BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

INSTITUTO DE CIENCIAS DE GOBIERNO Y DESARROLLO ESTRATÉGICO

Los factores que inciden en el cumplimiento de las políticas de protección de datos personales en las organizaciones: estudios de caso de escuelas particulares

T E S I S

Para obtener el grado de Doctora en Ciencias de Gobierno y Política

PRESENTA

Nadia Vélez Campos

ASESORES

Dr. Víctor Manuel Figueras Zanabria

Dr. Gabriel Purón Cid

Puebla, Pue. Julio, 2018

ÍNDICE

ÍNDICE DE TABLAS E ILUSTRACIONES **4**

GLOSARIO **5**

INTRODUCCIÓN **7**

CAPÍTULO I **20**

LA PROTECCIÓN DE LOS DATOS PERSONALES, UNA OBLIGACIÓN PARA LOS RESPONSABLES **20**

La definición de la protección de datos personales versus la *privacy* en la literatura **22**

La sanción como mecanismo de cumplimiento en leyes y tratados internacionales **31**

El papel de las autoridades de protección de datos ante el cumplimiento **35**

La exhaustividad de las leyes de protección de datos personales en la actualidad **38**

CAPÍTULO II **45**

LA NORMATIVIDAD QUE GARANTIZA EL CUMPLIMIENTO DE LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO **45**

El cumplimiento de la protección de datos personales en el marco jurídico mexicano **45**

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares como instrumento de cumplimiento **52**

a) Desarrolla principios internacionalmente reconocidos 52

b) Contiene los derechos ARCO 54

c) Establece procedimientos con los que los responsables deben de cumplir para garantizar el ejercicio de los derechos ARCO 58

d) Contempla infracciones y sanciones para quien realice conductas inadecuadas con relación al trato de la información 59

Las funciones del Inai ante los sujetos obligados **63**

Sanciones impuestas a los particulares por incumplimiento con la LFPDPPP **67**

Conclusión **68**

CAPÍTULO III **70**

TEORÍAS QUE EXPLICAN AL CUMPLIMIENTO **70**

Los modelos teóricos vinculados con el cumplimiento en las organizaciones **70**

Teorías vinculadas con el estudio del cumplimiento y la seguridad de la información **77**

Conclusión **82**

CAPÍTULO IV **87**

LOS PILARES DEL CUMPLIMIENTO EN LA TEORÍA INSTITUCIONAL **87**

Teoría institucional **87**

Los tres pilares de la teoría institucional **88**

Conclusión **98**

CAPÍTULO V **110**

ABORDAJE METODOLÓGICO **110**

Estrategia de investigación **111**

a) Selección de casos 111
b) Instrumento 117
c) Operacionalización de variables 119
d) Mapa de actores 123

CAPÍTULO VI 128

RESULTADOS 128
Caso A 128
Caso 2 143
Discusión 154

CAPÍTULO VII 169

CONCLUSIONES 169

BIBLIOGRAFÍA 176

Anexo 1. Tabla comparativa entre la LFPDPPP y la LFTAIPG 187

Anexo 2. Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Inai, 2014). 193

Anexo 3. Guía de preguntas 200

Anexo 4. Aviso de Privacidad Integral del Caso 1 202

Anexo 5. Aviso de Privacidad del Caso 2 211

ÍNDICE DE TABLAS E ILUSTRACIONES

Tabla 1 Leyes nacionales de protección de datos personales y privacidad 2016. Fuente: Banistar (2016) 39
Tabla 2 Leyes de protección de datos personales del mundo. Fuente: DLA Piper (2016) 42
Tabla 3 Principios de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares 54
Tabla 4 Derechos ARCO. Fuente: Estándares Internacionales sobre Protección de Datos Personales y Privacidad 58
Tabla 5 Artículos que establecen infracciones en la LFPDPPP. Fuente: Elaboración propia. .. 62
Tabla 6 Procedimiento de imposición de sanciones. Fuente: Curso de Introducción a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Inai (2013) 66
Tabla 7 Teorías que explican el cumplimiento de las políticas en las organizaciones. Fuente: elaboración propia. 83
Tabla 8 Tres pilares de la institucionalización (Scott, 2008; Geels, 2004) 90
Tabla 9 Factores institucionales que afectan el flujo de las empresas transnacionales y el outsourcing de las TI. Fuente: Kshetri (2007) 95
Tabla 10 Factores condicionantes en la implementación de políticas de sistemas de seguridad de la información. Fuente: Lopes y de Sá-Soares (2014) 96
Tabla 11 Factores de los tres pilares en diferentes áreas. Fuente: Geels (2004) 97
Tabla 12 Tabla de variables dependiente e independientes. Fuente: Elaboración propia. 108
Tabla 13 Selección de casos. Fuente: elaboración propia. 116
Tabla 14 Cuestionario. Fuente: Elaboración propia. 123
Tabla 15 Diagrama de flujo de datos personales en una organización. Fuente: elaboración propia. 124
Tabla 16 Factores que incidieron en el cumplimiento de las políticas de protección de datos personales en los estudios de caso. Fuente: Elaboración propia. 154

GLOSARIO

Aviso de Privacidad: documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la LFPDPPP.

Base de datos: el conjunto ordenado de datos personales referentes a una persona identificada o identificable.

Consentimiento: manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

Datos personales: cualquier información concerniente a una persona física identificada o identificable.

Datos personales sensibles: aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Disociación: el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

Encargado: la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

Instituto: Instituto Nacional de Acceso a la Información y Protección de Datos.

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

TIC: Tecnologías de la información.

Titular: la persona física a quien corresponden los datos personales.

Tratamiento: la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Transferencia: toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.

INTRODUCCIÓN

Los Estándares Internacionales sobre Protección de Datos Personales y Privacidad de 2009 —documento comúnmente identificado como la Resolución de Madrid (CINPPC, 2009) —, son el resultado de una labor conjunta de casi cincuenta países que se reunieron en la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad en 2009 (CIDPPC por sus siglas en inglés), y definen un dato de carácter personal como “cualquier información concerniente a una persona física identificada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados”. Estos datos pueden ser nombre, edad, teléfono, dirección, datos bancarios, dirección IP (*Internet Protocol*) o cualquier otra información que permita identificar o hacer identificable a una persona.

La Resolución de Madrid también considera a los datos personales sensibles de carácter personal como aquellos que: “a) Afecten a la esfera más íntima del interesado; o b) Cuya utilización indebida pueda: i) Dar origen a una discriminación ilegal o arbitraria, o ii) Conllevar un riesgo grave para el interesado”. Específicamente, los datos personales sensibles tienen que ver con la intimidad de la persona y pueden revelar aspectos relacionados con la salud, preferencia sexual, origen racial o étnico, religión, ideología, características físicas, si pertenece a algún partido político o si está afiliado a algún grupo sindical. El mal uso de esta información podría hacer víctima a la persona de discriminació n o amenazar sus derechos.

En la actualidad, la protección de datos personales es indispensable para el desarrollo de diferentes actividades económicas, políticas y sociales de los individuos y las organizaciones públicas y privadas. Gracias a las nuevas tecnologías de la información hay un flujo masivo de datos personales y son materia prima de la economía global. *Data, data everywhere, A special report on managing information* de The Economist (2010) menciona que, para 2010, empresas como Wal-Mart procesaban más de un millón de transacciones por hora de sus clientes y que Facebook almacenaba alrededor de 40 billones de fotografías. Otras firmas como Oracle, IBM y Microsoft han invertido

más de quince billones de dólares en la compra y desarrollo de software especializado en el manejo y análisis de datos. Esta industria, de análisis de datos, para 2010 tenía un valor estimado de más de cien billones de dólares y reportaba un crecimiento anual de casi diez por ciento.

En 2013 la OECD elaboró un estudio titulado *Exploring the Economics of Personal Data. A survey of methodologies for measuring monetary value*, con la finalidad de analizar un conjunto de metodologías para medir y estimar el valor monetario de los datos personales ante la carencia de un modelo internacionalmente reconocido. A pesar de sus intentos por realizar esta tarea, el estudio reconoce su dificultad debido a la gran cantidad de datos que se generan y que se usan para distintos fines. En este estudio, la OECD (2013) calcula el valor de los datos con base en la valuación del mercado y del individuo. Por ejemplo, un usuario activo de Facebook tiene un valor monetario de 149 dólares —con una capitalización de mercado de 201.3 billones de dólares y mil 350 millones de usuarios a nivel mundial— y uno de Twitter 114 dólares —con una capitalización de mercado de 32.5 billones de dólares y 284 millones de usuarios—.

En 2016 la Asociación Mexicana de Internet (Amipci por su acrónimo) desarrolló un documento titulado “Estudio sobre el valor económico de los datos personales” y utiliza esta metodología para calcular el valor monetario de un cliente de la empresa América Móvil (Telcel y Telmex), de 711 billones de pesos capitalización de mercado y 74 millones de clientes. Para esta compañía, los datos de un cliente valen 9 mil 670 pesos. De acuerdo con Amipci (2016), la metodología basada en capitalización de mercado es difícil de aplicar en México porque hay una participación limitada de empresas emisoras de acciones, además de que puede sobreestimar el valor de los datos personales.

Otra manera de calcular el valor de los datos personales que podría aproximarse a su valor real es mediante el cálculo del valor monetario que se basa en el ingreso bruto por registro. Esta metodología da un valor de seis dólares por usuario activo de Facebook, de 3.25 dólares de Twitter —que es una diferencia muy significativa a la de capitalización de mercado—, y diez mil 695 de América Móvil. Sobre esta metodología,

Amipci (2016) reconoce que es difícil de aplicar porque únicamente las empresas que participan en mercados de valores publican sus estados financieros.

En el documento, la OECD (en Amipci, 2016) también propone calcular el valor de los datos personales con las sanciones económicas impuestas por las violaciones en el tratamiento de los datos personales, que reflejan un valor de mercado real y el riesgo para las empresas. Sin embargo, como inconvenientes a este método, el cálculo se realiza conforme a los incumplimientos de la normatividad, no se consideran los costos de los daños causados por la violación de los datos personales y no incluye los costos de dañar la reputación empresarial.

Otra metodología que Amipci (2016) revisa es la valoración del individuo, y destaca que no existe una medida única del valor de los datos personales, sino que cada individuo estima el valor de sus datos de acuerdo con el tipo de información que provee y el uso que se vaya a hacer de ellos. Un estudio que Frog (en Amipci, 2016) realizó en Estados Unidos, India y China muestra tres niveles de datos con diferente valor monetario. En el nivel más alto los datos valen de dos mil 380 pesos hasta tres mil 360 pesos, incluye datos como número de seguridad social e información bancaria; en el nivel medio, que incluye historial y comportamiento de navegación (ubicación y compras en línea), los datos valen de 560 a 700 pesos y, en el nivel más bajo, que contiene datos básicos, tienen un valor de 42 a 84 pesos.

De acuerdo con información publicada en *The Financial Times* en 2013, los datos de una persona promedio se venden por menos de un dólar. Información tal como edad, sexo y su ubicación cuesta 0.0005 dólares, o 50 centavos de dólar por mil sujetos. Una persona que va a adquirir un carro, un producto financiero o unas vacaciones es más valiosa para las empresas que venden esos productos o servicios. Por 26 centavos por persona, los compradores acceden a listas de personas con problemas de salud o que toman medicamentos específicos. *Financial Times* (2013) desarrolló un calculador de su valor, de acuerdo con este, los datos personales de alguien con un perfil más especializado, por ejemplo, un profesionista, recién casado, con bebé, que padece determinadas enfermedades, con crédito bancario, propiedades, gustos e intereses

diversos, que practica diferentes actividades, pueden valer cinco dólares, por lo que, una base de datos de mil consumidores con este perfil puede costar hasta 5 mil dólares.

Actualmente existen páginas como *datacoup.com* que ofrecen a las personas de Estados Unidos obtener una ganancia por sus datos personales. Esta plataforma almacena datos financieros, demográficos, laborales, de educación, así como de redes sociales (Facebook, Twitter, Foursquare) y aplicaciones bancarias directamente de los titulares de los datos personales; los disocia para que la identidad del titular no sea revelada y los ofrece al mercado para su venta. El valor de los datos personales se estima dependiendo de la información que proporcionen. La plataforma se encarga de notificar a la persona cada vez que compran sus datos personales y les hace el pago vía *Stripe* o transferencias bancarias. Las personas pueden cobrar cuando su ganancia alcanza los cinco dólares y la plataforma congela la venta cuando llega a 25 dólares y el titular no los ha cobrado.

Dado el valor económico de los datos personales, las organizaciones públicas y privadas almacenan grandes cantidades para diferentes fines. En años recientes, las violaciones a su seguridad han puesto en evidencia la necesidad de resguardarlos. No solo los utilizan los gobiernos, organizaciones e individuos en lo particular, sino también para efectos criminales y su compra-venta ocurre en el mercado ilegal, que también les otorga un valor económico. Por ejemplo, en 2010 se dio a conocer en México la venta ilícita de bases de datos por 12 mil dólares en Tepito. En tres memorias externas era posible adquirir el padrón electoral, el registro vehicular y de licencias de conducir, datos de los policías, el parque vehicular del servicio federal, entre otros (Vélez, 2011). También, recientemente, la lista nominal de electores que se entrega a los partidos políticos en México, conformada por datos de 83.5 millones de mexicanos, estaba disponible al acceso público en el portal de Amazon de Estados Unidos (Animal Político, 2016).

Las consecuencias para los titulares de un mal uso de sus datos personales, ya sea que fueron perdidos accidentalmente o plagiados intencionalmente, pueden ser

significativas. Entre estas consecuencias, el Reglamento 679 (DOUE, 2016) menciona los daños y perjuicios físicos, materiales o inmateriales, como: pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio responsable del tratamiento relacionado con la pérdida de la seguridad de los datos personales. Sobre esto, en México, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef, 2016) registró 53 mil denuncias de posible robo de identidad con pérdidas para las víctimas del delito de 653 millones de pesos en 2016.

Para las organizaciones, el no cumplimiento y la violación a las políticas de protección de datos personales puede terminar en una sanción, divulgación no deseada, disminución de oportunidades de negocios o pérdidas económicas y de prestigio. En 2011, Sony sufrió una serie de ataques cibernéticos y reportó el robo de los datos personales de 77 millones de usuarios de PlayStation y de 25 millones de usuarios de Sony Online Entertainment —nombre, dirección, correo electrónico, sexo, fecha de nacimiento, nombre de usuario y contraseña, y también datos bancarios—. Tan solo por PlayStation, sus pérdidas fueron de 2 mil millones de dólares (Mendoza, 2012 y EFE, 2011).

Como resultado, la seguridad de los datos personales es un tema que concierne no sólo a los individuos y las organizaciones, sino también a los gobiernos (OECD, 2011). Diferentes reglamentos, tratados y resoluciones internacionales, indican la necesidad de que las sociedades modernas y sus gobiernos adopten políticas que permitan su procesamiento a la vez que garanticen su protección para preservar los derechos de los interesados.

Prueba de esto es el caso que se presentó después del 11 de septiembre de 2001, cuando la Unión Europea cerró acuerdos con otros Estados, como Estados Unidos, Canadá y Australia, para investigar y transferir los datos de quienes viajen entre esos países. Antes de 2001, las aerolíneas almacenaban estos datos únicamente con fines

comerciales, no tenían ningún propósito de investigación y no se relacionaban con el combate contra el terrorismo y el crimen organizado. Al paso de los años, la recolección de los datos personales se ha convertido en una actividad importante para detectar pasajeros peligrosos y tomar medidas preventivas antiterroristas necesarias (Nino, 2010).

Estas medidas preventivas de los gobiernos han ido al extremo de que algunos países de la Unión Europea impulsen iniciativas como la Directiva de 2002 y 2006 sobre la Retención de Datos, que buscan obligar a los proveedores de servicios de telecomunicaciones a recopilar datos sobre el tráfico electrónico de sus clientes y almacenarlos durante largos periodos de tiempo, con el fin de que las agencias policiacas y de seguridad nacional puedan acceder a ellos cuando sea necesario (Clarke, 2015). Todo esto a pesar de que el Supervisor Europeo de la Protección de Datos (EDPS por sus siglas en inglés) opine que la Directiva de Retención de Datos es, sin duda, el instrumento más invasor de la privacidad que haya adoptado la UE porque recopila datos personales indiscriminadamente y los somete a vigilancia (Hustinx, 2011).

El uso de las tecnologías de la información también ha hecho patente la necesidad de proteger los datos personales porque facilitan su almacenamiento, transferencia, pérdida o robo. Por ejemplo, *Data Breach Report* (Identity Theft Resource Center, 2015) reporta que, en Estados Unidos, durante 2015, hubo 411 pérdidas de bases datos personales en el sector financiero, negocios, educación, gobierno y salud, que se expusieron 11 millones, 678 mil cincuenta datos, ocasionados por *hacking*, transferencias a terceros, error o negligencia de un empleado, publicación en Internet o robo desde el interior de la empresa con dispositivos electrónicos. La información que más se ve comprometida en estas pérdidas es: número de seguridad social, números de tarjeta bancaria, cuentas de correo electrónico y datos de salud.

Otra función con la que cumplen las tecnologías emergentes es la vigilancia inteligente, como sistemas de verificación (datos biométricos para acceder a lugares controlados), detección y monitoreo (sensores que detectan explosivos o artículos prohibidos) o

información vinculante (historial crediticio) (Wright, Friedewald y Gellert, 2015). Las tecnologías de la información almacenan, monitorean, analizan, ponen a disposición y comparten con otros usuarios —personas, empresas, gobiernos— millones de datos personales. Se trata de sistemas intrusivos que deben regularse con sistemas legales robustos para prevenir la violación de los derechos fundamentales de sus titulares. Para esto, diferentes áreas como la informática y el derecho han desarrollado mecanismos que garantizan la seguridad de los datos, entre los que se encuentran leyes, lineamientos, tratados y distintas políticas. Actualmente, alrededor de cien países en el mundo cuentan con leyes de protección de datos personales que, en un principio, estuvieron motivadas por el avance de la tecnología que vulnera la seguridad de los datos.

En México, la Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (Enaid) (Inegi, 2016) destaca que 95.6% de la población urbana ha proporcionado alguna vez sus datos personales a las instituciones públicas o privadas —44.43 millones—; y 4.4% nunca lo ha hecho —1.87 millones—. Únicamente a empresas particulares, 79.22% de la población les ha entregado datos como nombre, domicilio, teléfono, sueldo y creencias religiosas. Esto quiere decir que las organizaciones tienen en su posesión la información de ocho de cada diez habitantes. En nuestro país existe normatividad que obliga a las organizaciones tanto del sector público como del sector privado a proteger los datos personales. No obstante, en el comunicado 404 del Instituto Nacional de Acceso a la Información Pública y Protección de Datos (Inai), con fecha de noviembre de 2016, el Instituto da a conocer que, desde la entrada en vigor de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), en 2012, a noviembre de 2016, resolvió diferentes Procedimientos de Imposición de Sanciones (Pisan) y, en 55 de estos casos, impuso una sanción económica a las organizaciones y/o personas físicas por incumplimiento por un total de 263 millones de pesos.

Según los registros del Inai, 36 de estas multas pertenecen al sector de servicios financieros y de seguros (150 millones 826 mil pesos), diez al de información en

medios masivos (42 millones 434 mil 347 pesos), y nueve al de comercio al por menor (17 millones 434 mil 347 pesos, de los que, hasta 2015, cuatro pertenecían al de servicios educativos con 10 millones 428 mil 840 pesos). Entre las infracciones cometidas con mayor frecuencia se encuentran, según el Inai (2016): tratar datos personales en contravención a los principios establecidos en la ley (licitud, información, responsabilidad, lealtad y consentimiento), recabar o transferir datos personales sin el consentimiento expreso de las personas y omitir el Aviso de Privacidad, o alguno o todos los elementos previstos en la norma. Además, en la página *web* del Inai (www.inai.org.mx), en la sección de Resoluciones, el Instituto hace un listado de los sujetos obligados que han tenido un procedimiento, ya sea de protección de derechos, verificación o sanciones. De un total de 179 resoluciones, en 2011 hubo dos casos; en 2012, 26; en 2013, 60; en 2014, 58; en 2015, 16, y en 2016, 17.

Mientras que México refuerza cada vez más su normatividad en la materia, las cifras evidencian brechas en el cumplimiento con estas políticas. Después de que la ley entró en vigor los casos aumentaron de 2012 a 2013 y 2014 a poco más del doble, aunque destaca que en 2015 y 2016 disminuyeron considerablemente —dieciséis y diecisiete, respectivamente—. Aunque no existen datos específicos sobre cuántos sujetos obligados cumplen con la ley, la Enaid (Inegi, 2016) da un dato revelador: 65% de la población manifiesta que las organizaciones a las que le proporcionaron sus datos le dieron a conocer y leyó un Aviso de Privacidad. Esto podría indicar —y es preocupante— que una tercera parte de las organizaciones incumplen la ley al no dar a conocer el Aviso de Privacidad.

A pesar de que se desconoce el porcentaje de sujetos obligados que han cumplido con la ley, en 2014, Deloitte realizó un estudio con 169 organizaciones pertenecientes al sector financiero, industria, manufactura, servicios, consumo, telecomunicaciones, hotelería, educación, salud, bienes raíces y energía, titulado “Privacidad y Protección de datos en México, 2014”, para determinar la situación en la que se encuentran con respecto a la implementación de la LFPDPPP. Un hallazgo de Deloitte pertinente para esta investigación es el interés que motiva a las organizaciones para dar cumplimiento

a la ley. De los encuestados, 33 por ciento tiene como prioridad asegurar el cumplimiento regulatorio, 19 por ciento quiere incrementar la confianza y lealtad de sus clientes, 18 por ciento mantener la reputación de la marca, 15 por ciento salvaguardar la infraestructura de TI crítica y 15 por ciento reporta otra motivación. Como precedente, la investigación de Deloitte (2014) señala que la protección de los datos en las organizaciones apunta más al cumplimiento de la ley por las sanciones que a la protección en sí de los datos personales. Algo similar detalla PwC México (2016) en su "Estudio de la Privacidad en México: más allá de los compromisos", al mencionar que los principales motivos para la implementación de programas de privacidad en las organizaciones son, en orden de relevancia: el cumplimiento legal o regulatorio, fortalecer la compañía, apoyar la estrategia de riesgos y gobierno, y distinguirse de la competencia. PwC México concluye afirmando que, "en México, la protección de datos personales sigue siendo un asunto de cumplimiento".

Ante la problemática planteada, esta tesis pretende contestar a la siguiente pregunta de investigación:

¿Qué factores inciden en el cumplimiento de las políticas de protección de datos personales en las organizaciones?

La intención de la LFPDPPP es garantizar que las organizaciones realicen un tratamiento adecuado de los datos personales, sin embargo, en la práctica, los resultados del cumplimiento pueden ser distintos a los esperados. Se trata de entes muy complejos cuyas decisiones para implementar y cumplir con las políticas dependen de múltiples factores que estudia esta investigación.

Para obligar al cumplimiento, a ejemplo de la legislación europea, la LFPDPPP es una ley sancionadora. Sus multas van desde 100 a 320 mil días de salario mínimo, el doble cuando se trata de datos personales sensibles o, incluso, prisión, de acuerdo con la infracción cometida. Hasta hace unos años, la protección de los datos personales no estaba regulada por ninguna ley mexicana que obligara a los particulares, por lo que es posible suponer que lo importante para las organizaciones a partir de la puesta en vigor de la ley era cumplir con la reglamentación para prevenir las multas.

Contestar la pregunta de investigación es de suma utilidad para orientar los esfuerzos del Inai, como órgano garante de la protección de datos personales en México, hacia la implementación exitosa de sus políticas en las organizaciones privadas. Dada la naturaleza de la LFPDPPP, es posible pensar que, en un inicio, las organizaciones cumplieron con sus políticas para evitar las sanciones a pesar de que no las consideraran necesarias o las rechazaran. Este pudo ser el factor que motivó al cumplimiento en un principio, pero también es posible que, con el paso del tiempo, las organizaciones fueran aceptando a la protección de los datos como un valor, mediante actividades como la capacitación o establecimiento de códigos de ética sobre el manejo de los datos para que, finalmente, vislumbren los beneficios que les proporciona ser organizaciones confiables y asimilen las prácticas del derecho.

En la literatura, la implementación de una política pública en las organizaciones se ha estudiado desde distintas teorías que corresponden a modelos normativos o racionalistas, coercitivos o remunerativos que sirven como hilo conductor. Entre ellas se encuentran la teoría del miedo (Witte, 1992; Johnston y Warketin, 2010; Kwon y Johnson, 2013), de la madurez (Kwon y Johnson, 2013; Nesensohn et al, 2014), del comportamiento planificado (Bulgurcu, Cavusoglu y Benbasat, 2010), elección racional (Bulgurcu, Cavusoglu y Benbasat, 2010) de la agencia (Mwakibinga, 2008; Eisenhardt, 1988) y la institucional (Scott, 2001).

Para responder la pregunta de investigación, esta tesis se basa en la teoría institucional que explica la pertinencia de los factores presentes en sus pilares reglamentario, normativo y cognitivo, al cumplir con las políticas de protección de datos personales en las organizaciones, bajo el supuesto de que es posible que las organizaciones cumplan por temor a la sanción o por el papel fundamental del liderazgo directivo, que corresponde al pilar reglamentario, sin dejar de lado que otros factores de los pilares normativo y cognitivo, como la capacitación, ética, asimilación de las TI o ser reconocidos como una organización confiable, también desempeñan un papel importante en la implementación, supeditados a la coercitividad de la ley. Diferentes autores demuestran la conveniencia de la teoría institucional en el estudio de las

organizaciones vinculado con la seguridad de la información (Campbell, 2007; Kshetri, 2007, Lopes y de Sá-Soares, 2014 y Geels, 2004).

A la luz de la teoría institucional, esta investigación plantea como hipótesis que:

> *La suma de los factores reglamentarios, normativos y cognitivos inciden positivamente en el cumplimiento de las políticas de protección de datos personales en las organizaciones.*

Además de buscar comprobar la hipótesis, entre los objetivos específicos se encuentra corroborar la utilidad de la teoría institucional en el ámbito de cumplimiento de las políticas de protección de datos personales en las organizaciones, e indagar sobre la influencia de los factores reglamentarios en el cumplimiento, bajo el supuesto de que este pilar es el que lo detona.

Para explorar a profundidad los factores que inciden en el cumplimiento con las políticas y dar respuesta a la pregunta de investigación, se eligió una perspectiva metodológica cualitativa, con dos estudios de caso en escuelas particulares ubicadas en la ciudad de Puebla.

En cada una de las organizaciones seleccionadas se realizaron entrevistas de profundidad a diferentes miembros, relacionados con la toma de decisiones y el tratamiento de bases de datos personales. Cada uno de los entrevistados respondió exhaustivamente a las preguntas sobre los factores reglamentarios, normativos y cognitivos de la teoría institucional que, desde su perspectiva, incidieron en el cumplimiento de las políticas de protección de datos personales.

Los resultados de las entrevistas se vaciaron en una matriz que facilitó el análisis de cada una de las variables. Además, hubo acceso a documentación (reglamentos, códigos de ética, formatos de inscripción, etcétera) útil para corroborar la información que dieron los entrevistados.

La tesis está dividida en seis capítulos. El primero de ellos ofrece un panorama sobre la evolución del derecho a la protección a los datos personales, con los principales

argumentos sobre su conceptualización (*privacy* vs. protección de datos personales). Además, destaca la necesidad de los países por legislar en la materia a raíz del riesgo que representó el avance tecnológico que facilitó su almacenamiento y difusión, el valor económico de los datos personales, el uso de las sanciones como mecanismo de cumplimiento de las leyes, así como el papel de las autoridades de protección de datos personales ante el cumplimiento. El capítulo finaliza haciendo énfasis en que para México era importante contar con leyes robustas que garantizaran su seguridad, para recibir los beneficios económicos y comerciales que esto le brinda a nivel internacional.

El segundo capítulo desarrolla el marco jurídico mexicano que garantiza el derecho a la protección de datos personales. Inicia con su reconocimiento como un derecho independiente de la privacidad en la Constitución Mexicana, hasta la emisión de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, dirigida al sector privado, y la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, que regula al sector público. Cada una de estas establece principios que constituyen los pilares del derecho, con los que los sujetos obligados deben cumplir, así como la garantía del ejercicio de los derechos ARCO. Particularmente, resalta la coercitividad de la ley de los particulares, sobre la que se desarrolla esta investigación, pues uno de los supuestos es que las sanciones de la ley motivan su cumplimiento. También sobresale la función promotora y ejecutora de Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Inai), como órgano garante. Concluye afirmando que, más allá de las multas y sanciones, como condición necesaria para el cumplimiento de la ley, debe esperarse que existan otros factores que incidan en este.

El capítulo tres detalla modelos teóricos vinculados con el cumplimiento en las organizaciones, clasificados en racionales, normativos e integrales. Entre estas teorías se encuentran la teoría del miedo, la teoría de la madurez organizacional, del comportamiento planificado, elección racional y la teoría de la agencia. Sin embargo, cada una de ellas da una explicación parcial desde su ámbito, mas no integral. La literatura señala que el cumplimiento es complementario, por lo tanto, una teoría desde

la que puede explicarse desde una perspectiva integradora es la institucional, cuya utilidad se ha demostrado en estudios referentes a la seguridad de la información. Por lo tanto, parte de los objetivos de esta investigación, además de explicar los factores que inciden en el cumplimiento, es demostrar su utilidad en esta área.

El cuarto capítulo profundiza en el pilar reglamentario, normativo y cognitivo de la teoría institucional. Esta parte del supuesto de que todas las organizaciones tienen un marco institucional que comprende reglas, normas, costumbres, roles y personajes que definen el comportamiento de toda organización, por lo que se plantea que contiene los elementos suficientes para este estudio, con base en investigaciones previas que destacan factores de cada uno de los pilares. En esta sección se definen las variables que guían la investigación, que son el cumplimiento (variable dependiente), la sanción, monitoreo, liderazgo directivo, ética organizacional, capacitación, aceptación de las tecnologías de las TIC y la reputación (variables independientes).

El abordaje metodológico describe la estrategia de investigación en el capítulo cinco, que abarca la selección de los casos, el instrumento, la operacionalización de las variables y el mapa de actores. A continuación, el capítulo seis presenta los resultados de las entrevistas de cada uno de los casos, por variables, para concluir con una discusión teórica.

Finalmente, se presenta un capítulo de conclusiones generales. En este, se reflexiona sobre la utilidad de la teoría institucional para estudiar el cumplimiento de las políticas de protección de datos personales en las organizaciones y los principales hallazgos de cada uno de los casos.

CAPÍTULO I

LA PROTECCIÓN DE LOS DATOS PERSONALES, UNA OBLIGACIÓN PARA LOS RESPONSABLES

Desde la década de los setenta, algunos Estados de Europa comenzaron a legislar a favor de la protección de datos personales con el fin de que el sector público y otros actores privados no abusen de su procesamiento. En general, estas leyes especifican una serie de derechos para los individuos y establecen buenas prácticas en el manejo de los datos personales que los responsables de las bases de datos deben cumplir. Su objetivo central es proteger a los ciudadanos y asegurar que los sujetos obligados utilizarán los datos de tal forma que la integridad y privacidad de las personas no pueda infringirse (De Hert y Gutwirth, 2006).

La protección de datos personales no tiene la naturaleza prohibitiva de una ley criminal. Esto se explica porque el titular de los datos no posee sus propios datos y tampoco puede evitar que sean procesados y, bajo ciertas condiciones, quienes son responsables de los datos personales tienen derecho a procesarlos. Por lo tanto, la protección de datos personales posee una naturaleza pragmática. Asume que los actores públicos y privados necesitan usar información personal y esto debe ser aceptado por las sociedades. El mensaje “puedes procesar datos personales bajo ciertas circunstancias” de una ley de datos personales reemplaza al “no matarás” de una ley criminal (De Hert y Gutwirth, 2006). Por esto, las leyes establecen buenas prácticas bajo las cuales los sujetos obligados pueden utilizar los datos personales, aunque también imponen sanciones por incumplimiento.

Las nociones de “procesamiento” y “datos personales” aparecen como parte central del concepto de protección de datos personales. En términos generales, “procesar” puede ser entendido como cualquier operación desarrollada en torno a los datos, tales como recolección, almacenamiento, difusión, uso, si pueden ser revelados, borrados o destruidos, y son considerados personales cuando hacen referencia a un individuo (Tzanou, 2013). Así, la protección de datos personales también puede ser entendida

como un marco legal de reglas que protegen los derechos, libertades e intereses de los individuos cuyos datos son recolectados, almacenados, procesados, compartidos o destruidos. Sin embargo, el objetivo primordial es asegurar que el tratamiento sea el adecuado, para lo cual se han establecido principios internacionalmente reconocidos como: finalidad, licitud, calidad, proporcionalidad, información, lealtad, responsabilidad y consentimiento (Tzanou, 2013).

La protección de datos personales no es prohibitiva. De Hert y Gutwirth (2006) hablan de la racionalidad detrás de la protección de los datos personales. En la esfera pública es casi natural asumir que las autoridades procesan la información personal necesaria para el desempeño de sus funciones en servicio de la sociedad. El objetivo central de la protección de los datos personales consiste en proveer procedimientos específicos para salvaguardar la privacidad de los individuos y promover la responsabilidad por parte de los gobiernos y los actores privados que procesan los datos. El alma de una ley de protección de datos personales no está en prohibir sino en canalizar, promover el cumplimiento y dotar a los titulares de los datos con el poder de defenderse de prácticas abusivas, pero también imponen sanciones por incumplimiento. En el sector público existe el conocimiento de que las autoridades pueden infringir fácilmente la privacidad de las personas y de que en todos los sistemas administrativos hay una urgencia por recabar, almacenar y usar los datos. Una de las funciones básicas de una ley administrativa tradicional de datos personales es normar su procesamiento y una lógica similar explica que Europa también comenzara a regular el procesamiento de los datos personales en posesión del sector privado, no solo del público (De Hert y Gutwirth, 2006).

La Directiva de Protección de Datos Personales de la Unión Europea ve a la protección de datos personales como parte de los derechos fundamentales y libertades naturales de las personas, en particular su derecho a la privacidad con respecto al procesamiento de los datos personales (Tzanou, 2013). A pesar de que el derecho a la protección de datos personales proviene del derecho a la privacidad e intimidad, se deslinda de estos en el punto en el que no necesariamente deben ser íntimos para ser protegidos, es

suficiente con que sean personales. Sin embargo, es necesario aclarar que una de las finalidades del derecho a la protección de datos personales es también garantizar la privacidad, así como la intimidad de la persona. Villanueva (2012) explica que es un derecho más amplio que la privacidad puesto que la contempla como un fin y, asimismo, tiene como objeto la autodeterminación informativa [1], la veracidad, confidencialidad y cuidado de los datos personales.

La definición de la protección de datos personales versus la *privacy* en la literatura

La protección de datos personales es un tema que en sus inicios fue objeto de estudio del derecho y provenía del derecho a la privacidad e intimidad. Autores como Fonseca (2010), definen a la privacidad como el "ámbito de la vida personal del individuo que se desarrolla en un espacio reservado y que el individuo tiene derecho a proteger de cualquier información". González (2014) mapea diferentes acepciones de la privacidad en la literatura y las divide en categorías básicas:

1. La privacidad puede entenderse como la protección de algo opuesto a lo público, ya sea:
    - **a.** Concebir a lo público como la autoridad gubernamental (Estado), o la comunidad o sociedad en general; lo privado se lee como "no oficial" o "no perteneciente a la *res pública*", porque se refiere a la vida familiar o a lo personal.
    - **b.** Si lo público es lo que se comparte, expone, lo común o abierto al otro, lo privado pertenece a un espacio cerrado, no expuesto, escondido, confidencial, solitario, de introspección, generalmente sin acceso o fuera de alcance.
2. También puede explicarse en el sentido de lo individual, personal o de uno mismo. Desde este punto de vista, exigir respeto por la vida privada de alguien es afirmar

[1] La autodeterminación informativa permite al titular de los datos decidir qué datos suyos pueden ser públicos y cuáles no, para qué fines se utilizan y con qué medios, cuáles son las limitaciones de uso.

que existe el derecho de vivirla bajo una serie de libertades, opuesto al control o alienación.

Para González (2014) esta clasificación ilustra los significados de la privacidad y lo privado que, en ocasiones, se construyen opuestos a lo que es público, pero no siempre. De hecho, como noción legal comúnmente se asocia con lo que es privado en el sentido de lo individual, personal o de uno mismo (punto 2).

Como precedente del derecho a la vida privada está el *right to privacy* (derecho a la privacidad), sobre el que escriben los autores Warren y Brandeis en 1890 en el artículo titulado *"The right to privacy"*. Desde finales del siglo XIX, los autores se adelantaron y vislumbraron el tema en cuestión para salvaguardar la privacidad e intimidad de las personas. En uno de sus párrafos sostienen que:

> Recientes inventos y métodos de negocios llaman la atención sobre el próximo paso que debe tomarse para la protección de la persona, y para asegurar al individuo lo que el juez Cooley denominó "el derecho a ser dejado en paz". Fotografías instantáneas y empresas periodísticas han invalidado el sagrado recinto de la vida privada y doméstica, y numerosos aparatos mecánicos amenazan hacer buena la predicción de que "lo que es susurrado en lo cerrado se proclamará desde los tejados" (Villanueva, 2010).

El concepto que Warren y Brandeis tienen de la privacidad se basa parcialmente en un caso inglés a mediados del siglo XIX, que expuso el uso del término de forma incidental. También afirman que la expresión ya había encontrado lugar en la ley francesa *relative à la presse* (Ley de Prensa) de 1968, que prohibía la publicación de hechos referentes a la *vie privée* (vida privada) de las personas a menos que tuvieran un interés público o que la publicación tuviera su consentimiento. Warren y Brandeis igualaron esto al *the rigth to be let alone* (derecho a estar solo) (González, 2014).

En 1960, Wiliam L. Prosser publicó un artículo que revisaba todo el conocimiento que hasta ese momento se había producido sobre la privacidad a partir de la publicación de Warren y Brandeis. Entre sus principales aportaciones está el reconocimiento de cuatro tipos de agravio a la privacidad: la intromisión a la soledad de una persona; la apropiación, para propósitos comerciales, del nombre de una persona, o de su identidad; la difusión de asuntos privados de una persona que pueden ser penosos, y la

publicación de algún acontecimiento que pone a una persona en el ojo público (González, 2014).

La protección de la privacidad en Estados Unidos no solo formó parte del derecho de responsabilidad civil, sino que eventualmente se volvió de orden constitucional para garantizar la protección de la privacidad de las personas en contra del gobierno. Aunque la Constitución de Estados Unidos no menciona el derecho a la privacidad como tal, las interpretaciones judiciales protegen varios de sus aspectos. Por ejemplo, el mismo Brandeis fue ministro de la Suprema Corte de Estados Unidos, desde donde argumentó que varios de los redactores de la Constitución ya reconocían el derecho a estar solo frente al Estado, y que ese derecho en particular lo tenían en alta estima (González, 2014).

En 1965 la Suprema Corte explícitamente declaró que las personas tienen el derecho constitucional a la privacidad, ubicado en las penumbras de una exhaustiva interpretación de la Declaración de Derechos de Estados Unidos. Desde esta perspectiva, el derecho a la privacidad se refiere a ser libre de la intromisión del gobierno, bajo la idea de que deben existir libertades más allá del control del Estado, aun dentro de una democracia. Este derecho a la privacidad abarca la protección y el derecho a la autonomía y a la autodeterminación (González, 2014).

A mediados de la década de los sesenta, el término privacidad en Estados Unidos tenía dos significados: por un lado, la usaban desde una perspectiva de ley civil como una referencia de sistema de agravios (intromisión a asuntos privados, publicación de acontecimientos privados o el uso de la imagen de una persona); y, por el otro lado, aparecía como un tema constitucional referente al rechazo de la interferencia de las autoridades públicas en la vida privada (González, 2014).

En enero de 1974, Nixon anunció que a fin de ese año se daría a la tarea de definir y proteger el derecho a la privacidad de cada norteamericano. Su finalidad era examinar el tema de recopilación, almacenamiento y uso de los datos personales por parte de la federación. Para ese momento, el Senado de Estados Unidos ya estaba investigando las grabaciones ilegales de Nixon que derivaron en el escándalo de Watergate y que

propiciaron su renuncia. A finales de ese mismo año emitieron la *Privacy Act* (Ley de Privacidad), cuyo propósito fundamental fue proteger la privacidad de los archivos de las personas que poseían las autoridades federales (González, 2014). A pesar de que está sustancialmente vinculada con los principios de las "prácticas injustas de información", la Ley de Privacidad no lo menciona como tal, sino que sistemáticamente se refiere a "salvaguardar la privacidad definida como un derecho personal y fundamental protegido por la Constitución de los Estados Unidos, que es afectado por la recopilación, conservación, uso y difusión de información personal". De esta manera, esta ley plasmó de manera novedosa el concepto de *informational privacy* (privacidad de la información) bajo el nombre de *privacy* (privacidad).

Este término —*privacy*— pronto generó ambigüedad en la legislación estadounidense, especialmente entre la Ley de Privacidad y la *Freedom of Information Act* (Ley de Libertad de Información) de 1966, que también es aplicable a la información que poseen las agencias federales y que alude a la privacidad, aunque no en el mismo sentido. La Ley de Libertad de Información permite publicar información que controla el gobierno, pero contiene varias excepciones, entre ellas la privacidad (González, 2014).

A pesar de que la protección de los datos personales proviene de la privacidad, no se trata de derechos idénticos. Privacidad y protección de datos son dos conceptos contenciosos dentro del discurso de la privacidad. Boniface (2012) asume que ambos pertenecen a distintos lados del Atlántico, es decir, Estados Unidos utiliza *privacy* (privacidad), mientras que Europa se refiere a protección de datos. Este uso territorial de los términos es problemático por dos razones. Primero, hay similitudes y diferencias entre ellos y, segundo, en Estados Unidos y Europa se oponen y coexisten de manera simultánea (Boniface, 2012). Esto sin dejar de mencionar que América Latina partía del concepto de *habeas data* (referente a "poseer los datos"), que proviene de la doctrina del *habeas corpus* (poseer el cuerpo) (Bygrave, 2004).

El término de protección de datos en Europa cobró auge a la luz del avance tecnológico. Las primeras investigaciones que se hicieron en Europa bajo la noción de la privacidad estuvieron vinculadas con el progreso de la tecnología. Tal es el caso del

Reino Unido, donde en 1973 el gobierno presentó un *White Paper*[2] para regular los sistemas de información computarizados tanto del sector público como del privado y proporcionar medidas de seguridad para la protección de las personas.

El Comité de Protección de Datos que crearon en 1975 presentó su reporte en 1978 (*Lindop Report*) con la amplia recomendación de adoptar una ley que abarcara los sectores público y privado, de establecer una autoridad que garantizara su complimiento y de registrar a los responsables de procesar los datos. Esto asentó una de las primeras bases que señalan el cumplimiento por parte de los sujetos que tienen a su cargo bases de datos personales.

No obstante, el reporte falló en que no generó una respuesta concreta, sino que fue hasta 1984 cuando el Consejo de Europa aprobó la *Convention for the Protection of Indivicuals with regard to Automatic Processing of Personal Data* (en español conocido como Convenio 108), que el Reino Unido aprobó su primera Ley de Protección de Datos (González, 2014). Así, desde la década de los setenta, la *privacy* de Estados Unidos no tuvo eco en Reino Unido, ni en el resto de Europa, en donde optaron por "protección de datos", orillados por el desarrollo de la tecnología.

Algunos investigadores ven a la protección de datos y a la privacidad como sinónimos e intercambian los términos, pero otros tienen una visión distinta. Cuijpers (en Boniface, 2012) cuestiona si el derecho a la protección de datos es lo mismo que el derecho a la privacidad. En su respuesta coincide con Peter Block en que no es así. Esto es porque, en palabras de Cuijpers (Boniface 2012), la privacidad es un derecho que otorga al individuo la posibilidad de salvaguardar su vida privada de cualquier intromisión, mientras que la protección de datos personales se refiere al procesamiento de los datos y no necesariamente se restringe a la esfera privada de las personas.

