, no se han dado a conocer pormenores de este proyecto y la normatividad del sector privado no ha sido modificada o ampliada a este respecto. En caso de que México logre poner en marcha dicho esquema, se convertirá en el primer referente de la región sobre los esquemas de certificación de DPD reforzando el liderazgo que ha sostenido en los últimos años en el rubro de protección de datos personales.
- Es recomendable que el INAI, de acuerdo con las facultades que le otorgan la LFPDPPP y su Estatuto Orgánico, defina y emita los parámetros normativos para la certificación de Profesionales de Privacidad en organizaciones privadas con el propósito de fomentar la protección de datos personales en dicho sector, difundir la tutela del derecho humano a la protección de datos y, por supuesto, incrementar el nivel de cumplimiento a la Ley que existe en las organizaciones, así como supervisar su cumplimiento desde un enfoque ético y proactivo.
- Los datos identificados, en particular, sobre la regulación legal de la Figura del Profesional de Privacidad en la región conducen a sostener que existe un déficit de profesionales de privacidad en virtud de que en 8 jurisdicciones de las 14 analizadas no existe un mandato legal expreso de contar con dicho funcionario y en aquellas en las que la obligación se encuentra vigente las estimaciones sobre el número de DPD son nulas.

• En virtud de la ausencia de Profesionales de Privacidad en la región resulta imperioso que las autoridades de control competentes y las organizaciones de los sectores público y privado realicen actividades de concienciación, formación y certificación de personas para ocupar el cargo de Profesionales de Privacidad de acuerdo con parámetros objetivos y verificables.

• La ausencia de Profesionales de Privacidad debidamente calificados y certificados por una APDP tiene efectos en la tutela del derecho humano a la protección de datos personales, pues no contar con profesionales encargados de vigilar el cumplimiento de la normativa, asesorar y apoyar en la interpretación y aplicación de esta puede dar lugar a una aplicación deficiente o no observancia del marco jurídico vigente, situación que se traduce en una debilidad institucional sobre la garantía del derecho humano a la protección de datos personales.

• A fin de regular y promover la adecuada operación de la Figura del Profesional de Privacidad en la región es recomendable que:

» **Se actualicen las normativas vigentes en las que actualmente no se prevé dicha figura o se regula de forma deficiente.**

» **Se actualicen las normativas vigentes para prever la existencia de esquemas de certificación generales y en particular los aplicables a la Figura del Profesional de Privacidad.**

» **Las APDP competentes refuercen sus actividades de concienciación, formación y capacitación tanto en el sector público como en el privado.**

» **De acuerdo con las facultades conferidas por las normativas vigentes o en el marco de las mejores prácticas internacionales, las autoridades de control competentes desarrollen y promuevan esquemas de certificación generales y particulares sobre DPD siguiendo los criterios internacionales existentes**

y normas internacionales como las normas EN-ISO/IEC 17000:2004 e ISO/IEC ISO/IEC 17024.

- Que resulta recomendable que las autoridades de control competentes de la región colaboren de forma activa y constante en la mejora de sus marcos jurídicos internos, así como en el diseño de esquemas de certificación generales y para los Profesionales de Privacidad de acuerdo con las normativas, tendencias y mejores prácticas internacionales.

Finalmente, no debe olvidarse también que, si bien la Figura del Profesional de Privacidad se puede perfilar como un componente importante para fomentar la tutela del derecho humano a la protección de datos personales en México y la región, la incorporación de dicha figura en las organizaciones no puede ser vista como una respuesta unívoca para cumplir con la normatividad vigente, sino que, frente a la complejidad de los tratamientos de datos personales, la ingente cantidad de datos tratados y el constante uso de tecnologías emergentes como la IA y el Big Data, las organizaciones deben mantener un estricto compromiso ético frente al tratamiento de datos personales e implementar programas de responsabilidad demostrada con amplios alcances y que respondan de forma proactiva a los desafíos que se derivan de un contexto complejo en el que la tecnología es una realidad omnipresente. Ante todo, se debe poner a la persona como el centro del derecho humano a la protección de datos personales, pues es el individuo el centro de protección de este derecho, y se deben establecer las condiciones para la tutela de sus derechos y libertades fundamentales con independencia del contexto en que ocurra el tratamiento de sus datos personales.