Bajo esta misma idea, De Hert y Gutwirth argumentan que el objeto real de la protección de datos personales es proteger a los individuos de la recolección

[2] Los *White Papers* son documentos que contienen las intenciones de un Gobierno de establecer sus propósitos de legislar sobre algún tema. En ocasiones pueden tener fragmentos de una ley que se esté elaborando. Esto proporciona bases para que los grupos interesados puedan consultarla y hacer modificaciones antes de que se entregue formalmente al parlamento.

injustificada, almacenamiento o difusión de su información personal. Esto último parece estar en deuda con el objetivo central de la privacidad, que es proteger contra alguna intromisión injustificada en la vida personal (Boniface, 2012).

Para refutar que la privacidad y la protección de datos personales son intercambiables, De Heart y Gutwirth (en Boniface, 2012) también sostienen que existen diferencias significativas entre los dos términos basadas en su alcance, metas y contenido. Además, reconocen que, obviamente, la privacidad ocupa un lugar primordial en las leyes de protección de datos personales, pero sería un error considerar que esta es su única preocupación. Las leyes de protección de datos personales sirven a una multiplicidad de intereses que van más allá de la concepción tradicional de la privacidad.

Aunque la privacidad y la protección de datos comparten ciertas características y metas, y con frecuencia se usan como sinónimos, De Hert y Schreuders (en Boniface, 2012) afirman que no son idénticas. Esto es porque, a pesar de que su raíz está en la protección de la privacidad, la protección de datos no necesariamente plantea temas de privacidad. Contrario a las reglas de la privacidad, las reglas de la protección de datos no son prohibitivas. En lugar de esto organizan y regulan la forma en la que los datos pueden ser legítimamente procesados bajo reglas transparentes, con el consentimiento del titular de los datos y que se conozca la responsabilidad del sujeto obligado.

En un intento por reconciliar los términos, autores como Schwartz y Reidenberg (en Boniface, 2012) mencionan el concepto *data privacy* (privacidad de datos), que Bygrave (2004) considera más apropiado porque comunica el interés central de la materia y crea un puente entre la concepción de Estados Unidos y Europa, a diferencia de *data protection* (protección de datos), cuya debilidad consiste en que su interés recae en las normas que deben aplicarse. Tal como Bygrave, otros autores utilizan términos similares. Karanka (en Boniface, 2012), por ejemplo, habla de *information privacy* (privacidad de la información) y explica que también se refiere a la protección de datos personales.

No obstante, De Hert y Gutwirth (2006) insisten en que el derecho a la protección de datos personales puede constituir uno de los aspectos del derecho a la vida privada, pero esto no significa que todos los datos personales necesariamente caigan en este concepto. Para sostener su argumento los autores y Boniface (2012) explican los roles de la privacidad y la protección de datos.

La privacidad adquiere un aspecto negativo cuando se impone como un instrumento de opacidad que impide la intromisión en asuntos particulares —por parte de gobiernos u otros actores privados— que pueden ser de interés público. Es una noción fundamental para resguardar a una sociedad que quiere limitar las relaciones de poder. Puede esconder actos inmorales o ilegales y se presta al contraargumento de que una sociedad abierta debería estar conformada por la transparencia de todos sus actores.

Como aspecto positivo, es un concepto que permite la libertad individual y juega un papel esencial en toda democracia constitucional que, precisamente, basa su legitimidad en el máximo respeto de las libertades individuales. Es un espacio —la esfera privada— en donde las personas son libres para desarrollarse sin la intervención pública, que garantiza el desarrollo individual de las personas (De Hert y Gutwirth 2006).

De Hert y Gutwirth (2006) afirman que el derecho a la privacidad no necesariamente implica que todo lo que protege es inviolable. Actualmente, ningún aspecto de la privacidad tiene precedencia absoluta sobre otros derechos e intereses. Eso incluye la confidencialidad del correo electrónico, la integridad física o el control de las personas sobre su información personal, como ejemplos. En un escenario real aparecen los derechos, libertades e intereses de los demás, así como las prerrogativas de las autoridades, por lo que las fricciones, tensiones y los conflictos crean la necesidad de buscar un balance entre los derechos e intereses que dan relevancia a la privacidad. En un Estado constitucional, la privacidad es una noción que adquiere más importancia cuando se involucra con otros intereses públicos y privados.

A primera vista, dado que la Directiva de Protección de Datos de la Unión Europea prevé un sistema de prohibiciones generales que demanda ciertas condiciones para

hacer legítimo el procesamiento de datos, pareciera que la privacidad y la protección de datos son de una misma naturaleza prohibitiva que reemplaza el “no procesar a menos que”. Esto haría de la protección de datos una herramienta de opacidad como aspecto negativo, al igual que la privacidad.

De Hert y Gutwirth (2006) argumentan que esto no es correcto por tres razones. Primero, la directiva se inspiró en normatividades nacionales que no se basaron en principios prohibitivos. Segundo, en su contenido provee un cúmulo de artículos que permiten el procesamiento de los datos personales. Por ejemplo, el artículo 7 establece que los datos pueden procesarse sin el consentimiento del titular de ser necesario para propósitos de interés legítimo, excepto cuando esos intereses invalidan los derechos fundamentales o las libertades del titular de los datos.

Para algunos autores, este artículo incluye el procesamiento de los datos para fines de marketing directo e, incluso, obliga a dudar y refutar la idea de que procesar datos es un principio prohibido o que depende del consentimiento. No obstante, existen excepciones a la regla. En primer lugar, una regla prohibitiva aplica a los datos personales sensibles porque pueden ser sujetos de discriminación. Esto no significa que la prohibición sea absoluta, pero las derogaciones son posibles solo bajo circunstancias estrictamente definidas, como razones de seguridad nacional.

La última razón que De Hert y Gutwirth (2012) utilizan para explicar a la privacidad como una aparente herramienta de la opacidad recae en el principio de finalidad. El propósito de este principio es aclarar para qué fines se recolectan los datos y durante qué tiempo serán necesarios. Como consecuencia, su uso debe limitarse a esos fines específicos. El corazón de la protección de datos personales es prevenir un mal uso por parte del responsable. En la actualidad, es necesario utilizar los datos para distintas finalidades, pero sería contradictorio utilizarlos para fines posteriores que son incompatibles con los originales. Por esto, es mediante el consentimiento del titular que los datos pueden utilizarse con otros propósitos. Esto puede interpretarse como un cambio que va de lo prohibitivo hacia una lógica que obedece a la necesidad de utilizar

los datos. Así, en vez de ser opaco, la transparencia legitima el procesamiento de la protección de datos (De Hert y Gutwirth, 2012).

Como conclusión, Boniface (2012) llega a tres puntos que distinguen la privacidad de la protección de datos personales.

Primero, en estricto sentido, la privacidad y la protección de datos son dos conceptos separados, aunque sus objetivos coinciden. Las diferencias entre los dos conceptos recaen en sus alcances, metas y contenidos. Para Boniface (2012) es importante señalar que los intentos por diferenciarlos —teniendo presente que la privacidad es prohibitiva y la protección de datos no— son elusivos.

Por ejemplo, uno de los mandatos legales que establece la Directiva para procesar los datos es el consentimiento. El consentimiento se refiere a la idea de que el titular de los datos debe tener el control del uso que se hace de ellos, y el control se refiere a que el mismo titular puede retirar su consentimiento para que el responsable de los datos ya no pueda procesarlos. El consentimiento también está vinculado con la autodeterminación informativa que le da autonomía al titular de los datos de conocer previamente las condiciones bajo las que se van a tratar los datos que tenga como consecuencia el consentimiento.

No obstante, aunque el consentimiento es una de las precondiciones para procesar los datos, no es absoluto. En ocasiones es difícil de obtenerlo directamente del titular de los datos o está sujeto a excepciones como la seguridad nacional. Por lo tanto, lo que Boniface (2012) destaca es que, hasta cierto punto, el consentimiento es un factor prohibitivo para las actividades que procesan los datos personales, lo que lo hace similar a la privacidad. Incluso interpreta que los mismos De Hert y Gutwirth reconocen que la protección de datos también prohíbe cierto tratamiento de ellos, por ejemplo, cuando se trata de datos sensibles. Sin embargo, ni el consentimiento ni los datos sensibles son algo prohibitivo desde el punto de vista de De Hert y Gutwirth, porque ellos argumentan que podría parecerlo, pero no es así puesto que se trata de “no procesar a menos que”.

La segunda conclusión a la que llega Boniface (2012) es que los dos conceptos son cada vez más usados de forma indistinta. Como menciona Kuner (en Boniface, 2012), en el llamado a un marco internacional hay una tendencia a mezclar los términos de privacidad y protección de datos. Por ejemplo, la Resolución aprobada en Estrasburgo en 2008 se refiere a los dos términos, o el Global Privacy Standard (Estándares Globales de Privacidad) de 2006 también menciona varias veces "privacidad", pero los principios se refieren al consentimiento, limitación o acceso, que tradicionalmente se atribuyen a la protección de datos.

La tercera conclusión es que normalmente no se da el contexto en el que se utilizan los conceptos de privacidad o de protección de datos, sino que es necesario ver con detenimiento cuáles son los principios, el alcance y la aplicación. Para Boniface (2012), es importante conocer el contexto para saber cuál es el uso correcto.

Esta investigación no hace uso indistinto de ambos términos, sino que los distingue como derechos independientes y se decanta por el uso del concepto de "protección de datos personales", propio de Europa; y no de *privacy*, de Estados Unidos; ni de *habeas* data, tendencia latinoamericana, o de privacidad de datos, aunque se reconoce que la protección de datos personales proviene de la privacidad.

La sanción como mecanismo de cumplimiento en leyes y tratados internacionales

Gellert (2015) expone que la regulación de la protección de datos personales tiene sus bases en las amenazas que representaba el desarrollo de la tecnología sobre la privacidad, puesto que fue a partir de entonces que los países, principalmente europeos, comenzaron a legislar en la materia por el almacenamiento sistematizado de los datos.

Entre los primeros antecedentes con los que se cuenta aparece la República Federal de Alemania, cuya ley fue promulgada en 1970 para proteger la información que utilizaba la policía, debido a que en la década de los cuarenta los nazis controlaban la

información de la población con los datos del censo y archivos del gobierno para identificar a los judíos y otros grupos (Gregorio, 2004). Esta ley se denominó *Hessiche* Datenschutzgesetz (Ley de Protección de Datos de Hesse) (González, 2014) —de hecho, el término de "protección de datos" proviene del alemán *datenschutz*, que tuvo mayor aceptación en Europa (Bygrave, 2004)—.

Otro ejemplo es Suecia, que para 1970 era de los países más computarizados, lo que le permitía generar bases de datos interconectadas; Francia, cuya *Loi informatique et libertés* (Ley de Protección de Datos) fue resultado del proyecto SAFARI, un número de identificación personal utilizado para distintas bases de datos; o Canadá, donde a partir de la década de los sesenta la administración pública introdujo el uso de las computadoras en mayor escala.

A partir de entonces, otros países europeos comenzaron a sumarse a las leyes en materia de protección de datos personales: Suecia, 1973; Portugal, 1976; Austria, 1978; España, 1999, etcétera. Estados Unidos, con el *Right to Privacy*, también fue un pionero en este tema porque habló sobre el derecho de exclusión (*the right to be alone*), que velaba por la intimidad e individualidad, asimismo dictó el *Fair Credit Reporting Act* para intentar regular el trato genérico de los datos personales que después dio origen a la *Privacy Act* de 1974. En Latinoamérica, Argentina fue de los primeros países en establecer una ley sobre datos personales, seguido de Nicaragua, Paraguay, Chile, Colombia, Costa Rica y México, entre otros.

Estas leyes son normas jurídicas bilaterales, externas, heterónomas y coercibles, a diferencia de las normas morales que son unilaterales, internas, autónomas e incoercibles. Su carácter bilateral quiere decir que cumplen con la condición de imponer deberes correlativos de facultades o conceden derechos y obligaciones, siempre existe una figura que puede ser la autoridad, que exige el cumplimiento de la norma por su estructura imperativo-atributiva, como las autoridades de protección de datos. Son externas porque se refieren a los actos externos de las personas y al íntimo cuando trascienden para la colectividad, es decir, son de carácter social y no solo individual; son heterónomas porque las elaboran las autoridades o representantes de los

individuos, y son coercibles porque pueden hacerse cumplir aun en contra de la voluntad del obligado (García Máynez, en Cárdenas, 2010).

Las normas jurídicas de la protección de datos personales establecen derechos y obligaciones, son permisivas en el sentido el que organizan y regulan la forma en la que los datos pueden ser legítimamente procesados bajo reglas transparentes, con el consentimiento del titular de los datos y que se conozca la responsabilidad del sujeto obligado; contienen mecanismos que hacen posible su uso y almacenamiento bajo ciertas condiciones, establecen principios para el tratamiento y calidad de los datos, medidas de seguridad físicas y tecnológicas, y existe una autoridad competente que vigila el cumplimiento e impone obligaciones y sanciones a los responsables. Este último mecanismo coercitivo —sanciones— se vuelve indispensable para garantizar el cumplimiento de la política dado el valor que poseen los datos personales y los riesgos que puede representar un mal uso, pérdida o acceso no autorizado.

Las leyes nacionales de protección de datos establecen sanciones a las infracciones y entran dentro de la clasificación de las leyes perfectas que imponen un castigo, y de leyes más que perfectas porque además de la sanción imponen una reparación pecuniaria y adquieren un carácter coercitivo. Se trata, entonces, de leyes punitivas a pesar de que invitan a las buenas prácticas de protección de datos personales.

Además de esto, existen documentos relevantes que fomentan la protección de datos personales en posesión del sector público y privado. Estos documentos han servido como marco de referencia para la creación de leyes, acuerdos y tratados en distintos países que han generado redes para garantizar su protección. También contienen principios rectores para el flujo transfronterizo de la información que establecen criterios para el manejo de datos entre los países.

Es importante resaltar que no son normas cuyo cumplimiento puede ser exigido ante los tribunales competentes pues no poseen una naturaleza punitiva, únicamente funcionan como acuerdos para el procesamiento adecuado de los datos que los países pueden cumplir y establecen mecanismos comprensivos para lidiar con los datos, como procedimientos para el flujo internacional, respeto y salvaguardo de la confidencialidad,

intercambio de información y temas diversos como intercambios, costos y disputas (APEC, 2010). Entre estos destacan:

- La Convención para la protección de los individuos con respecto al procesamiento automático de datos personales de 1981 (mejor conocido como Convenio 108), del Consejo de Europa y la Comisión Europea
- La Directiva 95/46/CE del Parlamento Europeo (la Directiva) y del Consejo del 24 de octubre de 1995, relativa a la protección de datos personales y a la libre circulación de estos datos
- El Marco de privacidad transfronterizo del Foro de Cooperación Económica Asia-Pacífico (APEC) de 2004
- Los Estándares Internacionales sobre Protección de Datos Personales y Privacidad (ICDPPC, 2009)
- Las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales de 2013
- El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 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, que derogó la Directiva 95/46/CE a partir del 25 de mayo de 2018
- Estándares de Protección de Datos Personales para los Estados Iberoamericanos 2017

El artículo 83 del Reglamento 679 (DOUE, 2016) añadió algo novedoso con respecto a las sanciones. Establece que las autoridades de control de cada país son quienes garantizarán la imposición de las multas administrativas que se impondrán en función de las circunstancias de cada caso individual.

Estas multas pueden variar desde 10 millones de euros como máximo, o el equivalente al dos por ciento del volumen de negocio total anual global del ejercicio financiero anterior cuando se trata de una empresa, cuando la infracción concierne a los artículos 8, 11, 25 a 39, 41, 42 y 42 referentes a las obligaciones del responsable y del encargado, de los organismos de certificación o de la autoridad de control; o de 20

millones de euros como máximo o el equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior cuando se trata de una empresa, cuando la infracción concierne a los artículos 5, 6, 7, 9, 12 a 22, 44 a 49 y 58 referentes a los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento, los derechos de los interesados, las trasferencias de datos a un destinatario en un tercer país o una organización internacional o el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control.

A lo anterior, en su artículo 83 fracción 9 añade que:

> Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo de la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competente, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control.

Esto quiere decir que el nuevo Reglamento garantiza la aplicación de las multas, aun en caso de que uno de los 28 Estados miembro no las contemple si incurre en alguna infracción, a diferencia de la Directiva 95, vigente hasta 2018, que no contiene este apartado. Con esto, el Reglamento hace énfasis en la importancia que tienen las multas para garantizar la protección de los datos personales: deja de ser un instrumento de buenas prácticas de cooperación entre Estados miembro para el procesamiento de los datos y se convierte en un instrumento coercitivo con capacidad de sanción. Estas sanciones las imparten las autoridades de control de cada país.

El papel de las autoridades de protección de datos ante el cumplimiento

Hasta este momento se ha hablado de las sanciones, pero ¿quién es el encargado de imponerlas y qué funciones cumple? Bajo el esquema de leyes generales de protección de datos personales, algunos países optaron por tener un órgano independiente encargado de garantizar el ejercicio del derecho dentro de un marco legal, conocido

como autoridades de protección de datos (DPA por sus siglas en inglés) (Schütz, 2012).

Estas autoridades no solo desempeñan un papel de *ombudsmen*, auditores, consultores, educadores, capacitadores, consejeros políticos y negociadores, sino que, además, se espera que sean capaces de establecer las infracciones de la ley competente y mecanismos de sanción, monitoreo, investigación e intervención para atender las reclamaciones (Kloza y Moscibroda, 2014), con el fin de generar un cambio de conducta cuando los actores públicos o privados violen la ley (Bennett y Raab, 2006).

A nivel internacional, para los estándares de la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (ICDPPC por sus siglas en inglés), uno de los principales problemas para la protección de los datos personales es que los países no cuenten con una autoridad supervisora independiente, como ocurre en Japón (Greenleaf, 2014), que fomente la cooperación entre las autoridades de cumplimiento en casos que tengan que ver con el intercambio de información personal entre diferentes jurisdicciones (ICDPPC, 2016).

Específicamente, el artículo 117 del Reglamento 679 (DOUE, 2016) dicta sobre las autoridades de control que:

> El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa.

El mismo Reglamento también hace especial énfasis en las funciones y poderes efectivos que deben tener las autoridades de protección de datos personales. Estos poderes son de investigación, correctivos y sancionadores, y de autorización y consultivos, fundamentales para asegurar el cumplimiento de las leyes. Para lograrlo, las autoridades también deben generar medidas de sensibilización dirigidas hacia los

responsables y encargados del tratamiento que apelen no solo al cumplimiento de la regla, sino que, además, destaquen la importancia de la protección de los datos personales como un valor organizacional.

En estas funciones que el Reglamento 679 les atribuye a las DPA, Jóri (2015) distingue entre su papel de promotor y ejecutor. Como promotor emite recomendaciones libres de carácter jurídico a los sujetos involucrados; como ejecutor, es decir, autoridad administrativa, dicta órdenes jurídicas que siguen un orden administrativo aplicable. Como ejecutor, una DPA puede ordenar la supresión o rectificación de datos o imponer multas directamente al responsable de los datos. Una característica común del papel de promotor, así como de ejecutor, es que la DPA en estos casos no tiene la intención de cambiar el entorno legal: su objetivo es únicamente implementar las regulaciones ya existentes proporcionadas por la ley de protección de datos.

Para el autor, sería ideal que las DPA cumplan con sus dos funciones, aunque en ocasiones las circunstancias inclinan la balanza más hacia una u otra. Jóri (2015) plantea dos hipótesis. En la primera afirma que un énfasis fuerte en la función promotora indica alto nivel en la protección de los datos personales en un país y que la DPA está funcionando bien. Si la DPA mantiene una atmósfera legal y no legal sana y participa en el diseño de las políticas, eso también es señal de que es fundamentalmente independiente.

En su función de promotora, la DPA es una activista. Tiene una visión clara sobre sus metas y cómo lograr el balance entre el derecho a la protección de los datos personales y otros derechos o intereses. En este papel, también tiene presencia fuerte en los medios y difunde la importancia del derecho a la protección de los datos personales. Su activismo, la oportunidad de formular opiniones sobre la ley y su frecuente aparición en los medios de comunicación podrían dar pie a que el DPA entre en el espacio de la política.

Por otro lado, si la función de ejecutor de las leyes domina a la de promotor, entonces el nivel de la protección de los datos personales y la independencia de la DPA son dudosos. Como ejecutor, la DPA aplica las disposiciones de la ley en los

procedimientos administrativos en función de las regulaciones legales del área. La aplicación y la mediación requieren menos presencia en los medios. También, cuando la DPA es ejecutora, rara vez entra en la esfera política (Jóri, 2015).

Ambas funciones relativas a la aplicación de la ley de protección de datos —ejecutor/promotor— han prevalecido en los años recientes, aunque Jóri (2015) se atreve a afirmar que las DPA de la UE se concentran más en la aplicación que en la promoción y en buscar nuevas herramientas para asegurar el cumplimiento. Cabría preguntarse si la DPA mexicana —el INAI—, que ha seguido el modelo europeo, también es más ejecutora que promotora del derecho, más promotora que ejecutora, o ambas.

La exhaustividad de las leyes de protección de datos personales en la actualidad

En una investigación sobre las preferencias de los consumidores con respecto a la importancia que dan a la protección de sus datos personales, 97.4 por ciento de ellos, casi la totalidad, consideran importante que sean protegidos por un marco legal específico (Veghes et al, 2011).

De acuerdo con Banistar (2018), alrededor de cien países en el mundo, de 193 oficialmente reconocidos hasta 2018 por la Organización de las Naciones Unidas[3], han adoptado leyes de protección de datos personales o privacidad que protegen los datos personales que están en posesión de organizaciones públicas y/o privadas. Estas leyes han sido creadas con el fin de otorgar mayor protección de los datos personales, aumentar el flujo de transacciones económicas, comerciales, y para el fortalecimiento del intercambio de investigación científica y técnica (Solange y Moreno, 2014).

Kuner (2011) hace hincapié en la necesidad de reconocer que este flujo transfronterizo de datos personales conlleva tanto riesgos como beneficios: mientras que la transferencia de datos personales a países con estándares mínimos en la protección

[3] http://www.un.org/en/member-states/index.html

de datos tiene riesgos, la transferencia de datos personales a países con mayores estándares de protección, además de aumentar la protección de los datos, representa beneficios económicos. Razón por la cual existe una tendencia internacional de cumplir con convenios y acuerdos internacionales que homogenizan la protección de datos personales para facilitar su flujo transfronterizo.

En el siguiente mapa, en azul destacan los países que cuentan con leyes exhaustivas, en rojo los que están pendientes o tienen la obligación de promulgar y en blanco los que no tienen ley. Como se observa, los países que son parte de una organización, comunidad, acuerdo o tratado internacional, como el Foro de Cooperación Económica Asia-Pacífico, la Unión Europea o la Organización para la Cooperación y Desarrollo Económicos, cuentan con leyes que Banistar (2016) califica como exhaustivas.

LEYES DE PROTECCIÓN DE DATOS PERSONALES
Y PRIVACIDAD DE LA INFORMACIÓN

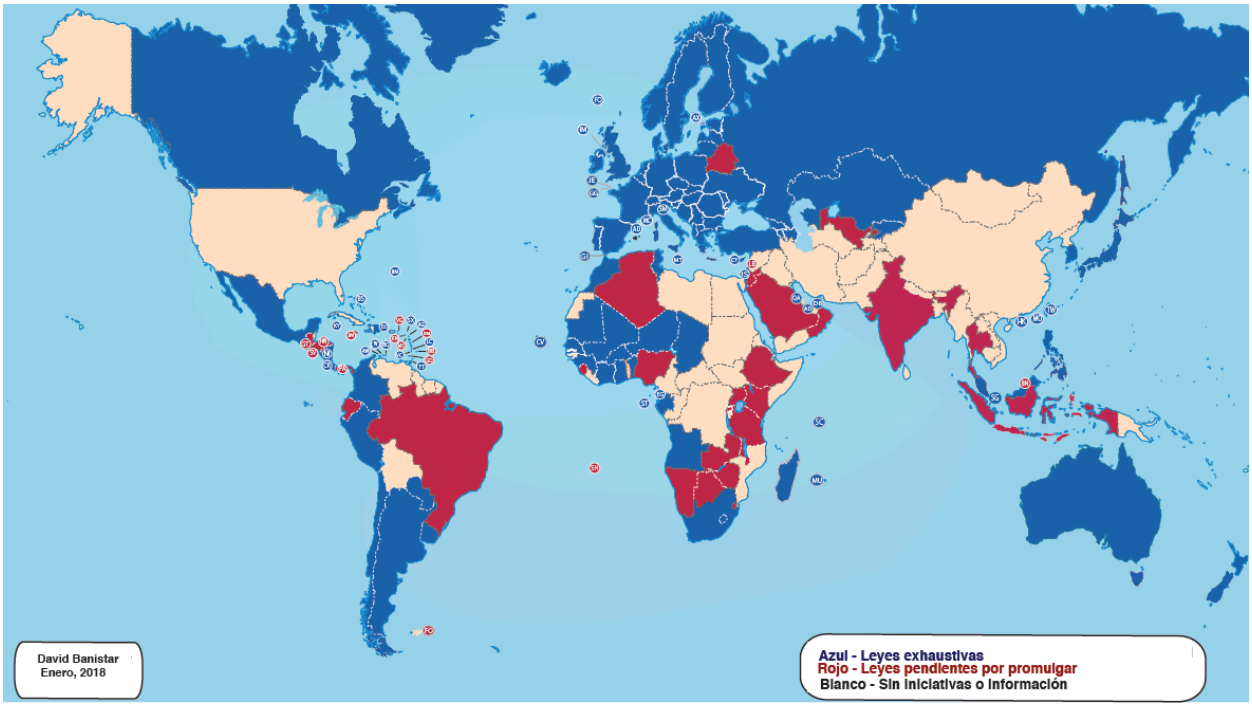


Tabla 1 Leyes nacionales de protección de datos personales y privacidad 2016. Fuente: Banistar (2018)

Así como hay países que cuentan con leyes de protección de datos personales, otros han optado por las leyes sectoriales a pesar de la tendencia internacional por homogenizar la protección de datos personales y, en otros casos, hay países que combinan las leyes generales con las sectoriales, en los que las primeras brindan un marco común y las segundas llenan espacios vacíos.

En comparación con las leyes generales de protección de datos personales, es difícil determinar los alcances y cumplimiento en la práctica de las leyes sectoriales, que se traduce en el nivel real de protección de los datos (Blume, 2015). Como ejemplo, sobresale el caso de Estados Unidos, cuyo marco legislativo no incluye una ley específica de protección de datos personales sino una reglamentación sectorial. Es decir, hay distintas leyes y regulaciones federales y estatales mediante las cuales las organizaciones pueden cumplir con el derecho a la privacidad, según su acepción. Según el reporte *Data Protection Laws of the World* (DLA Piper, 2016), EE. UU. cuenta con veinte leyes nacionales sobre privacidad, además de las leyes que tienen sus cincuenta estados, tan solo en California hay 25 leyes que regulan la privacidad de los datos en distintos sectores.

Estas leyes sectoriales en Estados Unidos pertenecen a servicios del sector financiero que han implementado medidas de la *Gramm Leach Bliley Act*, también conocida como *Financial Services Modernization Act* (Ley de Modernización de Servicios Financieros) de 1999, que establece cómo sus sujetos obligados pueden colectar, usar y revelar datos personales.

De manera similar, en el contexto del sector salud, el Departamento de Salud y Servicios Humanitarios es responsable de dar cumplimiento a la *Health Insurance Portability and Accountability Act* (Ley de portabilidad y responsabilidad de seguros de salud) de 1996, que requiere a sus sujetos obligados notificar a las personas con un aviso de prácticas de privacidad. O el caso de sectores más vulnerables, como la *Children's Online Privacy Protection Act* (Ley para la protección de la privacidad infantil en línea) de 1998. Asimismo, en Estados Unidos tampoco existe una autoridad

competente que garantice el cumplimiento de la protección de los datos personales y la imposición de sanciones, sino que, a nivel federal, la autoridad responsable depende de la ley en cuestión o de códigos civiles. Los afectados pueden demandar a los responsables por los daños que les pueda causar la negligencia en la obtención o el uso de la información personal (Sotto y Simpson, 2014; DLA Piper, 2016).

Una medida implementada por las organizaciones privadas en Estados Unidos es el *Safe Harbor Program* (puerto seguro). Se trata de un mecanismo que permite las transferencias de datos personales de la Unión Europea a Estados Unidos. Las compañías estadounidenses que se suman a este programa de manera voluntaria, sin estar obligados por ninguna ley, deben desarrollar políticas autorregulatorias de privacidad que obedezcan a los principios de información, elección, transferencia, seguridad, integridad de los datos, acceso y cumplimiento, con el fin de satisfacer los requerimientos de la Unión Europea (Colonna, 2014).

Ornelas e Higuera (2013) explican que esta oposición aparente al modelo europeo está basada en la idea de que la regulación excesiva puede inhibir las relaciones comerciales y económicas, por lo que el mercado debe ser capaz de autorregularse siempre que el consumidor muestre interés. Estados Unidos únicamente regula en algunos sectores que impliquen alto riesgo, como el financiero o salud, y no existe una regulación general sobre el tema. Concluyen que la protección de datos personales en Estados Unidos no es un derecho fundamental, sino "parte de la lógica del comercio justo" (Ornelas e Higuera, 2013).

Como prueba de esto, en marzo de 2017, la administración de Trump anuló un apartado referente a la "Protección de la intimidad de los clientes de servicios de banda ancha y otros servicios de telecomunicaciones", promulgado por la Comisión Federal de Comunicaciones que, principalmente, obligaba a las compañías prestadoras de servicios de telecomunicaciones a informar a sus clientes sobre el tratamiento de su información personal, adoptar medidas de seguridad y requería el consentimiento de los usuarios para vender sus datos. Además de deshacer tales obligaciones, también

prohíbe al órgano regulador volver a imponer restricciones similares (Congress.gov, 2017).

Por lo tanto, en EE. UU., las organizaciones que cumplen con medidas protectoras no es solo por el carácter coercitivo de las leyes sectoriales, sino también por intereses comerciales, por voluntad propia o por los beneficios que representa.

El siguiente mapa que desarrolló DLA Piper (2016) destaca el nivel de reglamentación y su implementación en cada país. En color rojo aparecen los que califica como fuerte; en naranja es robusto; amarillo, moderado, y verde es limitado.

MAPA DE LEYES DE PROTECCIÓN DE DATOS PERSONALES EN EL MUNDO

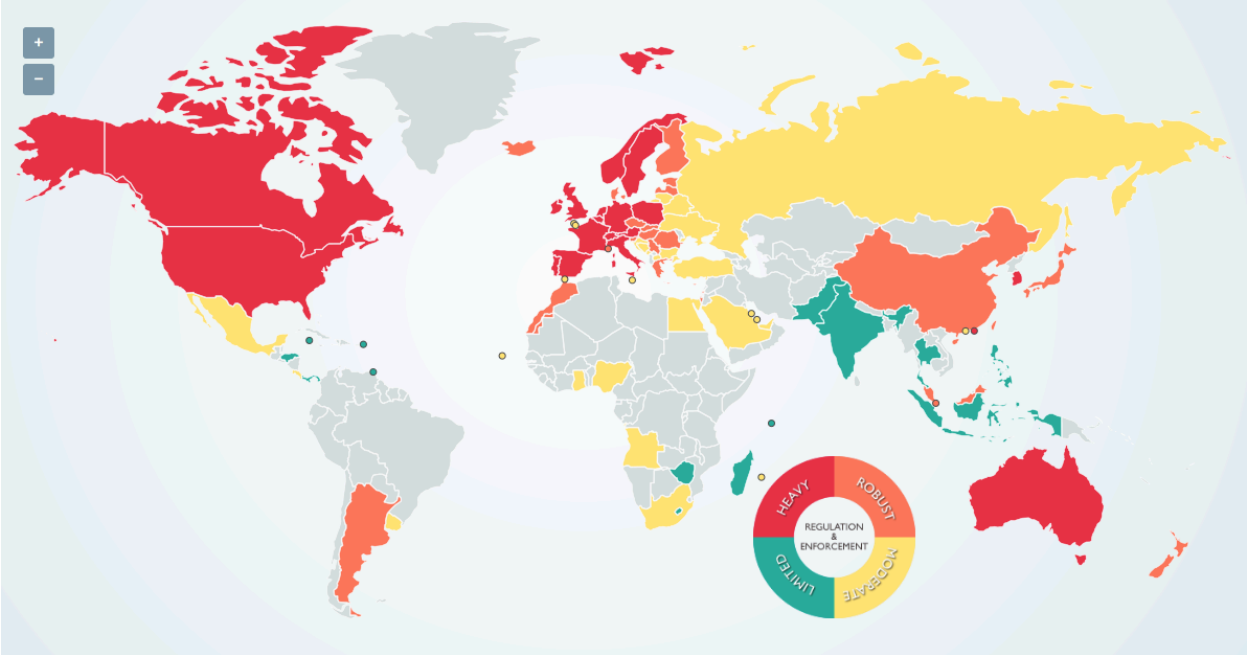


Tabla 2 Leyes de protección de datos personales del mundo. Fuente: DLA Piper (2018)

De este mapa llama la atención que, no obstante que Estados Unidos no tiene una ley específica de protección de datos personales, es uno de los países con una regulación (sectorial) y aplicación fuerte. A diferencia del caso de México que, a pesar de que

cuenta con una ley federal que protege los datos personales que Banistar (2016) califica como exhaustiva, DLA Piper (2018) lo evidencia como un país con una reglamentación e implementación de nivel moderado en comparación con el Reglamento de la Unión Europea. Esto, a pesar de que actualmente, México cuenta con leyes que Banisar califica como exhaustivas.

Por esto, Solange y Moreno (2014) destacan que para México era importante adoptar políticas de protección de datos personales exhaustivas y cumplir con ellas porque, en el ámbito internacional, aumentó la posibilidad de ser parte del Convenio 108, que establece un marco seguro para la transferencia de datos personales (Blume, 2015). Las autoras comentan que el hecho de que México se integrara a este Convenio no es cuestión menor. Los beneficios de la adhesión, que ocurrió en mayo de 2018, fueron (Solange y Moreno, 2014):

a. La apertura de flujos de inversión extranjera al brindar certeza jurídica en los intercambios comerciales transfronterizos con los Estados Partes

b. Generación de empleos y fomento de la inversión extranjera

c. Fortalecimiento de la relación comercial entre México y los Estados Partes al cumplir con los estándares internacionales en materia de privacidad

En otras palabras, la adhesión de México es un precedente en las gestiones para obtener el reconocimiento de la Unión Europea como un país que da un nivel de protección adecuado a los datos personales, con el fin de facilitar su flujo entre sus Estados miembro y México sin mayor requerimiento adicional (Solange y Moreno, 2014; Blume, 2015). Asimismo, Velasco (2015) asegura que adoptar estas políticas también permitirá cumplir con los requerimientos de otros marcos regionales emergentes, como el Marco de Privacidad del flujo transfronterizo de datos personales de APEC.

Fue a partir de esta tendencia internacional por homogenizar las leyes de protección de datos personales que México también se sumó. Esta tesis busca descubrir cuál es el papel que desempeñan los factores que motivan el cumplimiento de la ley en las

organizaciones, teniendo presente que el alma de toda ley es garantizar derechos, establecer obligaciones y principios con los que deben cumplir los sujetos obligados.

CAPÍTULO II

LA NORMATIVIDAD QUE GARANTIZA EL CUMPLIMIENTO DE LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

Toda actividad política, económica y social requiere los datos de las personas para operar. Por lo tanto, es necesario que los sistemas jurídicos emitan normatividad para garantizar su uso adecuado. Actualmente, México reconoce la protección de los datos personales como un derecho constitucional y, desde hace más de una década, comenzó a dar pasos importantes en la materia. Este capítulo realiza un breve recorrido por el marco jurídico mexicano que sienta los derechos y principios que los sujetos obligados deben de cumplir y garantizar, así como las sanciones aplicables en caso de infracción.

El cumplimiento de la protección de datos personales en el marco jurídico mexicano

Hasta hace unos años, la Constitución Política de los Estados Unidos Mexicanos protegía el derecho a la privacidad sin hacer mención específica de los datos personales. La libertad de expresión y el derecho a la información estaban garantizados en el artículo sexto. En su artículo séptimo, la Constitución se refería a la libertad de imprenta y también señalaba como límite la vida privada de terceros y, por último, el artículo 16 hacía mención de la privacidad. También había otras disposiciones y leyes que, desde su ámbito, garantizaban la seguridad de la información.

A pesar de que los artículos constitucionales protegían el derecho a la privacidad, fue hasta la puesta en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), publicada en 2002 —que define a los datos personales como la información que concierne a una persona física y cuyo artículo cuarto estaba dedicado al derecho de la protección de datos personales—, y la

creación del Instituto Federal de Acceso a la Información (Inai)[4] en ese mismo año, que México dio un gran avance en la protección de datos. A partir de entonces, el Inai se convirtió en la autoridad correspondiente para atender la protección de datos y, a la vez, garantizar el acceso a la información pública. Entre sus amplias facultades era el encargado de vigilar, supervisar, investigar, inspeccionar y sancionar las conductas indebidas para garantizar el cumplimiento y observancia de la LFTAIPG.

Los sujetos obligados de la LFTAIPG únicamente eran los órganos públicos federales. Para operar y subsanar sus carencias —por ejemplo, no contenía los derechos ARCO—, el Inai pronunció una serie de lineamientos generales y resoluciones de carácter administrativo a nivel federal para regular a los sistemas de datos personales públicos en el país (Vélez, 2011).

Hasta ese momento la protección de datos personales todavía no era reconocido como un derecho fundamental en la Constitución mexicana. De acuerdo con Ornelas y Martínez (en Vélez 2011), aparentemente México ya contaba con una normatividad en la materia. A pesar de que sólo se trataba de un acercamiento a la protección de datos personales, los pasos que dio el Inai fortalecieron el derecho a la protección de datos.

Por su parte, las legislaciones estatales en materia de transparencia y acceso a la información comenzaron a agregar a su contenido la protección de datos personales en posesión del sector público con órganos estatales que velaban su cumplimiento. Se trata de leyes locales que se hicieron entre 2004 y 2005, cuando el concepto de protección de datos personales todavía no estaba bien definido en México.

Ante la aparición de estas leyes, Villanueva (en Vélez, 2011) vislumbró la necesidad de una normativa de orden general que estableciera aplicaciones puntuales en cada estado, bajo un mismo procedimiento y principios, puesto que cada ley se hizo a imagen y semejanza de las necesidades políticas de cada entidad federativa. “Tienen algunos puntos en común pero también muchas diferencias sustantivas que dan cuenta

[4] Como parte de las modificaciones en la Ley General de Trasparencia y Acceso a la Información Pública de 2015, el Instituto, que hasta entonces usaba el acrónimo Ifai, cambió su nombre a Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos, con el acrónimo Inai, que será utilizado en este documento porque es su nombre actual.

del profundo desconocimiento que hay en la materia y del propósito de tener una ley por cumplir con esa finalidad independientemente de que sirva o no" (Villanueva, en Vélez, 2011):

> Sus deficiencias recaen principalmente en los mecanismos de protección de datos personales, la definición de los alcances de la ley y los mecanismos que tienen para asegurar el cumplimiento de la norma. Hay un problema de carencia de carácter técnico jurídico porque los medios no están suficientemente bien elaborados para cumplir con el fin que es la protección de datos, y porque hay leyes parciales que, dependiendo del estado, algunas son más protectoras, semicomprensivas o reducidas que otras. Todo esto provoca que la protección de datos personales sea un tema similar al acceso a la información pública antes de la reforma al artículo 6º. Constitucional cuando las leyes no eran uniformes, porque no hay una regulación específica en el ámbito constitucional de datos personales que diga qué elementos deben incluir de forma desglosada y, como consecuencia, se genera dispersión legislativa (Villanueva, en Vélez 2011).

A partir de 2010, estas legislaciones sufrieron reformas para actualizarse o se reemplazaron por otras que cumplían con estándares mínimos de la protección de datos personales. Entre los estados que hasta 2017 contaban con una ley específica de datos personales estaban: Campeche (2012), Coahuila (2008), Colima (2012), Distrito Federal (2008), Guanajuato (2006), Estado de México (2012), Morelos (2003), Oaxaca (2008), Puebla (2013) y Tlaxcala (2012).

En 2007 una reforma al artículo 6º de la Constitución Política de los Estados Unidos Mexicanos introdujo de manera expresa la protección de los datos personales y de la información referente a la vida privada, así como el derecho de acceso y corrección de datos en posesión de los entes públicos. Fue la primera vez que la Constitución hizo referencia a la protección de datos personales. Sin embargo, era indispensable proteger también los datos personales que estaban en posesión de particulares, puesto que México ya formaba parte de tratados internacionales con países federales que tenían legislación en torno a la materia, como Argentina y Canadá. Incumplir con los requisitos y compromisos establecidos internacionalmente al privar a la Federación la facultad de tutelar las relaciones jurídicas derivadas del tratamiento de datos personales en posesión de los particulares podía crear consecuencias para el Estado Mexicano (Dictamen art. 73).

En 2008 se reconoció el derecho de toda persona a la protección de su información como un derecho fundamental independiente en una reforma al artículo 16 Constitucional. La reforma le añadió un segundo párrafo al artículo que hablaba explícitamente de los datos personales, reconoció su naturaleza autónoma que lo distingue de otros derechos fundamentales y plasmó los derechos de acceso, rectificación, cancelación y oposición (ARCO) (Dictámenes de Primera Lectura, en Vélez, 2011). La reforma al artículo 16 Constitucional también reconoció el derecho que tiene el titular de disponer de manera libre, informada y específica el uso de los datos personales sobre la base del consentimiento (Vélez, 2011).

Otra de las modificaciones que tuvo la Constitución se encuentra en el artículo 73, al que se le añadió la fracción “XXIX-O” que dio al Congreso la facultad para expedir leyes que protegieran los datos personales que estuvieran en posesión de los particulares, tales como bancos, hospitales, escuelas, aseguradoras, etcétera. Esta reforma le dio al legislador la oportunidad de elaborar una ley federal que protegiera los datos personales en posesión de los particulares. Dicha ley debía plasmar principios, derechos, procedimientos, infracciones, la existencia de una autoridad correspondiente y un régimen de transferencias internacionales de datos de acuerdo con estándares internacionales, además de brindar seguridad jurídica a los datos de las personas que se utilizan en las transferencias internacionales (Dictamen art. 73).

El resultado de esto fue la Ley de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) de 2010, junto con su reglamento, publicado en el Diario Oficial de la Federación en diciembre de 2011. Con esta ley, México se colocó entre las democracias que cuentan con un marco normativo que regula esta materia, se alineó con los países miembros de la OCDE, de la APEC y de la Unión Europea, y garantiza la seguridad del flujo transfronterizo de datos, con las ventajas de carácter económico que le confiere. El órgano garante seguía siendo el Inai, que cambió su nombre a Instituto Federal de Acceso a la Información y Protección de Datos.

La LFPDPPP, junto con las reformas a la Constitución en 2009 y a la LFTAIPG, conformaron lo último en materia regulatoria para la protección de datos personales en

posesión de sujetos públicos y particulares[5]. Sin embargo, el problema de la dispersión normativa para el derecho de protección de datos personales en México hacía evidente la necesidad de subsanar la desigualdad. Por un lado, una ley federal regula el sector privado, mientras que el sector público se dividía en una ley federal y las estatales. Expertos en la materia, como López Ayllón y Marbán Laborde, también cuestionaban si debía haber 32 leyes de datos personales o una ley general aplicable a toda la Federación para el sector público (Solange y Moreno, 2014).

Para enmendar la dispersión legislativa, una nueva reforma constitucional publicada en el Diario Oficial de la Federación el 7 de febrero de 2014 modificó la naturaleza jurídica del Inai y sus homólogos en los estados y la Ciudad de México, para convertirlos en órganos constitucionales autónomos. También dio facultad al Congreso de la Unión para expedir una ley general que desarrollara los principios y bases en materia de protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno. Esta reforma trajo

[5] Una de las principales críticas hechas a la legislación española en torno a la protección de datos, se encuentra precisamente en que regula de forma sectorial a las instituciones públicas y privadas. El mismo cuestionamiento podría hacerse a esta nueva reglamentación en México, puesto que no es el carácter de público o privado lo que pone en peligro la intimidad de las personas, sino el uso que se hace de su información. Pérez Luño (2001) señalaba que las lesiones del sector privado no son, necesariamente, menores que las que pueden realizarse en el poder de las entidades gubernamentales, por lo que no debería existir diferencia entre uno y otro frente a los posibles abusos perpetrados.
Ballester Fernández (en Vélez, 2011) afirma que: "Nosotros en España lo hemos unificado, las personas son únicas, entonces no distinguimos entre empresas privadas o empresas públicas. La misma reglamentación tiene que funcionar para todas las instituciones. Así, lo que se hace es que se discrimina y nosotros lo que hemos hecho es concentrado. Sólo tenemos una ley de privacidad que además también emana de las directivas europeas". Pero, a pesar de que en España poseen una misma ley, su ley es sectorial porque distingue los ficheros públicos de los privados, a lo que agrega: "Se menciona específicamente que las bases de datos públicas tienen que estar protegidas de una manera mucho más especial, por ejemplo, los datos de la policía o de los contribuyentes. Los gobiernos tienen muchos más datos de carácter personal y lo que se ha hecho es que se ha modificado todo en un solo modelo: niveles de datos básicos, medios y altos. Entonces debe protegerse cada uno de esos distintos tipos de nivel. Es mucho más simple aplicar los mismos criterios independientemente de que sean públicos o privados, por ejemplo, pueden existir empresas privadas del ámbito sanitario que van a aplicar las mismas medidas de seguridad que una del sector públicos". Y añade que la discriminación se genera porque las instituciones públicas que tienen mayor poder pueden ejercer mayor abuso sobre los datos de las personas (Vélez, 2011).
Sumado a esta desigualdad, cabe destacar que la LFTAIPG tuvo que implementar los lineamientos de protección de datos personales adicionales para llenar los vacíos que tenía en esta materia. Una de sus debilidades de la LFTAIPG es que no garantiza los derechos de ARCO, únicamente garantiza el acceso y la modificación de los datos. Las principales diferencias y similitudes de las dos legislaciones vigentes hasta el momento, se encuentran contenidas en el **Anexo 3**. Recaen en las definiciones, derechos, principios, plazos, obligaciones, excepciones, infracciones, sanciones, delitos, etcétera. En general, la LFTAIPG, para suplir sus vacíos, recurre a los Lineamientos que detallan de forma más específica la forma en que procede este derecho.

cambios significativos para la protección de datos personales (Solange y Moreno, 2014):

1. Modificó la naturaleza jurídica del Inai, así la de sus homólogos en los estados y la Ciudad de México. Se convirtieron en órganos constitucionales autónomos. Esto los hizo independientes de los poderes legislativo, ejecutivo y judicial. Les brindó autonomía técnica, de gestión y de presupuesto, y les dio personalidad jurídica y patrimonio propios. De esta manera, se convirtieron en organismos autónomos cuya misión es garantizar el cumplimiento del derecho a la protección de datos personales.
2. El órgano constitucional tiene la facultad de promover actos inconstitucionales que vulneren el derecho que defienden, en contra de leyes de carácter federal, estatal y de la Ciudad de México, así como de tratados internacionales a los que México pertenece.
3. Dada su nueva naturaleza, los miembros de los órganos garantes del derecho a la protección de datos personales podrán ser sometidos a juicio político (artículo 110, párrafos primero y segundo).
4. El artículo 6º. Constitucional llamó a más sujetos obligados a cumplir con la legislación en materia de transparencia y acceso a la información pública, misma que también aplica para la protección de datos personales:

> El organismo garante tiene competencia para conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales de cualquier autoridad, entidad, órgano u organismo que forme parte de alguno de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal; con excepción de aquellos asuntos jurisdiccionales que correspondan a la Suprema Corte de Justicia de la Nación, en cuyo caso resolverá un comité integrado por tres ministros. (Artículo 6º., apartado A, fracción VIII, párrafo cuarto de la Constitución Política de los Estados Unidos Mexicanos).

5. En principio, las resoluciones del órgano autónomo se convirtieron vinculatorias, definitivas e inacatables, tal como lo establece el artículo 6º., apartado A, fracción VIII, párrafo séptimo). Sin embargo, la Suprema Corte de Justicia de la

Nación podrá interponer el recurso de revisión cuando la seguridad nacional esté en peligro.

6. Todas las autoridades y servidores públicos adquirieron la obligación de coadyuvar con el órgano constitucional autónomo.
7. El artículo 73, fracción XXIX-S facultó al Congreso de la Unión para:

> (Para) expedir las leyes generales reglamentarias que desarrollen los principios y bases en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno.

Como respuesta a la reforma, en enero de 2017, el Diario Oficial de la Federación publicó la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPSO) (DOF, 2017). Son sujetos obligados por esta ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órgano autónomo, partidos políticos, fideicomisos y fondos públicos; así como los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal. Los responsables (sujetos obligados) deben establecer y mantener medidas de seguridad para proteger los datos personales que posean contra cualquier daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Al igual que la LFPDPPP, la LGPDPPSO establece que el Instituto y los organismos garantes pueden imponer sanciones para garantizar su cumplimiento, que van desde una amonestación pública o multa que corresponde a la cantidad de 150 hasta 500 veces el valor diario de la Unidad de Medida y Actualización —equivalente al salario mínimo—. Las sanciones de carácter económico no pueden pagarse con recursos públicos y en caso de reincidencia se puede imponer una multa equivalente hasta el doble de la que se hubiera determinado. Es importante resaltar que estas multas no se comparan con las de la ley de los particulares, que ascienden hasta 320 mil días de salario mínimo, o el doble en caso de reincidir e, incluso, prisión. Esta diferencia en las

sanciones no significa que los datos personales en posesión de los particulares sean más vulnerables que las que están en posesión de los entes públicos.

Las leyes estatales tuvieron un plazo de seis meses para ajustarse a las disposiciones de la LGPDPPSO a partir de su entrada en vigor. A pesar de que esto ya ocurrió, esta investigación únicamente analiza el cumplimiento del sector privado con la LFPDPPP.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares como instrumento de cumplimiento

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares incluye una doble vertiente. Por un lado, impone obligaciones que los responsables de las bases de datos deben cumplir para que usen la información de acuerdo con los principios establecidos y, por el otro, da al titular el derecho de controlar su información que posea cualquier particular: aseguradoras, bancos, tiendas departamentales, universidades, etcétera. En su artículo segundo, la ley establece quiénes son sus sujetos obligados:

> Art. 2. Son sujetos regulados por esta ley, los particulares que 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.

También resalta cuatro ejes desarrollados que dan pauta a los sujetos obligados para cumplir con la protección de los datos personales que están bajo su responsabilidad. Específicamente, consisten en (Senado de la República, 2010):

a) Desarrolla principios internacionalmente reconocidos

El objetivo primordial de los principios es asegurar que el tratamiento que los sujetos obligados hacen de los datos personales sea el adecuado. Es un conjunto de derechos

que garantizan la protección uniforme de los datos personales, no solo en México, sino a nivel internacional (ICDPPC, 2009). La ley de los particulares en México atiende los principios recogidos en la Resolución de Madrid aprobada en 2009, y hace hincapié en que la causa que hace legítimo el tratamiento de la información personal es el consentimiento del titular, que se caracteriza por ser libre, específico, informado e inequívoco (Senado de la República, 2010).

El capítulo II de la LFPDPPP contiene los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. Cada uno de ellos se explica a continuación.

Principios de la LFPDPPP

Principio	Definición
Licitud	El principio de licitud obliga al responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional.
Consentimiento	El responsable deberá obtener el consentimiento para el tratamiento de los datos personales, salvo ciertas excepciones. La solicitud del consentimiento deberá ir referida a una finalidad o finalidades determinadas. El consentimiento puede ser tácito o expreso. Es libre, específico, informado e inequívoco. Le da legitimidad al tratamiento de los datos.
Información	El responsable deberá dar a conocer al titular la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales. La persona responsable deberá facilitar a los interesados, al menos, información acerca de su identidad, de la finalidad para la que pretende realizar el tratamiento, de los destinatarios a los que prevé ceder los datos de carácter personal y del modo en que los interesados podrán ejercer los derechos ARCO, así como cualquier otra información necesaria para garantizar el tratamiento leal de dichos datos de carácter personal.
Calidad	Se cumple con el principio de calidad cuando los datos personales tratados sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados. Se presume que se cumple con la calidad en los datos personales cuando estos son proporcionados directamente por el titular, y hasta que este no manifieste y acredite lo contrario, o bien, el responsable cuente con evidencia objetiva que los contradiga. La persona responsable deberá limitar el periodo de conservación de los datos de carácter personal tratados al mínimo necesario. De este modo, cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades que legitimaron su tratamiento deberán ser cancelados o

	convertidos en anónimos.
Finalidad	Los datos personales sólo podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en el aviso de privacidad. La finalidad o las finalidades establecidas deberán ser determinadas, lo cual se logra cuando con claridad, sin lugar a confusión y de manera objetiva se especifica para qué objeto serán tratados los datos personales. La persona responsable se abstendrá de llevar a cabo tratamientos no compatibles con las finalidades para las que hubiese recabado los datos de carácter personal, a menos que cuente con el consentimiento inequívoco del interesado.
Lealtad	El principio de lealtad establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad. No se podrán utilizar medios engañosos o fraudulentos para recabar y tratar datos personales.
Proporcionalidad	Sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido. En particular, la persona responsable deberá realizar esfuerzos razonables para limitar los datos de carácter personal tratados al mínimo necesario.
Responsabilidad	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquellos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano. Para cumplir con esta obligación, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines.

Tabla 3 Principios de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

b) Contiene los derechos ARCO

Para Davara Fernández, en sí mismo, el dato personal no es el que necesita la protección, sino su titular cuando lo hace identificable, como lo explica en sus propias palabras (en Frutos, 2014):

> El dato, en sí mismo, no necesita protección alguna. Sin embargo, cuando el dato se une a una persona, es algo distinto. Ya no protegemos entonces al dato, sino al titular del mismo, a la persona. Es más, cuando el dato se une a la persona se convierte en información personal.
>
> En este mismo sentido, las normativas en protección de datos persiguen proteger al individuo frente al ilícito tratamiento de la información personal que le concierne. Es decir, el individuo es el

> titular del derecho. Es un derecho subjetivo, no se trata de una protección per se, sino de la protección del individuo que dicha información cierne (Davara Fernández, en Frutos, 2014).

Aunado a esto, los Estándares Internacionales sobre Protección de Datos Personales y Privacidad (ICDPPC, 2009) reconocen los derechos de acceso, rectificación, cancelación y oposición (ARCO) que acompañan a la protección de los datos personales. Kamarinou, Millard y Kuan (2016) también escudriñan el derecho a tener acceso, corregirlos, suprimirlos o de objetar su uso, como derechos individuales. Los derechos ARCO son importantes porque brindan al titular de los datos la posibilidad de decidir sobre el tratamiento que los sujetos obligados de las leyes dan a su información personal y resguardarla de cualquier ilícito.

La LFPDPPP prevé los mecanismos necesarios para ejercer los derechos ARCO ante los responsables de las bases de datos en su capítulo cuatro. El artículo 22 señala que:

> Cualquier titular, o en su caso representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos.

Por lo tanto, es fundamental que toda organización que trata datos personales garantice el cumplimiento de los derechos ARCO para brindar seguridad no solo al dato, sino a sus titulares que pueden ser identificados o identificables.

El **derecho de acceso** significa que el titular puede acceder a las bases de datos para saber si existe información suya y qué tratamiento le están dando, cómo la obtuvieron, por qué medio, cuál es el fin de la recolección, por cuánto tiempo se va a conservar. Es decir, los interesados pueden ejercer control sobre su información personal ya que, en principio, cualquier persona puede consultar la información que haya proporcionado a un tercero que forme parte de una base de datos (Gacitúa, 2014). Es obligación de las organizaciones hacer cumplir este derecho y dar respuesta a la solicitud del titular, aun cuando el responsable no tenga información del solicitante. Según el artículo 33 de la LFPDPPP, la obligación se cumple cuando el titular tiene a su disposición los datos personales que solicitó, ya sea mediante copias, documentos electrónicos o cualquier otro medio que señale el aviso de privacidad.

El **derecho de rectificación** se ejerce cuando los datos son inexactos o incompletos, como lo señala el artículo 24 de la ley de los particulares. El titular de los datos puede corregir sus datos tras un cambio de domicilio, por ejemplo. Para fines de promoción y prestación de servicios, es conveniente que las organizaciones mantengan actualizadas sus bases de datos. La rectificación cumple con el principio de calidad por la actualidad de los datos, porque busca que el tratamiento sea fiel reflejo de la realidad (Gacitúa, 2014).

El **derecho de cancelación** brinda la facultad de exigir al responsable de la base de datos que suprima su información cuando no se cumplen los principios y deberes, siempre que no sea parte de un contrato, que no exista alguna disposición legal de por medio, no se obstaculicen procedimientos judiciales o administrativos, sean necesarios para proteger los intereses del titular, realizar una acción de interés público o sean indispensables para la atención, gestión, prevención o diagnóstico médico (Art. 26 de la LFPDPPP). Con esto, el titular manifiesta su voluntad de “terminar la relación jurídica con el responsable del tratamiento por voluntad unilateral del interesado” (Aparicio, en Frutos, 2014).

Finalmente, con el **derecho de oposición** el titular puede oponerse al tratamiento de sus datos bajo una causa legítima y de manera justificada. (Art. 27 de la LFPDPPP). Por ejemplo, una persona puede oponerse a que las organizaciones utilicen sus datos con fines de promoción; para apoyar al derecho, entes de gobierno, como la Procuraduría Federal del Consumidor cuenta con mecanismos como las listas de exclusión, en las que de forma gratuita y con constancia de inscripción, los interesados pueden darse de alta para no ser irrumpidos por la mercadotecnia.

El siguiente cuadro explica cómo opera cada uno de los derechos ARCO que tienen que cumplir las organizaciones en México.

Derechos ARCO

Derecho	Operación del derecho
Acceso	1. El interesado tendrá derecho a recabar de la persona responsable, cuando así lo solicite, información relativa a los concretos datos de carácter personal objeto de tratamiento, así como al origen de dichos datos, a las finalidades de los correspondientes tratamientos y a los destinatarios o las categorías de destinatarios a quienes se comuniquen o pretendan comunicar dichos datos. 2. Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo. 3. La legislación nacional aplicable podrá limitar el ejercicio reiterado de estos derechos, que obligaría a la persona responsable a responder múltiples solicitudes en intervalos cortos de tiempo, excepto en aquellos casos en los que el interesado haga constar en su solicitud un interés legítimo.
Rectificación	1. El interesado tendrá derecho a solicitar a la persona responsable la rectificación de los datos de carácter personal que pudieran resultar incompletos, inexactos, innecesarios o excesivos. 2. Cuando proceda, la persona responsable rectificará los datos de carácter personal conforme a lo solicitado. Deberá, además, notificar este extremo a los terceros a quienes se hayan comunicado los datos de carácter personal, siempre que los mismos fueran conocidos.
Cancelación	1. El interesado tendrá derecho a solicitar a la persona responsable la cancelación de los datos de carácter personal que pudieran resultar incompletos, inexactos, innecesarios o excesivos. 2. Cuando proceda, la persona responsable rectificará los datos de carácter personal conforme a lo solicitado. Deberá, además, notificar este extremo a los terceros a quienes se hayan comunicado los datos de carácter personal, siempre que los mismos fueran conocidos. 3. La cancelación no procederá cuando los datos de carácter personal deban ser conservados para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable o, en su caso, por las relaciones contractuales entre la persona responsable y el interesado.
Oposición	El interesado tendrá derecho al tratamiento de sus datos de carácter personal cuando concurra una razón legítima derivada de su concreta situación persona. 2. No procederá el ejercicio de este derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable. 3. Cualquier interesado podrá oponerse, igualmente, a aquellas decisiones que conlleven efectos jurídicos basadas únicamente en un tratamiento automatizado de datos de carácter personal, excepto cuando la decisión hubiese sido expresamente

	solicitada por el interesado o sea precisa para el establecimiento, mantenimiento o cumplimiento de una relación jurídica entre la persona responsable y el propio interesado. En este último caso, el interesado debe tener la posibilidad de hacer valer su punto de vista, a fin de defender su derecho o interés.

Tabla 4 Derechos ARCO. Fuente: Estándares Internacionales sobre Protección de Datos Personales y Privacidad

c) Establece procedimientos con los que los responsables deben de cumplir para garantizar el ejercicio de los derechos ARCO

No basta con que la LFPDPPP y su Reglamento contengan principios y derechos, también es necesario que existan deberes y mecanismos de cumplimiento. Estas obligaciones consisten en:

1. Mantener la confidencialidad de los datos personales que prevalece aún después de terminada la relación jurídica.
2. Poner a disposición de los usuarios el Aviso de Privacidad. El aviso de privacidad cumple con el principio de información porque pone a disposición del titular el tratamiento que el responsable hará de sus datos, con el fin de otorgarle pleno control de ellos.

   Contiene la identidad y domicilio del responsable, los datos personales que serán sometidos al tratamiento, señalar qué datos sensibles recaba y con qué finalidad, los mecanismos para que el titular manifieste su negativa para el tratamiento de datos que no son necesarios para cumplir con la relación jurídica con el responsable, indicar si los datos se transfieren a terceros y con qué fin con una cláusula de consentimiento, establecer los medios y procedimientos para el ejercicio de los derechos ARCO, los mecanismos y procedimientos para poder revocar el consentimiento, las opciones y medios para limitar el uso o divulgación de datos personales, informar sobre el uso de mecanismos en medios remotos o locales de comunicación que permitan recabar datos de manera automática y simultánea cuando el titular hace contacto con los mismos, y los procedimientos y medios para comunicar cambios al aviso de privacidad. (Art. 16).

3. Designar a un responsable de protección de datos personales al interior de la organización. Puede ser una persona o un departamento que dará trámite a las solicitudes de los interesados para el ejercicio de sus derechos ARCO. Parte de su función también es fomentar la protección de datos personales al interior de la organización mediante programas de capacitación, fundamental para el cumplimiento (Art. 30).
4. Realizar un plan de trabajo para implementar las medidas de seguridad: los responsables deben garantizar la integridad y disponibilidad de los datos. Las medidas de seguridad deben ser administrativas, físicas y/o técnicas para la protección de los datos personales, mismas que deben ser documentadas en análisis de riesgo, análisis de brecha, revisiones o auditorías, capacitación, entre otras. El Reglamento establece de los artículos 59 al 66 todo lo referente a la seguridad de los datos personales que las organizaciones deben cumplir.
5. Establecer el proceso de atención al ejercicio de derechos ARCO e informar mediante el aviso de privacidad la manera en cómo la organización garantiza los derechos para dar cumplimiento.
6. Establecer las condiciones bajo las que la organización realiza las transferencias nacionales y/o internacionales a terceros y comunicarlas en el aviso de privacidad (Art. 36 y 37).
7. Hacer un análisis de brechas en las medidas de seguridad técnicas, físicas y administrativas. Realizar un inventario de las bases de datos existentes en la organización. Realizar un análisis de riesgos de los datos personales.

d) Contempla infracciones y sanciones para quien realice conductas inadecuadas con relación al trato de la información

Esta investigación sostiene que las sanciones son el factor principal que obligan a las organizaciones al cumplimiento, puesto que la LFPDPPP es una ley coercitiva al igual que las leyes europeas. ¿Pero qué justifica la naturaleza punitiva de estas leyes? Los datos personales son toda la información que identifica o hace identificable a una persona, de estos, se distinguen los datos personales sensibles como estado de salud,

creencias religiosas, ideologías, afiliación sindical, características físicas, huella digital, origen racial o étnico, preferencia sexual. El manejo de los datos personales no es una cuestión menor, su mal uso o acceso no autorizado podría poner en riesgo la integridad del titular de los datos o hacerlo víctima de discriminación.

Precisamente, el alma de la protección de los datos personales tiene sus orígenes en la Alemania nazi, cuando controlaba a la población con los datos del censo y los archivos del gobierno para identificar a judíos y a otros grupos víctimas de genocidios (Gregorio, 2004). Fue tal la conmoción que la Constitución alemana de la posguerra incluyó el derecho de privacidad y, actualmente, estos acontecimientos sirven como referencia para la protección de los datos personales, cuya necesidad de ser salvaguardados incrementó con el desarrollo de las tecnologías de la información y comunicación que facilitan su almacenamiento y transferencia.

Estos acontecimientos justifican que las leyes de protección de datos que surgieron en Europa a partir de 1970 establecieran multas y sanciones que aplican dependiendo de la infracción que cometa el responsable. Entre estas leyes y tratados internacionales, destaca el Reglamento 679 que marca multas hasta por 20 millones de euros y, como elemento innovador, puede obligar a los Estados miembro incluso si su legislación no contemplara multas administrativas.

La ley mexicana, que toma el ejemplo de las leyes europeas, principalmente de la española, también es una ley punitiva, aunque esto no significa que sea una ley prohibitiva, puesto que permite el tratamiento adecuado de los datos bajo determinadas condiciones establecidas por los principios y derechos mencionados anteriormente, que deben garantizar los sujetos obligados.

Los artículos 61, 62, 63 y 64 de la LFPDPPP indican que el Inai es el órgano responsable de determinar si el responsable recae en incumplimiento en la protección de derechos. De ser así, impondrá sanciones e infracciones de acuerdo con el presunto incumplimiento. Las multas ascienden hasta 320 mil días de salario mínimo, el doble en caso datos personales sensibles o de reincidencia e, incluso, prisión. El siguiente cuadro abarca las multas y sanciones que impone la ley por infracciones:

Artículos que establecen infracciones en la LFPDPPP

Artículo 63	Artículo 64
I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley;	I. El apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular, en los términos previstos por esta Ley, tratándose de los supuestos previstos en la fracción I del artículo anterior;
II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales; III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable; IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley; V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley (I. La identidad y domicilio del responsable que los recaba; II. Las finalidades del tratamiento de datos; III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos; IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley; V. En su caso, las transferencias de datos que se efectúen, y VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley. En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.); VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares; VII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64;	II. Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo anterior;
VIII. Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley (El responsable o terceros que intervengan en	III. Multa de 200 a 320,000 días de salario mínimo vigente en el

cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.); IX. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12 (El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular.); X. Transferir datos a terceros sin comunicar a estos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos; XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable; XII. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley; XIII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible; XIV. Obstruir los actos de verificación de la autoridad; XV. Recabar datos en forma engañosa y fraudulenta; XVI. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares; XVII. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos; XVIII. Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley (No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.), y XIX. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.	Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo anterior, y IV. En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. Tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

Tabla 5 Artículos que establecen infracciones en la LFPDPPP. Fuente: Elaboración propia.

Para establecer las sanciones, el artículo 65 indica que el Instituto deberá considerar la naturaleza del dato, la improcedencia notoria de la negativa del responsable para realizar los actos solicitados por el titular, el carácter intencional o no de la acción u omisión constitutiva de la infracción, la capacidad económica del responsable y la reincidencia.

Según el artículo 66 de la LFPDPPP, las sanciones se impondrán sin perjuicio de la responsabilidad civil o penal que resulte. Los artículos 67 a 69 indican lo referente a los delitos en materia del tratamiento indebido de los datos personales:

> Artículo 67.- Se impondrán de tres meses a tres años de prisión al que, estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.
>
> Artículo 68.- Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.
>
> Artículo 69.- Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.

Así como comprende multas y sanciones, la ley también establece la posibilidad a los sujetos obligados de refutar las resoluciones del órgano garante, el Inai, en la imposición de multas. Esto nos conduce, ahora, a conocer cuáles son las atribuciones del Instituto, como la autoridad de la protección de los datos personales en México, para que los sujetos obligados cumplan con sus responsabilidades.

Las funciones del Inai ante los sujetos obligados

En el caso mexicano, en 2015, la DPA responsable de la protección de los datos personales nuevamente cambió su nombre a Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (Inai). Su nombre no es cuestión menor puesto que indica que, además de cumplir con lo dispuesto por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) de 2002 y la Ley General de Trasparencia y Acceso a la Información Pública (LGTAIP) de 2015,

el Instituto también debe vigilar la observancia de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) de 2010 y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) de 2017.

El hecho de que el Inai observe el acatamiento de dos derechos opuestos que son el acceso a la información y la protección de datos personales, hace que la misión del Instituto sea muy compleja. A pesar de esto, México cumple con una condición importante para el Reglamento 679, que es contar con una autoridad autónoma que regule el tratamiento de los datos personales, como lo señala el artículo 37 de la LGTAIPG, que no solo se refiere al Inai, sino también a los órganos estatales que regulan en materia de transparencia, acceso a la información y protección de datos personales del sector público:

> Los organismos garantes son autónomos, especializados, independientes, imparciales y colegiados, con personalidad jurídica y patrimonio propios, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsables de garantizar, en el ámbito de su competencia, el ejercicio de los derechos de acceso a la información y la protección de datos personales, conforme a los principios y bases establecidos por el artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, así como por lo previsto en esta Ley y demás disposiciones aplicables.

De este artículo destaca que la naturaleza jurídica del Inai le permite ser un organismo con autonomía operativa, de decisión y presupuesto para desempeñar las atribuciones que señala el artículo 41 de la misma ley, el 89 de la LGPDPPSO y 38 y 39 de la LFPDPPP.

En lo que se refiere específicamente a la ley de los particulares, que es de interés para esta investigación, el Inai no solo tiene la atribución de difundir, promover y vigilar el derecho a la protección de los datos personales (Art. 38), sino que también debe verificar el cumplimiento de las disposiciones de la ley (Art. 39, Fracc. I).

Entre otras de sus funciones se encuentra interpretar la ley, dar apoyo técnico a quienes lo soliciten, emitir criterios y recomendaciones, divulgar estándares y mejores prácticas internacionales, conocer y resolver los procedimientos de protección de derechos y de verificación, cooperar con otras autoridades de supervisión y organismos

nacionales e internacionales, rendir un informe anual al Congreso de la Unión, acudir a foros internacionales, elaborar estudios de impacto sobre la privacidad, desarrollar, fomentar y difundir análisis, estudios e investigaciones en la materia y sobre las demás que le confieran la ley y otros ordenamientos aplicables (Art. 39 de la LFPDPPP).

Estos artículos enmarcan la función promotora y ejecutora del Inai como DPA que menciona Jóri (2015). Por ejemplo, ha desarrollado concursos que fomentan la participación de los sujetos obligados con buenas prácticas de protección de datos personales, como el Premio de innovación y buenas prácticas en la protección de datos personales, el Concurso para ser Comisionada y Comisionado Infantil, conferencias anuales con motivo del Día Internacional de Protección de Datos Personales, y ha impulsado estudios como la Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales 2016 (Enaid).

También, para incentivar la participación de las organizaciones, la Ley contempla los esquemas de autorregulación, que son códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que las personas físicas o morales pueden convenir entre ellas o con organizaciones gubernamentales, mas hasta este momento el Inai no los ha impulsado en la práctica.

Desde 2004, la Agencia Española de Protección de Datos (AEPD) desarrolló un registro que es un catálogo público de consulta gratuita en el que, de manera voluntaria, las organizaciones públicas y privadas se dan de alta para dar a conocer qué bases de datos desarrollan, qué tipos de datos almacenan, con qué finalidad o si los transfieren.

De alguna manera, el fichero español incentiva a las organizaciones para que su mercado las identifique como empresas responsables con los datos personales. Aunque la AEPD tampoco vigila quién no ha cumplido, su catálogo es una manera de obligar a las organizaciones a cumplir con las disposiciones de su ley, porque, de no estar ahí, el castigo se lo podría aplicar su mercado. A enero de 2017, en el Registro General de Protección de Datos hay inscritas casi 4 millones y medio de bases de

datos de titularidad privada (AEPD, 2017). Sería deseable que, en un futuro próximo, el Inai pudiera impulsar una medida como esta, aunque hasta este momento lo rebasan sus capacidades y las disposiciones que debe observar.

Es fundamental destacar que el Inai no monitorea qué sujetos obligados ya cumplieron o no. Pareciera que la función de vigilancia se consuma en la imposición de las sanciones cuando ocurre un presunto incumplimiento de algún principio o disposición de la LFPDPPP (Artículos 61 y 62), después de que concluyen los procedimientos de protección de derechos o de verificación cuyas resoluciones lo ordenen, como señalan los artículos 59 y 60. Esta atribución —que es una de las más importantes del Inai—, puntualiza y pone a prueba la función ejecutora de la DPA mexicana y su capacidad coercitiva en la materia, porque en ella recae que se protejan los derechos del titular presuntamente afectado. La siguiente figura ejemplifica los pasos de imposición de sanciones que sigue el Instituto, ya sea por procedimientos de protección de datos o por verificaciones.

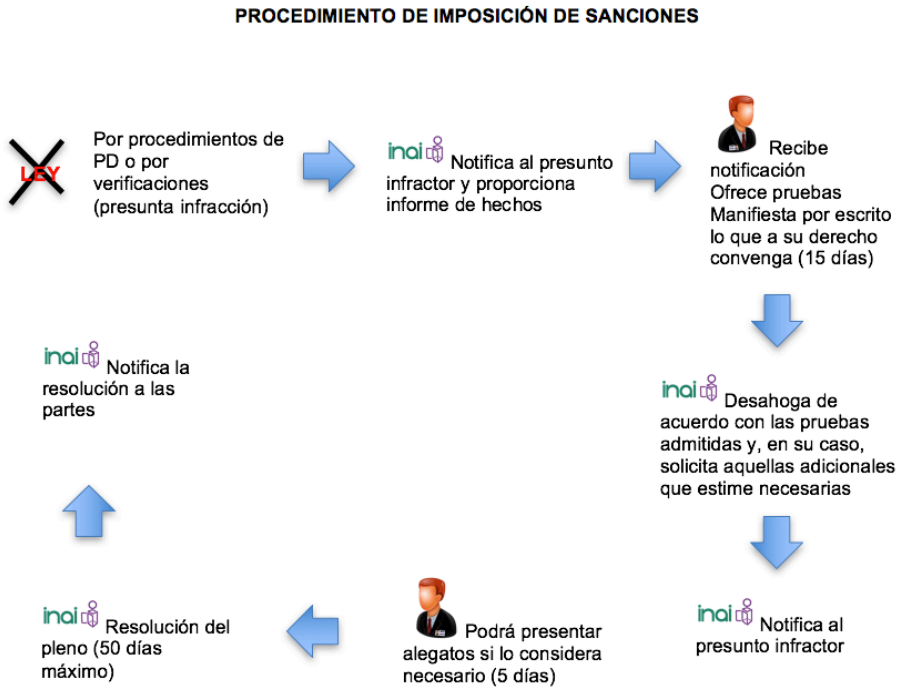


Tabla 6 Procedimiento de imposición de sanciones. Fuente: Curso de Introducción a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Inai (2013)

El inai aplica las multas a los responsables del tratamiento de los datos personales, que pueden ser personas físicas o morales, identificadas en el aviso de privacidad, independientemente de quién cometa la infracción dentro de la organización. Por su cuenta, el responsable podría expedir una sanción, amonestación o, incluso, demanda vía legal a quien la haya realizado, pero eso no significa que el Inai no sancionará a la figura identificada en el aviso porque es la responsable del tratamiento de los datos.

Sanciones impuestas a los particulares por incumplimiento con la LFPDPPP

Como se menciona en el apartado anterior, una de las atribuciones más importantes del Inai es impartir sanciones a los presuntos infractores. A partir de la puesta en vigor de la LFPDPPP y su reglamento, el Inai dio a conocer que, desde 2012 a noviembre de 2016, ha resuelto diferentes Procedimientos de Imposición de Sanciones (Pisan) y, en 55 de estos casos, impuso una sanción económica a las organizaciones y/o personas físicas por incumplimiento, que rebasa los 266 millones de pesos.

Según los registros del Inai (2016), 36 de estas multas pertenecen al sector de servicios financieros y de seguros (150 millones 826 mil pesos), diez al de información en medios masivos (42 millones 434 mil 347 pesos), y nueve al comercio al por menor [17 millones 466 mil pesos, de los que, hasta 2015, cuatro correspondían al de servicios educativos por 10 millones 428 mil 840 pesos). Entre las infracciones cometidas con mayor frecuencia se encuentran, según el Inai (2016): tratar datos personales en contravención a los principios establecidos en la ley (licitud, información, responsabilidad, lealtad y consentimiento), recabar o transferir datos personales sin el consentimiento expreso de las personas y omitir el Aviso de Privacidad, o alguno o todos los elementos previstos en la norma.

Para aminorar la sanción, España, por ejemplo, desde 2011 tiene la figura del apercibimiento que evita la sanción económica a muchas empresas, o la posibilidad de inmovilizar bases de datos cuando la infracción es muy grave y el tratamiento de los datos es de alto riesgo para los derechos y libertades fundamentales de los

interesados. Con la figura del apercibimiento, la imposición de sanciones, de 2012 a 2016, se redujo de veinte a doce millones de euros, aunque la disminución también está relacionada con que el nivel de cumplimiento es mayor, dado el descenso de 10 mil a 8 mil denuncias (Prieto, 2016). Con todo y que las denuncias han menguado, Prieto (2016) manifiesta que atender esa cantidad de querellas colapsa los recursos de la autoridad española.

En comparación con los datos españoles, a fin de 2016, en México, el Inai (2016) había atendido 674 solicitudes de protección de derechos y recibido mil 838 denuncias de las que, en mil 401 casos, inició un expediente de investigación preliminar; en 381 orientó al particular sobre los alcances de la Ley, en 56 recondujo porque se trataba de temas relacionados con solicitudes de derechos ARCO, y en 173 inició el procedimiento de verificación. Cabe recordar que esto es únicamente en materia de protección de datos personales, porque el Inai también es el órgano garante de la transparencia y acceso a la información, por lo que esta doble función podría rebasar las capacidades sancionadoras del Instituto.

Conclusión

La LFPDPPP plasma principios, obligaciones y derechos internacionalmente reconocidos que los sujetos obligados deben cumplir para garantizar la seguridad de los datos personales y facilitar su flujo transfronterizo. Por tratarse de una ley coercitiva, como primer planteamiento, esta tesis supone que la imposición de multas y sanciones obliga a los responsables al cumplimiento, como afirma Miranda (2016): “La Ley es condición necesaria, pero no suficiente, falta la aplicación, porque muchas veces lo que necesitamos no son leyes perfectas, sino que estas se apliquen por las autoridades responsables y competentes, porque una ley sin sanción es simulación”. No obstante, también es de esperarse que existan otros factores, además de la sanción, que intervengan en este proceso de implementación.

El siguiente capítulo analiza diferentes estudios que se han realizado acerca del cumplimiento de una política pública y, específicamente, sobre la seguridad de la información, que conduzcan a responder el interés central de esta investigación sobre el papel de los factores presentes en el cumplimiento.

CAPÍTULO III

TEORÍAS QUE EXPLICAN AL CUMPLIMIENTO

Las leyes de protección de datos personales responden a la necesidad de salvaguardar los datos de robo, pérdida o mal uso por parte de quienes los almacenan; previene que esto perjudique la integridad o seguridad de las personas y permite su utilización para el desarrollo de distintas actividades bajo medidas transparentes.

En la actualidad, aproximadamente cien de 194 países en el mundo cuentan con leyes de privacidad o protección de datos personales —según el término que adopten—, que obligan tanto al sector público como al privado. No obstante, su existencia no garantiza su cumplimiento, puesto que el funcionamiento de las organizaciones es fundamental para implementar las medidas de protección y seguridad necesarias.

Este capítulo se aproxima a las principales aportaciones teóricas sobre el estudio del cumplimiento de políticas de seguridad de la información en las organizaciones. Finalmente, se decanta por la teoría institucional como el lente de investigación.

Los modelos teóricos vinculados con el cumplimiento en las organizaciones

Autores como Rainey (2009) definen a las organizaciones como un grupo de personas que trabajan juntas para conseguir una *meta* mediante la obtención de recursos del *medio ambiente.* Transforman esos recursos cumpliendo con *tareas* y aplicando *tecnologías* para mejorar su *desempeño* y alcanzar sus objetivos mediante la *organización* de sus actividades. La organización incluye el *liderazgo*, en este proceso, los líderes guían el desarrollo de *estrategias* para cumplir con las metas establecidas y establecer estructuras y procesos. Dichas *estructuras* son la designación y división de responsabilidades dentro de la organización, logradas mediante la jerarquía, reglas y regulaciones, y especialización de las personas y grupos.

La división de la responsabilidad determinada por la estructura de la organización divide a las metas de la organización en componentes en los que tanto individuos como grupos pueden concentrarse. Esta división de responsabilidades requiere que las actividades individuales sean coordinadas. Las estructuras como reglas, regulaciones y niveles jerárquicos pueden ayudar a la coordinación. Los *procesos* son menos observables físicamente, son actividades más dinámicas que requieren de la coordinación, determinan las relaciones, toma de decisiones, evaluación, comunicación, resolución de conflictos, cambio e innovación. Dentro de las estructuras y procesos, las *personas* y *grupos* responden a *incentivos* que se les ofrecen para su mejor desempeño (Rainey, 2009).

Dado que las organizaciones son entes muy complejos en los que intervienen recursos humanos, metas, tareas, procesos, reglas, regulaciones, toma de decisiones, tecnologías, división del trabajo, liderazgo, valores, y no existe un marco teórico específico sobre el cumplimiento de políticas públicas que explique todos sus elementos, para su estudio se han desarrollado investigaciones teóricas y empíricas desde diferentes disciplinas como la sociología, administración pública, psicología social y la ciencia política, que aplican según sea el objeto de estudio.

O'tool y Younts (en Revuelta, 2007) opinan que, dado que todos los elementos que interactúan en el proceso de implementación de una política en una organización son muy complejos, cada enfoque o teoría es insuficiente para explicarlo, porque un solo modelo no puede abarcar todos los factores que determinan su éxito o fracaso. En otras palabras, para Bardach (en Revuelta, 2007) una teoría general del proceso de cumplimiento es prácticamente irreal. Para Parsons (en Revuelta, 2007), el uso del marco teórico adecuado dependerá de qué es lo que se quiere analizar.

Foorthuis y Bos (2011) definen al cumplimiento como el estado de conformidad entre el comportamiento de los actores —personas u organizaciones— y las normas —reglas predeterminadas, políticas, procedimientos, estándares, lineamientos, principios, leyes y otras formas de orden—. Es posible alcanzar el cumplimiento a pesar de diferentes motivaciones, causas o circunstancias, incluso, un actor puede cumplir con alguna

norma sin interiorizarla y sin modificar sus creencias. Esto quiere decir que el cumplimiento también existe aun cuando no es intencionado, porque el cumplimiento no intencional también es cumplimiento.

Cuánto cumplimiento y qué actores son los responsables son factores que dan más complejidad a la implementación y a sus resultados. Los estándares de cumplimiento y hacer cumplir las políticas queda en manos de profesionales o de miembros de la organización, por esto, quién es responsable de implementar las políticas es un tema crucial, así como la causa que motiva el cumplimiento de la implementación (Parsons, 2007).

Un aspecto importante es establecer cuánto cumplimiento debe haber de la política en cuestión y quién es el responsable. El actor competente debe establecer qué nivel considera aceptable —100%, 80% o 50%, por ejemplo—. Posiblemente no es conveniente hacer un esfuerzo o recurso adicional que no sea significativo en la implementación. El estándar de cumplimiento puede ser elevado en algunas áreas y muy bajo en otras. Esto puede estar asociado a las instancias encargadas de la implementación y los criterios para llevarla a cabo. Por ejemplo, hay políticas que competen a burócratas del sector público y otras a profesionales del sector privado (Hood, en Parsons, 2007).

Otro punto relevante que concierne al tema es el no cumplimiento, que puede ser de dos tipos. El primero es la transgresión; se refiere a cuando no se cumple con la norma por una violación a la ley, provocada porque el actor en cuestión no tenía interés en implementarla o porque ignoraba cómo hacerlo. El segundo, la subversión, se refiere a una situación en la que el actor intenta socavar intencionalmente el cumplimiento, o al menos una parte de sus procedimientos, movido por un interés individual. En un contexto organizacional, la subversión apunta a problemas políticos, conflictos estructurales o de interés (Foorthuis y Bos, 2011).

Para el estudio del cumplimiento, la literatura distingue dos tipos de teorías: racionalistas y normativas. En el primero, que también se identifica como reglamentario (Siddiki, Basurto y Weible, 2012), los actores eligen racionalmente entre sus

alternativas y basan su decisión de cumplimiento o no cumplimiento en el análisis de costos/beneficios. En este tipo de acercamiento, el castigo y las recompensas aparecen como una forma de modificar el comportamiento no deseado (Foorthuis y Bos, 2011), de tal manera que el cumplimiento reglamentario proviene de motivaciones intrínsecas —convicción, temor o culpa— y extrínsecas —sanciones formales, monitoreo— (Siddiki, Basurto y Weible, 2012).

En la segunda perspectiva, las reglas se interiorizan y adoptan legítimamente. Las teorías normativas no establecen que el cumplimiento de un actor sea irracional, sino que los actores institucionalizan las reglas o prácticas, aunque las reglas ambiguas, complejas, numerosas, con cambios constantes o que no son fáciles de aplicar, pueden obstaculizar el cumplimiento (Foorthuis y Bos, 2011). Bajo el modelo normativo, el actor cumple por 'actuar de forma apropiada', 'hacer lo correcto' o por 'el deber de cumplir' con las reglas formales, y no por un análisis racional del costo-beneficio que pasa a segundo plano (Etienne, 2010).

El no cumplimiento también puede ocurrir por falta de capacidad, conocimiento o compromiso, pero, a diferencia de las teorías racionalistas, el modelo normativo lo dirige, mas no lo sanciona. Los métodos para lograr el cumplimiento se enfocan en aumentar la capacidad del actor mediante la cooperación, el apoyo o la capacitación para hacer las reglas más claras y más fáciles de cumplir (Foorthuis y Bos, 2011). No obstante, Etienne (2010) es enfático al escribir que el vínculo entre la moralidad y las reglas no debería darse por sentado con el cumplimiento.

Para Foorthuis y Bos (2011) es importante destacar que ambos modelos no son excluyentes, sino que se complementan para analizar desde diferentes lentes qué influencia el cumplimiento de los actores. En su modelo de cumplimiento, Etzioni (en Lunenburg, 2012) identifica tres fuerzas por las que los individuos dentro de una organización cumplen con las políticas: 1) coercitividad, con la aplicación de castigos; 2) recompensa o remuneración (conducta utilitaria) —teorías racionalistas/reglamentarias—; 3) convicción o moral, mediante recompensas intrínsecas, identificación de metas o interés en el trabajo —teorías normativas—, o por

todas. De esta manera, el cumplimiento puede ser coercitivo, remunerativo o por convicción. A la convicción o moral, Etzioni las relaciona con lo normativo, mientras que lo coercitivo y utilitario son racionales porque el individuo hace un análisis de la sanción y del costo-beneficio de cumplir con la regla. El autor lleva, por tanto, a la integración de factores racionales y normativos para el estudio del cumplimiento, y no los vislumbra como ajenos uno del otro como hacen otros autores (Wiener, 1982), sino que hace énfasis en que las organizaciones pueden combinar dos e, incluso, tres tipos de causas del cumplimiento (Lunenburg, 2012).

El cumplimiento se entiende mejor cuando se vincula al modelo racional con el normativo porque explican diferentes perspectivas, como lo hacen Penley y Gould (1988), quienes, con base en Etzioni, conjuntan aspectos morales, utilitarios y coercitivos en su investigación sobre el compromiso de los empleados en las organizaciones. A pesar de que el cumplimiento puede deducirse desde una diversidad de elementos, en su planteamiento original, Etzioni sostiene que existe un factor predominante que depende de la estructura y tipo de participación de los individuos dentro de la organización (Penley y Gould, 1988), porque poseen una predisposición personal para conducirse de forma específica al interior de la misma (Wiener, 1982).

Lunenburg (2012) afirma algo similar cuando escribe que algunas organizaciones emplean los tres tipos de factores, pero la mayoría se apoya más en uno que en los otros dos. En otras palabras, Etzioni (en Penley y Gould, 1988) y Lunenburg (2012) aclaran que el cumplimiento puede ser normativo, racional o ambos, y ponen de manifiesto que hay un factor que predomina, aunque no aclaran cuál es.

Al respecto, Etienne (2010) hace una aportación muy importante al afirmar que el cumplimiento ‘voluntario’ normalmente está asociado a prácticas de control y sanción que regulan a quienes no cumplen, porque los castigos señalan las obligaciones normativas que todos los actores a quienes se dirigen deben cumplir. Si las sanciones desaparecen, el cumplimiento normativo se debilita y las violaciones o infracciones pueden aumentar (Gezelius, 2002).