Referencias

Referencias bibliohemerográficas:

Barco Vega, Gregorio, *El derecho humano a la protección de datos personales en México*, Actas del III Coloquio Internacional de Investigadores en Derecho, España, Revista Jurídica de la Universidad de León, núm. 3, 2016, p. 145, Disponible en https://centros.unileon.es/derecho/files/2018/02/Revista-Juridica-ULE-num-3.pdf

Davara Abogados, *Cómo garantizar la protección de los datos personales, Guía Auxiliar para diagnosticar y cumplir con la legislación en la materia al interior de una organización,* **México**, Revista IDC Asesor Jurídico y Fiscal, septiembre de 2017.

Davara F. de Marcos, Isabel, *"Protección de datos personales", en Derechos del Pueblo Mexicano, México a través de sus constituciones,* México, Miguel Ángel Porrúa, 2016.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Isabel Davara F. de Marcos (Coord.), *Diccionario de Protección de Datos Personales*, México, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2020, disponible en http://inicio.inai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf

Guías y documentos de autoridades especializadas:

Agencia Española de Protección de Datos, *Esquema de Certificación de Delegados de Protección de Datos*, Redactado por el Área de Certificación de la Agencia Española de Protección de Datos 23 de diciembre 2019. Versión 1.4, , Disponible en https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf

Autoridade Nacional de Proteçao de Datos, *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, versión 2*, abril, 2022, Disponible en https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf

Comité Europeo de Protección de Datos Personales, *Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento, Versión 3.0*, 4 de junio de 2019, Disponibles en https://edpb.europa.eu/sites/default/files/files/file1/edpb_guide

lines_201801_v3.0_certificationcriteria_annex2_es.pdf

Commission Nationale de l'Informatique et des Libertés (CNIL), *Certification scheme of DPO skills and knowledge*, Disponible en https://www.cnil.fr/sites/default/files/atoms/files/cnil_certification-scheme-dpo-skills-and-knowledge.pdf

Datatilsynet, *Encuesta al Delegado de Protección de Datos Sobre las condiciones laborales de los Delegados de Protección de Datos y el cumplimiento de la legislación de protección de datos en las empresas noruegas*, septiembre, 2021.

Grupo de Trabajo sobre Protección de Datos del Artículo 29, *"Directrices sobre los delegados de protección de datos (DPD)"*, Adoptadas el 13 de diciembre de 2016, Revisadas por última vez y adoptadas el 5 de abril de 2017, disponibles en https://www.aepd.es/es/documento/wp243rev01-es.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), *Recomendaciones para la Designación de la Persona o Departamento de Datos Personales*, Disponibles en https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/RecomendacionesDesignar.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), *"Recomendaciones para los sujetos obligados en la designación del oficial de protección de datos personales"*, Disponibles en https://home.inai.org.mx/wp-content/uploads/Recomendaciones-para-los-sujetos-obligados-en-la-designación-del-oficial-de-protección-de-datos-personales-1.pdf

Reporte titulado *"Monitoring compliance of EU institutions and bodies with Article 24 of Regulation (EC) 45/2001, Report on the Status of Data Protection Officers elaborado por el Supervisor Europeo de Protección de Datos* elaborado en diciembre de 2012 y que se encuentra en https://edps.europa.eu/data-protection/our-work/publications/reports/report-status-data-protection-officers-dpos_en

Superintendencia de la Industria y Comercio de Colombia (SIC), *Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)*, Disponible en https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Unidad Reguladora y de Control de Datos Personales, *Documento de Trabajo sobre Delegado de Protección de Datos Personales*, Disponible en https://www.gub.uy/unidad-reguladora-control-datos-personales/sites/unidad-reguladora-control-datos-personales/files/documentos/publicaciones/Documento%20de%20trabajo%20Delegado%20de%20PDP.pdf

Normatividad empleada: Normatividad nacional

Constitución Política de los Estados Unidos Mexicanos.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos Generales de Protección de Datos Personales para el Sector Público.

ACUERDO mediante el cual se aprueba la adición de un título décimo primero a los Lineamientos Generales de Protección de Datos Personales para el Sector Público y la modificación y adición de una fracción XXV al artículo 25 y una fracción XIII al artículo 42 del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Normatividad internacional Normativa europea

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Normatividad vigente en Latinoamérica: Argentina

Ley 25.326
Decreto 1558/2001

Brasil

Ley General de Protección de Datos (Ley N° 13.709/2018)
Resolución CD/ANPD Nº 2

Chile

Ley No. 19.628 sobre Protección a la Vida Privada

Colombia

Ley Estatutaria No. 1581
Decreto 1377 de 2013 que Reglamenta parcialmente la Ley 1581 de 2012
Decreto 620 de 2020