Además, cualquier indicio de que las sanciones no disuaden a los no cumplidores, puede percibirse por los actores como prueba de que la norma ha perdido su fuerza moral (Grasmick y Scott, 1982). Con esto, Etienne (2010), Gezelius (2002) y Grasmick y Scott (1982) dan mayor peso al modelo racional/reglamentario que al normativo porque, en otras palabras, la norma está supeditada a la regla, tanto, que la mayoría de las organizaciones operan eficientemente debido a que lo reglamentario es un factor predominante (Cialdini y Goldstein, 2004). Para los autores, 'el deber ser' se cumple primero porque existe una sanción y después se acepta e interioriza (o no). Incluso, Cialdini y Goldstein (2004) postulan que la obediencia ocasionada por la sanción o el temor está tan arraigada en las organizaciones, que provoca que los subordinados cumplan con lo que se les indica aun si las órdenes contravienen a la ética.

Lo anterior refuerza la propuesta de Etzioni cuando se refiere a la presencia de un factor predominante que, en este caso, es la sanción, pero no hay que olvidar que para el autor el cumplimiento es integral —racional y normativo—. Aunque las acciones impuestas por regulaciones inducen a las organizaciones a satisfacer los mandatos por obligación o una valoración de costo-beneficio, e invierten en la implementación de una política, crear una mentalidad de cumplimiento por obligación y no por convicción puede ser una pérdida de recursos (Kwon y Johnson, 2013) porque los factores racionales y normativos son necesarios para el cumplimiento.

Otra contribución de Etzioni y Wiener que destaca para el cumplimiento es que ellos no consideran a las organizaciones únicamente como un conjunto, sino que conjeturan que están conformadas por subactores. Aunque algunas teorías de la perspectiva normativa y racional tienden a considerar a los actores como agentes unitarios, Foorthuis y Bos (2011) coinciden en que una perspectiva más amplia del cumplimiento necesita disgregar a los actores en subactores. La literatura vislumbra que las sanciones influencian el cumplimiento a nivel organizacional, pero la coercitividad de la regla también causa efectos a nivel individual, puesto que los individuos racionalizan el costo o beneficio de cumplirla y, en un plano cognitivo, interiorizan la normatividad. Esto quiere decir que una organización está compuesta por unidades estructurales,

como departamentos, y subunidades, como programas, sus proyectos y equipos. Además, todas estas entidades tienen miembros individuales y las motivaciones para cumplir con las políticas pueden diferir entre los (sub)actores. Foorthuis y Bos (2011) proponen tres niveles conceptuales de análisis.

El primero vislumbra a la organización como un todo, una división o una red de organizaciones. En este nivel, los directivos determinan las estrategias y políticas que la organización va a implementar en sus diferentes áreas y personal, para buscar el cumplimiento (Foorthuis y Bos, 2011), con prácticas como evaluación, capacitación, sanciones o recompensas, considerando presiones externas en forma de leyes o mejores prácticas.

El segundo nivel incluye varios tipos de colectivos de los que se espera el cumplimiento, ellos existen dentro de las empresas como departamentos y sus subunidades y programas, proyectos y equipos. Estos colectivos tienen mayor alcance local y pueden tener una agenda propia inconsistente con las políticas de la empresa.

El tercer nivel es el de los individuos. Las decisiones y conductas personales son determinantes para el cumplimiento (Foorthuis y Bos, 2011). Algunos estudios evidencian la incidencia de factores racionales —en particular sanciones formales, estímulos o mecanismos de miedo— en las organizaciones, directivos (Li, Zhang, Sarathy, 2010 y Kwon y Johnson, 2013) y en los individuos (Li, Zhang y Sarathy, 2010; Herath y Rao, 2009; Pahnila, Siponen y Mahmood, 2007); así como de factores normativos en los individuos (Gezelius, 2002; Shaw, 2012). Esta investigación, en particular, centra su interés en el nivel organizacional.

Para recapitular, autores como Hood, Burch, Wood y Etzioni hacen énfasis en la coercitividad para el cumplimiento de las políticas. Por ejemplo, Hood habla de sanciones y persuasión con mensajes, Burch y Wood mencionan las sanciones positivas y negativas, y Etzioni explica que el cumplimiento puede ser normativo, coercitivo o remunerativo. Lo importante es que ninguno de estos modelos es excluyente, sino que sus enfoques se complementan para el estudio del cumplimiento de una política.

Precisamente sobre esto, Etzioni tiene dos aportaciones. Primero, matiza la relevancia conjunta de factores racionales y normativos para el cumplimiento de las políticas en las organizaciones. Segundo, puntualiza que, de acuerdo con las condiciones de la organización, existe un factor que sobresale y, aunque no indica cuál, Etienne (2010), Gezelius (2002) y Grasmick y Scott (1982) dan preeminencia a factores racionales/reglamentarios, como la sanción, sobre los normativos, cuando escriben que, si las sanciones desaparecen, el cumplimiento normativo se debilita y las violaciones o infracciones pueden aumentar.

La intención de esta tesis es, justamente, descubrir cuáles son los factores que intervienen en el cumplimiento de las políticas de protección de datos personales, como el temor a las consecuencias por el incumplimiento, la búsqueda de una recompensa o el cumplimiento por sí mismo, porque el comportamiento es racional, pero también normativo por la internacionalización de valores. Pero bajo el postulado de que, en el cumplimiento de las políticas de protección de datos personales, predomina el modelo racional sobre el normativo, con un análisis a nivel organizacional. El siguiente apartado abarca las principales teorías racionales y normativas desde las que se ha investigado la seguridad de la información para conducirnos a la más conveniente para el presente estudio.

Teorías vinculadas con el estudio del cumplimiento y la seguridad de la información

En este punto es importante retomar el propósito de esta investigación: descubrir cuál es el papel que desempeñan los factores a nivel organizacional que motivan el cumplimiento de las políticas de protección de datos personales, como variable dependiente, una vez que en México ya existen leyes con procedimientos que las organizaciones deben implementar. De acuerdo con la literatura revisada hasta este momento, no hay una teoría de protección de datos personales desde la cual sea posible explicar específicamente el cumplimiento de la implementación de estas políticas en las organizaciones, así como tampoco se vislumbra una teoría que abarque

todos los factores que lo afectan, considerando que los autores escriben sobre el cumplimiento racional o normativo. Las exploraciones en torno a la seguridad de la información dan luz para vincularla con la protección de datos personales.

La literatura referente a la seguridad de la información destaca que la dependencia de las TIC representa un gran reto para las organizaciones. Forzosamente, las conduce a mejorar sus prácticas en seguridad y buscar soluciones para hacer uso adecuado de la información. Cumplir con los parámetros se considera como un criterio que demuestra que la organización toma los pasos adecuados para proteger la información organizacional (Kirsch y Boss, 2007; Siponen, Pahnila y Mahmood, 2010), y no cumplir con las políticas de la seguridad de la información puede afectar la operación de todas las áreas que tienen acceso a los datos o que son responsables de información sensible (Kankanhalli et al, en Alkalbani, 2016).

Dado que el cumplimiento está asociado con el grado de conformidad de lo establecido con lo realizado (Foorthuis y Bos, 2011), una manera de medirlo es sabiendo qué procedimientos reglamentarios implementan las organizaciones. Es decir, requerimientos legislativos, políticas corporativas e iniciativas en materia de privacidad, puesto que esto se considera como un criterio para demostrar que la organización protege adecuadamente la información (Kirsch y Boss, 2007; Siponen, Pahnila y Mahmood, 2010).

Björk (2004) también pone como ejemplo de medición estándares de calidad o políticas internas que son portadoras de buenas prácticas y rutinas. En el caso de México, Deloitte (2014) mide al cumplimiento de las organizaciones con base en los procedimientos que señala la LFPDPPP. Su estudio da indicios sobre las actividades que los responsables están obligados a cumplir y en qué porcentaje lo han hecho, a pesar de que no hace mención sobre las causas que originan el incumplimiento, lo que conduce nuevamente a la inquietud de esta investigación, que es conocer el papel que desempeñan los factores que lo motivan a nivel organizacional.

Algunos estudios, como *Health-care security strategies for data protection and regulatory compliance*, de Kwon y Johnson (2013), utilizan teorías desde otras

disciplinas para reconocer de forma empírica la relación causal entre seguridad y percepción del cumplimiento, los efectos de los recursos de seguridad sobre la protección de datos personales y el cumplimiento de la normatividad. En su investigación, los autores identifican cómo los recursos de seguridad de la información influyen en la protección de datos y el cumplimiento de la normatividad, con base en la madurez operacional de la organización.

La teoría del miedo es muy útil para el planteamiento original de esta tesis porque hace énfasis en la coerción para el cumplimiento desde el modelo racional, donde el miedo a la sanción o castigo es el principal motor y el castigo puede operar a nivel organizacional, lo impone el mercado o la ley, y a nivel individual, con el desprestigio o sanciones dentro de la organización. Sin embargo, autores como Etzioni o Penley y Gould hacen énfasis en la integración de factores racionales y normativos y, la teoría del miedo, en particular, únicamente vislumbra el ámbito racional de los individuos, pero en un contexto organizacional. Por lo tanto, no es suficiente para explicar al cumplimiento.

Kwon y Johnson (2013) también utilizaron la teoría de la madurez organizacional para saber en qué posición se encuentran las organizaciones y cómo pueden mejorar en materia de seguridad de la información. Andersen y Jessen, en Gonzalez, Marle y Bocquet (2007), definen la madurez como un estado en el que la organización tiene las condiciones óptimas para alcanzar sus objetivos, es decir, un proyecto maduro significa que la organización está perfectamente organizada para implementarlo. Para Nesensohn et al (2014), la madurez implica el desarrollo de procesos explícitos y consistentes, refleja su eficacia y eficiencia en la búsqueda de metas, y se conceptualiza en las acciones de las personas. Esta última noción, según Skulmoski, en Nesensohn et al (2014), puede articularse en términos de percepción de una organización, además de combinar acciones operacionales con capacidades, habilidades y actitudes.

Sin duda, la contribución de la teoría de la madurez es muy valiosa, pero solo se ubica en el modelo de las teorías normativas porque se centra en las características, el

‘estado de las cosas’ y en alcanzar las metas de la organización, y no explica cuáles son los factores que la llevan a un determinado nivel de madurez. Una organización madura supone la institucionalización de lo reglamentario y normativo, y la teoría queda a deber qué la conduce a ese estado.

Por otro lado, Bulgurcu, Cavusoglu y Benbasat (2010) discuten que muchas organizaciones reconocen que sus empleados, considerados como el eslabón más débil para la seguridad de la información, también pueden ser el mejor recurso en el esfuerzo por reducir los riesgos vinculados con la misma. Los investigadores identifican los antecedentes del cumplimiento de los empleados con las políticas de seguridad de información (PSI). Específicamente, indagan cuáles son los factores que motivan a los empleados a cumplir con los requerimientos de las PSI, para proteger la información de la organización. Esto, con base en la teoría del comportamiento planificado y la elección racional.

La teoría del comportamiento planificado (TCP) sugiere que la acción humana está conducida por tres miramientos: Las creencias de comportamiento se refieren a las posibles consecuencias del comportamiento, las normativas pertenecen a las expectativas normativas de otros, y las controladas obedecen a factores que facilitan o impiden el desempeño del comportamiento. La teoría de la elección racional explica cómo los individuos toman decisiones cuando se enfrentan con opciones, de acuerdo con los costos y beneficios. En la toma de decisiones, el individuo primero identifica las opciones y sus posibles resultados. Cada resultado puede estar asociado con costos y beneficios dependiendo de la satisfacción que le produce al individuo. Después de medir mediante la percepción los posibles resultados de la acción, el individuo determina cuál es la mejor opción (Bulgurcu et al, 2010).

Como lo indican sus nombres, la teoría del comportamiento planificado y de la elección racional pertenecen al modelo racional de las teorías y, al igual que la teoría del miedo, son insuficientes para explicar el cumplimiento porque únicamente lo entienden desde la perspectiva en la que el actor evalúa el costo-beneficio. Aunque se enfocan en la

coercitividad como elemento fundamental, no contemplan el valor de la normatividad que complementa al cumplimiento.

En la literatura también aparece la teoría de la agencia que la academia ha utilizado para áreas como contabilidad, economía, marketing, ciencia política, sociología y administración (Eisenhardt, 1989). Es una aplicación alterna de la elección racional porque explica cómo los directores delegan la implementación a los agentes, mediante el establecimiento de un contrato y el monitoreo como herramientas para reducir la brecha de cumplimiento (Cerna, 2013). En este proceso de delegar, el agente evalúa el cumplimiento en torno a intereses personales y lo racionaliza, por tal motivo, también se encuentra dentro del modelo de teorías racionales, mas no integrales.

Otros estudios como *Institutionalization of information systems security policies adoption: factors and guidelines*, de Lopes y de Sá-Soares (2014), *IT and organizational change: an institutionalist perspective* (Avgerou, 2000), *Explaining history of eGovernment implementation in developing countries: an analytical framework* (Wahid, 2011), *Institutionalisation as a process of interplay between technology and its organisational context of use* (2009), *Institutional factors affecting offshore business process and information technology outsorcing* (Kshetri, 2007) o *Investigating the Impact of Institutional Pressures on Information Security Compliance in Organizations* (AlKalbani et al, 2016) utilizan la teoría institucional para conocer los factores que motivan el cumplimiento de políticas de seguridad y las TIC en las organizaciones.

La teoría institucional plantea que, desde una perspectiva institucional, las organizaciones son como son porque esa es su manera legítima de organizarse. La idea central detrás de esta teoría es que las acciones organizacionales reflejan patrones dentro de una organización y en el medio al que pertenecen. Por lo tanto, es posible predecir prácticas de comportamientos legítimos que derivan de valores culturales, tradiciones empresariales, historia de las firmas, aspectos administrativos, etcétera, dentro de una organización (Eisenhardt, 1988).

Esta teoría es útil porque hace referencia a pilares —factores— reglamentarios, normativos y cognitivos, mediante los que las organizaciones introducen nuevas

disposiciones. Con el fin de que las organizaciones mejoren la implementación de una política es indispensable que conozcan cuáles son dichos elementos que facilitan u obstaculizan este proceso. Para esto, la teoría institucional ayuda a entender la influencia de las estructuras en el comportamiento de los individuos, es decir, en el institucionalismo hay insertado un conjunto de reglas y normas que rigen un comportamiento, desde una perspectiva integradora como la que explica Etzioni (en Lunenburg, 2012), e inciden en la implementación de una nueva disposición en las organizaciones.

A pesar de que esta teoría no se ha utilizado hasta este momento específicamente en el análisis de la implementación de políticas de protección de datos personales, otras investigaciones han demostrado ampliamente su utilidad para estudiar la adopción de medidas de seguridad de la información.

Conclusión

En conclusión, los factores que motivan el cumplimiento en la implementación de las políticas de protección de datos personales en las organizaciones pueden conocerse desde distintas teorías que se mencionan en este capítulo. El recorrido teórico es necesario porque marca pautas para acercarse a su estudio en función de decidir cuál es la más conveniente para los fines de esta investigación. Los principales modelos parten de teorías normativas, racionalistas o integradoras. El siguiente cuadro las clasifica.

Teorías que explican el cumplimiento de las políticas en las organizaciones

	Teoría / autor que sustenta	Factor que influencia el cumplimiento
Teorías normativas	Alina, 2014; Foorthuis y Bos, 2011	Convicción, valores, ética, apropiación de las normas

	Teoría de la madurez organizacional (Kwon y Johnson, 2013; Nesensohn et al, 2014)	Cumplimiento de metas
Teorías racionalistas	Teoría del miedo/ teorías coercitivas (Foorthuis y Bos, 2011; Siddiki, Basurto y Weible, 2012; Burch y Wood; Mwakibinga y Buvik, 2013; Schneider, 1974; Kwon y Johnson, 2013; Johnston y Warkentin, 2010)	Miedo a la sanción
	Teoría de la elección racional (Bulgurcu, Cavusoglu y Benbasat, 2010)	Costos y beneficios
	Teoría del comportamiento planificado (Bulgurcu, Cavusoglu y Benbasat, 2010)	Consecuencias del comportamiento
	Teoría de la agencia (Mwakibinga, 2008; Eisenhardt, 1988)	Contrato, interés personal
Teorías integrales	Teoría institucional (Lopes y de Sá-Soares, 2014; Avgerou, 2000; Wahid, 2011; Kshetri, 2007; AlKalbani et al, 2016; Scott, 2008; Bjorck, 2004)	Factores reglamentarios, normativos y cognitivos
	Organizaciones modernas (Etzioni, 1964)	Convicción o moral, recompensa o remuneración, o todas.

Tabla 7 Teorías que explican el cumplimiento de las políticas en las organizaciones. Fuente: elaboración propia.

Como se observa, las teorías indican distintos factores que influencian el comportamiento de las organizaciones y cada factor depende del tipo de teoría en cuestión. Por ejemplo, en una teoría racionalista, como la de elección racional, la conducta está determinada por el costo/beneficio o castigo/recompensa que los actores perciben para el cumplimiento; en la teoría del miedo, el factor detonante es el temor a una sanción por la coercitividad de la ley; en las teorías de orden normativo, los factores que motivan el cumplimiento están vinculados con la ética, el liderazgo o alcanzar las metas. Todos estos factores provenientes de distintas teorías se complementan para explicar el cumplimiento de una política en las organizaciones, pero cada uno, por sí mismo, da una explicación parcial.

La literatura señala que es muy difícil que una sola teoría abarque todo el proceso de cumplimiento por su complejidad, intervienen recursos humanos, metas, tareas, procesos, reglas, toma de decisiones, valores, etcétera. Sin embargo, hay un tercer grupo de teorías que abarcan tanto elementos racionalistas como normativos. Autores como Etzioni (1964) sostienen esta postura. Una teoría desde la que es posible entender de manera integral los factores que motivan el cumplimiento, bajo advertencia de limitarse a las variables con mayor presencia en la literatura relacionada con la protección de datos personales, es la teoría institucional. Los argumentos para afirmar que la teoría institucional es la adecuada para esta investigación son los siguientes:

Conjunta factores reglamentarios, normativos y cognitivos que ayudan a comprender el comportamiento de los individuos en un contexto organizacional. Esto quiere decir que en el institucionalismo está insertado un conjunto de reglas y normas que rigen el comportamiento, e inciden en el cumplimiento de nuevas disposiciones en las organizaciones. Numerosos autores destacan la conveniencia de esta teoría en el estudio de las organizaciones, relacionada con la seguridad de la información (Campbell, 2007; Kshetri, 2007, Lopes y de Sá-Soares, 2014, Geels, 2004, Bjorck, 2004 y AlKalbani et al).

Desde una perspectiva reglamentaria, el mecanismo de cumplimiento es coercitivo porque ocurre mediante la aplicación de reglas, leyes y sanciones. Investigaciones sobre el cumplimiento han encontrado explicación en la coercitividad de la regla porque demuestra la reducción de los riesgos al inducir a un comportamiento esperado mediante la sanción y, además, porque es un catalizador para el cumplimiento en las organizaciones. Al respecto, diferentes investigadores plantean la relación entre la coercitividad y el cumplimiento (Siddiki, Basurto y Weible, 2012; Mwakibinga, 2008; Kwon y Johnson, 2013, y Johnston y Warketin 2010). Es pertinente recordar, también, la aportación de Etienne (2010), Gezelius (2002) y Grasmick y Scott (1982), que dan más valor a la coerción en un nivel organizacional.

La protección de datos personales en México cumple con esta característica. La LFPDPPP es una ley reglamentaria con carácter coercitivo puesto que impone multas

económicas en caso de incumplimiento (artículos 63 y 64 de la ley), y prisión por incurrir en algún delito en materia del tratamiento indebido de los datos personales (artículos 67 a 69). Es de esperarse que la ley disminuya los comportamientos no deseados de los sujetos obligados con sus medidas punitivas tanto para individuos como organizaciones. Los resultados de Deloitte (2014) evidencian que una de las motivaciones de la implementación es cumplir con la ley, esto podría tener su origen en la sanción.

Pero la coercitividad reglamentaria podría no ser la única explicación para el cumplimiento de la ley —aunque sí una de las más sobresalientes—. Por ello, la literatura menciona otros modelos teóricos que también dan respuesta y deben ser considerados. Desde el ámbito normativo, el cumplimiento ocurre cuando las normas son interiorizadas y adoptadas legítimamente dentro de las organizaciones. Esto no significa que se trate de una elección irracional, sino que intervienen otros factores como convicción, capacitación, valores, ética. Alina (2014), por ejemplo, hace referencia a la ética, estándares y valores, y Kwon y Johnson (2013) toman a la madurez organizacional como referente, pero, ¿desde qué teoría es conveniente estudiar el espacio normativo de la implementación en las organizaciones?

Una vez más, la teoría institucional también considera este aspecto fundamental en la implementación de una política en las organizaciones que es la cuestión normativa, que segrega en los pilares normativo y cognitivo. Como se menciona, las sanciones son un factor determinante para que los sujetos obligados de la LFPDPPP den cumplimiento a la regla. Sin embargo, es deseable que la elección del cumplimiento no la motiven únicamente las reglas, leyes y sanciones, sino que también intervengan otros factores que no conlleven únicamente a cumplir con lo que indica la ley, y que, además, fomenten mejores prácticas en materia de protección de datos personales en las organizaciones en un plano normativo. Esto podría ser un reflejo de que interiorizan la protección de los datos personales o que hacen el esfuerzo de adoptarla legítimamente a nivel cognitivo, como otro pilar institucional.

Para la teoría institucional las organizaciones son multifacéticas y las reglas, normas y rutinas se establecen como lineamientos confiables para el comportamiento social, incluso dentro de una organización (Wahid, 2011). Es una teoría que contempla aspectos reglamentarios —leyes, sanciones—, normativos —valores y normas— y cultural-cognitivos —interiorización de la norma— y da una explicación más amplia que se ha demostrado empíricamente en diversos estudios sobre las organizaciones, vinculada con la implementación de políticas de seguridad de la información y las TIC (Lopes y de Sá-Soares, 2014; Avgerou, 2000; Wahid, 2011; Kshetri, 2007; AlKabalni et al, 2016).

La suma de las sanciones, más el consenso, más las recompensas, más los valores, más la satisfacción, más la convicción, dan mayor fortaleza al estudio de las organizaciones. Además, explica el cumplimiento a nivel organizacional, desde una búsqueda racional de intereses, rutinas, hábitos, costumbres o convenciones, y va más allá de explicaciones parciales, como las que brinda la teoría del miedo, de la madurez o la elección racional, por ejemplo.

Por lo tanto, la teoría institucional guía a esta investigación para indagar sobre, si ya existen leyes que protegen los datos personales, cuáles son los factores que propician su cumplimiento en las organizaciones, si la seguridad por sí misma —que reflejaría que han interiorizado la protección de los datos personales— o el cumplimiento con la ley y las reglas —por temor a las sanciones—, bajo el supuesto de que en un inicio el motor del cumplimiento es la sanción pero, después, se añaden otros factores normativos. Esta teoría se eligió a pesar de que no se ha puesto a prueba en esta materia en particular, por lo que, uno de los objetivos de esta investigación es demostrar su utilidad.

CAPÍTULO IV

LOS PILARES DEL CUMPLIMIENTO EN LA TEORÍA INSTITUCIONAL

El capítulo tres explora los enfoques teóricos desde los que se ha estudiado el cumplimiento en la implementación de una política pública. Como resultado de esa revisión, la teoría pertinente para esta investigación es la teoría institucional, a pesar de que no se ha utilizado en esta materia en particular.

Las instituciones, así como las organizaciones, comprenden elementos reglamentarios, normativos y culturales-cognitivos que, junto con otras actividades y recursos, dan estabilidad y significado a la vida de las organizaciones (Scott, 2001). Scott (2008) destaca que estos tres elementos: reglamentarios, normativos y culturales-cognitivos, como los pilares de las instituciones y organizaciones, pueden ser vistos de manera independiente, pero de manera integrada dan más fuerza y resistencia a las estructuras. Como explica D'Andrade (en Scott, 2008), las sanciones sociales, más la represión para lograr consenso, más la recompensa, más los valores, pueden actuar juntos para dar más fuerza directiva a un sistema.

Este capítulo estudia los conceptos básicos de la teoría, a la vez que determina los factores que explican el cumplimiento a partir del pilar reglamentario, normativo y cognitivo.

Teoría institucional

De acuerdo con Richard Scott (2008), la teoría institucional aparece en el escenario de las organizaciones en la década de los setenta y ha generado interés y atención por las preguntas que plantea, tales como: ¿por qué las organizaciones de un mismo tipo, como escuelas y hospitales, ubicadas en lugares dispersos, se parecen una a la otra?, ¿por qué si las reglas formales son frecuentemente ignoradas, se mantienen los

recursos y energías para mantener esas estructuras?, ¿por qué y cómo surgen las leyes, reglas y demás tipos de sistemas regulatorios y normativos?, ¿cómo se considera el comportamiento dentro de las organizaciones, refleja la búsqueda racional de intereses y el ejercicio consciente de una elección, o es un comportamiento guiado por convenciones, rutinas o hábitos?, entre otros cuestionamientos. A partir de entonces, dirige su atención y reconoce su aplicación a nivel individual y organizacional (Scott, 2008; Dacin, Goodstein y Scott, 2002).

La teoría institucional tiene sus orígenes en la economía, ciencia política y sociología. Esta teoría ve a las organizaciones como multifacéticas, estructuras sociales durables construidas con elementos simbólicos, actividad social y recursos materiales (Wahid, 2011). Considera el proceso mediante el cual las estructuras (reglas, normas y rutinas) son establecidas como lineamientos confiables para el comportamiento social. También representa la forma en la que estos elementos son creados, propagados, adoptados y adaptados a través del tiempo y espacio, así como la forma en la que declinan o caen en el desuso (Scott, en Lopes y de Sá-Soares, 2014).

Está ligada con las organizaciones en el sentido en que “toda organización necesita un marco institucional (conjunto de las “reglas” relevantes para esa organización) donde se establece lo que la organización y sus miembros pueden o deben hacer en circunstancias específicas” (Vergara, 2010). En otras palabras, el análisis de las instituciones puede aportar a este campo puesto que todas las organizaciones tienen en su estructura un marco institucional, entre lo que Vergara (2010) destaca: reglas, normas, costumbres roles y personajes que condicionan y marcan el funcionamiento de toda organización.

A continuación, se describe cada uno de los pilares institucionales.

Los tres pilares de la teoría institucional

Los sistemas reglamentarios, normativos y cultural-cognitivo son identificados por la teoría institucional como los ingredientes vitales de las organizaciones. Los tres

elementos generan un constante movimiento del consciente al inconsciente, “de lo legalmente establecido a lo que se da por sentado” (Hoffman, en Scott, 2008:50). Estos tres ingredientes pueden ser vistos como facetas que contribuyen entre sí, son interdependientes y, a su vez, se robustecen en un marco que encapsula y exhibe la fuerza y resiliencia de las estructuras institucionales. A pesar de que este modelo inclusivo tiene sus fortalezas, también enmascara diferencias significativas. La definición envuelve tres conceptos que necesitan ser especificados. Para Scott (2008) más allá de la búsqueda de una concepción integral de las definiciones, se logra un avance más significativo al distinguir entre los diferentes elementos e identificar sus supuestos, mecanismos e indicadores.

El siguiente cuadro aclara estos tres elementos — tres pilares— reglamentarios, normativos y culturales-cognitivos, esenciales para la creación de nuevas organizaciones o para realizar algún cambio en las ya existentes. El pilar reglamentario restringe y regula el comportamiento mediante reglas formales, sanciones y castigos. La normatividad hace énfasis en los valores y normas como elementos de presión dentro de la organización, esto lo convierte en una obligación social. El tercer pilar, que son las estructuras culturales-cognitivas, sostiene significados que son compartidos entre los actores de las estructuras reglamentarias y normativas. Los pilares pueden ser creados, mantenidos, alterados o destruidos (Scott, 2008):

Pilares de la Institucionalización			
	Reglamentario	**Normativo**	**Cultural-cognitivo**
Bases del cumplimiento	Conveniencia	Obligación social	Se da por sentado
Base del orden	Reglas	Expectativas vinculantes	Esquema constitutivo
Mecanismos	Coercitivo	Normativo	Mimético
Lógica	Mediación	Propiedad	Ortodoxo
Sentimiento	Culpabilidad / Inocencia	Vergüenza/ Honor	Certeza/ Confusión
Bases de	Sanciones legales	Moralmente gobernado	Culturalmente apoyado,

legitimación			conceptualmente correcto
Factores de cumplimiento	Reglas formales, leyes, sanciones, incentivos, recompensas y castigos, sistemas de poder, protocolos	Valores, normas, expectativa de roles, códigos de conducta, obligaciones	Prioridades, agenda, creencias, paradigmas, lenguaje

Tabla 8 Tres pilares de la institucionalización (Scott, 2008; Geels, 2004)

La concepción **reglamentaria** asume que las instituciones restringen y regulan las conductas mediante reglas y leyes. Las reglas son sistemas simbólicos portadores en el proceso de institucionalización. De acuerdo con García y Martínez (en Wahid, 2011), en una organización, estos sistemas son mecanismos que restringen el comportamiento y dan lineamientos para las soluciones. El aspecto reglamentario incluye reglas, monitoreo y sanciones y, si es necesario, recompensas o castigos con la intención de influir en el comportamiento.

Diferentes autores destacan la pertinencia de las reglas formales en una organización (Geels, 2004; Hodgson, 1998). Este proceso opera a través de la difusión, que puede ser por mecanismos informales como las costumbres, o mediante aparatos más formales asignados a actores especializados, como la policía, las cortes o los jueces. Dado que este pilar hace especial énfasis en el cumplimiento de las reglas escritas y la necesidad de tener "árbitros" para mantener el orden establecido, su mecanismo primario para ejercer el control es la coacción (Scott, 2008).

El sistema de reglas da legitimidad, pero esta creencia puede ser superficial porque, a pesar del reconocimiento, esto no significa que se comparta que son justas o necesarias. Es decir, las personas pueden reconocer que las reglas son válidas sin que se apropien de ellas (Scott, 2008). No obstante, Hetcher *et al.* (en Scott, 2008) mencionan que las reglas condicionan el comportamiento de los individuos porque calculan el costo beneficio de sus acciones, es decir, consideran las recompensas o castigos que pueden provenir de individuos, organizaciones o del mismo Estado.

Este pilar apunta que, para que el orden prevalezca en las organizaciones, es necesario que exista un sistema de reglas que se apoye en la vigilancia y en el poder de las sanciones (Scott, 2008). Las organizaciones reglamentarias se adhieren al cumplimiento para evitar las sanciones (Hoffman, 1999, en Kshetri, 2007) y la legitimidad de estas organizaciones se centra en las exigencias de los gobiernos y sus leyes (Kelman, 1987).

En el pilar reglamentario, las leyes ejercen presión formal en los directivos para implementar ciertas reglas y prácticas de seguridad de la información. Es el nivel responsable de asegurar que los departamentos e individuos cumplan con las leyes y sus disposiciones aplicables, porque infringirlas puede resultar en una acción legal contra la propia organización (AlKalbani et al, 2016). Esto las obliga a revisar sus prácticas de protección de datos personales, cumplir con ellas y, si es necesario, establecer un reglamento interno. En México, la ley que despliega presión formal en los particulares es la LFPDPPP y su reglamento.

El énfasis **normativo** indica que los sistemas normativos (valores y normas) dan una dimensión establecida, evaluativa y obligatoria de la vida social. Los valores son definidos como “la concepción de lo deseable, con la que los estándares o comportamientos existentes pueden ser comparados y evaluados”, y las normas se refieren a la manera en “la que las cosas deberían ser hechas”. El pilar normativo está compuesto por rutinas, procedimientos, roles, creencias, paradigmas, códigos y culturas, y establece metas u objetivos, pero también designa procedimientos o caminos para alcanzarlos (Scott, 2008). Confieren valores, expectativas de roles, deberes, derechos o responsabilidades. Algunas de estas reglas normativas aplican a toda una colectividad, mientras que otras sólo son para actores o posiciones, (Geels, 2004), por lo tanto, son para las organizaciones como un ente y a nivel directivo, sus departamentos y personal.

Normalmente, los sistemas normativos son vistos como imposiciones y restricciones sobre el comportamiento dentro de las organizaciones, y lo son —es pertinente recordar la aportación de Etienne (2010) cuando escribe que el cumplimiento normativo está asociado a una práctica de control racional—, pero, a su vez, empoderan y

habilitan la acción. Confieren derechos y responsabilidades, privilegios y deberes, permisos y mandatos (Scott, 2008). Para Schneider (1999), las prácticas dentro de las organizaciones son más consistentes cuando toman en cuenta los sistemas de valores. La base del cumplimiento de este pilar deriva de las obligaciones sociales y cuando no se asimilan pueden caer en sanciones por incumplimiento (Grewal and Dharwadkar, 2002).

La tercera concepción centra su atención en los **elementos culturales y cognitivos**. Esta concepción asume que los procesos cognitivos internos están influenciados por estímulos culturales externos y las respuestas individuales son la representación de la interiorización de dichos estímulos (Scott. 2008). Esto se refiere a la manera en la que las personas advierten, categorizan e interpretan los estímulos del exterior (Kshetri, 2007) porque los factores cognitivos, aunque se manifiestan a nivel individual, provienen del entorno (Berguer and Luckman, 1967).

De acuerdo con Douglas (en Wahid, 2011), las categorías culturales pueden ser entendidas como contenedores cognitivos en los que los intereses sociales son definidos y clasificados, discutidos, negociados y librados. Es la interiorización de los individuos en las organizaciones de las reglas del pilar reglamentario y de las prácticas y rutinas del normativo.

Para los teóricos cultural/cognitivos, en muchos casos, el cumplimiento se da porque otra manera de actuar es inconcebible y las rutinas se siguen porque “se dan por sentadas”. Si se quiere entender o explicar un comportamiento, es necesario tomar en cuenta no solo el objetivo, sino además la interpretación subjetiva de quien lo realiza. El cognitivo apunta al poder de los modelos para determinados tipos de actores y líneas de acción, a la vez que enfatiza la relevancia de la identidad. La dimensión afectiva de este pilar se expresa en sentimientos de afecto, certidumbre y confidencia, por un lado, y por sentimientos negativos de confusión o desorientación, por el otro (Scott, 2008).

Los tres pilares generan bases de legitimidad dentro de las organizaciones. De acuerdo con Schuman (en Scott, 2008), la legitimidad es la percepción generalizada de que las acciones de una organización son deseables o apropiadas dentro de un sistema social

de reglas, valores y creencias. El énfasis reglamentario establece que las organizaciones legítimas son aquellas que operan de acuerdo con requerimientos legales. La concepción normativa obliga a una base más moral para la legitimidad, se obtiene mediante prácticas como capacitación o establecimiento de rutinas. El punto de vista cultural/cognitivo apunta hacia el reconocimiento de un rol o modelo de estructura, es el punto en el que los individuos se apropian de la normatividad y la interiorizan.

Concerniente al cumplimiento en la implementación de las políticas de protección de datos personales en las organizaciones, es posible afirmar que la fusión de los tres pilares da más consistencia y fuerza a los resultados esperados en la implementación, porque su presencia o ausencia puede conducir al éxito o fracaso. Sin embargo, aunque las organizaciones están compuestas por una serie de elementos que se combinan, hay uno o algunos que dominan, y su superioridad la da el área desde la que se estudian. Por ejemplo, economistas y teóricos se enfocan en los reglamentarios, los sociólogos favorecen a los normativos, y los antropólogos y sociólogos organizacionales hacen énfasis en los cultural-cognitivos (Scott, 2004).

En el capítulo anterior, Etienne (2010), Gezelius (2002) y Grasmick y Scott (1982) hablan sobre la preeminencia del modelo racional sobre el normativo en el cumplimiento. En este mismo sentido, Scott (2004) afirma que un pilar puede ser más dominante, dependiendo del enfoque de estudio, sin determinar cuál es, y otros científicos (AlKalbadi et al, 2016) refuerzan las postulaciones de los tres autores y de Scott en una investigación empírica que realizaron desde la teoría institucional para conocer el impacto de las presiones coercitivas, normativas y miméticas.

AlKabaldi et al (2016) dan más peso al pilar reglamentario cuando sostienen que, aunque los tres afectan positivamente al cumplimiento, la reglamentación genera mayor presión sobre los directivos para obligarlos a cumplir con las medidas de seguridad en las organizaciones. La coercitividad de las leyes y reglamentos juegan un papel preponderante que los mueve a la toma de decisiones para actuar en pro del cumplimiento (Alkalbadi et al, 2016), porque esto les da legitimidad como organización (Edwards, Mason y Washington, 2009). Esto quiere decir que la teoría institucional

resalta motivos (muy racionales) para cumplir con estándares y políticas de seguridad de la información (Björk (2004).

En una organización puede existir una combinación de elementos. En los sistemas sociales estables, se observan prácticas que persisten, “se dan por sentadas” y las reglas formales las respaldan. Cuando los pilares están alineados se fortalecen las organizaciones (Scott, 2008). No obstante, en ocasiones será uno o dos pilares los que soporten un orden, o uno asumirá la primacía. De igual manera, los pilares pueden estar desalineados y soportar o motivar diferentes opciones y comportamientos. Con base en los argumentos teóricos, en particular, esta tesis da preeminencia al pilar reglamentario en el cumplimiento.

Por otro lado, utilizar la teoría institucional también ayuda a explicar, controlar y entender la dinámica de la seguridad de la información en todos los niveles de las organizaciones (Bjorck, 2004). La literatura demuestra que la teoría ha estudiado el primer nivel organizacional directivo (Lopes y de Sá-Soares, 2014), resulta pertinente recordar que, según Foorthuis y Bos (2011), es ahí donde se desarrollan las estrategias que la organización va a implementar en sus diferentes áreas y personal, de quienes se espera el estado de conformidad con las medidas de la organización en materia de datos personales.

En algunas investigaciones que utilizan la teoría institucional es posible encontrar los pilares reglamentarios, normativos y cultural/cognitivos. Un ejemplo es el estudio de Kshetri (2007), que identifica los elementos que integran cada pilar, como muestra el siguiente cuadro. Destacan en negrita los factores de cada uno.

Factores institucionales que afectan el flujo de las empresas transnacionales

Pilar institucional	**Constructor**	**Mecanismos de influencia sobre procesos de negocios en las transnacionales y outsorcing de las TI**
Reglamentario	- Rigor de las **leyes** de privacidad en el país de origen - El **Estado de derecho** en el	- **Control** sobre el flujo de información como forma de proteccionismo encubierto

	país destino	- Las **dificultade**s asociadas con la **ejecución de contratos** disminuyen el valor creado por subcontratación en el extranjero
Normativo	- Las **presiones** sindicales y públicos contra *offshore* y *outsourcing* en el país de origen - La existencia de asociaciones comerciales o **profesionales** que trabajan en el país de destino	- Usar obligaciones **éticas** y sociales - Hacer cumplir la **ética y códigos de conducta**. Dar los **conocimientos** suficientes para fortalecer el estado de derecho
Cognitivo	- **Cultura** moderna de administración en el país destino - Compatibilidad **cultural** entre el país de origen y el de destino	- Métodos científicos y sistemáticos para dirigir una organización y crear **valores** - Aumenta la **confianza** de la empresa-cliente relacionada con la seguridad de la información - Similitud del idioma, **comprensión** de prácticas comerciales y vínculos étnicos

Tabla 9 Factores institucionales que afectan el flujo de las empresas transnacionales y el outsourcing de las TI. Fuente: Kshetri (2007)

Por su parte, en su investigación, Lopes y de Sá-Soares (2014) señalan factores facilitadores e inhibidores por cada pilar:

Factores condicionantes en la implementación de políticas de sistemas de seguridad		
Pilar institucional	**Factores facilitadores**	**Factores inhibidores**
Reglamentario	Establecimiento de **reglas** para los sistemas de seguridad **Funcionarios** de seguridad proactivos Aplicar para **certificaciones** de calidad Existencia de **voluntad política** Tener la **aprobación del Ejecutivo** (la Dirección) **Monitoreo** del cumplimiento de la política Capacidad para **sancionar** algún abuso	La no-aprobación de las políticas por el Ejecutivo **Desobediencia** de los usuarios

	Limitar la capacidad del ayuntamiento	
Normativo	**Mayor dependencia de las TI** para el **desempeño de funciones** Aumento del número de riesgos de las TI **Participación** en programas de ciudades digitales Expansión de la infraestructura de TI **Formación ética** para los usuarios	Falta de financiación del Estado para **capacitar** a los usuarios de las TI Falta de **capacitación** La **complejidad** de la formulación de las políticas
Cultural-cognitivo	El documento de la política no sea largo Que la política sea **conocida** por los usuarios Al explicar a los usuarios las ventajas de tener una política de los sistemas de seguridad de la información**, involucrar a los usuarios** en la implementación de las políticas Formación para los técnicos de las TI sobre las políticas de seguridad de la información **Impactos** de los incidentes que han tenido a causa de las políticas de sistemas de seguridad de la información	Pérdida de tiempo **Resistencia** de los usuarios Falta de consciencia de las políticas de sistemas de información **Visión reducida** de las iniciativas **Satisfacción** con la protección que únicamente dan las TI El ayuntamiento es pequeño y, por lo tanto, las políticas no son necesarias (**aceptación**) La infraestructura de las TI es pequeña

Tabla 10 Factores condicionantes en la implementación de políticas de sistemas de seguridad de la información. Fuente: Lopes y de Sá-Soares (2014)

Finalmente, Geels (2004) también desarrolla un esquema para identificar los factores de los tres pilares en diferentes áreas, como muestra de que cada régimen, dependiendo de su actividad, presenta sus propias condiciones para el cumplimiento:

Factores de los tres pilares en diferentes áreas			
Área	**Reglas formales**	**Normatividad**	**Cognitivo**

Régimen tecnológico y de maquinaria	**Estándares** técnicos, especificaciones de maquinaria, requerimientos funcionales, reglas contables, subsidios	**Procedimientos** de pruebas, conocimiento de la empresa	**Expectativas**, agenda de problemas técnicos, estrategias de solución de problemas
Ciencia	Investigación formal, límites profesionales, **reglas** de subsidios	Procedimientos de publicación, normas de citación, **valores y normas** académicas	**Paradigmas, criterios** y métodos de producción de conocimiento
Política	**Regulaciones** administrativas y procedimientos legislativos, estándares	**Metas**, interacciones de gobierno y las industrias, roles del gobierno	**Ideas** sobre la efectividad de los instrumentos, **percepción** de las políticas, problemas de agenda
Usuarios, mercados y redes de distribución	Construcción de mercados por medio de **leyes y reglas,** derechos de propiedad, leyes de calidad, reglas de lealtad, subsidios, impuestos, reglas de seguridad	**Valores culturales** en los sectores del mercado, formas en las que los mercados interactúan con las firmas, roles en la relación entre usuarios y firmas	Prácticas y **preferencias** de los usuarios, **creencias** sobre la eficiencia, **percepción** de los mercados

Tabla 11 Factores de los tres pilares en diferentes áreas. Fuente: Geels (2004)

Como se observa de los cuadros anteriores, en el pilar reglamentario, los factores de cumplimiento que desempeñan un papel coercitivo son las leyes, reglas, sanciones, estándares, monitoreo y el rol directivo. También destaca que las reglas operan a nivel organizacional, por departamentos e individual, porque el nivel directivo que las implementa, debe supervisar su aplicación y cumplimiento en todas las áreas. Dentro de los factores normativos aparecen los valores, metas, procedimientos, ética, capacitación, códigos de conducta. Se trata de factores implementadores de actividades y rutinas dentro de las organizaciones para establecer como una práctica común lo que señalan las reglas, pueden ser a nivel de organización, departamentos e individuos. Finalmente, en el pilar cognitivo, sobresalen las creencias, preferencias, paradigmas, aceptación de una nueva herramienta (tecnológica), expectativas, percepciones, satisfacción.

Estos factores operan en todos los niveles y se presentan cuando el actor interioriza o no la regla y la normatividad. Las variables de esta tesis se eligieron con base en los factores que se resaltan en negro de cada una de las tablas.

Conclusión

Mediante los factores facilitadores e inhibidores identificados por Wahid (2011), basado en Scott (2008), y las aportaciones de Kshetri (2007), Lopes y de Sá-Soares (2014) y Geels (2004), este estudio se extenderá al ámbito de la implementación de las políticas de protección de datos personales, utilizando el enfoque institucionalista, para conocer qué factores motivan su cumplimiento en las organizaciones. Los factores inhibidores y facilitadores desarrollados en la literatura permitirán responder a esta inquietud, mediante el uso de los pilares de la teoría institucional.

La literatura arroja los factores de mayor incidencia para el cumplimiento de acuerdo con cada pilar. Específicamente, en el reglamentario están presentes el establecimiento de reglas, sanciones y monitoreo (Scott, 2008; Lopes y de Sá-Soares, 2014 y Kshetri, 2007) a los que las organizaciones se adhieren para no sufrir las penalizaciones por incumplimiento (Kshetri, 2007); esto quiere decir que la base del cumplimiento para estas organizaciones se centra en la conveniencia de evitar el castigo. En el pilar normativo destacan las rutinas, procedimientos, roles (liderazgo), creencias, paradigmas, códigos de ética y de conducta, valores, (Scott, 2008; Lopes y de Sá-Soares, 2014 y Kshetri, 2007) capacitación y certificaciones (Lopes y de Sá-Soares, 2014). En el cultural cognitivo resaltan factores como compatibilidad cultural, claridad del mensaje, confianza empresa-cliente (Scott, 2008; Lopes y de Sá-Soares, 2014 y Kshetri, 2007), aceptación de las TI, involucrar a los usuarios y tamaño de la organización (Lopes y de Sá-Soares, 2014).

Esta investigación plantea que la coercitividad de la ley es el detonador del cumplimiento para la protección de los datos personales en las organizaciones, con base en las aportaciones de Etienne (2010), Gezelius (2002) y Grasmick y Scott (1982), que dan mayor peso al modelo racional/reglamentario sobre el normativo. El

pilar reglamentario de la teoría institucional resulta pertinente para este estudio porque, precisamente, destaca la relación de las sanciones, multas y monitoreo de las reglas formales —que es el modelo de las leyes de protección de datos personales del mundo y la de México— con la implementación de nuevas políticas, y AlKabaldi et al (2016) refuerzan la idea de que la reglamentación ejerce presión a partir de la cual deriva la normatividad.

La protección de los datos personales es una práctica relativamente nueva en México. Sus primeros antecedentes se encuentran en la Ley de Transparencia de 2002; hasta ese momento, no había reglas formales que dictaran cómo debían tratarse los datos personales ni que impusieran sanciones a las infracciones. A ejemplo de las leyes europeas que son exhaustivas y sancionadoras, la LFPDPPP también contiene multas y sanciones que modifican los hábitos y conductas de los sujetos obligados, y los constriñen a implementar las disposiciones de la ley en todas las áreas de las organizaciones, con el fin de que la comunidad internacional considere a México como un país que brinda tratamiento adecuado a los datos personales para formar parte del Convenio 108.

Sin embargo, si las organizaciones en México cumplen con las leyes para evitar el castigo como sugiere esta tesis, no significa que se haya apropiado de ellas, ni que las interioricen o que las consideren necesarias. Esto lo explica el pilar reglamentario de la teoría institucional, y también da lugar a la presencia de sus otros dos pilares para fortalecer el cumplimiento en un nivel normativo y cognitivo, porque un tema como la protección de datos personales, que tiene un ámbito muy extenso de acción, no puede ser labor únicamente del ejercicio reglamentario de la ley y de la vigilancia del Inai como órgano garante, sino que las mejores prácticas y la conciencia individual dentro de las organizaciones responsables también deben contribuir. Esto sin menoscabar la importancia de las sanciones para la implementación en primer lugar.

La literatura demuestra la importancia del aspecto normativo en la implementación de una política porque el cumplimiento ocurre cuando la norma se interioriza. El pilar normativo de la teoría institucional explica “cómo deben ser las cosas” y establece procedimientos o caminos para alcanzar los objetivos de la ley y cumplir, no solo por

las sanciones sino también porque, como lo explican los factores normativos, la protección de los datos se vuelve un valor para la organización. La literatura indica que, normalmente, la normatividad puede percibirse como impuesta porque proviene de una regla, esta investigación busca conocer su pertinencia con el cumplimiento para determinar si los factores del pilar normativo inciden en la implementación para complementar a las reglas formales.

Una vez que existe una regla formal que obliga al cumplimiento, que en este caso es la LFPDPPP, las organizaciones deben contribuir con quehaceres en su interior para fortalecer este derecho como un valor organizacional, dando a conocer las responsabilidades de cada departamento e individuos con capacitación constante fomentando buenas prácticas, que corresponde al estudio del pilar normativo. Estas son maneras en las que las organizaciones refuerzan el cumplimiento para que no recaiga únicamente en la regla. La existencia de prácticas como la capacitación y códigos de ética son importantes porque las pérdidas de datos pueden ocurrir por desconocimiento, transferencias a terceros, errores o negligencia de los empleados (ITR, 2015).

Pero, ¿qué pasa una vez que ya hay reglas formales que fuerzan a cumplir con las disposiciones y prácticas establecidas dentro de las organizaciones? ¿Los actores cumplen por evitar algún castigo, por las prácticas o porque ya interiorizaron la regla y los valores? ¿Qué es lo que motiva el cumplimiento? En un inicio, por tratarse de un derecho nuevo en México, es de esperarse que las organizaciones cumplan por temor a la sanción, es decir, para prevenir las multas, pero es posible que una vez que cumplen con las reglas formales y que establecen prácticas que fomentan el tratamiento adecuado, a nivel individual, perciban los beneficios de cumplir con las leyes porque han interiorizado la regla y el valor, y que, a su vez, se hayan familiarizado con las prácticas. Por el contrario, podría existir rechazo, y el cumplimiento recaería únicamente en la normatividad y la reglamentación o, en su defecto, solo en la reglamentación. Esta interiorización se explica en el pilar cognitivo de la teoría institucional.

Como lo indica la teoría, el cumplimiento puede apoyarse únicamente en uno o dos pilares, aunque se fortalece cuando intervienen los tres. Esta tesis, en particular, sostiene la supremacía del pilar reglamentario. Para saber qué factores motivan la protección de los datos personales en las organizaciones, se seleccionaron los más pertinentes que destaca la literatura.

Del pilar reglamentario, los factores a estudiar son las sanciones (Hovi, Stokke y Ulfstein, 2005; Kudic y Banaszak, 2009; Kite, 1964 y Baron, 1988), monitoreo (Mwakabinga, 2008; Urpelainen, 2014; Gray y Silbey, 2014 y Canales, 2011) y liderazgo directivo (Peterson et al, 2003; Berkeley, 1988; Rainey, 2009 y Noruzy et al, 2012); del pilar normativo, la ética organizacional (Fort, 1966; Solomon, 1993; Philips y Margolis, 1999; Treviño, Weaver y Reynolds, 2006; Alina 2014) y capacitación (Aguinis y Kraiger, 2009; Goldstein, 1980; Good, 2013 y Alina, 2014), y del pilar cognitivo, la asimilación de las TIC (Truex, Baskerville y Klein, 1999; Boynton, Zmud y Jacobs, 1994 y Rainey, 2009) y la reputación (Peeples, 2002; Smith, 2004).

El cumplimiento es el estado de conformidad entre el comportamiento de los actores y las normas; la sanción es un mecanismo coercitivo de cumplimiento que produce miedo y corrige o modifica comportamientos; el monitoreo es una herramienta que verifica el cumplimiento; el liderazgo directivo es importante porque de él depende que se cumplan las tareas de la empresa, está vinculado con la toma de decisiones; la ética organizacional tiene que ver con valores y principios de los empleados dentro de las organizaciones; la capacitación es la adquisición de habilidades, conocimiento o actitudes que mejoran el desempeño en las organizaciones; la asimilación de las TIC tiene una influencia positiva si se cuenta con la capacitación y conocimiento suficiente dentro de las organizaciones porque facilitan el almacenamiento y uso masivo de datos personales, a la vez que los hacen vulnerables y, finalmente, que las organizaciones sean reconocidas como confiables y les brinda buena reputación en el mercado.

Esta investigación analiza la siguiente relación, donde:

- Variable dependiente (X): cumplimiento

- Variables independientes (Y): sanción, monitoreo, liderazgo directivo, ética organizacional, capacitación, asimilación de las TIC y reputación.

El siguiente cuadro describe cada una de las variables.

TABLA DE VARIABLES DEPENDIENTE E INDEPENDIENTES

Variable dependiente	
Cumplimiento	El cumplimiento es la única variable dependiente a la que influencian las independientes en esta investigación. La literatura lo define como el estado de conformidad entre el comportamiento de los actores —personas u organizaciones— y las normas —reglas predeterminadas, políticas, procedimientos, estándares, lineamientos, principios, leyes y otras formas de orden— (Foorthuis y Bos, 2011); también es un acto de elección entre dos opciones —cumplir o no cumplir— (Sutinen, Rieser y Gauvin, 1990). Capítulos anteriores hacen énfasis en que no todos los actores alcanzan un cumplimiento de cien por ciento, sino que cada uno establece su propio nivel aceptable o deciden no cumplir. El cumplimiento es, por tanto, el grado de apego a los procedimientos sistemáticos, requerimientos legislativos, políticas corporativas o estándares de calidad (Foorthuis y Bos, 2011; Björk, 2004). Siahann (2013), Siddiki, Basurto y Weible (2012) y Mwakabinga (2008), en sus investigaciones, se enfocan en categorías reglamentarias para saber si las organizaciones efectúan o no lo que deben hacer.
Variables independientes	
Pilar reglamentario	
Sanción	La literatura en torno a la sanción la define como un mecanismo frecuentemente utilizado para garantizar el cumplimiento de una ley por su coercitividad inherente.

	También es uno de los factores más importantes del pilar reglamentario de la teoría institucional. Se trata de un mecanismo eficaz que hace que las organizaciones cumplan con una política y disminuyan la probabilidad de eludir la conducta esperada. Algunas investigaciones demuestran la utilidad de las sanciones para prevenir conductas no deseadas porque la amenaza de una sanción produce miedo (Rothbarth, 1968) que corrige o modifica comportamientos (Baron, 1988). Por el impacto que tiene en los actores (Hovi, Stokke y Ulfstein, 2005), es el elemento más fuerte que conduce al cumplimiento (Kite, 1964). En temas de seguridad de la información, aumenta las conductas que lo fortalecen (Pahnila, S., Siponen, M. & Mahmood, A., 2007; Herath y Rao, 2009). Sin embargo, la eficacia en el cumplimiento no se logra con una multitud de sanciones, sino que los resultados óptimos se obtienen con la elección y combinación correcta de ellas (Kudic y Banaszak, 2009). Tenbrunsel y Messick (en Treviño, Weaver y Reynolds, 2006) demuestran que una sanción débil o mal aplicada puede ser peor para fomentar una conducta no deseada que la ausencia total de ellas. Gray y Silbey (2014) observan tres maneras de interpretar la relación de la reglamentación y los actores de la organización: como amenaza para la persona y su empleo, una aliada para la productividad de la organización o un obstáculo para la innovación eficiente. Cuando la sanción se percibe como una amenaza, el cumplimiento se entiende solo como una lista de tareas que realizar, independientemente de que genuinamente estén alineados a las metas de la organización; aun así, sigue siendo cumplimiento.
Monitoreo	Para que exista cumplimiento no basta con la amenaza de una sanción, sino que su eficacia también debe verificarse. Si la vigilancia al cumplimiento es baja, entonces aumenta la probabilidad de que los actores no cumplan o que cometan actos ilegales (Herath y Rao, 2009). El monitoreo es una herramienta que garantiza el cumplimiento de una política y la obtención de mejores resultados (Urpelainen, 2014). Su eficacia se ha demostrado en distintas investigaciones sobre seguridad de la información (Mwakabinga, 2008; Herath y Rao, 2009). Frecuentemente, los actores de la organización perciben al monitoreo como una actividad que infunde miedo porque es una amenaza constante, como si los supervisores únicamente vigilaran a la espera de obtener evidencia de

	incumplimiento o estuvieran preocupados por buscar la manera de aplicar un castigo (Gray y Silbey, 2014). Si el supervisor se ve como a alguien más que quien impone el castigo, sino como a quien puede consultarse en determinada situación, entonces se vuelve un aliado. Esta es la forma ideal en la que los supervisores deberían concebirse en las organizaciones (Ayres y Braithwaite, 1992), habría menos casos de incumplimiento si quien inspecciona desarrolla relaciones de cooperación con quienes regula (Canales, 2011). La literatura demuestra que el monitoreo es un factor determinante para el cumplimiento de las disposiciones que las organizaciones implementan (Mihai y Alina (2013). El capítulo I de esta tesis habla sobre el papel de las autoridades de protección de datos personales (DPA) y, específicamente, el capítulo II hace mención de las funciones y capacidades del INAI en México como órgano garante, en donde queda claro que, a pesar de que es sancionador, únicamente castiga si un afectado interpone un reclamo, mas no tiene un mecanismo de monitoreo establecido que vigile qué sujetos obligados cumplen o no.
Liderazgo directivo	Para la teoría institucional, la parte directiva de una organización es un promotor reglamentario de cumplimiento. Una visión individualista sobre el liderazgo asume que los líderes directivos tienen un impacto crucial en el desempeño de la organización que encabezan, algunos autores han utilizado esta variable junto con otras para demostrar su influencia positiva en el aprendizaje y la innovación (Peterson et al, 2003; Berkeley, 1988; Noruzy et al, 2012). Una organización no alcanzará sus metas con efectividad mientras no sea dirigida por un superior (líder directivo) adecuado que desarrolle metas propias, que sepa cómo hacer las cosas, que dé un 'salto emprendedor' para mover a la organización y la lleve por otro curso con la objetividad necesaria (Lewis, en Rainey, 2009). El éxito de la organización depende, en cierto grado, de la asociación de las habilidades del directivo con las tareas de la empresa. Es pieza clave para influir en la innovación de políticas y programas (Noruzy et al, 2012). En las organizaciones, el liderazgo juega un papel primordial para que los individuos exploren, renueven y apliquen su conocimiento, de tal forma que alcancen los objetivos planteados (Noruzy et al, 2012). La literatura afirma que los líderes son importantes para el desempeño de una organización (Berkeley, 1988) porque se

	vinculan con el compromiso, satisfacción, confianza y 'comportamientos cívicos' por parte de los empleados; además, pueden generar conciencia y aceptación de una nueva disposición (Hermosilla et al, 2016). Desde la teoría institucional, Scott (2004) afirma que el liderazgo directivo está asociado con la implementación o no implementación. Cuando se trata de la seguridad de la información, los directivos asumen un rol fundamental para la toma de decisiones que dan cumplimiento a prácticas operativas. Si ellos no ejecutan acciones, las consecuencias para la organización pueden ser dramáticas (Kajava et al, 2006).
Pilar normativo	
Ética organizacional	Donaldson y Dunfee (1944, 1955), Fort (1966) y Solomon (1993) sostienen que las organizaciones deben contar con códigos de ética que establezcan cómo deben conducirse los individuos. Las organizaciones afectan la conducta de sus miembros porque pasan un número considerable de horas en ellas, por lo que se vuelven parte de un entorno que los influencia (Phillips y Margolis, 1999) y conforman su cultura organizacional (Treviño, Weaver y Reynolds, 2006). Además, las organizaciones imprimen un sello en la sociedad porque moldean el flujo de capital, recursos naturales y laborales, además de que influyen en las comunidades locales. Si la ética es parte de la conducta en los negocios, también debe introducirse en las organizaciones, por lo tanto, este es un factor fundamental del pilar normativo de la teoría institucional para explicar al cumplimiento. Treviño, Weaver y Reynolds (2006) categorizan los factores que influencian una conducta ética a nivel individual y organizacional. En los individuos, puede ser por motivación moral, juicio moral, afectividad o identidad; en las organizaciones, la recompensa o el castigo, cultura/clima organizacional ético, liderazgo, el lenguaje o una infraestructura ética. Los elementos de un contexto organizacional que influencian una conducta ética son múltiples: presión laboral, insatisfacción laboral ocasionada por un mal salario o cuando los méritos de la persona no se toman en cuenta o conflicto de roles. Los autores destacan la importancia de las recompensas y castigos sobre la conducta ética en una organización, aunque las recompensas no necesariamente la fomentan tanto como la presencia de un riesgo por cometer una falta, es decir, un castigo. Esto que recuerda que, para esta investigación, el pilar

	reglamentario da pauta al normativo para el cumplimiento. Otro factor importante para la ética organizacional es el liderazgo ético. Un líder que se conduce éticamente demuestra una conducta normativa adecuada mediante sus actos y relaciones interpersonales, y la transmite a sus seguidores mediante el refuerzo y la toma de decisiones. De esta manera, los líderes éticos impulsan esta conducta dentro de las organizaciones y la reproducen (Treviño, Weaver y Reynolds, 2006). Alina (2014) refuerza la importancia del liderazgo al concluir que el factor más importante para implementar de manera exitosa la conducta ética y su cumplimiento en la organización es que se dé desde los superiores porque el comportamiento de los directores impacta en el de los miembros de la organización. Mihai y Alina (2013) plantean que la organización debe asumir la responsabilidad de promover valores éticos y principios en sus empleados y proveedores para evitar problemas como fraude, corrupción, conflictos de interés, sobornos, desconfianza, gratificaciones o rivalidades. También sugieren la efectividad de un programa de cumplimiento para los códigos de ética que mitigue los riesgos de incumplimiento, así como sistemas de comunicación internos que los den a conocer. Los códigos de ética fortalecen y dictan cómo debe ser la conducta de los miembros de la organización con base en sus valores organizacionales y establecen una serie de principios que de no seguirlos los consideran mala conducta (Alina, 2014). Por lo tanto, es necesario que las organizaciones se interesen y responsabilicen por promover prácticas honestas que eliminen cualquier duda con respecto a su ética, porque hacerlo fortalece el cumplimiento de una nueva disposición, que en este caso es la protección de datos personales.
Capacitación	La capacitación es la adquisición de habilidades, conocimiento o actitudes que mejoran el desempeño individual, en equipo y organizacional dentro de un ambiente laboral (Goldstein, 1980; Aguinis y Kraiger, 2009). Autores como Campbell (1971), Wexley (1984), Latham (1988) o Alina (2014) han mostrado interés en estudiar la relevancia de la capacitación en las organizaciones porque las ayuda a cumplir con sus objetivos. Para que sea exitosa, debe involucrar a todo el personal de la organización, incluidos los directivos (Alina, 2014; Good, 2013). Con respecto a la seguridad de la información, mejora el desempeño porque el conocimiento y las habilidades fluyen a todos los niveles organizacionales donde ocurren los procesos (Kajava et al, 2006).

	La LFPDPPP da pauta a las organizaciones para que capaciten a su personal, es uno de los procedimientos con los que tienen que cumplir, lo que convierte a este factor en una variable más que debe estudiarse como parte del pilar normativo porque contribuye positivamente con el cumplimiento.
Pilar cognitivo	
Asimilación de las tecnologías de la información y comunicación	La influencia de las tecnologías de la información en el diseño de las organizaciones se ha investigado de manera creciente en los últimos años (Truex, Baskerville y Klein, 1999). Las computadoras, Internet, el correo electrónico, el almacenamiento en la nube y otras formas de información y comunicación transforman la vida organizacional con efectos dramáticos difíciles de describir (Rainey, 2009). El uso de las TIC forma parte de las actividades operacionales y estratégicas de una organización. Pero no basta con que estén presentes, es necesario que los directivos y el personal las asimilen y cuenten con la capacitación y conocimiento suficiente, porque esto influencia positivamente su aplicación y efectividad. Si permea un clima que las gestiona, crece una percepción compartida y duradera de los beneficios de trabajar con ellas, es decir, los miembros de la organización las asimilan cuando se relacionan con las prácticas, procedimientos y formas vinculadas con las actividades de las TIC, para el cumplimiento de sus propias tareas (Boynton, Zmud y Jacobs, 1994). Esto es de suma relevancia porque las TIC facilitan el almacenamiento y uso masivo de datos personales, a la vez que los vulneran, y es necesario que las organizaciones las utilicen adecuadamente para un tratamiento óptimo.
Reputación	La literatura resalta lo importante que es para las marcas que sus clientes o usuarios confíen en la calidad de sus productos o servicios para gozar de una buena reputación en el mercado, y asume que respaldan su prestigio con mercancías y servicios a los que sus clientes están acostumbrados a recibir en una transacción (Peeples, 2002). Al respecto, por ejemplo, para que el comercio electrónico ganara la confianza de sus usuarios, fortaleció algunas actividades desde la ética —no violar la privacidad de las personas, aplicar medidas de seguridad en sus transacciones, no enviar correos electrónicos no deseados, entre otros—, implementó medidas de autorregulación, cumplió con las consideraciones legales, proveyó información de contacto en la web, comenzó a responder dudas y aclaraciones y estableció las condiciones de compra y precios de los productos transparentes (Peeples, 2002),

	porque había evidencia de que los consumidores no confiaban en los proveedores en línea lo suficiente como para establecer una relación con ellos (Grabner-Kraeuter, en Smith, 2004). En el tema de protección de datos personales, Direct Marketing Association (DMA, 2015) evidencia que la reputación es un factor crítico para que los usuarios decidan compartir sus datos con las organizaciones, por lo que deben diseñar mecanismos que la fortalezcan como parte esencial de su quehacer. Para esta investigación, es un elemento clave para mantener una cultura sana de protección de datos personales. En México, Deloitte (2014) revela que, de las organizaciones que encuestó, únicamente diecinueve por ciento está interesado en incrementar la confianza de sus clientes para que sepan que sus datos estarán seguros y que no van a utilizarlos con otros fines y dieciocho por ciento busca mantener la reputación de la marca como una empresa confiable. Según esta encuesta, es el segundo motivo para dar cumplimiento a la ley después de las sanciones. Por su parte, la Enaid (Inegi, 2016) dio a conocer que a 84 por ciento de la población en el país le preocupa que las organizaciones públicas o privadas a las que les dio sus datos puedan hacer mal uso de ellos. Por esto, el cumplimiento de los procedimientos de la ley en las organizaciones también lo determina la importancia que le den a que sus clientes y que demás empresas gocen de buena reputación como confiables.

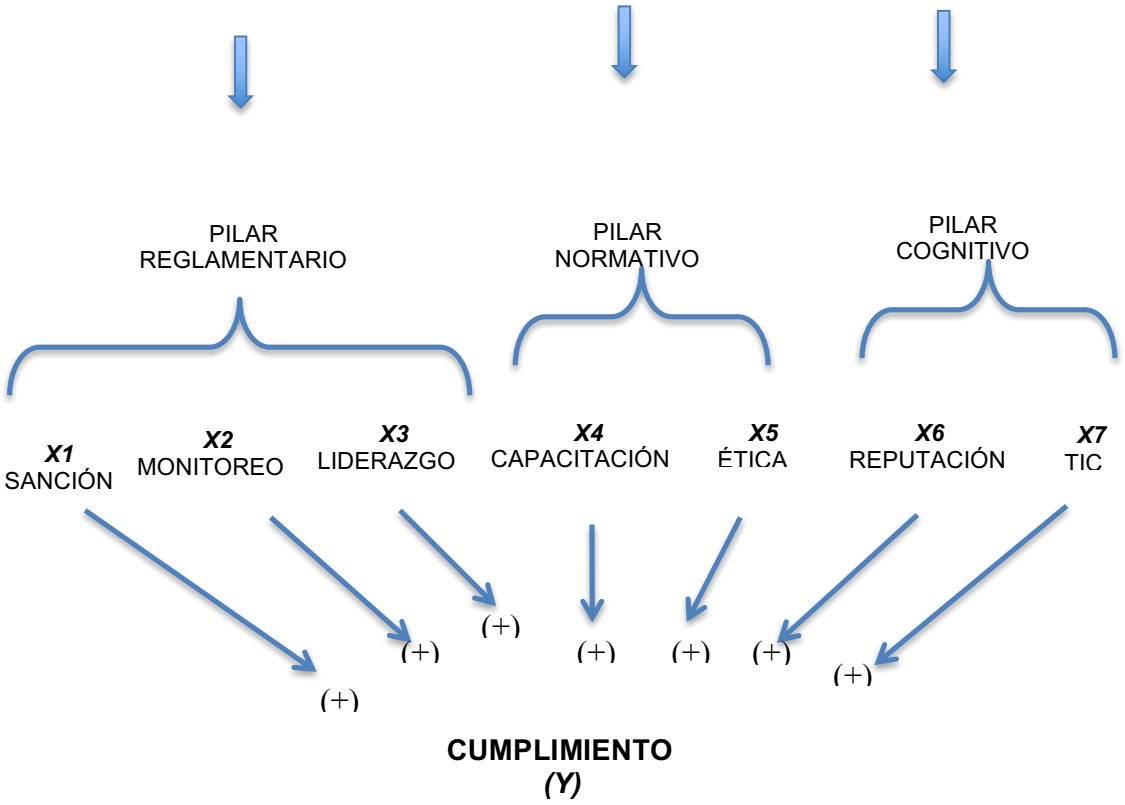
Tabla 12 Tabla de variables dependiente e independientes. Fuente: Elaboración propia.

La discusión de este capítulo asienta que los factores de los pilares institucionales influencian el cumplimiento de las políticas de protección de datos personales en las organizaciones, lo que conduce al desarrollo de un modelo conceptual de investigación que se muestra en la siguiente figura. En él, convergen las variables independientes procedentes de los pilares reglamentario, normativo y cognitivo de la teoría institucional, y conjunta el estudio de las teorías racionales y normativas para explicar al cumplimiento.

La expectativa teórica es que, a mayor presencia de cada uno de los factores del pilar reglamentario, normativo y cognitivo, mayor será el cumplimiento.

MODELO DE INVESTIGACIÓN

TEORÍA INSTITUCIONAL



Fuente: Elaboración propia

El siguiente capítulo describe la metodología que conduce a la comprobación de la hipótesis planteada.

CAPÍTULO V

ABORDAJE METODOLÓGICO

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares se aprobó en julio de 2010 y su Reglamento en diciembre de 2011. Los sujetos obligados tenían hasta julio de 2011 para designar a la persona o departamento de datos personales y publicar el aviso de privacidad, y debían cumplir con el ejercicio de los derechos ARCO a partir de enero de 2012. Sin embargo, como plantea esta tesis, sin que exista alguna cifra de cumplimiento, las organizaciones han cumplido en distinto grado. A raíz de esto, la pregunta de investigación es la siguiente:

¿Qué factores inciden en el cumplimiento de las políticas de protección de datos personales en las organizaciones?

La hipótesis planteada es:

H1. Los factores reglamentarios influyen más en el cumplimiento de las políticas de protección de datos personales en las organizaciones, por temor a las sanciones, que los normativos y cognitivos que procuran la protección en sí misma de los datos personales.

Hasta este momento, en México hay escasa investigación sobre el tema, por lo que esta tesis realiza estudios de caso de carácter exploratorio, a la luz de la teoría institucional, para identificar las condiciones organizacionales del cumplimiento. Para hacer observables los conceptos que derivan de la literatura (Sartori, 2002), los factores reglamentarios, normativos y cognitivos de los pilares de la teoría institucional fungen como guía para el estudio de las variables independientes que explican al cumplimiento, como variable dependiente, en la dinámica de la implementación de las políticas de protección de datos personales dentro de las organizaciones. Por lo tanto:

La variable dependiente, “Y”, es el cumplimiento (CUMP).

Las variables independientes, “X”, son: del pilar reglamentario, sanción (SANC), monitoreo (MONI) y liderazgo directivo (LIDE); del normativo, ética organizacional (ÉTIC) y capacitación (CAPA), y del cognitivo, asimilación de las tecnologías de la información (TIC) y reputación (REP).

Con el fin de alcanzar el cometido de este proyecto de investigación, el presente capítulo expone la estrategia de investigación, que incluye la selección de casos e instrumento, operacionalización de variables y mapa de actores.

Estrategia de investigación

a) Selección de casos

Como se menciona previamente, el propósito de esta tesis de carácter exploratorio es identificar las condiciones organizacionales del papel que desempeñan los factores que motivan el cumplimiento de las políticas de protección de datos personales. Para lograrlo, se desarrolla desde una aproximación cualitativa con estudio de casos, estrategia enfocada en comprender las dinámicas de situaciones particulares (Eisenhardt, 1989), de forma intensiva, a profundidad (Gerring, 2009). Diferentes investigaciones en las Ciencias Sociales han utilizado los estudios de caso por su utilidad para explorar y explicar los comportamientos dentro de las organizaciones (Alina, 2014; Yin, 2011; Adler, Goldoftas & Levine, 1999); por ejemplo, específicamente, Avgerou (2000) analiza el cambio organizacional referente a las TI en Pemex desde la perspectiva institucionalista.

La ventaja de los estudios de casos, a pesar de que han sido desacreditados en comparación con los estadísticos porque no pueden hacerse generalizaciones a partir de ellos (Bunge, 2007), es que permiten explorar mecanismos causales para ver cómo interactúan las variables dependientes e independientes ante la ausencia de estudios empíricos que no ofrecen un anclaje sólido (Gerring, 2009), identificar el comportamiento de las organizaciones con respecto al cumplimiento desde los

individuos entrevistados y plantear preguntas e hipótesis para futuras indagaciones (Cortés, 2008). Mediante estudios de casos, esta investigación pretende platear hipótesis que contribuyan a generar más estudios vinculados con la protección de datos personales en México. Hasta el momento, es un tema poco explorado.

El argumento principal de esta investigación es que la suma de los factores reglamentarios, normativos y cognitivos fortalecen el cumplimiento porque este es integral. Debido a la complejidad de las organizaciones, las reglas, normas y costumbres son indispensables para sus operaciones. Sin embargo, se hace énfasis en que si no existiera una ley que obliga, es posible que la protección de datos personales no se hubiera considerado en el quehacer de las organizaciones en México.

Este planteamiento se explora con la selección de dos casos pertenecientes al sector educativo que permiten observar cómo inciden las variables independientes en el cumplimiento. Por definición, la muestra para un estudio de caso es pequeña y se seleccionan con base en los objetivos de la investigación (Gerring, 2007); Hernández, Fernández y Baptista (1991) afirman que en los estudios cualitativos el tamaño de la muestra no es relevante desde un punto de vista probabilístico, porque el interés central no es establecer generalizaciones a una población más grande sino entender el fenómeno de estudio.

Con base en lo anterior, la pregunta de investigación se responde con la elección de casos que pertenecen a organizaciones privadas, prestadoras de servicios educativos de escuelas que imparten desde preescolar hasta preparatoria en Puebla. Los argumentos para su selección responden a lo siguiente.

Como se explica en el capítulo II, la normatividad que rige al sector público y el sector privado en materia de protección de datos personales es distinta, a pesar de que se trata del mismo derecho. En enero de 2017, el Diario Oficial de la Federación publicó la Ley General para armonizar las leyes estatales, establecer los principios, deberes y obligaciones de los sujetos obligados del sector público y poner este derecho a la altura de su regulación con el sector privado. Aun así, persisten diferencias sustanciales entre las leyes de ambos sectores que se mencionan en el Capítulo II, referentes, entre otros

aspectos, a las sanciones. Por lo tanto, esta tesis se enfoca únicamente al sector privado.

El segundo argumento se basa en que son de este sector económico porque tal es la preocupación a nivel internacional que la 35 Conferencia Internacional de Autoridades de Protección de Datos Personales y Privacidad de 2013 hace énfasis en proteger al sector educativo en la era digital, a la vez que incentiva a las autoridades de protección de datos personales de los países a brindar más capacitación en las escuelas. El proyecto de “Introduciendo temas de protección de datos y privacidad en la Unión Europea” (Arcades, por su acrónimo en inglés) posee esta alma plasmada en la “Conferencia de educar sobre temas de protección de datos personales y privacidad”. En México, el Inai también enfoca sus esfuerzos mediante actividades como el “Concurso infantil para ser Comisionada y Comisionado 2017”, para motivarlos a participar con ideas sobre la protección de datos personales.

Tercero, en nuestro país, para 2016, el sector educativo ocupaba el tercer lugar en incumplimiento. Según datos oficiales, en el comunicado 404 del Inai (2016), el Instituto dio a conocer que, desde la entrada en vigor de la LFPDPPP, en 2012, a noviembre de 2016, había resuelto diferentes Procedimientos de Imposición de Sanciones (Pisan), y en 55 de estos casos impuso una sanción económica a las organizaciones y/o personas físicas. Según sus registros, 36 de estas multas pertenecen al sector de servicios financieros y de seguros (150 millones 826 mil pesos), diez al de información en medios masivos (42 millones 434 mil 347 pesos), y nueve al de comercio al por menor (17 millones 434 mil 347 pesos, de los que, hasta 2015, cuatro pertenecían al de servicios educativos con 10 millones 428 mil 840 pesos).

Lo anterior evidenció que debe atenderse no solo por el incumplimiento, sino además por el tipo de datos que las escuelas recaban, incluyendo datos sensibles de alumnos, familiares y prospectos, como son de identificación, laborales, académicos, financieros, de salud, psicológicos, biométricos, creencias religiosas y características físicas.

Cuarto, las razones por las que se hace en Puebla son, entre otras, por la conveniencia, bajo costo de la investigación y a que la autora ha tenido contacto con

las escuelas. También se realiza un esfuerzo por obtener una muestra representativa con relación a la posición que el estado y municipio ocupan en el Censo de escuelas, maestros y alumnos de educación básica y especial (Cemabe) que realizó la Secretaría de Educación Pública (SEP, 2015), y al nivel de cumplimiento de cada escuela elegida con la LFPDPPP como se describe a continuación.

Quinto, según el Cemabe (SEP, 2015), el estado de Puebla ocupa el tercer lugar en número de centros de educación básica y media superior con 10 mil 578 centros educativos, después del Estado de México y Jalisco (18 mil 983 y 11 mil 996, respectivamente). Esta posición lo hace significativo para ser sujeto de estudio. Otro dato que hace representativo no solo al estado sino, específicamente, al municipio, es que, según el mismo censo, de todos los municipios del país, este concentra el mayor número de alumnos censados, con 353 mil 864 estudiantes de nivel básico.

A pesar de que la selección de casos podía variar sobre la marcha porque es posible que alguno no aportara información —característica propia de la investigación cualitativa—, los autores sugieren que la muestra puede ser de uno o varios casos. Siguiendo el ejemplo de Gray y Silbey (2014) y de Small (2009), del universo de escuelas que reporta el Cemabe en Puebla, para esta tesis se eligieron dos casos representativos para responder a la pregunta de investigación y estudiar a profundidad la variable dependiente.

La selección obedece al principio de máxima similitud en ambos, es decir, son lo más homogéneos posible (Gerring, 2007). Los criterios son:

a) Sector al que pertenecen: privado,
b) Nivel al que pertenecen: imparten desde preescolar a preparatoria (nivel de educación básica y media superior),
c) Tamaño de la organización: el número de alumnos inscritos supera los mil alumnos y el personal administrativo en nómina es equiparable,
d) Costos de inscripción y colegiatura: las cuotas de inscripción y colegiatura están dentro del mismo rango, y
e) Prestigio: las dos son instituciones de reconocida trayectoria.

Principalmente, cumplen con otra condición, que es su situación con respecto a la variable dependiente, el cumplimiento, para lo que Tashakkori y Teddlie (1998) y Gerring (2007) sugieren el principio de máxima diferenciación. De tal forma que se eligen dos escuelas: una que cumple en mayor grado y otra que cumple en menor grado con los procedimientos que indica la LFPDPPP. Analizar casos opuestos fue importante para la investigación porque, si lo que se buscaba era la causa de la implementación, debían considerarse datos positivos y negativos para eliminar el sesgo.

La identidad de las escuelas es confidencial para conservar el anonimato de los resultados. Por lo tanto, la investigación identifica como “Caso 1” a la que cumple en mayor grado y “Caso 2” la que cumple en menor grado.

Para determinar que las escuelas cubrían los requisitos de mayor o menor grado con respecto al cumplimiento, el Anexo 4 detalla qué acciones realizaron de la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Inai, 2014). Esta guía contiene 93 reactivos de comprobación para los principios de licitud, lealtad, consentimiento, información, proporcionalidad, finalidad, calidad, responsabilidad, confidencialidad, seguridad, así como de la relación responsable-encargado y las transferencias.

Esta se contestó con información de los casos seleccionados. El Caso 1 reportó que sí cumple con 76 reactivos, no cumple con diez y siete no aplican. Por otro lado, el Caso 2 cumple con diez reactivos, no cumple con 76 y siete no aplican.

Los datos que se presentan en la siguiente tabla corresponden al ciclo escolar 2016-2017.

SELECCIÓN DE CASOS

	CASO 1	**CASO 2**
Preescolar a preparatoria	Escuela que cumple en mayor grado	Escuela que cumple en menor grado

Particular	Sí	Sí
Número de alumnos inscritos	2,342	965
Personal administrativo en nómina	47	34
Rango de colegiaturas	6,970-10,895 pesos (10 pagos mensuales)	2,344-3605 pesos (10 pagos mensuales)
Reinscripción	18,220-23,810 pesos	3,400-5,100 pesos
Fecha de fundación	1942	1917

Tabla 13 Selección de casos. Fuente: elaboración propia.

El Caso A es una escuela particular que cumple en mayor grado con los procedimientos que indica la Ley señalados en la variable dependiente CUMP, verificados en la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Inai, 2014). Es una institución educativa de prestigio fundada en 1942 e imparte desde nivel preescolar a preparatoria.

El segundo caso es una escuela particular que ha cumplido en menor grado con los procedimientos que indica la Ley. El incumplimiento se sustenta con la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Inai, 2014) (ver anexo 4). También se trata de una institución de prestigio desde su fundación en 1914, que imparte desde preescolar hasta preparatoria.

Es importante destacar que, aunque el número de alumnos y el rango de colegiaturas varía, la selección de casos se sostiene porque ambas son instituciones similares en términos de estructura, las dos brindan servicios de preescolar a preparatoria, son particulares, con trayectoria reconocida que ha consolidado su permanencia en Puebla

y deben proteger los datos personales que están en su posesión en la manera que indica la LFPDPPP. Además de esto, lo que se estudia son los factores que incidieron en la implementación de las políticas de protección de datos personales e, independientemente del número de alumnos inscritos, el proceso de implementación y los requisitos a cubrir son los mismos para ambos casos.

b) Instrumento

Los datos se recabaron con dos instrumentos: entrevistas semiestructuradas y documentación.

Las entrevistas semiestructuradas son útiles para saber los puntos de vista de los entrevistados sobre las variables del estudio y conseguir respuestas detalladas del cumplimiento con las políticas de protección de datos personales a nivel de las organizaciones. Este instrumento da libertad al investigador de realizar preguntas adicionales para profundizar más en el tema y obtener más información porque son más flexibles y abiertas (Hernández, Fernández y Baptista, 1991).

También permite indagar sobre percepciones, motivaciones o expectativas de los sujetos con respecto a las políticas de protección de datos personales en las organizaciones en las que se desenvuelven para conocer los factores de cumplimiento. En la sección de mapa de actores se describen las características, roles y niveles de los sujetos entrevistados.

Chong, en Gerring (2009), defiende la ventaja de las entrevistas sobre los cuestionarios para entender el proceso por el que las personas realizan la toma de decisiones, ya que recopilan evidencia para argumentar la causalidad entre las variables. Aunque las preguntas pueden variar durante las entrevistas y el orden no es necesariamente el mismo que presenta la guía, giran alrededor de las variables elegidas para saber qué papel desempeñan los factores que motivan el cumplimiento de las políticas de protección de datos personales en las organizaciones.

Además, la entrevista es un instrumento ampliamente utilizado en otras investigaciones (Avgerou, 2000; Baptista, 2009; Adler, Goldoftas y Levine, 1999). Las preguntas que se plantean se basan en la teoría y en investigaciones previas vinculadas con el cumplimiento y seguridad de la información, adaptadas a los estudios de casos de esta tesis. Se incorporaron medidas recomendadas por Podsakoff et al (2003, 888) para prevenir el sesgo, referentes a:

1. Aumentar la validez: las preguntas fueron claras y concisas, sin ambigüedad. Para lograrlo, la entrevista se realizó con base en una guía prediseñada con indicaciones claras para su desarrollo.
2. Proteger el anonimato de los casos para mitigar el miedo a ser evaluados. Las variables se eligieron de tal forma que pudieran ser informativas, pero al mismo tiempo no afectar información sensible. Además, se adoptaron medidas precautorias para garantizar la confidencialidad de la información que proporcionaron.

Para complementar las entrevistas, también se pidió examinar documentos de las escuelas participantes en el estudio, como códigos de ética, minutas de juntas, expedientes que hayan generado de alguna solicitud de derechos ARCO y material de las capacitaciones que imparten si es que aplicaban. Esta información fue útil para tener evidencia del tratamiento que hacen de los datos personales. Como fuente, la avalan diversos trabajos (Avgerou, 2000; Baptista, 2009; Adler, Goldoftas y Levine, 1999), además, tienen la ventaja de que es información que generan los propios sujetos que participan en la investigación (Hernández, Fernández y Baptista, 1991).

La expectativa de las entrevistas y documentación es obtener información detallada sobre el cumplimiento de las políticas de protección de datos personales para comprobar (o no) la hipótesis planteada y explorar a fondo el papel que desempeñan los factores reglamentarios, normativos y cognitivos para establecer mecanismos causales. A pesar de que con los resultados obtenidos no puedan hacerse

generalizaciones, sí pueden dar pie a nuevas hipótesis para futuras investigaciones que aporten al tema.

c) Operacionalización de variables

Las variables de este estudio provienen de la revisión de la literatura y de la teoría institucional. El siguiente apartado las hace operables desde otras investigaciones que dan validez a las preguntas y justifican su aproximación metodológica.

i. Cumplimiento

Dado que esta tesis se refiere específicamente al cumplimiento esperado de una ley, sus procedimientos son los que indican el grado de conformidad por parte de las organizaciones. Al respecto, uno de los propósitos del estudio de Deloitte (2014) fue identificar el nivel de cumplimiento de los sujetos obligados con la LFPDPPP en México. Para hacer operable esta variable, planteó preguntas sobre si las organizaciones cumplieron o no los deberes que indica la ley. Con este mismo fin, el Inai (2014) generó la "Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares", que apunta los procedimientos que deben realizar los sujetos obligados referentes a los principios de licitud y lealtad, consentimiento, información, proporcionalidad, finalidad, calidad, responsabilidad; deberes de confidencialidad y seguridad, y obligaciones ligadas a las transferencias.

ii. Sanción

La LFPDPPP contiene artículos dedicados especialmente a la imposición de sanciones en caso de que los sujetos obligados incumplan o cometan alguna infracción (ver Capítulo II). Lo que se espera en esta investigación es que las sanciones afecten a las organizaciones de tal manera que las obliguen a cumplir con las políticas de protección de datos personales, independientemente de que las interioricen o no. Es decir, la

sanción se asocia positivamente con el cumplimiento organizacional. Esta investigación se aproxima a la variable con base en Mwakabinga (2008).

iii. Monitoreo de actividades

Como parte del pilar reglamentario de la teoría institucional, se busca saber si su ausencia afecta al cumplimiento, bajo la premisa de que el monitoreo está asociado positivamente a él. Las preguntas que hacen operable esta variable son adaptaciones de Mwakabinga (2008) y Siddiki, Basurto y Weible (2012) al caso mexicano.

iv. Liderazgo directivo

Del liderazgo, como lo mencionan los autores, también se espera que afecte positivamente a la implementación.

v. Ética organizacional

Para el análisis de la ética en las organizaciones, otros estudios de caso, como el de Alina (2014), evalúan los códigos de ética y conducta implementados por tres organizaciones. Las preguntas para el estudio de esta variable se desarrollaron con base en las aportaciones conceptuales de los autores.

vi. Capacitación

Como señala la literatura, la capacitación incide de forma positiva en el cumplimiento. Para hacerla operable, esta investigación utiliza los conceptos antes mencionados con base en Mwakabinga (2008).

vii. Asimilación de las tecnologías de la información y comunicación (TIC)

Para medir la familiaridad, conocimiento y clima de las TIC en las organizaciones que las vincula con el cumplimiento de las medidas de seguridad que indica la LFPDPPP (Capítulo II), Boynton, Zmud y Jacobs (1994) plantean preguntas que esta tesis adapta para sus fines.

viii. Reputación

De los reactivos desarrollados para operacionalizar esta variable con base en los autores, adaptada al caso de la protección de datos personales en México, se espera encontrar una incidencia positiva en el cumplimiento.

Con las variables y sus reactivos, esta investigación busca conocer su influencia en el cumplimiento mediante la metodología descrita en el siguiente capítulo. La guía de preguntas completa se presenta en la siguiente tabla.