Costa Rica

Ley No. 7975
Ley No. 8968
Decreto Ejecutivo No. 37554-JP del 30 de octubre del 2012

Ecuador

Ley Orgánica de Protección Datos Personales

Nicaragua

Ley de Protección de Datos Personales

Panamá

Ley 81 de 2019 sobre Protección de Datos Personales
Reglamento de la Ley 81

Paraguay

Ley No. 1682
Ley 1969

Perú

Ley No. 29733 de Protección de Datos Personales
Reglamento de la ley 29733
República Dominicana
Ley No. 172-13

Uruguay

Ley 18.331 de Protección de Datos Personales y Acción de Habeas Data
Ley No. 19.030
Ley N° 19670
Decreto N° 64/020
Decreto 414/009

Normatividad soft law empleada:

Red Iberoamericana de Protección de Datos (RIPD) *"Estándares de Protección de Datos para los Estados Iberoamericanos"* Disponibles en https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

Criterios jurisprudenciales:

Tesis de jurisprudencia 2a./J. 35/2019 (10a.) con rubro *PRINCIPIO DE PROGRESIVIDAD DE LOS DERECHOS HUMANOS. SU NATURALEZA Y FUNCIÓN EN EL ESTADO MEXICANO*, publicada en la Gaceta del Semanario Judicial de la Federación, Libro 63, febrero de 2019, Tomo I, página 980.

Documentos publicados en internet:

Centre for Information Policy Leadership (CIPL), *"Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Pro*

tection Regulation", CIPL GDPR Interpretation and Implementation Project, noviembre de 2016, Disponible en https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf

Instituto Nacional de Estadística, Geografía e Informática (INEGI)/ Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), *"Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales" (ENAID)* **2019**, Disponible en https://www.inegi.org.mx/programas/enaid/2019/#Documentacion

Instituto Nacional de Estadística, Geografía e Informática (INEGI), *"Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Federal 2021"*, Disponible en https://www.inegi.org.mx/programas/cntaippdpf/2021/

Instituto Nacional de Estadística, Geografía e Informática (INEGI), *"Las empresas en los Estados Unidos Mexicanos: Censos Económicos 2019"*, 2020, Disponible en https://www.inegi.org.mx/contenidos/productos/prod_serv/contenidos/espanol/bvinegi/productos/nueva_estruc/702825198817.pdf

Instituto Nacional de Estadística, Geografía e Informática (INEGI), *COMUNICADO DE PRENSA NÚM. 305/20 16 DE JULIO DE 2020*, https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2020/OtrTemEcon/CenEconResDef2019_Nal.pdf

Instituto Nacional de Estadística, Geografía e Informática (INEGI), *COMUNICADO DE PRENSA NÚM. 299/22 26 DE MAYO DE 2022*, Disponible en https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/denue/denue2022.pdf

International Association of Privacy Professionals (IAPP), *"Study: GDPR's global reach to require at least 75,000 DPOs worldwide"*, 9 de noviembre de 2016, Disponible en https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/

International Association of Privacy Professionals (IAPP), *"Study: An estimated 500K organizations have registered DPOs across Europe"*, Mayo 2019, Disponible en https://iapp.org/news/a/study-an-estimated-500k-organizations-have-registered-dpos-across-europe/

ISMS Forum España, *"El libro Blanco del DPO",* España, Disponible en https://www.ismsforum.es/ficheros/descargas/el-libro-blanco-del-dpo---isms-forum-y-data.pdf

Kiran Bhageshpur, *"Data Is The New Oil -- And That's A Good Thing"*, Forbes, 2019, disponible en https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/#29aa27157304

PricewaterhouseCoopers, ASUG, *Estudio de la privacidad en México 2016: más allá de los compromisos*, 2017, Disponible en https://asug.mx/wp-content/uploads/2017/06/20170602-pg-flyer-estudio-privacidad-asug.pdf

PricewaterhouseCoopers, Entrada *"Más del 50% de las empresas mexicanas asegura que su industria podría sufrir incidentes de ciberseguridad"*, 11 de noviembre de 2020, Disponible en https://www.pwc.com/mx/es/prensa/archivo/2020/20201111-dti-vf1.pdf

The EU-funded "T4DATA" programme, (Grant Agreement number: 769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01), *"The DPO Handbook, Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, (Regulation (EU) 2016/679)*, Disponible en https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf

Anexo

Leyes de protección de datos en Latinoamérica

País	Ley aplicable	Recomendaciones de APDP
Argentina	Ley 25.326 Decreto 1558/2001	No
Brasil	Ley General de Protección de Datos Resolución CD/ANPD Nº 2 de 27 de enero de 2022	Sí. Se ha publicado la Guía Orientadora de Definiciones de Agentes de Tratamiento de Datos Personales y Responsable.
Chile	Ley No. 19.628 sobre Protección a la Vida Privada	No
Colombia	Ley Estatutaria No. 1581 Decreto 1377 Decreto 620 de 2020	Sí. La SIC emitió la Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability) en la que se aborda la figura del OPD.
Costa Rica	Ley No. 7975 Ley No. 8968 Decreto Ejecutivo No. 37554-JP del 30 de octubre del 2012	No
Cuba	Ley 149/2022 “De Protección de Datos Personales”	No
Ecuador	Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales	No

México (sector privado)	Ley Federal de Protección de Datos Personales en Posesión de Particulares Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares	Sí. El INAI ha emitido las Recomendaciones para la Designación de la Persona o Departamento de Datos Personales.
México (sector público)	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados Lineamientos Generales de Protección de Datos Personales para el Sector Público	Sí. El INAI ha emitido las Recomendaciones para los sujetos obligados en la designación del oficial de protección de datos personales.
Nicaragua	Ley de Protección de Datos Personales	No
Panamá	Ley 81 de 2019 sobre Protección de Datos Personales Reglamento de la Ley 81	No
Paraguay	Ley No. 1682 Ley 1969	No
Perú	Ley No. 29733 de Protección de Datos Personales Reglamento de la ley 29733.	No
República Dominicana	Ley No. 172-13	No

Uruguay	Ley 18.331 de Protección de Datos Personales y Acción de Habeas Data Decreto 414/009 Ley No. 19.030 Ley N° 19670 Decreto N° 64/020	Sí. La Unidad Reguladora y de Control de Datos Personales ha publicado un documento de trabajo sobre DPD.

Leyes de protección de datos en Latinoamérica

País	¿Es obligatorio designarlo?	Perfil	Funciones	¿Existe certificación para DPD o similar?
Argentina	No	No se define	No se definen	No
Brasil	Sí. Sin embargo, de acuerdo con la Resolución CD/ANPD N° 2 este requisito no aplica para las pequeñas empresas	Se recomienda considerar los conocimientos en protección de datos y seguridad de la información a un nivel que satisfaga las necesidades de las operaciones de tratamiento de datos personales de la organización.	•Aceptar quejas y comunicaciones de los titulares, brindar aclaraciones y adoptar medidas; •Recibir comunicaciones de la autoridad nacional y adoptar medidas •Orientar a los empleados y contratistas de la entidad sobre las prácticas a ser adoptadas en relación a la protección de datos personales; y •Ejercer otras atribuciones determinadas por el controlador o establecidas en normas complementarias.	No

Chile	No	No se define	No se definen	No
Colombia	En el Decreto 1377 se establece la obligación de Responsables y Encargados de designar a una persona o área que asuma la función de protección de datos personales y dé trámite a las solicitudes de los Titulares. El Decreto 620 de 2020 establece que todo responsable y encargado deberá designar a una persona o área que asuma la función de protección de datos personales, quien dará trámite a las solicitudes de los Titulares, quien deberá, además de cumplir los lineamientos de la SIC	No se define	•Velar por el respeto de los derechos de los titulares de los datos personales respecto del tratamiento de datos que realice el prestador de servicios ciudadanos digitales. •Informar y asesorar al prestador de servicios ciudadanos digitales en relación con las obligaciones que les competen en virtud de la regulación colombiana sobre privacidad y tratamiento de datos personales. •Supervisar el cumplimiento de lo dispuesto en la citada regulación y en las políticas de tratamiento de información del prestador de servicios ciudadanos digitales, así como del principio de responsabilidad demostrada.	No

			•Prestar el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos. •Atender los lineamientos y requerimientos que le haga la Delegatura de Protección de Datos Personales de la SIC o quien haga sus veces.	
Costa Rica	No	No se define	No se definen	No
Cuba	No	No se define	No se definen	No
Ecuador	Sí. De acuerdo con los supuestos numerados en el artículo 48.	No se define	•Asesorar al responsable, al personal del responsable y al encargado del tratamiento de datos personales, sobre las disposiciones contenidas en la LOPD, su reglamento, las directrices, lineamientos y demás regulaciones. •Supervisar el cumplimiento de las disposiciones contenidas en la LOPD, su reglamento,	

			las directrices, lineamientos y demás regulaciones emitidas por la APDP; •Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, y supervisar su aplicación; •Cooperar con la APDP y actuar como punto de contacto con dicha entidad, con relación a las cuestiones referentes al tratamiento de datos personales; y •Las demás que llegase a establecer la APDP con ocasión de las categorías especiales de datos personales.	