CUESTIONARIO

Variable	**Preguntas**
Cumplimiento	1. ¿Cómo se enteraron de que hay una Ley de Datos Personales con la que deben cumplir? 2. ¿Cuáles han sido las razones por las que la organización cumple con la ley?
Sanción	3. Conoce las multas, ¿sabe las consecuencias de no cumplir con la ley? 4. Las multas de van desde los 100 a los 320 mil días de salario mínimo (vigentes en la Ciudad de México). ¿Qué tanto influyen para que la organización cumpla con los procedimientos que indica la Ley?
Monitoreo	5. ¿Han recibido alguna inspección por parte de una autoridad/superior para verificar el cumplimiento de la protección de datos personales? ¿Cómo ha sido? 6. ¿Qué tan importante sería que una autoridad como el Inai monitoree periódicamente las actividades de la organización con respecto al uso que hace de los datos personales?
Liderazgo	7. ¿En quién recayó la decisión de implementar la ley en su organización para proteger los datos personales? 8. ¿Cómo propicia la dirección el cumplimiento con la protección de los datos

	personales en la organización? ¿Cómo cuidan que, efectivamente, se cumpla con lo de datos personales?
Ética	9. ¿Cómo fomentan el tratamiento ético de los datos personales? 10. ¿Alguna vez han hecho algo como comprar bases de datos para contactar a posibles usuarios o le han ofrecido dinero a cambio de una base de datos que pertenece a la organización? Si no, ¿qué haría en el supuesto de que ocurriera? ¿Cómo contactan a nuevos clientes?
Capacitación	11. ¿Con qué frecuencia realizan programas de capacitación para incrementar el conocimiento sobre las reglas del uso de los datos personales? ¿Cuándo fue la última vez que les dieron capacitación? 12. ¿Estar capacitado sobre cómo usar los datos personales tiene algún impacto en el tratamiento que se hace de ellos en la organización? 13. ¿Qué hacían antes de la ley qué hacían para proteger los datos personales? ¿Qué hacen ahora?
TIC	14. ¿Qué prácticas implementa la organización para garantizar la protección de los datos personales con las TIC? 15. ¿Han tenido alguna fuga de información como archivos o bases de datos desde computadoras o el servidor que haya afectado a la organización? ¿Cómo lo han resuelto? ¿Qué problemas han tenido o qué han mejorado? ¿Cómo estaban antes?
Reputación	16. ¿Qué tan importante es para la organización que sus clientes confíen que sus datos personales están seguros? 17. ¿Qué tipo de actividades realizan en la organización para que sus clientes conozcan el tratamiento que hacen de sus datos personales? 18. ¿Alguna vez han realizado actividades como llamar o enviar correos electrónicos a sus prospectos sin su consentimiento? Preguntar sobre el procedimiento de

	prácticas para enviar publicidad.

Tabla 14 Cuestionario. Fuente: Elaboración propia.

La guía completa de la entrevista como se realizó con el entrevistado está disponible en el Anexo 5.

d) Mapa de actores

El capítulo III define a las organizaciones como un conjunto de personas que trabajan en coordinación para alcanzar una meta. Parte del insumo que requieren para el cumplimiento de sus objetivos son los datos personales; el siguiente diagrama ilustra cómo puede ser el flujo de la información personal dentro de una organización:

DIAGRAMA DE FLUJO DE DATOS PERSONALES EN UNA ORGANIZACIÓN

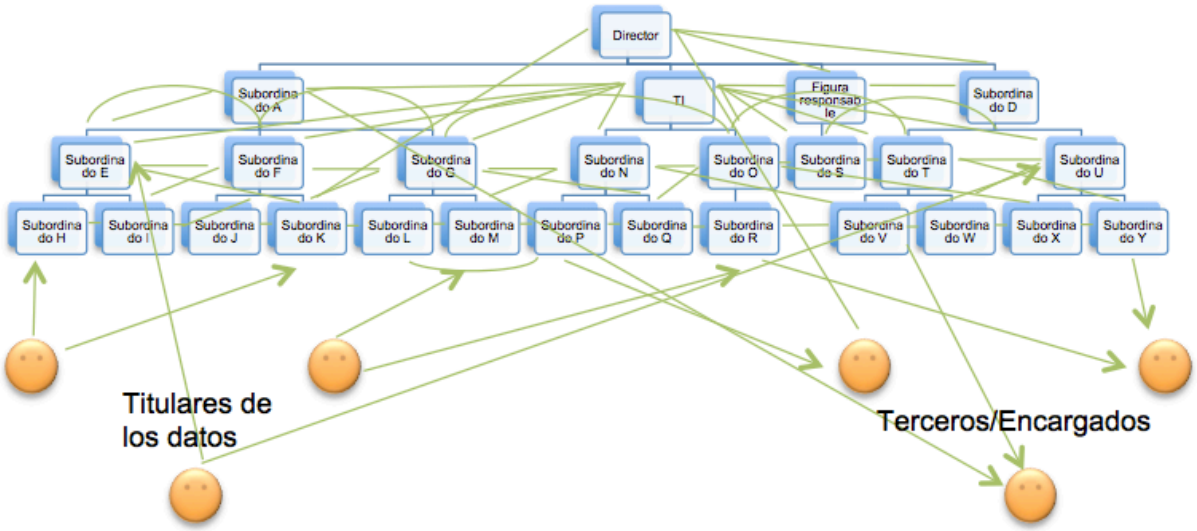


Tabla 15 Diagrama de flujo de datos personales en una organización. Fuente: elaboración propia.

Como se aprecia, dentro de una organización, los datos personales fluyen constantemente desde el momento en el que el titular los proporciona para cumplir con distintos fines determinados, establecidos en el Aviso de Privacidad. Por ejemplo, una base de datos de fotografías de los titulares (pueden ser empleados o usuarios), para la que se contrata a una compañía (encargado), puede compartirse al interior de la organización y con terceros para distintos fines: al departamento de seguridad para tener acceso e identificación, al área de diseño para credenciales, con el personal de otras áreas para identificar a sus miembros, al área de TI para subir las fotografías a algún portal interno, también se comparte con otro proveedor para impresión de materiales diversos o con alguna autoridad correspondiente en caso de que lo soliciten, que deberán brindar las mismas medidas de seguridad a los datos.

En algunos casos, los miembros de la organización únicamente tendrán acceso, en otros podrán modificarlos e, incluso, podrían sustraerlos o cruzarlos con otras bases de

datos disponibles que hagan más identificables a los titulares si no se cuenta con las medidas de seguridad adecuadas.

Con la aparición de la LFPDPPP, se hizo indispensable que las organizaciones tomaran la decisión de implementar las políticas de protección de datos. Como lo define Rainey (2009), corresponde a la parte directiva guiar las estrategias que la estructura organizacional debe seguir. Por esta razón, las entrevistas se realizaron a la parte directiva de las dos organizaciones que estuvieron involucradas con la toma de decisión de implementar (o no) las políticas.

Sin embargo, fue importante que las entrevistas no se realizaran únicamente a los directivos o a la figura del responsable porque, como señala la literatura, aunque exista un interés genuino, es posible que no sea el mismo para los individuos en diferentes niveles y esto afecta el cumplimiento de la organización (Foorthuis y Bos, 2011). En palabras de Parsons (2007), el cumplimiento de una política también tiene un contexto organizacional en el que los individuos toman parte. Para ejemplificar esto, en su investigación, Avgerou (2000) entrevistó a subdirectores y los miembros de sus áreas, al director general de TI y a sus subdirecciones, el gerente de TI en el corporativo y al equipo directivo de TI dentro y fuera de la sede. Alkabani et al (2016) también afirman que encuestar a personas con distintos roles en las organizaciones robustecen y generalizan los resultados de una investigación.

Por lo tanto, las entrevistas se aplicaron a personas que ocupan distintos cargos directivos dentro de las escuelas, así como a quienes están vinculados con el tratamiento de los datos personales, que desempeñan un papel importante en el proceso de cumplimiento de la ley: director/gerente, subdirecciones, persona responsable de los datos personales, director de TI o similar, responsables de áreas.

Del Caso A, se entrevistó a la Dirección General, Dirección de Tecnologías de la Información, Dirección de Recursos Humanos, Dirección Administrativa, a la persona designada como Responsable de los datos personales, a la responsable del área de Admisiones, responsable de Becas SEP y a la responsable de la Consejería y Comité de Inclusión de Preescolar.

Del caso B, se entrevistó a la Dirección General, Dirección de Secundaria, Psicopedagogía, Contador General, Becas y Difusión, Responsable de Informática y asistentes de secundaria y preparatoria.

Cabe destacar que en los estudios de caso no existe un número de entrevistas indicado, sino un mapa de actores apropiado. Por lo tanto, las entrevistas que se realizaron fueron las indispensables para obtener la información que se buscaba con respecto a la incidencia de los pilares de la teoría institucional en el cumplimiento con la Ley. Concluyeron en el momento en el que comenzó a repetirse en ambos casos. En total, fueron dieciséis, con una duración entre 30-40 minutos cada una.

Entre la documentación revisada de cada caso se encuentra:

Caso 1:

- Avisos de Privacidad Integral en sus diferentes versiones (para padres de familia, para el personal y proveedores)
- Código de Ética
- Contrato con proveedores
- Solicitudes de beca institucional y SEP
- Formato de inscripción

Caso 2:

- Aviso de Privacidad
- Contrato de prestación de servicios del bachillerato no escolarizado
- Contrato de prestación de servicio de maternal
- Formato de inscripción de maternal, preescolar, primaria, secundaria y bachillerato
- Contrato de prestación de servicios de preescolar, primaria, secundaria y bachillerato
- Procedimiento para coordinar la inscripción

- Formato para trámite de ayuda institucional o beca SEP
- Código de ética y políticas de trabajo

A continuación, el siguiente capítulo da a conocer los resultados de las entrevistas realizadas a los actores seleccionados, y se discute cada una de las variables desde la perspectiva institucional.

CAPÍTULO VI

RESULTADOS

Este capítulo tiene por objetivo dar a conocer los resultados obtenidos de las entrevistas realizadas a los actores participantes de los Casos A y B, cuya selección se describió en el capítulo anterior.

En primer lugar, se presenta lo más relevante de las respuestas de Caso A. En segundo lugar, se describen los resultados del Caso B. Finalmente, a partir de ambos casos, se establece un diálogo con la teoría para conocer la incidencia en cada una de las variables.

Caso A

Cumplimiento

En marzo de 2011, los directores de las áreas (Dirección General, Administrativa, Tecnológica, Deportiva, de Preescolar, Primaria, Secundaria y Preparatoria) asistieron a una conferencia que organizó la firma de servicios profesionales, Deloitte México, para dar a conocer los mandatos de la entonces nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares. En esta, recibieron información sobre los cambios que tenían que implementar para el resguardo de los datos personales y los tiempos con los que debían cumplir. Para complementar, verificaron las acciones que realizó la asociación de colegios a la que pertenecen y los lineamientos de otros actores que podían repercutir, como Derechos Humanos y la Secretaría de Educación Pública (SEP).

Entre sus primeras actividades, el Caso A dio cumplimiento al artículo 30 de la ley, referente a designar a una persona o departamento de datos personales, para que diera trámite a las solicitudes de los titulares para el ejercicio de los derechos ARCO. Inicialmente, nombraron a una persona del área de Relaciones Institucionales bajo la

supervisión de la Dirección Administrativa. Posteriormente, debido a movimientos internos de la organización, se designó a la Jefatura de Normatividad como el área responsable de la protección de datos personales, que así se denomina en adelante.

Otra actividad que realizaron fue generar los Avisos de Privacidad para los padres de familia, personal y proveedores, y mantenerlos actualizados conforme a los lineamientos del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Inai). Estos cumplieron con los requisitos del ABC del Aviso de Privacidad que emitió el órgano garante en 2013. La última versión del Aviso publicada en la página web de la organización para los padres de familia, corresponde al 15 de agosto de 2016[6].

De acuerdo con la Dirección General, el motivo principal para el cumplimiento fue "que ya había una ley y tenías que cumplir con ella, punto". Como consecuencia, verificaron los lineamientos que debían observar, como el tiempo de conservación de la información o qué tipo de datos podían pedir a los padres de familia para no ser excesivos, y la implementaron.

A continuación, se describen las variables independientes que explican este cumplimiento, seleccionadas a partir de la teoría institucional.

Liderazgo

Loa entrevistados coincidieron en que la decisión de implementar la ley la tomó la Dirección General, "todos los asuntos que tienen que hacerse siempre los da la Dirección General". Su primera acción fue determinar quién podría ser la persona responsable de los datos, aunque reconocieron que es una responsabilidad institucional.

También confirmaron que algo clave para el cumplimiento dentro de la organización fue el interés del área directiva, específicamente de la Dirección de Finanzas en ese momento.

[6] El Aviso de Privacidad Integral del Caso 1 está disponible en el Anexo 4.

De acuerdo con los entrevistados, desde un principio, la dirección se involucró en la implementación en cien por ciento. También reportaron que el director les informa frecuentemente sobre las nuevas leyes y las pautas a seguir. Específicamente, se enteraron de la ley desde el mismo año en que se publicó. “La institución no es de las que deja de lado esto, sale algo nuevo e inmediatamente nos informan”, declaró la Jefatura de Normatividad, responsable de la protección de datos personales.

Actualmente, en la organización, los procedimientos de la ley corresponden a la Jefatura de Normatividad en colaboración con todas las direcciones. Con respecto a su desempeño, hay quien considera que debería darles más información y retroalimentación porque es el área inmersa en el tema. “Creo que debería estar diciendo: ‘miren, está esta certificación’, para que las direcciones estén pendientes, no caer en un estado de conformidad y no confiarse de que ellos lo están checando”. Asimismo, en entrevista, la Dirección Tecnológica, mencionó que: “nosotros también debemos estar al pendiente de detalles porque por algo empezó el área de informática en esta situación”.

Por otro lado, para el cumplimiento de la ley, en el ámbito digital, la Dirección de Recursos Humanos destacó que es muy oportuno que la Dirección Administrativa sea muy abierta para hacer cambios importantes en la escuela.

En este caso en particular, los entrevistados compartieron la idea de que el liderazgo se comprometió con el tema, lo que provocó un impacto positivo en el cumplimiento de la ley. Como lo señala la literatura, para que la organización alcance sus objetivos, es necesario que existan líderes que la conduzcan hacia ellos. Por tanto, la decisión de la Dirección General de atender los requerimientos para la protección de los datos personales, fue fundamental. Es pertinente destacar que esta determinación por parte del liderazgo también obedeció a factores como la sanción, entre otros, que se describe a continuación.

Sanción

Las multas también fueron un factor preciso para el cumplimiento. Cuando se preguntó sobre el conocimiento e influencia de las multas y las sanciones, la Dirección General manifestó: “yo no quiero estar en la cárcel ni quiero que el Colegio ande rodando por infringir esta nueva ley en repetidas ocasiones”.

Por su parte, la Dirección Tecnológica del Caso 1 comentó que no recuerda exactamente cómo ni cuándo supieron de la Ley, pero que en ese momento los datos personales estaban resguardados con medidas de seguridad altas y niveles de consulta para cada usuario. Sin embargo, al conocer las consecuencias posibles de que los datos estuvieran a la vista, sí causó preocupación porque, a pesar de que se informaron oportunamente, no sabían con exactitud cómo operaba la ley.

“Surgió la situación de temor, en su momento, por la cuota que se iba a manejar, no recuerdo cuánto era, pero se iba a manejar un castigo…”. La entrevistada reportó que, hace siete años, lo que motivó que implementaran la ley “en un principio fueron las multas. También era cárcel, eso fue lo que realmente nos movió, no porque no nos importara proteger los datos, porque los teníamos realmente resguardados”.

Aunque hubo otros factores determinantes para cumplir con la ley, la figura responsable de la protección de datos del Caso 1 también hizo énfasis en la importancia de las multas: “Primero por las multas, porque si no cumples con la ley, ya sabes; segundo, la seguridad de la comunidad escolar y, tercero, los beneficios que tiene que todos estemos en un ambiente seguro”. De acuerdo con la entrevistada, el motor de la implementación fueron las sanciones, porque todo tenía que estar para una fecha determinada. También recordó los spots amenazadores del órgano garante cuando se emitió la ley.

A pesar de que la Dirección General asumió el cumplimiento y de que, como responsable en la organización, proyectó las sanciones y las consecuencias, la Jefatura de Normatividad percibe que los miembros de las direcciones todavía no las dimensionan. Esto es porque han identificado descuidos que vulneran la seguridad de

la información. Por ejemplo, tienen reportados casos en los que algún profesor dejó abierto el sistema de calificaciones en la computadora de su salón de clases. Por su parte, el Departamento de Admisiones afirmó que el personal conoce con claridad que existen multas en caso de no cumplir con la ley y el problema en el que podría involucrarse el Colegio y el personal mismo en caso de hacer algo fuera de la línea.

Ligado a lo anterior, el contrato laboral hace referencia a una sanción legal en caso de incumplimiento, pero hasta el momento de las entrevistas no se había presentado ningún caso que hiciera necesaria su aplicación.

Para recapitular, cabe concluir que la coercitividad de las sanciones fortaleció el cumplimiento con la ley a nivel organizacional, como un factor racional/reglamentario del enfoque institucional. La sanción cumplió con su cometido de inducir a los individuos al comportamiento esperado, ocasionado por el temor.

Monitoreo

Con respecto al monitoreo, ninguna instancia institucional, como correspondería al Inai o a la SEP, ha monitoreado el cumplimiento de la ley. Es un tema que la escuela ha dilucidado con la ayuda de despachos, abogados, la asociación de colegios a la que pertenecen o autoridades por iniciativa propia.

En una ocasión recibieron a miembros del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Puebla (Itaip), para dar cursos a padres y alumnos. Sin embargo, no se concretaron porque no tuvieron espacio en su calendario y únicamente se reunieron con los directores.

Hay casos concretos en los que la organización entrega información a instancias gubernamentales, por ejemplo, bajo orden judicial, en situaciones de divorcio o a la SEP, cuando les requiere datos de los alumnos y sus padres. Antes de hacerlo, solicitan asesoría de sus abogados para saber si la tienen que proporcionar y cómo deben proceder.

Por su parte, la organización no ha establecido ningún mecanismo formal para verificar el cumplimiento. La Dirección General lo atañe a la falta de recursos, de tiempo y que es una sola persona la encargada del tema (la Jefatura de Normatividad). A pesar de que inicialmente la Dirección Tecnológica estuvo muy involucrada con dar cumplimiento a la ley, reconoce que de cuatro años a la fecha se desconectó del tema porque hay un departamento responsable de los datos personales dentro de la escuela que es la Jefatura de Normatividad. Sin embargo, considera que sí sería importante que existiera algún monitoreo frecuente por parte de alguna autoridad o dentro de la misma escuela que dé seguimiento a sus actividades.

La teoría señala la necesidad de tener "árbitros" que verifiquen el cumplimiento. A pesar de que el órgano garante no monitorea qué sujetos obligados de la ley cumplen o no con ella, está la amenaza latente de su facultad sancionadora. Por esta razón, en este Caso 1, el monitoreo se percibió desde su aspecto positivo, es decir, como el aliado para indagar sobre nuevas disposiciones que coadyuven al cumplimiento, con el fin de prevenir el castigo económico de las multas y la pérdida de confianza de sus clientes.

Ética

La conciencia de manejar información privada fue lo primero que motivó a la dirección general a cumplir con la ley. En palabras del director general:

> "No puedo dejar un expediente volteado para que tú puedas decir que la persona que acaba de salir que vino a arreglar esto o a solicitar prórroga para su pago. No tienes por qué saberlo, ni la nómina. En mi caso en particular, ese fue el factor principal que me dijo, ah, caray, esto tiene que ver con proteger a terceros que han depositado la confianza en esta institución de la cual yo soy responsable".

Referente a esto, hizo una comparación con las leyes de tránsito:

> "Cobro conciencia de que ponerme el cinturón de seguridad me protege a mí; si se lo pongo a mi nieto y a mi hijo es para prevenir que en un accidente resulte algo terrible. Claro que si por no llevarlo hay una multa y si no quiero pagar esa multa me lo tengo

> que poner, pero primero es cobrar conciencia de por qué está esa ley. Si no la cumplo y está esa multa, pues más merezco".

Los demás entrevistados confirman el valor de la ética para la organización cuando aseguran que el tratamiento de los datos personales recae en el deber ser, puesto que las escuelas son formativas, no destructoras. Por lo tanto, la ética es un valor fundamental para el cumplimiento dentro de la institución. Cada una de las personas que trabajan allí están porque confían en ellos y porque son personas responsables que avalan sus valores y los del colegio, tanto por ética como por lo que proclama la institución. Una entrevistada del área de psicopedagogía comentó:

> "Como Colegio, uno de nuestros valores es la honestidad, y dentro de esta honestidad es tener mucho cuidado con datos muy particulares de las familias. Por un lado, la ética como parte de los valores del colegio y, por otro, la ética personal, por tu formación y desempeño académico. Por ejemplo, como psicóloga tengo acceso a datos muy, muy personales y debo tener cuidado con la confidencialidad. No puedes comentar los datos con cualquier persona".

Según palabras del área de Admisiones, la Escuela 1 transmite la ética a través de todo el desempeño. Les dejan muy clara cuál es la filosofía y la misión de la organización, así como el manejo de los datos personales, que ha sido más específico a través de los años. Por ejemplo, debido a la ley, ahora cuentan con el Aviso de Privacidad. Conocen lo que deben hacer en el área, actúan por ética y siempre están en contacto con la Jefatura de Normatividad para hablar sobre alguna situación en particular, bajo confidencialidad y privacidad.

Además, la escuela cuenta con un Código de Ética y un reglamento, aunque la Dirección de Tecnología señaló que no hay seguimiento al manual y que, posiblemente, si lo consultaron, lo hicieron la primera vez. También firman un documento en el que declaran que ellos son responsables de los datos personales y que deben usarlos con confidencialidad.

Como conclusión, la ética es un valor presente en el desempeño profesional de quienes conforman la organización. Aun antes de la ley, protegían la información bajo

el precepto de la privacidad por principios de ética; mas a partir de la ley, se demostró que la norma estuvo supeditada a la regla porque esta reforzó el valor del deber ser ético.

Capacitación

La organización recibió capacitación explícita para directivos por parte del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Puebla (Itaip) y del Inai, y para el personal administrativo por parte de la Jefatura de Normatividad. La última capacitación fue al inicio del ciclo escolar 2016, cuando entró el personal nuevo. Al respecto, esta jefatura reportó que “cada ciclo escolar es picar piedra porque a lo mejor un nuevo maestro no sabe y, si tiene sentido común, cuida los datos personales, si no, empezamos de cero”.

A pesar de que desde un inicio la organización se preocupó por dar cumplimiento a la ley y de que actualmente cuentan con un área responsable específica, que es la Jefatura de Normatividad, la Dirección Tecnológica señaló que, desde hace dos o tres años, no ha recibido indicaciones ni actualizaciones porque, a opinión suya, se encuentran en un estado de confort. “Esperaría retroalimentación continua, por lo menos que nos digan que estamos igual que el año pasado, para que estemos pendientes. También sé que esto no es de una sola línea, nosotros también deberíamos pedir esa información, lo cual no hemos hecho”.

Los entrevistados reportaron que la organización siempre había visto por la seguridad de la información aun antes de la ley. Sin embargo, a partir de ella han adoptado diferentes disposiciones para darle cumplimiento. “Tratamos de proteger y que lo que hacemos tenga que ver con las indicaciones que tenemos para asegurar ser lo más congruentes posible con nuestro sistema”, manifestó el área de Admisiones.

Entre las principales acciones que realizaron a partir de la ley fue generar el Aviso de Privacidad, que colocaron en diferentes puntos para que esté a la vista en todas las áreas en distintos formatos, como en los contratos de prestaciones de servicios, en Caja, Admisiones y la página web. “Si no estás de acuerdo (con el tratamiento que se

hace de tus datos personales), hay consentimiento para que digas no estoy de acuerdo, pero si vas a trabajar o estudiar en la escuela, tienes que firmar", afirmó la Dirección General.

Para el personal, el Aviso de Privacidad está disponible en el portal interno al que acceden con usuario y contraseña. Es obligación de la organización comunicar esto a los empleados desde el inicio de su relación laboral y se renueva anualmente. Los proveedores, de igual forma, están informados del uso que se hace de sus datos personales.

El Caso 1 tomó todas estas medidas porque, como comentó la Dirección General, "imagínate que escuchan en la radio o cualquier cosa, y nos preguntan qué van a hacer con los datos de salud, por ejemplo, así les quitamos la incertidumbre de qué hacemos con ellos, acceden al Aviso y ahí dice, por ejemplo, que es para las becas". Además del Aviso de Privacidad, el Código de Ética también incluye un apartado referente al tratamiento de datos personales.

Antes de la ley sí se daban datos del personal o las familias cuando los solicitaban, aunque se ignora si hablaban con el director o si había un documento de por medio. La Jefatura de Normatividad manifestó que: "hemos cerrado filas, cualquier información cruzada, tienen que preguntarme a mí y ya veo si se puede proporcionar o no".

También realizan actividades como no tener información a la vista, guardar todos los expedientes bajo llave, no proporcionar datos sin la acreditación como lo señala la ley, mantener los datos personales actualizados, y aun para el personal de la organización, si requieren información adicional a la que tienen acceso, siempre se les pregunta para qué la solicitan.

Otra de las actividades que cambiaron fue que, por ejemplo, antes publicaban las listas de calificaciones afuera de los salones para que pudieran consultarlas y eso exhibía a los estudiantes, ahora esa es una práctica prohibida. La privacidad de las fotografías de los estudiantes fue otro punto de atención, especialmente por las redes sociales.

Por otro lado, algunos alumnos de preparatoria son mayores de edad y ellos tienen el derecho de autorizar el manejo de sus datos personales. Por lo tanto, establecieron lineamientos para tener su consentimiento para que su tutor tuviera acceso a sus calificaciones.

También determinaron el tiempo que el personal de cada área puede conservar las bases de datos y qué debían hacer con la documentación una vez que concluye su finalidad. Antes de la ley no tenían considerados estos aspectos, pero al inicio de cada ciclo escolar, ahora hacen énfasis en ellos.

En entrevista al área de Psicopedagogía, sabe que, en caso de pérdida o fuga de datos personales, debe reportarle a su directora y a la Dirección General; tiene indicaciones sobre lo que debe de hacer, mas no está establecido en ningún protocolo. Reconoce la conveniencia de tener políticas o lineamientos específicos en lo que corresponde a cada área, y justificantes por escrito que reflejen que han entregado la información y a quién. Hasta el momento estas acciones no se han desarrollado porque la Jefatura de Normatividad está conformado por una sola persona y no tiene la capacidad suficiente para llevarlas a cabo.

Por otro lado, el área de Admisiones reportó que, cuando un padre de familia solicita información sobre su hijo vía telefónica, por procedimiento hacen preguntas clave para confirmar su identidad. A pesar de que es una indicación muy clara con la que deben cumplir, no hay un monitoreo, pero es un protocolo establecido.

La Dirección de Recursos Humanos tenía cinco meses en el cargo en el momento de la entrevista. Reportó que, desde que ingresó, no había recibido capacitación formal. El uso discrecional que hacía de los datos personales obedecía más a las indicaciones que le dejó la persona que anteriormente estaba en el cargo: “Lo poquito que conozco es que debemos proteger todos los datos que nuestros colaboradores traen”.

Esta área identificó claramente quién es la persona responsable de la protección de datos personales, es decir, la Jefatura de Normatividad, pero no había recibido capacitación: “No tengo conocimiento de cuánto tiempo debo conservar los

expedientes, en mi empleo anterior eran relacionados con quince años de archivo muerto". Por la antigüedad de la organización, conservan archivos desde hace cuarenta años. No cuentan con un procedimiento que indique qué hacer con los archivos. "Aquí todo es muy hablado, entendido, pero no hay nada escrito, por eso apenas estoy planeando los procedimientos", y explicó que hay actividades que realizan porque "toda la vida lo hemos hecho así. Eso es una barrera muy fuerte para innovar".

El área de Psicopedagogía recordó que la última capacitación general que tuvieron fue hace cinco años, cuando les notificaron qué podía suceder en caso de cometer una falta. Aunque no han tenido capacitaciones recientes, desde entonces, en su área, constantemente los actualizan y les indican con qué deben tener cuidado y qué información pueden solicitar a los padres de familia. Además, constantemente reciben indicaciones de la Jefatura de Normatividad. Saben que Psicopedagogía trabaja con datos personales muy delicados porque son evaluaciones de los alumnos y entrevistas con padres de familia que utilizan en consejería.

Un caso que evidenció la necesidad de que existan procedimientos formalmente establecidos en la organización, es que las entrevistas de psicopedagogía con los padres de familia generalmente son escritas y, en ocasiones, este pide tomarle una fotografía o solicita una copia. La indicación que tiene el área es de proporcionarla, pero no genera ningún documento en el que conste que la entregaron con firma de recibido.

La transición para cumplir con las medidas establecidas ha sido paulatina. Han pasado seis años desde que apareció la ley y desde entonces han implementado nuevas disposiciones, según se han requerido. "Ha habido más cuidado en los detalles, aunque no es de la noche a la mañana", según palabras de la Dirección General. Por su parte, la Jefatura de Normatividad considera que el hecho de que hasta el momento no hayan tenido que responder ninguna solicitud de derechos ARCO, significa que es señal de que sus capacitaciones han tenido resultado en el cumplimiento.

Para concluir, las prácticas que fomentan la protección de los datos personales han servido para asentar el cumplimiento de las políticas en la organización, porque de acuerdo con los entrevistados, logró permear el deber ser de la privacidad y el cuidado de la información. Sin embargo, para que siga surtiendo efecto, es necesario que la Jefatura de Normatividad programe capacitaciones con más periodicidad para abarcar al personal que se incorpora y reafirmar el cumplimiento.

Incorporación de las TIC

El sistema de bases de datos con los que cuenta la Escuela 1 es muy robusto; cada año invierten mil dólares para mantenerlo actualizado. La Dirección General es quien autoriza todo lo que se implementa en materia de las TIC para proteger la información, pero delega la mayor parte de la decisión a la Dirección Tecnológica. Según palabras de la Dirección Tecnológica, nunca han tenido robos de información, generan respaldos diarios y cuentan con las medidas de seguridad técnicas que requiere la ley: “Siempre hemos tenido la certeza de que nuestros datos están protegidos”. Sin embargo, no cuentan con ninguna certificación “porque a lo mejor no es tan necesaria”.

Por su parte, la Dirección de Recursos Humanos consideró que antes no habían incorporado más las TIC porque “el empleado era muy consentido y se preocupaban mucho más por la comodidad del empleado, que por lo que estaba sucediendo en avances tecnológicos”. Por esto, opinó que en algún momento la organización se quedó atrás, pero se está actualizando, porque “el director es una persona muy abierta para que todos esos cambios ayuden a que el colegio tenga ese crecimiento tecnológico, pero la escuela arrastra la falta de apertura o la visión para digitalizar la información desde hace tiempo”.

Como punto débil, la Jefatura de Normatividad ignora si han invertido en sistemas de seguridad de la información porque atribuye que es función de la Dirección Tecnológica, aunque está consciente de que deberían de trabajar nuevamente en coordinación. Sin embargo, sabe que las áreas académicas tienen cierto acceso a la información, y si requieren datos y no están a su disposición, tienen que llenar un

formato en el que los solicitan. Si lo amerita, se les da, pero afirmó que no cualquiera puede tener acceso a una base de datos.

Un área que no resguarda debidamente su información es la de becas. Durante cada ciclo escolar, almacena el contenido de alrededor de 250 solicitudes de becas, de preescolar a secundaria, en una memoria externa (Universal Serial Bus-USB) y en archivos impresos. Si se perdiera esa USB ocasionaría un problema muy serio para la organización porque contiene información sensible de los padres de familia.

En ocasiones, la Dirección Tecnológica le ha cuestionado qué pasaría si llegara a perder la USB y le ha planteado la posibilidad de subir la información a la nube. Al respecto, comenta que la principal dificultad es que el programa que usa para procesar su información no es compatible con todos los sistemas operativos de los distintos planteles y no tiene un área fija para realizar su función, por lo que siempre depende de que le designen un equipo y espacio para trabajar.

Por otro lado, el Comité de Inclusión planteó generar un archivo general digital que abarcara desde preescolar a preparatoria, que solo puedan utilizar en Consejería o las personas autorizadas dependiendo de los departamentos, pero sin subir a la nube la información. Hasta el momento de las entrevistas, su proyecto estaba en proceso de planeación.

Con respecto al uso de aplicaciones de mensajería instantánea y redes sociales, el Caso 1 fomenta la incorporación de las TIC para un desempeño más eficiente de sus funciones. No obstante, ha tenido que establecer nuevas reglas sobre casos específicos, como no difundir datos personales de sus estudiantes en los grupos de WhatsApp, en los que participan miembros del Colegio y padres de familia, para no exponerlos.

A pesar de que en el Caso 1 permea el deber ser de la protección de los datos personales y de que cuentan con sistemas de bases de datos robustos, se encuentra con una limitante ante la falta de asimilación del uso adecuado de las TIC. Desde el

punto de vista institucional, los miembros de la organización no han interiorizado sus beneficios y esto podría generar brechas en el cumplimiento.

Reputación

El Caso 1 es una escuela con más de 70 años de trayectoria, por lo que la Jefatura de Normatividad, manifestó que “muchos vienen a aprender con nosotros, siempre ha sido una institución que procura ir a la vanguardia”.

La Jefatura de Normatividad del Caso 1 reconoce que en la comunidad no había mucha conciencia sobre el tratamiento de los datos personales, pero esto ha cambiado con el tiempo, porque los padres de familia solicitan con frecuencia que sus hijos no salgan en las fotografías, cuando antes estas prácticamente pasaban de mano en mano. Atribuye este resultado al trabajo del colegio en difundir las medidas de privacidad: “No sé en qué porcentaje, pero de los que he visto, han tenido respuesta favorable, de más conciencia”.

Para el Caso 1 es muy importante que los papás sepan que sus datos están protegidos porque ellos lo preguntan. Por esta razón, hacen énfasis en esto constantemente. No se los entregan a nadie sin su consentimiento, solo recaban los datos que necesitan e informan cuál es la finalidad de su tratamiento. El colegio cuida la confidencialidad de la información de sus alumnos. Si el padre de familia dice que no autoriza que sus hijos aparezcan en fotografías, es una negativa rotunda en la organización.

Para el Caso 1 es importante brindar a los papás la confianza de que sus datos personales están resguardados correctamente. Cuando los requieren en caso de disputas por patria potestad, por ejemplo, la dirección correspondiente es muy cuidadosa para hablar con el padre de familia para ver qué necesita, pero no se entregan sin filtros. Uno de ellos es pedir algún documento que valide la información requerida o una orden del juez.

La información que proporcionan los padres de familia es confidencial, y ellos agradecen y valoran que por teléfono les hagan preguntas para validar su identidad antes de darles cualquier información cuando la solicitan por este medio. Siempre

hacen énfasis en que es por su seguridad y se les notifica que pueden consultar el Aviso de Privacidad.

El Caso 1 es una escuela reconocida en Puebla, por eso en un inicio le preocupó que los padres de familia confiaran en que sus datos personales estaban seguros. Hay familias con niveles socioeconómicos altos; la fuga de información podría exponer la integridad del propio estudiante o de sus familiares. Lo mismo en caso de que se difundiera que algún alumno tiene un padecimiento, porque la información podría utilizarse de forma inadecuada. Según la Dirección Tecnológica, fue de los aspectos que también motivaron cumplir con la Ley.

Como lo señala la teoría institucional, los factores cognitivos son esenciales para el cumplimiento. Cuando los individuos interiorizan el valor del resguardo adecuado de los datos personales, esto se refleja en la reputación y, como consecuencia, aumenta la confianza en la relación organización-cliente. Por lo tanto, para cuidar la reputación de la organización es necesario cuidar los datos personales que poseen porque, con esto, generan confianza.

Para recapitular, desde la perspectiva institucional, la fusión de los tres pilares —reglamentario, normativo y cognitivo—, da más consistencia y fuerza a los resultados esperados, sin embargo, hay uno que puede predominar. En el Caso 1 en particular, destacaron las variables independientes del pilar reglamentario sobre las del normativo y el cognitivo. Específicamente, la coercitividad de la sanción demostró su capacidad de generar presión sobre los directivos para obligarlos a cumplir con la ley. Esto, sin hacer de lado otros factores que también fueron fundamentales, como la ética y la reputación de la organización. En la sección de discusión que se presenta más adelante, se presentan más argumentos al respecto.

A continuación, se presentan los resultados del Caso 2.

Caso 2

Cumplimiento

La implementación de las políticas de protección de datos personales en el Caso 2 ocurrió en febrero de 2013, cuando publicaron su Aviso de Privacidad, por el que pagaron en un sitio web que ofrecía el servicio de generarlos con costo (500 pesos). A decir de los entrevistados, cumplieron porque una "instancia" lo pidió —refiriéndose al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales—, pero a partir de entonces, no se le ha dado mayor seguimiento.

Los entrevistados narraron, cada uno por su cuenta, cómo ocurrió la implementación. Por ejemplo, uno clave, el contador general, detalló que el Inai mandó correos para invitarlos a cumplir con la ley, al igual que Hacienda, también se enteraron por los spots en la radio. Por su parte, la Dirección General recordó que: "yo supongo que nos dijo la SEP, nos explicaron esto de los datos. Se pagó por Internet, al banco, a la instancia".

La asistente de la Dirección General fue la persona que se encargó de realizar el trámite para pagar el Aviso de Privacidad, y la misma que se designó como la responsable de la protección de datos personales, para dar respuesta a las solicitudes de derechos ARCO, como lo indica el Aviso de Privacidad[7], en cumplimiento con la ley. Sin embargo, a tres años de que ya no labora en la organización, este no se ha modificado.

A continuación, se presentan los resultados de las variables que definen el cumplimiento en el Caso 2.

Liderazgo

A pesar de que el director general ha tomado las decisiones para implementar los requerimientos de otros organismos públicos, como el Sistema Estatal de Protección

[7] El Aviso de Privacidad del Caso 2 aparece en el Anexo 5.

Civil[8], y de que siempre se ha preocupado por cuidar los requerimientos legales, como lo señaló el Contador General, el tema de protección de datos personales no ha tenido el mismo interés. El propio director general indicó que: “No nos hemos interesado, seamos sinceros… Quizá no valoramos esas instancias que pone el Estado, si las pone supongo que es porque se han robado datos, pero en esta escuela no se fijan”. Esto es porque desde que la ley entró en vigor, no han recibido ninguna visita de ninguna instancia que verifique su estatus de cumplimiento.

La falta de atención al tema la perciben los demás miembros de la organización, quienes reconocen que los responsables de implementar (o no) son los administrativos (la Dirección General), porque esa área implanta los procesos.

El director de la escuela reconoció que no se involucró con la ley desde su aparición por falta de interés, sino que delegó el tema a la asistente que estaba en ese momento, quien investigó y le notificó al Contador General para que realizara el pago para generar el Aviso de Privacidad.

Esta información la confirman más actores de la organización. Según palabras de otros entrevistados, como la Dirección de Secundaria, en un inicio la Dirección General les dio a conocer quién era la persona responsable de la protección de datos personales y que ya estaba el aviso de privacidad, pero a quien este señala ya no labora en la organización y no se ha actualizado: “No sé si ya está estipulado porque esto se tiene que hacer por ley, se tiene que dar de alta, dar de baja el otro, no lo sé”.

Además, agregó que necesitan implementar algo más para que la gente tenga conciencia del tema, y atañó esta decisión a la cabeza de la organización, es decir, la Dirección General. Asimismo, apuntó que es necesario que la persona que está directamente como responsable (aunque no logró identificar quién es) debe involucrarse más en el proceso.

[8] Que establece medidas de prevención enfocadas a salvaguardar la integridad física de las personas que se encuentran en el inmueble ante una situación de alto riesgo.

Los miembros entrevistados de la organización coincidieron en que la decisión de instruir tendría que bajar desde la Dirección General a todas las áreas: “Yo creo que desde la Dirección General puede instruirnos a todas las secciones para que se cumpla mejor (la ley)”, indicó el Contador General. Un entrevistado más de la Dirección de Secundaria también afirmó que es indispensable que la Dirección General le dé seguimiento, “sabemos que es importante, pero no nos ha caído el veinte de que es muy importante”.

La Dirección General de esta institución atribuyó la falta de cumplimiento con la ley a la poca información sobre las consecuencias que podía haber para la escuela, pero principalmente, a que “esto es de humo”, como lo expresó en sus propias palabras, porque, desde que se implementó la ley, no han recibido ninguna inspección que verifique su cumplimiento y los sancione. En este caso, destacó que el director ignora cuál puede ser el castigo por incumplimiento, porque cuando se le preguntó si conoce las consecuencias de no cumplir con la Ley, su respuesta fue: “Seguramente multas, como todo”.

Lo mismo ocurrió con los demás entrevistados, quienes también desconocen las sanciones. Sin embargo, la dirección de Secundaria opinó que “el cumplimiento ocurrió porque es una obligación, no obstante, el proceso de implementación fue difuso”.

Al igual que en el Caso 1, en el Caso 2 el liderazgo también desempeñó un papel fundamental, pero para que la escuela cumpliera en menor grado. La falta de interés que en repetidas ocasiones señaló la Dirección General, también estuvo motivada porque no percibió a las sanciones como una verdadera amenaza. Como lo señala la teoría, cuando las sanciones no se aplican y no existe un monitoreo, la regla pierde su fuerza coercitiva, tal y como ocurrió en esta organización.

Sanción

La Dirección General de esta institución atribuyó la falta de cumplimiento con la ley a la poca información sobre las consecuencias que podía haber para la escuela, pero principalmente, a que “esto es de humo”, como lo expresó en sus propias palabras. En

este caso, destacó que el director ignoraba cuál puede ser el castigo, porque cuando se le preguntó si conoce las consecuencias de no cumplir con la Ley, su respuesta fue: “Seguramente multas, como todo”.

Lo mismo ocurrió con los demás entrevistados, quienes también desconocían las sanciones. En palabras de la Dirección de Secundaria, “el cumplimiento ocurrió porque es una obligación, no obstante, el proceso de implementación fue difuso”.

A pesar de que la teoría resalta que hay motivos muy racionales para el cumplimiento, en el Caso 2 las sanciones no tuvieron la fuerza suficiente para mover al liderazgo, porque no representaron una amenaza latente. En parte, esto se debió a la falta de monitoreo del órgano garante ni de ninguna otra instancia, que verifique y sancione, como lo muestran los resultados a continuación.

Monitoreo

La falta de interés en cumplir con la ley se observa en que, desde febrero de 2013, fecha en que le pagaron a una empresa para que les generara un aviso de privacidad —que por ley debía estar desde enero de 2011—, no han recibido ninguna inspección por parte de ninguna autoridad como el Inai o de la SEP, como lo manifestó la Dirección General. Esto también provocó que no se informaran más sobre las actividades que deberían realizar:

“Claro que no (me preocupa), estamos en 2017, ¿y quién ha venido aquí? Ha venido Protección Civil, la Secretaría del Trabajo y de todos tengo diez, diez con todos los requisitos de auditoría, seguridad e higiene. Esto (la protección de datos personales) es de humo”, fueron palabras de la Dirección General. Lo que muestra que la falta de monitoreo por parte de una instancia gubernamental fue fundamental para que la organización decidiera no cumplir a cabalidad con las especificaciones de la ley.

Ética

A pesar de no cumplir estrictamente con la ley, llama la atención que, de acuerdo con la Dirección General, “los datos personales no se democratizan demasiado”, es decir,

no los comparten con bancos ni organizaciones, además de la SEP. Tampoco se los dan a los padres de familia y los conservan en un sistema de organización de datos y en expedientes por escrito con la idea de resguardarlos y no malversar información. Este era el mismo tratamiento que hacían de los datos, incluso, antes de la ley, “porque nosotros no dilapidamos datos, la gente tiene derecho a su privacidad, eso ya lo hacemos desde hace muchos años”.

La Dirección General reportó que solamente usan los datos para lo que se deben de usar, como los trámites escolares, y añade que los papás lo saben, puesto que nunca han tenido ninguna queja por parte de ellos.

La Dirección de Secundaria manifestó que: “Nosotros, como profesionistas, inmiscuidos en la educación, se les hace saber (al personal) del cuidado y el nivel de compromiso que tenemos al tener una información que es personal”. A pesar de que no han recibido capacitación formal, “es una práctica que hacemos diario, no damos información de más”.

Esto lo confirmó otro entrevistado del área de Psicopedagogía:

> “en esta área de la escuela, los datos personales se tratan con confidencialidad y solo las personas encargadas tienen acceso. Ahora, desde la ética, nosotros no compartimos información. Somos una escuela de valores que son parte de nuestra misión y visión, nos quedan tan claros que nadie nos dice que debemos portarnos éticamente, se da por parte del colegio”.

Además, el Contador General expresó que, por tratarse de una escuela, siempre han tratado los datos personales de los alumnos con ética, protegiendo su privacidad. Como medida de seguridad, antes de contar con el aviso, si alguien solicitaba datos, tenía que enviar una carta dirigida al director general, y el reglamento interno le decía al personal cómo deben informar al exterior lo que es importante.

En palabras del entrevistado del Departamento de Becas y Difusión, para garantizar la privacidad de la información se conjuntaron la ética profesional, la formación y la experiencia. Derivado de eso, tenían que estar conscientes de las consecuencias que

podía ocasionar el tratamiento inadecuado de los datos personales, tanto para la institución como para el mismo alumno, como el daño moral o la pérdida de confianza por parte de los padres de familia. Para la Dirección General, el cumplimiento “no está por escrito, es un acuerdo tácito de palabra”.

La persona a cargo del Departamento de Informática asumió que la responsabilidad de implementar y dar cumplimiento a la ley es de la Dirección General, aunque compartió la visión de que, al ser una escuela, están basados en valores como el respeto, la honestidad y la ética, “desde el principio nuestros estándares son de ética”.

En el Caso 2, la protección de los datos personales obedeció, sobre todo, a la ética más que a la coercitividad de las sanciones o el monitoreo. Esto es porque ante la ausencia de un monitoreo que obligara al liderazgo al cumplimiento, los valores de la organización condujeron a sus actores a actuar con responsabilidad para proteger la información de la matrícula.

Capacitación

A pesar de que la ética es una causa por la que protegen los datos personales en el Caso 2, no han desarrollado otras actividades para resguardarlos adecuadamente, como la capacitación, ni por iniciativa propia en congruencia con la ética, ni por dar cumplimiento a la Ley.

Incluso, el director no recordó con exactitud cómo se enteraron de la LFPDPPP. Al preguntarle esto, contestó: “Supongo que nos dijo la SEP, nos explicaron esto de los datos”. Y, con respecto a cómo generaron el Aviso de Privacidad, expresó que: “Al banco, se paga por internet al banco, a la instancia”, contestó, suponiendo que la “instancia” a la que le pagaron es el órgano garante, es decir, el Inai. Pero la confusión se evidencia porque el generador del Aviso de Privacidad del Inai es gratuito.

Asimismo, ante la falta de capacitación, la información no se comunicó adecuadamente al personal de la organización, a quienes el Aviso se les dio a conocer por “el letrero grande, no más” (con referencia al Aviso de Privacidad antes mencionado). No

indagaron de qué se trataba la ley y únicamente les avisó a los directores de cada nivel en una junta en la que les dio a conocer el Aviso de Privacidad.

La falta de capacitación se atribuye a la falta de interés de la Dirección General en el tema. Se hizo evidente cuando se le preguntó si conocía los derechos ARCO y qué haría si un titular de los datos personales desea ejercerlos. La respuesta fue: "¿Derechos qué?", y "¿entiendo que quisiera un papá que se borraran sus datos? Pues concederlo, tranquilamente, si una persona pide que los eliminemos, los eliminamos", ignorando las condiciones que la ley establece específicamente para el derecho de cancelación.

Información similar es la que se recabó de otras áreas, como la Dirección de Secundaria, que se enteraron de la ley por los medios de comunicación o por pláticas con conocidos de cuando el Inai empezó a exigir a todas las instancias el cumplimiento.

Las entrevistas evidenciaron que el cumplimiento ocurrió de manera tardía y que el personal no recibió capacitación adecuada: "Hace cuatro ciclos escolares (2013) se publicó el documento que avalaba que ella (a quien señala el aviso de privacidad) era la persona con la cual se podían dirigir y que llevaba el control de todo esto", apuntó la Dirección de Secundaria. A pesar de que periódicamente hacen reuniones por área (consejos técnicos), tratan temas generales, pero capacitaciones en sí sobre el tema, no han tenido.

Otros comentarios del área de Psicopedagogía corroboraron la respuesta: "Había una persona responsable que se encargó de dar información y de decir que la escuela estaba protegiendo los datos, pero más allá de la información de la página web, no hubo una capacitación formal".

Además, los integrantes del Caso 1 entrevistados confundieron al Inai con la empresa que les ofreció el servicio de generar el aviso de privacidad. Según el contador general, "primero nos mandaron la invitación y ya pagamos para hacer el trámite y nos lo mandaron por correo, lo imprimimos primero en un papel grande y nos dieron la

instrucción de ponerlo en la entrada de la escuela y nos dijeron que si teníamos algún dominio en internet ponerlo a la vista de todos".

A lo anterior, cabe aclarar que el generador de avisos de privacidad del Inai es gratuito. Hubo otras empresas ajenas al órgano garante que sí promovieron ese servicio con costo.

Además, ignoraban en qué momento se realizó alguna actividad concerniente a la ley. Sabían que el aviso de privacidad está en la página, que lo mencionan en algunos documentos en los que piden datos personales, pero también hay quien no sabía que cuentan con este y desconocen quién es la persona a cargo o qué actividades se han realizado. El Departamento de Becas y Difusión comentó que, "hasta donde yo sé, creo que podría ser el mismo administrativo o la Dirección General".

Están conscientes de que es necesario estar capacitado porque es un tema delicado. No se ha hecho por falta de interés de la Dirección General. En particular, en algunas áreas que conservan información durante diez años, como la de becas, desconocen qué pasó con los archivos previos a ese periodo o cómo se van a desechar los expedientes que solo tienen vigencia de un año.

La falta de capacitación fue muy evidente en el Departamento de Informática, que no tenía conocimiento de la ley, lo que se demostró cuando se le preguntó por los derechos ARCO y respondió que no sabía de qué se tratan. También ignoraba si hay sanciones, no sabía si alguna autoridad monitorea y, como consecuencia, tampoco realizaba ninguna actividad para monitorear al interior de la escuela. Además, afirmó que es una escuela muy tradicional porque las actividades para proteger los datos personales antes y después de la ley no han variado.

Este factor influyó en que el cumplimiento en la organización se dé en menor grado, pero obedece a que a la Dirección General no le dio la importancia necesaria. Esto confirmó que es necesario que las organizaciones cuenten con líderes que las lleven al alcance de sus objetivos.

TIC

La escuela cuenta un sistema de organización de datos propio desde hace quince años. Solo el Departamento de Informática tiene acceso a toda la información; los departamentos únicamente tienen acceso a lo que les corresponde. Esto confirma su compromiso con la seguridad de los datos personales, mas no con la ley. La Dirección General mencionó que: “Nunca hemos recibido ningún aviso de informática para decirnos que se robaron los datos, no tenemos paranoia”, misma que le atribuye a la ley.

No obstante, la ética con la que trataban los datos personales no es suficiente al momento de acatar medidas de seguridad. Como mencionó el área de Psicopedagogía: “Nosotros tenemos un proceso de cinco años que, a lo mejor, alguien puede venir y llevárselo… No tenemos un candado específico, más que nuestras claves de acceso, pero es muy fácil clonar”.

El Departamento de Informática, a pesar de la evidente falta de conocimiento de la ley, consideró que el tratamiento que hacen de los datos personales es muy bueno. Desde su punto de vista, en comparación con otras escuelas, están muy seguros porque no tienen datos cargados en la nube, por lo tanto, no los pueden vulnerar. Sin embargo, no realizan pruebas de seguridad.

Incorporar las TIC para garantizar la seguridad de los datos personales es esencial para cualquier organización. Desde el punto de vista institucional, su infraestructura debería coadyuvar con el cumplimiento en la medida en que los individuos asimilen sus beneficios y utilidad. En el Caso 2, en particular, contaban con un sistema con el que están familiarizados desde hace quince años. Esto les da la confianza de que su información está resguardada de manera segura, aunque identificaron huecos que podrían ocasionar fuga de información.

Reputación

Aunque se trata de una escuela con trayectoria “reconocida durante muchos años”, en palabras de la Dirección General, “en esta pobre escuela no se fijan”. Esto es porque

desde que se publicó la ley, no han recibido ninguna visita de una instancia gubernamental para evaluar el cumplimiento.

La Dirección General mencionó que para la escuela es importante cuidar debidamente los datos personales y la privacidad de la información. Al preguntarle si los papás estaban enterados de cómo los protegen, contestó que sí se les dice, “ese letrero de ahí lo leen mucho” (señala a una versión impresa del Aviso de Privacidad), aunque, continúa, “claro, 80% no se fija en el nombre de la secretaria, que era la anterior, la que pagó el aviso”. Actualmente, la secretaria que señala el Aviso como la persona responsable de la protección de datos personales, que dependía de la Dirección General, ya no labora en la organización, sin embargo, no se ha actualizado.

Las actividades que han realizado para cumplir con la ley no reflejaron la importancia que el director señala que tienen los datos personales y su privacidad. En sus propias palabras, “quizá no es tan coherente, lo mínimo es que no dilapidamos sus datos”. Es decir, cumplen con acciones mínimas, como tener un Aviso de Privacidad —no actualizado—, y la capacitación se ha limitó a avisar a los directores sobre el mismo.

A pesar de que más entrevistados opinaron de manera similar al afirmar que para la institución es muy importante que los papás sepan que sus datos personales están protegidos porque les da tranquilidad, el supuesto interés no va de acuerdo con las acciones emprendidas, por lo que reconocen que necesitan implementar algo más para que la gente tenga conciencia del tema.

La reputación es un factor importante para la escuela porque simboliza la confianza que los padres de familia tienen en ella, sin embargo, las actividades que realiza para cumplir con la ley son insuficientes para demostrar la importancia que los entrevistados afirman en torno a la seguridad de los datos personales. “Yo creo que debe estar nivelado a ambos lados porque todos los que estamos acá manejamos datos, pero no está nivelado, hace falta información, más conciencia entre los maestros y el administrativo para darle importancia”, reconoció el Departamento de Becas y Difusión.

Sobre la reputación, del Caso 2 destaca el hecho que, de acuerdo con los entrevistados, la reputación de la organización es muy importante. Desde el punto de vista institucional esta creencia debería ser equivalente a las medidas que adoptan para garantizar el cumplimiento con la ley, porque se ubica dentro del nivel cognitivo, en el que el este se ha interiorizado. No obstante, no es así. Esto podría explicarse a que en la organización están comprometidos éticamente con la protección de los datos personales y la privacidad de la información, mas no con la ley, porque su coercitividad no produjo el efecto esperado.

En general, el Caso 2 evidencia que las sanciones no fueron lo suficientemente efectivas para lograr que la Dirección General cumpliera en mayor grado con las políticas señaladas por la ley. Esto en parte se debió a la falta de un monitoreo por parte del órgano garante, que ocasionó que la amenaza del castigo menguara. Sin embargo, como afirma la teoría, el cumplimiento puede deberse a una combinación de factores. En este caso, la ética fue un elemento del pilar normativo que reemplazó al reglamentario.

La siguiente tabla resalta lo más relevante con respecto al comportamiento de los factores de cada pilar, en cada caso estudiado.

FACTORES QUE INCIDIERON EN EL CUMPLIMIENTO DE LAS POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES EN LOS ESTUDIOS DE CASO

	Caso 1	**Caso 2**
Pilar reglamentario	El liderazgo tomó parte activa en el cumplimiento para que se desarrollaran los procedimientos de la ley Existió voluntad de la Dirección General Las sanciones ejercieron presión coercitiva sobre el liderazgo La falta de monitoreo por parte del órgano garante, que ejecuta	Si no hay monitoreo, la amenaza de la sanción no ejerce coerción sobre el liderazgo La falta de compromiso del liderazgo impide el cumplimiento A pesar de que las sanciones son elevadas, si no se perciben como una amenaza no producen resultados

	las sanciones, se compensó con el aspecto positivo del monitoreo, porque lo vieron como un aliado para realizar consultas	
Pilar normativo	La protección de datos personales es compatible con la ética de la organización Las medidas adoptadas en las capacitaciones para proteger los datos personales han dado resultados positivos Las capacitaciones periódicas fortalecen el cumplimiento	La ética de la organización impulsa la protección de los datos personales porque es compatible con sus valores La falta de capacitación puede originar una brecha en el cumplimiento porque se desconocen los procedimientos de la ley
Pilar cognitivo	La asimilación de las TIC fortalece el cumplimiento La falta de la misma puede ocasionar brechas en el cumplimiento La reputación de la organización es clave para el cumplimiento porque la hace confiable	La familiaridad con las TIC coadyuva al cumplimiento Las brechas en las TIC pueden ocasionar brechas en el cumplimiento La organización percibe que la reputación es importante para tener la confianza de sus clientes

Tabla 16 Factores que incidieron en el cumplimiento de las políticas de protección de datos personales en los estudios de caso. Fuente: Elaboración propia.

Discusión

El cumplimiento de las políticas de protección de datos personales en las organizaciones depende de diversos factores que, por sí mismos, no son suficientes para explicarlo. La literatura se afianza en diferentes variables dependiendo de la teoría desde la que se estudia. En particular, los pilares de la teoría institucional hacen énfasis en los factores reglamentarios, normativos y cognitivos que ofrecen un panorama para su análisis.

Los hallazgos de esta investigación confirman la influencia de las reglas, normas, y costumbres en el comportamiento de las organizaciones, específicamente, en el ámbito del cumplimiento de una ley. Aunque no es posible generalizar por tratarse de dos

casos de estudio, los resultados pueden ser útiles para fomentar el tratamiento adecuado de los datos personales y encaminar nuevas investigaciones.

Para encaminar el análisis y el diálogo con la teoría, en primera instancia, es necesario identificar si el pilar reglamentario, efectivamente, es el que ejerce mayor influencia en el cumplimiento por su efecto restrictivo y sancionador, como se plantea en la hipótesis, o si el normativo y cognitivo también pueden tener la misma influencia.

Como comienzo, las tres variables seleccionadas del pilar reglamentario tienen efectos distintos en cada caso. Por las respuestas de los entrevistados, es posible afirmar que el pilar reglamentario no ejerció la misma fuerza sobre el Caso 2 como ocurrió en el Caso 1. Esto se discute con mayor profundidad a continuación.

En particular, en el caso 1, que cumplió en mayor grado, se percibió más influencia de la sanción y el liderazgo. Ambos factores fueron fundamentales para el cumplimiento, tal y como lo describieron los entrevistados. Sin embargo, la ausencia de una entidad que opere como “árbitro” para vigilar su desempeño pareciera no afectar negativamente, porque se compensó con el papel de los directivos, de las sanciones y de la ética institucional para nivelar la balanza.

En este sentido, hay opiniones que difieren con respecto a qué predominó más, si la sanción o la ética la que motivó la seguridad de los datos y el cumplimiento de la ley. No obstante, hubo respuestas que dieron más peso a las multas cuando afirmaron “yo no quiero estar en la cárcel”, o “las multas, en un principio fueron las multas”, por lo que es pertinente recordar en este diálogo que la teoría enfatiza el valor de la coacción para el cumplimiento, por el impacto que tiene en los actores, tanto en los directivos como en el resto del personal.

Cuando la teoría señala que las leyes ejercen presión formal en los directivos para que implementen las reglas, se consuma en el caso 1 con suficiente fuerza, al grado de que se aseguraron de que los departamentos e individuos cumplieran con las disposiciones de la ley, porque, de lo contrario, la organización y el propio individuo pueden derivar

en una acción legal: “Primero por las multas, porque si no cumples con la ley, ya sabes”.

¿Habrían cumplido inmediatamente, como ocurrió, si la ley no fuera sancionadora? Es pertinente recordar que la legislación mexicana de los particulares, establece multas que ascienden a los 320 mil días de salario mínimo, el doble cuando se trata de datos sensibles o de reincidencia e, incluso, prisión. Por lo tanto, las multas jugaron un papel determinante para que la parte directiva decidiera dar cumplimiento, tal como lo señala la teoría, puesto que es coercitiva.

El Caso 1 cumplió con la ley en cuanto supieron de ella. Los entrevistados señalaron que, desde un principio, la dirección se involucró en la implementación en cien por ciento. “Todos los asuntos que tienen que hacerse siempre los da la Dirección General”. Perciben al liderazgo como “abierto”, “involucrado”, interesado en el tema”, “comunicador”, “no es de los que deja de lado…”. Esto contribuyó positivamente a hacer legítimo el cumplimiento, porque, además apegarse al sistema de reglas para evitar las sanciones, también era necesario que el liderazgo actuara favorablemente para que la regla institucional prevaleciera en la organización.

De acuerdo con la literatura, una organización no alcanza sus metas con efectividad a menos que la dirija un líder adecuado; es parte fundamental porque se vincula con el compromiso, satisfacción, confianza, y genera aceptación de una nueva disposición. Esto quiere decir que, si desde la cabeza de la organización se aceptó la nueva ley y desde ahí se transmitió a sus miembros, hay mayor posibilidad de aprobación, como ocurrió en el caso 1, donde el conocimiento de la ley y la conciencia sobre la protección de los datos personales permeó en todas las áreas, como se apreció en las entrevistas.

Al respecto, es evidente que, si el liderazgo no hubiera tomado la decisión, los procedimientos de la ley no se habrían implementado, por lo que se confirma su influencia en el cumplimiento, como parte del pilar reglamentario. En el Caso 2, por su parte, el liderazgo no activó el cumplimiento porque los otros dos factores reglamentarios, que eran el monitoreo y la sanción, no ejercieron presión.

¿Qué hay del monitoreo? Como lo indican los artículos 38 y 39 de la LFPDPPP, el INAI es el órgano que difunde, promueve y vigila el derecho a la protección de datos personales. Como se analizó con anterioridad, el Inai únicamente desempeña un papel promotor y ejecutor que emite multas cuando existe un presunto incumplimiento de algún principio o disposición de la ley. No monitorea qué sujetos obligados cumplen con la ley y cuáles no.

No obstante, el hecho de que el órgano garante no monitoree, en el Caso 1 no demeritó el cumplimiento, porque, en primer lugar, estaba la amenaza latente de la imposición de sanciones y, en segundo lugar, la dirección se comprometió con el cumplimiento.

De manera similar, al interior de la organización identificada como Caso 1, tampoco establecieron mecanismos de monitoreo formales, pero los entrevistados hicieron hincapié en que conocen las consecuencias si cometen alguna infracción y en cómo también interviene su ética personal y profesional.

El monitoreo no debe percibirse solo como una actividad para infundir miedo, sino que el supervisor también puede ser visto como un aliado a quien consultar. En una situación así, el incumplimiento disminuye si existe una relación de cooperación, como lo confirmaron los entrevistados con respecto al área designada Responsable dentro de la organización, con la que tienen acercamiento cuando existe alguna duda con respecto al tratamiento de los datos personales, o con el jefe inmediato. “En mi caso, mi jefa siempre está muy al pendiente, ella está súper atenta a cualquier duda que tengamos, estamos en contacto constante; no es necesariamente un monitoreo, pero nos dice que nuestro protocolo es ‘este’”.

Asimismo, el Caso 1 buscó asegurar que la implementación que realizó era la adecuada, tanto con la capacitación gratuita del órgano garante, dirigida específicamente al sector educativo, como con la guía de asociaciones a las que pertenece y despachos.

En este sentido, el monitoreo, en el Caso 1, desempeñó el papel positivo de aliado más que de castigador. Por lo tanto, sí puede aseverarse que este rol influyó en el cumplimiento de la ley.

¿Ocurrió lo mismo en el caso 2? No. Así como en el caso 1, la sanción, el liderazgo directivo y el monitoreo fueron factores determinantes para el cumplimiento de la ley, en el Caso 2 ocurrió lo contrario, principalmente, por el liderazgo, que fue un factor importante de cumplimiento mínimo con la ley, como lo señalaron los entrevistados.

En el Caso 2, la dirección general dio instrucción de cumplir con la ley, sin embargo, no se cercioró de que el proceso se implementara adecuadamente porque lo delegó a la asistente particular que tenía en ese entonces y no le dio seguimiento. De 2013, cuando le pagaron a una página web generadora de avisos de privacidad, a la fecha, este no se ha actualizado. Incluso, conserva al nombre de la misma persona que se hizo cargo en ese entonces, como Responsable de dar trámite a las solicitudes de derechos ARCO, cuando ya no labora en la institución.

A pesar de que, efectivamente, hubo una instrucción de cumplir con el aviso y de que algunos documentos, como la solicitud de beca, hacen mención al tratamiento de los datos personales, la dirección general no se preocupó por instruir adecuadamente al personal. Los entrevistados coincidieron en que implementar los procedimientos de la ley debería ser responsabilidad de la dirección, "…yo creo que desde la dirección general puede instruirnos a todas las secciones para que se cumpla mejor".

Parece contradictorio que hayan mencionado que la dirección general siempre se ha preocupado por cuidar todos los requerimientos legales, pero, particularmente, al tema de protección de datos personales no prestó dio el mismo interés. Incluso, la propia dirección general mencionó que ha cumplido con lo que establecen otras instancias, como Protección Civil, pero reconoce que en cuanto a la ley de datos personales "no nos hemos interesado, seamos sinceros". Esto ocurrió porque, como se mencionó anteriormente, la amenaza de las sanciones fue efectiva, el miedo se disipó ante la ausencia del monitoreo que verificara el cumplimiento.

Esta falta de cumplimiento encuentra explicación no solo en el liderazgo sino también en los otros dos factores que se estudiaron del pilar reglamentario, que tampoco ejercieron fuerza suficiente sobre la dirección para llevarla hacia el cumplimiento. El monitoreo inexistente de ninguna autoridad fue clave en el Caso 2. La dirección general mencionó que, año tras año, tienen una evaluación de Protección Civil Municipal y, aunque afirma que cumplieron no solo porque los califican anualmente, sino por voluntad propia, el monitoreo constante en esta área sí los obligó a cumplir, a diferencia de lo que ocurrió con la ley de datos personales.

Incluso, la misma dirección general del Caso 2 hizo énfasis en que no han recibido ninguna inspección por parte del órgano garante para verificar el cumplimiento. Por lo tanto, se cuestiona si falta de monitoreo fue un factor determinante. Sí lo fue, a tal grado que ni siquiera las multas de la ley tuvieron el impacto esperado porque el órgano garante no vigila qué sujetos obligados cumplen y cuáles no. Sin embargo, esto no quiere decir que la coercitividad de la ley no tuvo peso, por el hecho de que, aunque el Caso 2 no estableció el proceso en cien por ciento, sí se ocuparon de implementar algunas medidas como el aviso de privacidad, porque era algo que debían tener por ley.

El hecho de que no hayan implementado en mayor grado como lo hizo el Caso 1, visto desde el punto de vista del pilar reglamentario, pareciera un círculo vicioso entre el liderazgo, el monitoreo y las sanciones. Es decir, el liderazgo no cumplió con implementar en mayor grado porque el órgano garante no monitorea y solo impone sanciones ante un presunto incumplimiento.

Con esto, se demuestra la importancia del pilar reglamentario en el cumplimiento. Como lo afirma la teoría, es necesario que exista un líder que encamine a las organizaciones hacia sus objetivos. En ocasiones, este andar hacia el cumplimiento puede estar motivado por reglas coercitivas, en este caso una ley, que establecen mecanismos para garantizarlo, y de procesos que lo vigilen. En otras palabras, si el líder no encamina a la organización, no solo al alcance de sus metas sino también al

cumplimiento de las reglas, por más que están existan, no son efectivas si no hay un liderazgo adecuado ni un sistema de monitoreo.

Pero estos no son los únicos factores que intervinieron en el cumplimiento. En esta investigación también se consideraron variables del pilar normativo, que explica el "deber ser" de las cosas, con mecanismos o caminos para alcanzar los objetivos de la ley, que hacen que los mandatos de la ley se interioricen.

Entre estos caminos del pilar normativo para alcanzar el cumplimiento, se encuentran la ética y la capacitación. Principalmente la ética, fue un factor que sirvió para reforzar las medidas adoptadas en el Caso 1 y subsanar las carencias ocasionadas por la falta de interés del liderazgo en el Caso 2.

Los entrevistados del Caso 1 repetidamente hicieron mención de la ética como un aspecto positivo a favor del cumplimiento. Tanto la ética de la institución como la ética profesional y personal de los trabajadores los movió a hacer uso adecuado de los datos personales.

Esta ética deriva de los valores del Caso 1, que permean desde el liderazgo a todo el personal. Antes de la publicación de la ley, la organización contaba con algunas medidas para proteger la documentación y fotografías de su matrícula, "siembre había tranquilidad de que el Colegio actuaba con principios éticos de responsabilidad". Mas una vez publicada la ley, cobraron conciencia de que tenían en su posesión información privada. La dirección general manifestó que se percató de la confianza que terceros depositaban en la institución de la cual él es el responsable.

La literatura describe que el líder que se conduce éticamente y lo demuestra mediante sus actos, lo transmite a sus seguidores y el comportamiento se replica. Tal efecto lo confirman los miembros del Caso 1, "…por ética también debes tener en confidencialidad los datos de la familia", "nos transmiten la ética a través de todo el desempeño", "somos personas responsables que avalamos nuestros valores, estamos cumpliendo con los valores del Colegio, tanto por ética como por lo que proclama la institución". De esta manera, la ética reforzó el cumplimiento con la ley.

De manera similar, en el Caso 2 la ética sirvió para remediar las carencias en el cumplimiento. Por tratarse de instituciones educativas, parte fundamental de su enseñanza está basada en la ética y los valores. “Somos una escuela de valores que son parte de nuestra misión y visión, nos quedan tan claros que nadie nos dice que debemos portarnos éticamente, se da por parte del Colegio”.

Es necesario destacar que, en este caso, la ética coadyuvó con la ley para proteger los datos personales, porque “entra tu formación, la experiencia, y derivado de eso sabes qué problemas puedes ocasionar a la institución y al mismo alumno, entonces ya hay una responsabilidad, no estás tratando con cualquier información”. Es decir, lo que no se logró a través del pilar reglamentario, con el liderazgo, monitoreo y sanciones, se obtuvo internamente por la ética y los valores de la institución.

De acuerdo con la literatura, las organizaciones son más consistentes cuando toman en cuenta los sistemas de valores, que también pueden verse como una imposición sobre el comportamiento.

Por otro lado, en el Caso 2 no hubo capacitación formal. Cuando se implementó el aviso de privacidad se hizo del conocimiento del personal que había una persona responsable, que difundió información sobre la ley en la organización. También hubo quien se enteró o informó por otra fuente o por iniciativa propia, “más bien fue interés de uno querer saber más sobre eso”, o se trató en reuniones con docentes, donde enfatizaron que los datos son exclusivos para el uso que se les va a dar, pero desconocen aspectos importantes que debieron enseñarse en una capacitación. Las actividades que hacían para proteger los datos personales antes de la ley no variaron con su aparición, continuaron girando en torno a su recopilación y resguardo.

¿Por qué es tan importante que el personal reciba capacitación sobre este tema? Adquirir conocimiento facilita el desempeño individual y colectivo para que los sujetos obligados cumplan con los objetivos de la LPDPPP. Por esta razón, el artículo 30 de la misma establece, como parte de las funciones del sujeto responsable de protección de datos personales, capacitar al personal para que sepa cómo cumplir con los principios

de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad que establece.

En el caso 2, la ética ha suplido la necesidad de proteger la privacidad de los datos personales y no compartirlos, “nosotros no dilapidamos los datos”, “en el departamento tenemos mucha confidencialidad”, “nos aseguramos de que no se comenten los casos”, “no compartimos la información”, “nadie más tiene acceso a la información”. Pero hay otros aspectos de la ley que no se han cubierto por falta de capacitación. Entre ellos, saber qué son los derechos ARCO, cuánto tiempo conservar la información, cómo generar respaldos, conocer bajo qué condiciones debe ser la transferencia de los datos o qué datos pedir para no ser excesivos, por ejemplo.

Esta situación ha generado carencias en el cumplimiento, tales como la actualización del Aviso de Privacidad, la capacitación, la implementación de medidas de seguridad y la designación de una persona responsable de la protección de datos personales en la organización. Los entrevistados señalan a la dirección como la principal responsable de llevar a cabo estas acciones. Una vez más, destaca su complicidad con la falta de cumplimiento de la ley.

Contrario al Caso 2, el Caso 1 sí se dio a la tarea de impartir capacitaciones a los directores, al personal administrativo y docente, aunque la última que reportaron los entrevistados fue en 2016.

A pesar de que los resultados de la capacitación han sido paulatinos en la organización, el conocimiento de la ley se identifica en las respuestas de los entrevistados. Por ejemplo, conocen cuáles son los derechos ARCO, saben cuánto tiempo conservar la información, no exponen documentos, solo reciclan papel que no contiene datos personales, si les solicitan datos personales verifican que sea la persona autorizada para entregárselos, identifican a la persona responsable dentro de la organización, recurren a ella si es necesario y conocen las multas.

¿Esto demuestra que las capacitaciones han tenido efecto en el cumplimiento? Sí, desde el pilar normativo, la capacitación ha repercutido positivamente en cumplir con la

ley. El Caso 2 cuenta con rutinas específicas para reforzar el cuidado de los datos personales, aunque reconocen que hay áreas de oportunidad. Por ejemplo, existe una brecha entre quienes se integraron al colegio y no han recibido capacitación y quienes sí las recibieron, "…no tuve capacitación de cómo hay que proteger los datos de las personas. Yo, como procedente del área de RR.HH., lo único que decía a las personas que me entregaban sus solicitudes y datos, era que iban a ser resguardados".

Al igual que el Caso 1, estas carencias de capacitación en el Caso 2 las subsanó la ética, el conocimiento que tenían de su trabajo anterior o que les hagan hincapié en que deben tratar los datos personales con confidencialidad, aunque esto no reemplaza a la capacitación formal.

Tanto en el Caso 1 como en el Caso 2, es evidente que la ética y la capacitación han sido clave para el cumplimiento con la ley, aunque no son factores que se implementen por sí mismos, sino que dependen de la voluntad de los líderes de las organizaciones para darles fuerza.

Los mismos entrevistados confirmaron lo anterior cuando aseveraron que la capacitación dependió de que la dirección se involucró y tomó conciencia de la importancia del tema y, caso contrario, cuando mencionaron que no se ha hecho por falta de interés de los propios directivos.

En este orden de ideas, aunque la teoría señala que el cumplimiento puede basarse únicamente en uno o dos pilares, se fortalece cuando intervienen los tres. Es por esto que también debe tomarse en cuenta el papel del pilar cognitivo en el estudio de los casos para determinar si, efectivamente, es el reglamentario el que tiene la supremacía.

En un nivel cognitivo, las rutinas se siguen porque "se dan por sentadas", como resultado del éxito o fracaso de los pilares reglamentario y normativo. Es la asimilación individual de la ley y de las normas de conducta, en la que el sujeto interioriza las acciones de la organización para aceptarlas o rechazarlas. Entran en este pilar la asimilación de las tecnologías de la información y la reputación.

La asimilación de las TIC es fundamental para el tratamiento adecuado de los datos personales en las organizaciones, porque permiten su flujo y almacenamiento. Por lo tanto, si existe una percepción positiva de su uso, se potencia su eficacia. Si esto no se ocurre en la organización, es posible que ocurra una brecha en el cumplimiento.

El artículo 60 del Reglamento de la LFPDPPP establece lineamientos muy específicos que los sujetos obligados deben seguir para adoptar medidas de seguridad de acuerdo con el riesgo inherente por tipo de dato personal, la sensibilidad de los datos personales tratados, el desarrollo tecnológico y las posibles consecuencias de una vulneración para los titulares.

En el Caso 1, el área responsable de TI aseveró que cuentan con mecanismos de seguridad electrónicos que cumplen con los requerimientos de la ley. Tienen sus propios servidores y un sistema de almacenamiento de bases de datos con candados de acceso para los usuarios. Además, generan respaldos diarios.

A pesar de que la organización cuenta con las herramientas electrónicas para resguardar la información, algunas áreas están más familiarizadas que otras con su uso. Por ejemplo, su propio director general del Caso 1 manifestó que no sabe de las TI, “eso lo lleva el área responsable (TI)”. Incluso, la figura responsable no pareció estar relacionada con las medidas de seguridad electrónicas, “tendrías que hablar con la encargada de TI para saber si hay algún sistema”.

Otro entrevistado dio a conocer que anualmente almacena el registro de aproximadamente 250 solicitudes de becas, con información sensible, en una memoria USB, porque no tiene un área fija de trabajo para darles trámite y el programa que utiliza es incompatible con diferentes sistemas operativos. Si por accidente llegara a perder su dispositivo, pondría en riesgo la integridad de las personas de quienes tiene almacenados sus datos personales.

También hay quien opina que el personal no está lo suficientemente familiarizado con las TIC. Esto representa una resistencia al cambio. En palabras de la Dirección de Recursos Humanos, esto se debe al ambiente paternalista de la organización, es decir,

a que “el empleado era muy consentido y se preocupaban mucho más por la comodidad del empleado que por lo que estaba sucediendo por procesos y avances tecnológicos”. Aunque reconoció que está haciendo un intento por ponerse a la vanguardia y digitalizar información.

Otra carencia con respecto a las TI es que, a pesar de que cuentan con un sistema de almacenamiento de bases de datos con candados de acceso, no pueden controlar el uso que los usuarios hacen directamente de los datos personales porque no tienen procesos establecidos por escrito que hayan permeado en la institución. No obstante, hay departamentos que sí están familiarizados con el sistema y lo utilizan adecuadamente.

Por lo tanto, a nivel cognitivo, en algunos de los entrevistados no se manifestó que haya permeado el conocimiento y aceptación de los beneficios de las TI como un aliado para la protección de los datos personales, a pesar de que cuentan con los mecanismos de seguridad suficientes indicados por la ley. De acuerdo con la literatura, la resistencia de los usuarios para utilizar las TI puede mermar el cumplimiento con la ley porque podría haber fuga de información.

Por su parte, el Caso 2 también cuenta con su propio sistema interno para almacenar las bases de datos con candados de acceso y contraseñas personales por usuario. Aparentemente, los integrantes de la organización, empezando por el director general, están familiarizados con las TI, “estamos hablando de que 90% del personal tiene acceso y hemos tenido capacitación. Hoy en día es mínima la persona que le da miedo”, “yo creo que el tratamiento es muy bueno, solo faltaría la parte donde los papás firman que están de acuerdo”, “en comparación con otras escuelas están muy seguros”.

Sin embargo, de manera similar a lo que ocurre en el Caso 1, es difícil controlar el uso individual que hacen de las bases de datos, “sí me preocupa que algún maestro se lleve información. De hecho, un maestro que se fue del colegio me pidió un archivo y se lo di, pero después dije, por qué si es información mía”. Casos como este, facilitan la fuga de datos por más que cuenten con un sistema, contraseñas o niveles de acceso

de acuerdo con las actividades que realizan, candados digitales o cierre de sesión automática.

Ambos casos han prestado atención particular al tema de las TI para dar cumplimiento a la ley, aunque pareciera que el Caso 2 las ha asimilado mejor que el Caso 1.

La importancia del pilar cognitivo radica en que las cosas se dan por sentado, es decir, hay una mente colectiva organizacional que comparte y reproduce una creencia positiva o negativa con respecto a alguna disposición de la organización, que puede compararse con la convicción de un adoctrinamiento.

Por lo tanto, es en este pilar donde encaja la reputación de las organizaciones. ¿De qué manera la reputación de las organizaciones influye en el tratamiento adecuado de los datos personales?

Si se comparte la idea de que los datos personales de la organización reciben un tratamiento adecuado, esto la convierte en una organización en la que sus clientes pueden confiar y se transforma en buena reputación, le da credibilidad en el mercado y prestigio ante su competencia. Un caso contrario podría significar pérdidas económicas para la institución porque podrían recibir menos inscripciones de nuevo ingreso.

La reputación es un factor crítico para que los usuarios decidan compartir sus datos personales. Para reforzar la buena reputación, en el Caso 1 han implementado mecanismos para informar a sus clientes sobre el tratamiento de los datos personales, “al papá siempre se le dice que es por su seguridad que podemos o no podemos dar su información, para algunos es valioso, porque agradecen que les hagamos preguntas para darles información”.

También evitan malas prácticas como hacer llamadas telefónicas para ofrecer sus servicios educativos o publicar imágenes de los alumnos para fines de publicidad o en redes sociales sin su consentimiento. “Para el Colegio, es importante brindarles la confianza que tienen en nosotros al saber que la información está protegida”,

El Caso 2 reportó respuestas similares, “es muy importante porque les da tranquilidad que uno les asegure a los papás que su información está protegida”, “es muy importante porque no es cualquier información”, sobre todo porque han tenido casos en los que los padres de familia se comunican para decir que recibieron una llamada para informarles que secuestraron a sus hijos, pero les dan la tranquilidad de hablar con ellos y les recuerdan que sus datos personales están seguros por parte de la organización.

No obstante, reconocen que las acciones en pro de la seguridad de los datos personales, no va de la mano con el interés que manifiestan tener en generar una buena reputación. “Yo creo que debe estar nivelado…, hace falta información, más conciencia entre los maestros y el administrativo para darle la importancia”. Y, una vez más, apuntan a la dirección general como la responsable de fomentar las prácticas que sostengan la reputación de la organización en el Caso 2.

Como conclusión, de acuerdo la teoría, el cumplimiento puede basarse en tres pilares, pero sostenerse en uno en particular. En esta investigación, específicamente, el pilar reglamentario demostró ser predominante tanto para que exista cumplimiento en mayor grado como para que ocurra en menor grado, como ocurrió en el Caso 1 y 2, respectivamente.

Lo anterior se explica porque en el Caso 1, la coercitividad de las sanciones ocasionó que los directores prestaran atención a la ley para tomar la decisión de implementarla. No cumplir con ella podía acarrear pérdidas económicas y de reputación. En el caso 2, de manera opuesta, la decisión de cumplir en menor grado recayó en la parte directiva de la organización y, a raíz de esto, se observaron deficiencias en el cumplimiento.

El balance con el cumplimiento se logró gracias a la intervención de los pilares normativo y cognitivo. Estos lo fortalecieron —CASO 1— y cubrieron sus debilidades —Caso 2—. Por ejemplo, en ambos casos, la ética fue un factor compatible con la protección de datos personales y la privacidad de la información. En el Caso 1, la ética de la organización fortaleció el cumplimiento porque la protección de datos personales congenia con sus valores. Especialmente, en el Caso 2, la ética sirvió para suplir las carencias originadas por la falta de interés del liderazgo por implementar la ley.

Del pilar cognitivo, por otro lado, la reputación también fue predominante. En repetidas ocasiones los entrevistados de los Casos 1 y 2 hicieron énfasis en que para ellos es muy importante que la organización goce de buena reputación y que conserven la confianza de sus clientes.

De esta manera, se cumple lo que señala la teoría institucional. El cumplimiento puede sostenerse en los tres pilares, pero, uno posee más fuerza. Los resultados de esta investigación demostraron que el pilar más fuerte es el reglamentario.

El siguiente capítulo presenta las conclusiones de la investigación.

CAPÍTULO VII

CONCLUSIONES

En repetidas ocasiones se ha mencionado que, por tratarse de estudios de caso, no es posible establecer generalizaciones con los resultados de esta tesis. No obstante, el estudio de los factores que inciden en el cumplimiento de las políticas de protección de datos personales en las organizaciones, a la luz de la teoría institucional, permite plantear nuevas hipótesis para futuras investigaciones.

El interés en realizar esta investigación estuvo motivado por la aspiración de generar más conocimiento sobre la protección de datos personales, y fortalecerlo como un valor organizacional, para que el tratamiento de los mismos no vulnere los derechos de los titulares.

Hasta este momento, no se cuenta con cifras exactas que den a conocer cuántos sujetos obligados cumplen con los requerimientos de la ley, como contar con un aviso de privacidad o designar a un área o persona responsable de dar respuesta a las solicitudes ARCO. La aproximación más cercana a estos datos la dio la Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (Enaid), que revela que, aproximadamente, una tercera parte de ellos aún no cuenta con uno. Esto significaría que únicamente dos terceras partes cumplieron con la ley, aunque, de entre los resultados de esta tesis, se concluye que contar con un aviso de privacidad tampoco es indicio de que la organización protege adecuadamente los datos personales.

El valor de esta investigación radica en que es un tema poco explorado. Dado el costo monetario de los datos personales y las consecuencias que puede tener su uso inadecuado, tanto para sus titulares como para los responsables de la información, es menester conocer las áreas de oportunidad de los sujetos obligados para que cumplan con los parámetros de la ley.

Esta investigación y sus conclusiones son de suma importancia porque saber qué motiva su cumplimiento en las organizaciones y qué lo inhibe, también es de utilidad para que el órgano garante reenfoque sus esfuerzos, sobre todo considerando los resultados de la Enaid. Como se mencionó anteriormente, los datos personales son indispensables para el desarrollo de todo tipo de actividades, pero la seguridad de los datos no es un tema que concierne únicamente a los individuos y a las organizaciones, sino también a los gobiernos. Esto es porque es su responsabilidad no concluye al establecer los mecanismos —leyes— para su tratamiento adecuado, sino que, además, tienen la obligación de garantizar su cumplimiento.

Precisamente, el modelo teórico institucional ayudó a vislumbrar los factores que incidieron en el cumplimiento con las políticas de protección de datos personales en los casos de estudio. A partir de sus tres pilares, reglamentario, normativo y cognitivo, las personas claves relacionadas con los datos personales en cada uno de los casos, dieron una perspectiva organizacional útil para analizar el cumplimiento.

De lo anterior, se concluye los siguiente.

La literatura asevera que las organizaciones son entes muy complejos. En el cumplimiento de una política, como es la protección de datos personales, intervienen diversos factores como la toma de decisiones, metas, tareas, procesos, valores, recursos humanos, materiales, etcétera, que la teoría institucional clasifica en reglamentarios, normativos y cognitivos.

Aunque la suma de los tres pilares da mayor fuerza al actuar de las organizaciones, la teoría enfatiza que el cumplimiento puede recaer únicamente en uno o dos, sin mencionar cuál en específico. En particular, esta tesis sostiene como hipótesis que el pilar reglamentario tiene mayor peso en el cumplimiento por la coercitividad de las sanciones. ¿Se cumple?

A pesar de que los casos de estudio se seleccionaron bajo el criterio de máxima similitud, evidentemente existieron factores que ocasionaron diferencias en el cumplimiento.

Para comenzar, antes de la ley, en el Caso 1 protegían los datos personales bajo su propia ética y parámetros. Sin embargo, su aparición tuvo un efecto sobre el liderazgo directivo para que adoptara las medidas que indicaba para darle cumplimiento.

Tal como lo señala la teoría, la coercitividad de la ley desempeñó un papel fundamental. Ejerció mayor presión sobre los directivos para encaminarlos hacia el cumplimiento y, a pesar de que el órgano garante no realizó monitoreo, persistió la amenaza de que impusiera una sanción por presunto incumplimiento. En este caso, se enteraron de que existía una ley con la que debían cumplir y lo hicieron, “porque si no, ya sabes”, “las multas”, “las sanciones”.

En el Caso 2, se observó que la falta de monitoreo menguó el efecto de las sanciones sobre el liderazgo directivo porque no hubo una autoridad que verificara su cumplimiento periódicamente. Por lo tanto, su interés en cumplir fue menor. Bajo la lógica de la dirección general, en ellos nadie se fijó ni han ido a inspeccionarlos como lo hacen otras instancias, por lo tanto, no prestó mayor atención. Esto no quiere decir que haya hecho caso omiso de toda la ley, porque sí hay cumplimiento.

Ante esto, es evidente que no es suficiente con que los gobiernos aprueben leyes, como la LFPDPPP, que establecen marcos que benefician el desarrollo de todo tipo de actividades, gracias al libre tránsito de los datos personales, estableciendo medidas para su tratamiento adecuado, sino que deben garantizar que su cumplimiento sea efectivo. Para lograrlo, es urgente que el órgano garante que busque otros mecanismos paralelos al monitoreo, porque si la amenaza no se cumple, la coercitividad de la ley pierde su eficacia.