México (sector privado)	De acuerdo con lo previsto por el artículo 30 de la Ley se debe designar una persona responsable o departamento de datos personales.	Las Recomendaciones señalan que la persona que tenga a su cargo o bajo su responsabilidad la función de protección de datos personales en posesión de la organización del responsable deberá poseer experiencia en materia de protección de datos personales, tener jerarquía o posición indicada dentro de la organización, contar con recursos suficientes, contar con conocimiento en la materia, visión y liderazgo para implementar la política de privacidad a lo largo de la organización y habilidades de organización y comunicación.	•Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales •Gestionar las solicitudes para el ejercicio de los derechos ARCO. •Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados. •Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, de acuerdo con las normativas aplicables. •Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.	No. Sin embargo, cabe señalar que se han modificado los LGPDPSP y el Estatuto Orgánico del INAI para establecer las bases del funcionamiento de un esquema de certificación.

			•Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO. •Asesorar a las áreas adscritas al responsable en materia de protección de datos personales.	
Nicaragua	No	No se define	No se definen	No
Panamá	Sí en el sector público. En el sector privado es optativo.	De acuerdo con el Reglamento se requiere una experiencia profesional previa en la materia y el conocimiento del sector de actividad de la entidad pública o privada en la que ejercerá sus funciones.	•Participar en tiempo y forma en las cuestiones referidas a la protección de datos personales. •Informar y asesorar al responsable del tratamiento o al custodio de la base de datos en las cuestiones relacionadas con el cumplimiento de la Ley 81 de 2019, del decreto o de cualquier disposición legal aplicable en cada caso.	

			·Supervisar el cumplimiento de la normativa. Para ello podrá examinar, a solicitud del responsable del tratamiento o del custodio de la base de datos o por iniciativa propia, tratamientos de datos personales que se estén llevando a cabo y realizar recomendaciones para la adopción de medidas correctoras necesarias cuando los tratamientos analizados no sean conformes con la normativa aplicable. ·Promover la capacitación de las personas que asuman tareas relacionadas con el tratamiento de los datos personales. ·Cooperar con la autoridad de control. ·Ser la unidad de enlace con la autoridad de control.	

			•Asesorar al responsable del tratamiento o al custodio de la base de datos en la respuesta a los requerimientos u observaciones formalmente notificados por la autoridad de control. •Ser la unidad de enlace con los titulares de los datos para las cuestiones relativas al tratamiento de los datos y a sus derechos.	
Paraguay	No	No se define	No se definen	No
Perú	No	No se define	No se definen	No
República Dominicana	No	No se define	No se definen	No
Uruguay	Sí. En los siguientes casos previstos en el Decreto 64/020: •Entidades públicas, estatales o no estatales y las privadas total o parcialmente de propiedad estatal.	•Conocimientos especializados en Derechos Humanos, con especial énfasis en Protección de Datos Personales •Poseer práctica en materia de Protección de Datos Personales.	•Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales. •Supervisar el cumplimiento de la normativa sobre dicha protección en su entidad.	

	•Entidades privadas que traten datos sensibles como negocio principal. De conformidad con lo establecido por el artículo 4° literal E) de la Ley N° 18.331 de 11 de agosto de 2008, son datos sensibles aquellos que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e información referente a la salud o a la vida sexual. •Entidades privadas que realicen tratamiento de grandes volúmenes de datos.[1]	Poseer práctica en materia de Protección de Datos Personales. •Aptitud para la adopción e implementación de las medidas dirigidas a la Protección de Datos Personales. •Contar con conocimiento del sector en el que desempeñará sus funciones. •Poseer capacidad de comunicación, habilidades personales y de negociación y conocimiento de gestión de riesgos.	•Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en materia de protección de datos personales. •Actuar como nexo entre su entidad y la Unidad Reguladora y de Control de Datos Personales.	

[1] Se considera tratamiento de grandes volúmenes de datos cualquier actividad en la que se realice un tratamiento de datos personales de más de 35,000 personas.

La Figura del Profesional de Privacidad en Latinoamérica. Estado actual y principales desafíos para su adecuada operación
Primera edición, noviembre 2023

Edición a cargo de la Dirección General de Promoción
y Vinculación con la Sociedad


inai
Instituto Nacional de Transparencia, Acceso a la
Información y Protección de Datos Personales