¿El pilar reglamentario afecta al cumplimiento? Por supuesto que sí. La aparición de una ley coercitiva fue el punto de partida que obligó a las organizaciones a prestar mayor atención en la manera en la que protegían los datos personales. Si no se hubiera creado la ley, no se habría manifestado este interés en adoptar medidas que los protegieran. Es necesario recordar que ambas organizaciones los cuidaban aun sin ley, pero debido a su coercitividad, las dos se ocuparon por establecer sus requerimientos, aunque hay una que cumplió en menor grado.

Sin embargo, para que el cumplimiento se fortalezca desde el pilar reglamentario, no es suficiente con que exista una ley sancionadora, también debe abarcar mecanismos de monitoreo y contar con el interés de quienes encabezan las organizaciones para que la ejecuten. De esta manera, a mayor coercitividad, monitoreo y liderazgo, mayor será el cumplimiento. Como lo demuestra el caso 2, si alguno de estos factores no adquiere la suficiente fuerza, esto se verá reflejado en el cumplimiento.

La teoría también explica que el cumplimiento no solo ocurre porque hay factores reglamentarios, sino también normativos. En los casos estudiados, la capacitación y la ética también fueron indispensables, pero cobraron fuerza porque existió la coercitividad de la ley que movió al liderazgo a establecer mejores prácticas para proteger los datos personales que permearan al resto de la organización.

En otras palabras, una vez que existió una ley que obligó a las organizaciones a implementar políticas de protección de datos personales, estas debían establecer actividades en su interior para fortalecer el derecho como un valor agregado. Para lograrlo, debían fomentarse buenas prácticas a través de la capacitación y la ética.

En el Caso 1, esto se logró de manera exitosa porque el liderazgo vio la necesidad de hacerlo, porque en caso contrario, podían incurrir en una multa. El Caso 2, por su parte, no reforzó esta área, pero, esto es una reacción en cadena que viene desde que el órgano garante no monitoreó el cumplimiento, por lo tanto, las sanciones no ejercieron ningún temor en la dirección general y no prestó más interés en el cumplimiento.

Bajo estas condiciones, se demuestra la supremacía del pilar reglamentario sobre el cognitivo en el cumplimiento, tanto para el caso que cumplió en mayor como en menor grado.

Finalmente, a nivel cognitivo, cuando la organización interioriza el valor de proteger los datos personales, este no puede desasociarse del uso las tecnologías de la información. Si las herramientas tecnológicas se perciben como un aliado, es decir, su uso se asimila al interior de las organizaciones en pro de la seguridad de los datos,

actuarán positivamente en el cumplimiento. Por el contrario, si existe rechazo, el riesgo de pérdida de información puede aumentar.

Esto lo demuestra el Caso 1, en el que una persona puede poner en riesgo la seguridad de la información que almacena en una memoria USB, porque no ha encontrado la manera de solucionar el problema que se expuso en los resultados, y tampoco se ha acercado al departamento de TI de la organización para diseñar una estrategia.

En el Caso 2, por el contrario, se evidencia mayor familiaridad con las TIC. Esta es una fortaleza para la organización, aunque en ambas hay evidencia de que tanto existen quienes las adoptan como a quienes no les son familiares e, incluso, las rechazan.

En este mismo nivel, cognitivo, en ambos casos se encontró que gozar de buena reputación también es parte fundamental para el cumplimiento. Aunque en el Caso 2 es contradictorio que, a pesar de que afirmaron que para ellos es importante que los padres de familia sepan que sus datos están protegidos, las medidas que implementaron no con congruentes con su afirmación.

Particularmente, en el Caso 1, sí han implementado mecanismos para informar a los titulares de los datos personales sobre el tratamiento que se hará de los mismos.

Para cerrar, se concluye que los tres pilares son importantes en el cumplimiento porque lo fortalecen. Es decir, se confirma que la suma de las sanciones, más el monitoreo del órgano garante, más el liderazgo de las organizaciones responsables de los datos personales, más la ética y la capacitación, y más la asimilación de las TI y la reputación, robustecen el cumplimiento. Esto se explica porque el cumplimiento es racional, pero también es normativo y cognitivo. Sin embargo, ninguno de esos factores se habría desencadenado con mayor énfasis si no existiera una ley que lo exija y líderes dentro de las organizaciones que lo cumplan. Por lo tanto, se confirma la hipótesis planteada.

Toda tesis supone alcances y limitaciones, útiles para considerar en futuras investigaciones. Primero, como se ha mencionado anteriormente, de los estudios de

caso no pueden establecerse generalizaciones, sin embargo, a partir de ellos pueden plantearse nuevas hipótesis para otras investigaciones. Esto ampliaría el espectro de la protección de datos personales.

Segundo, el criterio para seleccionar a los entrevistados fue que fueran los adecuados para responder a la pregunta de investigación. Llegó un punto en el que la información que arrojaron comenzó a repetirse. Por esto, el número de entrevistados no fue un criterio relevante.

Tercero, las variables se eligieron con base en la literatura de la teoría institucional. A diferencia de otras teorías desde las que se explicaba parcialmente el cumplimiento, esta dio una visión más amplia. No obstante, hay más variables que podrían agregarse al estudio en cada uno de los pilares. Un ejemplo es el aspecto económico de la organización, que en esta investigación no se consideró porque el proceso de implementación es exactamente el mismo, en uno u otro caso.

Cuarto, en el capítulo metodológico se justificó porqué la investigación únicamente seleccionó casos del sector educativo. Sin embargo, replicarla en otro sector, como el de salud o bancario, donde la sensibilidad de los datos personales demanda su tratamiento adecuado sería un paso a seguir. Se esperaría que los resultados fueran similares. De no ser así, otro paso a seguir sería la comparación entre sectores, bajo la ley de los particulares.

Quinto, en el capítulo metodológico también se explicó que la selección de casos obedeció al principio de máxima diferenciación en el cumplimiento. Originalmente se consideró tener un caso intermedio, sin embargo, se desechó porque se obtuvo información suficiente de los casos seleccionados. Esto es porque el análisis de un caso intermedio se cubrió con el de menor grado.

Sexto, para generalizar, se recomienda hacer una investigación mixta, con técnicas cualitativas y cuantitativas, con una muestra más diversa que involucre diferentes sectores. A partir de un estudio de esta naturaleza podrían establecerse

generalizaciones en torno al cumplimiento de las políticas de protección de datos personales en el sector privado. Esta tesis constituye un primer paso hacia ello.

Séptimo, otra limitante fue la normatividad, que, para los fines de esta investigación, solo permitió realizarla en el sector privado; en un futuro, podría desarrollarse una comparación entre organizaciones del sector público y privado. Por último, quinto, también podrían incorporarse otras variables que expliquen el cumplimiento desde la teoría institucional.

Octavo, la información obtenida en esta investigación ayudan a entender a qué factores obedece el cumplimiento. Como se mencionó anteriormente, esto beneficia tanto a los individuos, como organizaciones y gobiernos porque lo ayuda en la toma de decisiones informadas para encaminar nuevos esfuerzos que garanticen el cumplimiento de la ley.

Noveno, según se estudió en el capítulo teórico, más de una teoría podía explicar el cumplimiento de las políticas de protección de datos personales en las organizaciones. Sería arrogante afirmar que solo una teoría puede dar respuesta a la pregunta de investigación. Sin embargo, siempre existe una o dos que son las más pertinentes; en este caso, se eligió la teoría institucional por su aplicación empírica en temas relacionados con la seguridad de la información y las TIC. Con esta selección, se comprobó su utilidad en el tema de protección de datos personales, para el cual, de acuerdo con la literatura revisada, no se había aplicado.

BIBLIOGRAFÍA

1. Adler, P., Goldoftas, B., & Levine, D. (1999). Flexibility versus efficiency? A case study of model changeovers in the Toyota production system. *Organization science*, *10*(1), 43-68.
2. AEPD (2017). *Estadísticas mensuales del Registro General de Protección de Datos*. Situación a 31 de enero de 2017. Consultado en febrero de 2017. Disponible en http://www.agpd.es/portalwebAGPD/ficheros_inscritos/estadisticas/index-ides-idphp.php
3. Alina, A.(2014). The role of compliance in an organization. Ways of implementation. *Annals of Faculty of Economics*, 1(1), 17-22.
4. AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2016). Investigating the Impact of Institutional Pressures on Information Security Compliance in Organizations. *Australasian Conference on Information Systems.* Australia, Wollongong.
5. Aguinis, H., & Kraiger, K. (2009). Benefits of training and development for individuals and teams, organizations, and society. *Annual review of psychology*, *60*, 451-474.
6. Aiken, M. & Hage, J. (1966). Organizational alienation: A comparative analysis. *American Sociological Review.* Vol. 31. No. 4. Pp. 497-507.
7. Akua, I, & Adjei, S. (2008). Public social policy development and implementation: a case study of the Ghana National Health Insurance scheme. *Health Policy and Planning.* No. 23. Pp. 150-160. Oxford University Press.
8. Amipci. (2016). *Estudio sobre el valor económico de los datos personales.* Consultado en julio de 2016, desde https://amipci.org.mx/es/estudios.
9. Animal Político (2016). El INE denuncia la filtración de los datos de 83.5 millones de mexicanos a Amazon. Consultado en junio de 2016, disponible en http://www.animalpolitico.com/2016/04/el-ine-denuncia-la-filtracion-de-los-datos-de-83-5-millones-de-mexicanos-a-amazon/
10. APEC (2010). Cooperation Arrangement Cross-border Privacy Enforcement. Consultado en febrero de 2015, disponible en http://aimp.apec.org/ Documents/2010/ECSG/DPS1/10_ecsg_dps1_013.pdf.
11. Avgerou, C. (2000). IT and organizational change: an institutionalist perspective. *Information Technology and People.* Vol. 13, No. 4, Pp. 234-262. MCB University Press.
12. Ayres, I. & Braithwaite, J. (1992). *Responsive regulation: Trascending the Deregulation Debate.* Oxford: Oxford University Press.
13. Banistar, D. (2018). National Comprehensive Data Protection/Privacy Laws and Bills 2018 Map. Consultado en mayo de 2018. Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416
14. Baptista , J. (2009). Institutionalisation as a process of interplay between technology and its organisational context of use. *Journal Of Information Technology*, 24(4): 305-320.
15. Baron, R. A (1988) Negative Effects of Destructive Criticism: Impact on Conflict, Self-Efficacy and Task Performance. *Journal of Applied Psychology*. No. 73, Pp. 199-207.
16. Bennett, C. & Raab, C. (2006). *The governance of privacy: Policy instruments in global perspective.* MIT Press.

17. Berger, P. & Luckmann, T. (1967). *The Social Construction of Reality: A Treatise in the Sociology of Knowledge.* New York: Doubleday.
18. Berkeley, A. (1988). Does leadership make a difference to organizational performance? *Administrative Science Quarterly.* Vol. 33, No. 3, Pp. 388-400.
19. Björck, F. (2004). Institutional Theory: A New Perspective for Research into IS/IT Security in Organisations. Proceedings of the 37th Annual Hawaii International Conference on, IEEE2004.
20. Blume, P. EU adequacy decisions: the proposed new possibilities. *International Data Privacy Law*. Vol. 5. No. 1, Oxford University Press.
21. Boniface, A. (2012). Privacy and data protection in Africa: a state of the art. *International Data Privacy Law*. Vol. 2. No. 3, Oxford University Press.
22. Boynton, A., Zmud, R. & Jacobs, G. (1994). The Influence of IT Management Practice on IT Use in Large Organizations. *MIS Quarterly.* Pp. 299-318.
23. Bryman, A. (2012). *Social Research Methods*. Oxford: OUP.
24. Bygrave, L. (2004). Privacy in a global context: A comparative overview. *Scandinabian Studies in Law.* Vol. 46. Pp. 319-348.
25. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010), Information security policy compliance: An empirical study of rational-based beliefs and information security awareness. *MIS Quarterly*, 34, 3, 523–548.
26. Bunge, M. (2007). *Buscar la filosofía en las ciencias sociales.* México: Siglo XXI.
27. Campbell, J. (2007). Why would corporations behave in socially responsible ways? An institutional theory of corporate social responsibility. *Academy of management Review*. No. 32 (3), Pp. 946-967.
28. Canales, R. (2011). Rule bending, sociological citizenship, and organizational contestation in microfinance. *Regulation and Governance.* No. 5, Pp. 90-117.
29. Cárdenas, J. (2010). *Introducción al estudio del derecho*. México: Instituto de Investigaciones Jurídicas UNAM.
30. Cerna, L. (2013). The nature of policy change and implementation: a review of different theoretical approaches. *OECD.*
31. Chiravuri, A. & Ambrose, P. (2002). *A Theoretical Examina- nation of Organizational Downsizing and Its Effects on IS Orga- nizational Learning, Memory and Innovation*. Americas Conference on Information Systems, Dallas, Texas, Association for Information Systems.
32. Churchill, G. & Iacobucci, D. (2002). *Marketing Research: Methodological Foundations*, 8th Edition, South-Western Thomson Learning.
33. Cialdini, R., & Goldstein, J. (2004). Social influence: Compliance and conformity. *Annu. Rev. Psychol.*, No. *55*, Pp. 591-621.
34. Clarke, R. Data retention as mass surveillance: the need for an evaluative framework. *International Data Privacy Law*. Vol. 5, No. 2, Oxford University Press.
35. Colonna, L. (2014). Article 4 of the EU Data Protection Directive and the irrelevance of the EU-US Safe. *International Data Privacy Law*. Vol. 4. No. 3, Oxford University Press.
36. Congress.gov (2017). *S.J.Res.34 - A joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to "Protecting the Privacy of Customers of Broadband*

and Other Telecommunications Services". Consultado en mayo de 2017, desde https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34.
37. Condusef. (2016). *Desempeño de las Entidades Financieras a diciembre de 2016.* Consultado en febrero 2017. Disponible en https://www.gob.mx/condusef/prensa/se-registran-5-5-millones-de-reclamaciones-en-el-sistema-financiero-al-tercer-trimestre-de-2016.
38. Cortés, F. (2008). "Selección no aleatoria y validez", en Cortés F, Escobar, A. y González, A. *Método Científico y Política Social: A propósito de las evaluaciones cualitativas de programas sociales*. México: El Colegio de México.
39. Dacin, M. T., Goodstein, J., & Scott, W. R. (2002). Institutional theory and institutional change: Introduction to the special research forum. *Academy of management journal*, *45*(1), 45-56.
40. De Hert, P. & Gutwirth, S. (2006). "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power". En E. Claes, A. Duff y S. Gutwirth (editores) *Privacy and the criminal law.* Antwerp/Oxford, Intersentia, 61-104.
41. Delgado, L. (2009). El enfoque de las políticas públicas. En *Documentación sobre gerencia pública.* Junta de Comunidades de Castila-La Mancha.
42. Deloitte (2014). *Termómetro: Privacidad y protección de datos en México 2014*. Segunda edición.
43. Desai, V. (2015). Under the Radar: Regulatory Collaborations and their Selective Use to Facilitate Organizational Compliance. *Academy of Management Journal*. Vol. 59. No. 2. Pp. 636-657.
44. DLA Piper. (2018). *Data Protection Laws of the World.* Handbook. Consultado en mayo de 2018. Disponible en https://www.dlapiperdataprotection.com
45. DMA (2015). Data Privacy: what the consumer really thinks. *Journal of Direct, Data and Digital Marketing Practice.* Vol. 17, No. 1, Pp. 30–35.
46. DOF (2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
47. DOF (2017). Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados
48. DOUE. (2016). 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). Consultado en noviembre de 2016, disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679.
49. Edwards, J. , Mason, D. , and Washington, M. (2009). Institutional pressures, government funding and provincial sport organisations. *International Journal of Sport Management and Marketing.* No. 6, Vol. 2. Pp. 128-149.
50. EFE (2011). *Sony investiga el robo de datos de 77 millones de cuentas de PlayStation*. Periódico La Vanguardia. Consultado en julio de 2016. Disponible en http://www.lavanguardia.com/internet/20110427/54146138829/sony-investiga-el-robo-de-datos-de-77-millones-de-cuentas-de-playstation.html

51. Eisenhardt, K. (1988). Agency and institutional theory explanations: The case of retail sales compensation. *Academy of Management Journal.* Vol. 31, No. 3. Pp. 488-511. Stanford University.
52. Eisenhardt, K. (1989). Building Theories from Case Study Research. *The Academy of Management Review*. Vol. 14. No. 4. October. Pp. 532-550.
53. Etienne, J. (2010). *The impact of regulatory policy on individual behaviour: a goal framing theory approach*. Centre for Analysis of Risk and Regulation. London School of Economics and Political Science. No. 59.
54. Feld, L. P., & Frey, B. S. (2007). Tax compliance as the result of a psychological tax contract: The role of incentives and responsive regulation. *Law & Policy*, *29*(1), 102-120.
55. Finantiacial Times (2013). What is your data worth? Consultado en mayo de 2015, disponible en http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz2sS19P0dt.
56. Foorthuis, R. & Bos, R. (2011). A Framework for Organizational Compliance Management Tactics*. CAiSE 2011 International Workshops.* LNBIP 83, pp. 259-268. London: Springer.
57. Frutos, O. (2014). El derecho a la autodeterminación informativa en la era de la llamada videovigilancia en el sector privado en México. Una perspectiva desde la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y los retos pendientes. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías.* No. 12, Julio-Diciembre. Universidad de los Andes.
58. Gabel, H. L., & Sinclair-Desgagné, B. (1993). Managerial incentives and environmental compliance. *Journal of Environmental Economics and Management*, *24*(3), 229-240.
59. Gacitúa, A. (2014). *El derecho fundamental a la protección de datos personales en el ámbito de la prevensión y represión penal europea*. Tesis doctoral. Universidad Autónoma de Barcelona.
60. Geels, F. (2004). From sectoral systems of innovation to socio-technical systems: Insights about dynamics and change from sociology and institutional theory. *Research policy*, *33*(6), 897-920.
61. Gellert, R. (2015) Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. *International Data Privacy Law.* Vol. 5, No. 1, Oxford University Press.
62. Gerring, J. (2007). *Case study research.* Cambridge University Press. Pp. 90-122.
63. Gerring, J. /2009). The case study: What it is and what it does. En Boix, C. & Stokes, S. (Eds.) *The Oxford Handbook of Comparative Politics*. Oxford University Press.
64. Gezelius, S. (2002). Do norms count? State regulation and compliance in a Norwegian fishing community. *Acta Sociológica*. Vol. *45*, No. 4. Pp. 305-314.
65. Goldstein, I. (1980). Training in work organizations. *Annual review of psychology*, *31*(1), 229-272.
66. González, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Bruselas: Springer.
67. Gonzalez, N., Marle, F., & Bocquet, J. C. (2007). Measuring project maturity: example in a french automotive organization. In *International Conference on Engineering Design, ICED O* (Vol. 7, pp. 28-31).

68. Good, G. (2013). Unemployment Claims Management: A focus on compliance. *Journal of State Taxation.* S/N. November-december. Pp. 23-28.
69. Grasmick, H., & Scott, W. (1982). Tax evasion and mechanisms of social control: A comparison with grand and petty theft. *Journal of Economic Psychology*. Vol. *2*, No.3. Pp. 213-230.
70. Gray, G., & Silbey, S. (2014). Governing Inside Organization: Interpreting Regulation and Compliance. *American Journal of Sociology.* Vol. 120. No. 1 (julio 2014). Pp. 96-145.
71. Greenleaf, G. (2014). *Asian Data Privacy Laws: Trade & Human Rights Perspectives*. Oxford University Press.
72. Gregorio, C. (2004). *Protección de Datos Personales: Europa vs. Estados Unidos, todo un dilema para América Latina*. Consultado en Transparentar al Estado: la Experiencia Mexicana de Acceso a la Información. Consultado desde la Biblioteca Jurídica Virtual, en septiembre de 2014, http://www.bibliojuridica.org/libros/3/1407/12.pdf.
73. Grewal, R., Dharwadkar, R., 2002. The role of the institutional environment in marketing channels. *Journal of Marketing*, 66 (3), 82-97.
74. Harter, D.E. & Slaughter, S.A. (2003). Quality improvement and infrastructure activity costs in software development: A longitudinal analysis. *Management Science*, 49, 6, 784–800.
75. Heisenhardt, K. (1988). Agency and Institutional theory explanations: the case of retail sales compensation. *Academy of Management Journal.* Vol. 31, No. 3, Pp. 488-511.
76. Hermosilla, D., Amutio, A., da Costa, S. y Páez, D. (2016). El liderazgo transformacional en las organizaciones: variables mediadoras y consecuencias a largo plazo. *Journal of Work and Organizational Psychology.* No. 32, Pp. 135-143.
77. Hernández, R., Fernández, C. y Baptista, P. (1991) 4ª. Edición. *Metodología de la investigación*. México: Mc Graw Hill.
78. Herath, T., & Rao, H. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*. *47*(2), 154-165.
79. Hodgson, G.M., 1998. The approach of institutional economics. *Journal of Economic Literature*. No. 36, Pp.166–192.
80. Hovi, J., Stokke, O., & Ulfstein, G. (2005). *Implementing the climate regime.* London: Earthscan.
81. Hustinx, P. (2011). *Opinion of the European Data Protection Supervisor on the Evaluation Report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC).* European Data Protection Supervisor. Consultado en febrero de 2017, disponible en https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf.
82. ICDPPC, (2009). Resolución de Madrid: Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Consultado en mayo de 2013, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf.
83. ICDPPC (2016). Resolución sobre Cooperación Internacional para hacer cumplir la ley. *38ª. Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.* Marruecos.

84. Identity Theft Resource Center (2015). *Data Breach Reports, July 7, 2015.* Consultado en julio de 2015, disponible en http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html
85. Inai. (2013). Curso *Introducción a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* México.
86. Inai (2014). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* México.
87. Inai. (2016). Sector Financiero y de seguros, con mayor número de multas por infringir ley federal de datos personales: Inai. *Comunicado Inai/404/15*. 25 de diciembre de 2016.
88. Inegi. (2013). Directorio Estadístico Nacional de Unidades Económicas. Consultado en julio de 2015, disponible en http://www.beta.inegi.org.mx/app/mapa/denue/default.aspx.
89. Inegi. (2016). Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales. Consultada en enero de 2017. Disponible en http://www.beta.inegi.org.mx/proyectos/enchogares/especiales/enaid/2016/.
90. Johnston, A.C., y Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34, 3, 549–566.
91. Jóri, A. (2015). Shaping vs applying data protection law: two core functions of data protection authorities. *International Data Privacy Law*. Vol. 5. No. 2, Oxford University Press.
92. Kajava, J., Anttila, J., Varonen, R., Savola, R., & Roning, J. (2006). Senior executives commitment to information security-from motivation to responsibility. *Computational Intelligence and Security, 2006 International Conference.* Vol. 2. Pp. 1519-1522. IEEE.
93. Kamarinou, D., Millard, C. & Kuan, W. (2016). Cloud privacy: an empirical study of 20 cloud providers' terms and privacy policies —Par II. *International Data Privacy Law*. Vol. 6. No. 3, Oxford University Press.
94. Kelman, S., 1987. *Making Public Policy: A Hopeful View of American Government*. New York: Basic Books.
95. Kirsch, L., & Boss, S. (2007). The last line of defense: motivating employees to follow corporate security guidelines. *ICIS 2007 Proceedings*, 103.
96. Kite, W. (1964). Attributions of causality as a function of the use of reward and punishment. Doctoral dissertation. Sanford University.
97. Kloza, D. & Moscibroda, A. (2014) Making the case for enhanced enforcement cooperation between data protection authorities: insights from competition law. *International Data Privacy Law*. Vol. 4, No. 2.
98. Kshetri, N. (2007). Institutional factors affecting offshore business process and information technology outsorcing. *Journal of international management.* 13(1). Pp. 38-56.
99. Kudic, M., & Banaszak, M. (2009). *The Economic Optimality of Sanction Mechanisms in Interorganizational Ego Networks–A Game Theoretical Analysis*– No. 15. Halle Institute for Economic Research.
100. Kuner, C. (2011). Regulation of transborder data flows under data protection and privacy law: past, present and future. *OECD Digital Economy Papers,* No. 187, OECD Publishing.
101. Kwon, J., & Johnson, M. (2013). Health-Care Security Strategies for Data Protection and Regulatory Compliance. *Journal Of Management Information Systems*, *30*(2), 41-66.

102. Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, *48*(4), 635-645.
103. Lopes, I. & de Sá-Soares, F. (2014). Institutionalization of information systems security policies adoption: factors and guidelines. *IADIS International Journal on Computer Science and Information Systems.* Vol. 9, no.2, pp. 82-95.
104. Lunenburg, F. (2012). Compliance Theory and Organizational Effectiveness. *International Journal of Scholarly Academic Intellectual Diversity*. Vol. 14. No. 1.
105. Martinez, P. (2006). El método de estudio de caso: estrategia metodológica de la investigación científica. *Pensamiento y Gestión*. No. 20. Julio. Pp. 165-193. Colombia: Universidad del Norte.
106. Mendoza, V. (2012). *¿Cuánto valen los datos de tu empresa?* Revista Expansión. Consultado en Julio de 2016. Disponile en http://expansion.mx/emprendedores/2012/04/30/cuanto-valen-los-datos-de-tu-empresa.
107. Mihai, B. & Alina, A. (2013). Business Ethics Implementation in the Organizational Culture of Companies. Annals of The University of Oradea, *Economic Science Series.* No. 22, Pp. 44-53
108. Miranda, A. (2016). Panel Aplicación de la ley. Verificación, inspección y sanción, experiencias comparadas. Vulneraciones de seguridad. *Foro de Autoridades de Privacidad Asia-Pacífico*. México. Ed. 46. Diciembre de 2016.
109. Mwakibinga, F. (2008). *Public sector procurement in Tanzania: It's organization and practice.* Dissertation for the digree of Doctor of Philosophy. Noruega: Molde University College.
110. Mwakibinga, F. & Buvik, A. (2013). An empirical analysis of coercitive means of enforcing compliance in public procurement. *Journal of Public Procurement*. Vol. 13, Issue 2. Pp. 243-273.
111. Nesensohn, C., Bryde, D., Ochieng, D. E. G., y Fearon, D. (2014). "Maturity and maturity models in lean construction". *Australasian Journal of Construction Economics and Building*, *14*(1), 45-59.
112. Nino, M. (2010). The protection of personal data in the fight against terrorism New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon. *Utrecht Law Review*, *6*(1), 62-85.
113. Noruzy, A., Majazi, V., Azhdari, B., Nazari, S. & Rezazadech, A. (2012). Relations between transformational leadership, organizational innovation, and organizational performance: an empirical investigation of manufacturing firms. *The International Journal of Advanced Manufacturing Technology*, *64*(5-8), Pp. 1073-1085.
114. OECD. (2011). The evolving privacy landscape: 30 years after de OECD Privacy Guidelines. *OECD Digital Economy Papers.* No. 176, OECD Publishing.
115. OECD. (2013). *Exploring the Economics of Personal Data. A survey of methodologies for measuring monetary value*. Consultado en julio de 2016, desde dhttp://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/IE/REG%282011%292/FINAL&docLanguage=En

116. Ornelas, L., Higuera, M. (2013). La autorregulación en materia de protección de datos personales: la vía hacia una protección global. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías.* No. 9. Universidad de los Andes.
117. Pahnila, S., Siponen, M. & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences.* Hawaii.
118. Parsons, W. (2012). Políticas públicas: Una introducción a la teoría y a la práctica del análisis de políticas públicas. México: FLACSO. 3ª reimpresión.
119. Peeples, D. K. (2002). Instilling consumer confidence in e-commerce. *SAM Advanced Management Journal*, *67*(4), 26.
120. Penley, L. & Gould, S. (1988). Etzioni's model of organizational involvement: A perspective for understanding commitment to organizations. *Journal of Organizational Behavior*, *9*(1), 43-59.
121. Peterson, R., Martorana, P., Smith, B. & Owens, P. (2003). The impact of chief executive officer personality on top management team dynamics: one mechanism by wich leadership affects organizational performance. *Journal of Applied Psychology.* Vol. 88, No. 5, Pp. 795-808.
122. Phillips, R. A., & Margolis, J. D. (1999). Toward an ethics of organizations. *Business Ethics Quarterly*, *9*(4), Pp. 619-638.
123. Podsakoff, P., MacKenzie, J., Lee, J. & Podsakoff, N. (2003). Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Aplied Psycology.* Vol. 88, No. 5, Pp. 879-903.
124. Prieto, J. (2016). Panel Aplicación de la ley. Verificación, inspección y sanción, experiencias comparadas. Vulneraciones de seguridad. *Foro de Autoridades de Privacidad Asia-Pacífico*. México. Ed. 46. Diciembre de 2016.
125. Privacy Maturity Model (2011). Canada: American Institute of Certified Public Accountants, Inc. y Canadian Institute of Chartered Accountants.
126. Puente, X. (2015). Por una mayor cultura de protección de datos personales. *El Universal digital.* Consultado en julio de 2015, disponible en http://www.eluniversal.com.mx/entrada-de-opinion/articulo/ximena-puente-de-la-mora/nacion/2015/07/16/por-una-mayor-cultura-de#.VamQji0ypDM.twitter
127. Puhakainen, P. & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly,* Vol. 34, No. 4, Pp. 757-778.
128. PWC (2016). *Estudio de la Privacidad en México 2016: más allá de los compromisos.* México.
129. Rainey, H. (2009). *Understanding managing public organizations.* USA. HB Printing.
130. Revuelta, B. (2007). La implementación de políticas públicas. *Dikajon.* No. 16, Pp. 135-156. Colombia: Universidad de la Sabana.
131. Roth, A. (2006). *Políticas públicas: Formulación, implementación y evaluación.* Bogotá: Aurora. 4ª edición.
132. Rothbart, M. (1968). Effects of motivation, equity, and compliance on the use of reward and punishment. *Journal or Personality and Social Psychology*. Vol. 9, No. 4, Pp. 353-363.

133. Sabatier, P., & Mazmanian, D. (1980). The implementation of public policy: A framework of analysis. *Policy studies journal*, *8*(4), 538-560.
134. Sartori, G. (2002). *La política. La lógica y método en las ciencias sociales*. México: Fondo de Cultura Económica.
135. Shaw, R. (2012). *The influence of organizational culture on employee attitudes towards information security policy*, Capella University.
136. Schneider, C. (1974). Behavior Modification in Management: A Review and Critique. *Academy of Management Journal.* No. 17 (3). Pp. 528-549.
137. Schneider, A., 1999. US neo-conservatism: Cohort and cross-cultural perspective. *The International Journal of Sociology and Social Policy*. 19(12) 56-86.
138. Schütz, P. (2012). The Set Up of Data Protection Authorities as a New Regulatory Approach. In Gutwirth, S., Leenes, R., De Hert, P and Poullet, Y. (eds), *European Data Protection: In Good Health?* Springer.
139. Scott (2001). Institutions and Organizations. 2nd. Ed. USA: Sage Publications, Inc.
140. Scott, R. (2004). Institutional theory: Contributing to a theoretical research program. *Great minds in management: The process of theory development*, Pp. 460-485.
141. Scott, R. (2008). Institutions and organizations: ideas and interests. 3rd ed. USA: Sage Publications, Inc.
142. Siponen, M., Pahnila, S., & Mahmood, A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2).
143. Senado de la República (2010). Proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Gaceta del Senado. Gaceta LXI/1SPO-127/24881. Consultado en abril de 2015. Disponible en http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=24881
144. SEP (2015). Censo de escuelas, maestros y alumnos de educación básica y especial. Consultado en septiembre de 2016, disponible en http://www.gob.mx/sep/datos-abiertos/571e8d4f5a1a5e0100a51602.
145. Siddiki, S., Basurto, X., & Weible, C. (2012). Using the institutional grammar tool to understand regulatory compliance: The case of Colorado aquaculture. *Regulation & Governance*, *6*(2), 167-188.
146. Small, M. (2009). How many cases do I need? On science and the logic of case selection in field-based research. *Ethnography.* No. 10, Pp. 5-38.
147. Smith, A. (2004). Cybercriminal impacts on online business and consumer confidence. *Online Information Review*, *28*(3), 224-234.
148. Solange, M. y Moreno, J., Implicaciones de una ley general en materia de protección de datos personales. *División de estudios jurídicos*. No. 64, Publicaciones Centro de Investigación y Docencia Económica, A.C.
149. Sotto, L. & Simpson, A. (2014). United States. In Jay, R. (Ed). *Data Protection & Privacy in 26 jurisdictions worlwide.* Law Business Research, London.

150. Surry, S. & Ely, D. (2006). *Adoption, difussion, implementation, and institutionalization of educational technology*. USA: University of South Alabama. Consultado en abril de 2015, desde http://www.usouthal.edu/coe/bset/surry/papers/adoption/chap.htm
151. Sutinen, J., Rieser, A., & Gauvin, J. (1990) Measuring and Explaining noncompliance in Federally Managed Fisheries. *Ocean Development and International Law*, 21: 335-72.
152. Tashakkori, A & Teddlie, C. (1998). *Mixed Methodology.* California: SAGE.
153. Treviño, L. K., Weaver, G. R., & Reynolds, S. J. (2006). Behavioral ethics in organizations: A review. *Journal of management*, *32*(6), 951-990.
154. Truex, D., Baskerville, R. & Klein, H. (1999). Growing systems in emergent organizations. *Communications of the ACM*, Vol. *42,* No. 8, Pp. 117-123.
155. Tzanou, M. (2013). Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right. *International Data Privacy Law*. Vol. 3. No. 2, Oxford University Press.
156. Unisys Security Insights: Mexico. A consumer viewpoint (2015). Consultado en julio de 2015, desde http://www.unisys.com/ms/unisys-security-insights/mexico.
157. Urpelainen, J. (2014). A strategic theory of effective monitoring arrangements for international institutions. *Journal of Theoretical Politics.* October 2014 vol. 26 no. 4.
158. Van Meter, D. y Van Horn, Carl. (2007). El proceso de implementación de las políticas: un marco conceptual. En Aguilar, L. (Comp.), *La implementación de las políticas* (pp. 97-146). México: Porrúa.
159. Veghes, C.; Acatrinei, C.; Dugulan, D. & Palade, M. (2011). A marketing view over the role of the public authorities in the protection of the consumers' private space. *Annals of the University or Oradea*, *Economic Science Series*. No. 20, Vol. 2. Pp. 811-816.
160. Velasco, C. (2015). Accountability instruments under Mexico's data protection framework. *IAPP's Privaci Tracker.* January 16, 2015.
161. Vélez, N. (2011). *La protección de datos personales en México*. Tesis de maestría. México: UDLAP.
162. Vergara, R. (2010). *Organización e instituciones*. México: Biblioteca Básica de Administración Pública.
163. Villanueva, E. (2010). Derecho a la Vida Privada. Villanueva, E. (Coord.) *Diccionario de Derecho de la Información*. Tomo I. (413-419). México, D.F.: Editorial Jus.
164. Wahid, F. (2011). Explaining History of eGovernment implementation in developing countries: an analytical framework. En Janssen, M. et al (Eds). *Electronic Government*: *10th International Conference*. EGOV, Delft, The Netherlands, August/September 2011. Pp. 38-49.
165. Wiener, Y. (1982). Commitment in organizations: a normative view. *Academy of Management Review.* No. 7. Pp. 418-428.
166. Witte, K. 1992. "Putting the fear back unto fear appeals: The extended parallel process model". *Communication Monographs* (59), pp. 329-349.
167. Wright, D., Friedewald, M. & Gellert, R. (2015). Developing and testing a surveillance impact assessment methodology". *International Data Privacy Law*. Vol. 5. No.1, Oxford University Press.
168. Wright, D., Wadhwa, K., et al. (2014). Integrating privacy impact assessment in risk management. *International Data Privacy Law*. Vol. 4. No.3, Oxford University Press.
169. Wright, D. & Wadhwa, K. (2013). "Introducing a privacy impact assessment policy in the EU member states". *International Data Privacy Law*. Vol. 4. No.3, Oxford University Press.

170. Yin, R. (2011). *Applications of case study research*. Sage.

Anexo 1. Tabla comparativa entre la LFPDPPP y la LFTAIPG

	Sector Privado	Sector Público
Denominación oficial	Ley Federal de Protección de Datos Personales en Posesión de los Particulares	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental / Lineamientos de Protección de Datos Personales
Fecha de publicación	5 de julio de 2010	11 de junio de 2002
Vigencia Ley a partir de	6 de julio de 2010	12 de junio de 2002
Ejercicio del derecho desde	18 meses después de su publicación	12 de junio de 2003
Artículos en ley	69	64
Artículos transitorios	8	11
Reglamento de ley	Al año siguiente después de su entrada en vigor	Sí
Aspectos que regula	Protección de datos personales	Transparencia, acceso a la información, protección de datos personales
Objeto	La protección de los datos personales en posesión de los personales, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.	Proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal. / Establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, para asegurar su tratamiento adecuado e impedir su transmisión ilícita y lesiva para la dignidad y derechos del

		afectado (Cap. I, Primero).
Sujetos obligados	Personas físicas o morales de carácter privado, excepto sociedades de información crediticia y personas sin fines de divulgación.	Poderes Ejecutivo, Legislativo y Judicial de la Federación, órganos constitucionales autónomos, tribunales administrativos federales y cualquier otro órgano federal.
Algunas definiciones	Aviso de privacidad: Documento físico, electrónico o de cualquier otro formato generado por el responsable para disposición del titular. Bases de datos: Conjunto de datos personales referentes a una persona identificada o identificable. Bloqueo: Identificación y conservación de datos personales una vez cumplida la finalidad para determinar posibles responsabilidades con su tratamiento hasta el plazo legal. Consentimiento: Manifestación de la voluntad del titular de los datos mediante la cual se efectúa su tratamiento. Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización pueda dar origen a discriminación o conlleve un riesgo grave para éste. Días: Días hábiles Disociación: Procedimiento mediante el cual los datos personales no pueden asociarse al titular. Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable. Fuente de acceso público: Aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, en conformidad con lo señalado en el Reglamento. Instituto: Instituto Federal de Acceso a la Información y Protección de Datos. Ley: LFPDPP. Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales. Secretaría: Secretaría de Economía. Tercero: La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos. Titular: La persona física a quien corresponden los datos personales. Tratamiento: La obtención, uso, divulgación o almacenamiento	LFTAIPG Datos personales: Cualquier información concerniente a una persona física, identificada o identificable. Instituto: Instituto Federal de Acceso a la Información Pública y Protección de Datos. Información: La contenida en los documentos que los sujetos obligados generen, obtengan, adquieran, transformen o conserven por cualquier título. Información reservada: Aquella información que se encuentra temporalmente sujeta a alguna excepción. Sistema de datos personales: El conjunto ordenado de datos personales que estén en posesión de un sujeto obligado. Unidades administrativas: Las que de acuerdo con la normatividad de cada uno de los sujetos obligados tengan la información de conformidad con las facultades que les correspondan. LDP Destinatario: Cualquier persona física o moral pública o privada que recibe datos personales. Encargado: El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el Responsable para llevar a cabo el tratamiento. Sistema “Persona”: Aplicación informática desarrollada por el Instituto para actualizar el listado de los sistemas de datos personales que posean las dependencias y entidades para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos. Responsable: Servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales. Titular de los datos: Persona física a quien se refieren los datos personales que sean objeto de tratamiento.

	de datos personales, por cualquier medio. Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.	Transmisión: Entrega total o parcial de sistemas de datos a cualquier persona distinta al Titular. Transmisor: Dependencia o entidad que posee los datos personales objeto de la transmisión. Tratamiento: Operaciones y procedimientos físicos o automatizados que permitan recabar, registrar, reproducir, conservar, organizar, modificar, transmitir y cancelar los datos personales. Usuario: Servidor público facultado por un instrumento jurídico o autorizado por el Responsable que utiliza cotidianamente los datos personales.
Principios de protección	Licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.	LFTAIPG: Adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido. LPD: Licitud, calidad, acceso y corrección, de información, seguridad, custodia y consentimiento para su transmisión
Excepciones al consentimiento	isto en una ley, los datos estén en fuentes de acceso público, los sometan a un procedimiento previo de disociación, cumpla nes derivadas de una relación jurídica entre el titular y el ble, exista una situación de emergencia que potencialmente ñar a un individuo en su persona o en sus bienes, y sean ables para cuestiones de salud mientras el titular no esté en es en términos que establece la Ley General de Salud, o cuando esolución de una autoridad competente.	Sean necesarios por razones estadísticas, científicas o de interés general previstas en la Ley, cuando se transmitan entre sujetos obligados o entre dependencias y entidades, cuando exista orden judicial, a terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos, y en los demás casos que establezcan las leyes (Art. 22).
Plazo para eliminar información una vez cumplida su finalidad	72 meses (seis años)	a) El que se haya establecido en el formato físico o electrónico por el cual se recabaron; b) El establecido por las disposiciones aplicables; c) El establecido en los convenios formalizados entre una persona y la dependencia o entidad, y d) El señalado en los casos de transmisión.
Obligaciones del responsable	Velar por el cumplimiento de los principios de protección de datos (Art. 14). Informar a los titulares de los datos la información que se recaba de ellos y con qué fines, mediante el aviso de privacidad	El responsable deberá hacer del conocimiento al Titular de los datos la mención de que serán protegidos en términos de lo dispuesto por la Ley, el fundamento legal y la finalidad del

	(Art. 15). Las vulneraciones de seguridad ocurridas, serán informadas por el responsable al titular, a fin de que pueda tomar las medidas correspondientes (Art. 20). El responsable o terceros deberán guardar confidencialidad, aun después de finalizar su relación con el titular o con el responsable (Art. 21).	Sistema de datos personales (LDP).
Derechos de los Titulares	Acceso, rectificación, cancelación y oposición ante el responsable o terceros (arts. 22 y 25).	Acceso, modificación (Arts. 24 y 25 LFTAIPG).
Plazo para comunicar la determinación adoptada	20 días (art. 32)	
Plazo para proceder	15 días a partir de la notificación (art. 32)	Diez días para acceso (art. 24 LFTAIPG). 30 días para modificación (art. 25 LFTAIPG).
Excepciones a los derechos de los titulares	Cuando el solicitante no sea el titular de los datos personales, o el representante legal no está correctamente acreditado. Cuando el responsable no tiene en su base de datos al solicitante. Cuando lesionen los derechos de un tercero. Cuando haya un impedimento legal o la resolución de una autoridad competente. Cuando la rectificación, cancelación u oposición haya sido realizada anteriormente.	En caso de negarse, el Comité de Información deberá fundar y motivar la improcedencia total o parcial de las modificaciones que se solicitaron, e indicar al titular.
Costos de solicitud	Gratuito (excepto cargos de envío que corren por cuenta del titular). Únicamente se cobrará un costo de no mayor a tres días de salario mínimo vigente en el Distrito Federal, cuando la persona reitera su solicitud en un periodo menor a doce meses.	Gratuito (excepto cargos de envío que corren por cuenta del titular). Si la persona reitera su solicitud en un periodo menor a doce meses el costo no deberá ser superior al costo de los materiales utilizados y el costo de envío.
Transferencia de datos	Necesita el consentimiento del titular para la transferencia a terceros nacionales o extranjeros. No será necesario el consentimiento cuando: La transferencia esté prevista en una Ley o Tratado al que México pertenezca; Sea necesaria para prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la	Se realizarán cuando así lo prevea de forma expresa una disposición legal y cuando medie el consentimiento del titular (Lineamiento vigésimo segundo). No será necesario el consentimiento de acuerdo con lo convenido en el art. 22 de la LFTAIPG: Razones estadísticas, científicas o de interés previstas en la ley.

	gestión de servicios sanitarios; Se realice a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o cualquier sociedad del mismo grupo; Sea necesaria por un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero; Para salvaguardar un interés público, o para la procuración o administración de justicia; Sea precisa para reconocer, ejercer o defender un derecho en un proceso judicial, y Mantenga o cumpla una relación jurídica entre el responsable y el titular.	Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando se utilicen para el ejercicio de facultades propias de los mismos. Cuando exista orden judicial. A terceros, cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales, que no deberán utilizar los datos para propósitos distintos a aquéllos para los que se les transmitieron. En los demás casos que establezcan las leyes.
Obligaciones del Instituto	Difunde el conocimiento del derecho a la protección de datos, promover su ejercicio, vigilar su cumplimiento e imponer sanciones según corresponda (arts. 38 y 39).	Supervisar la protección de los datos y establecer las sanciones correspondientes al incumplimiento de la Ley y los lineamientos (Cap. VII Lineamientos).
Contenido de la solicitud de acceso, rectificación, cancelación u oposición ante el Instituto / Recurso de revisión	Nombre del titular, representante legal y tercero interesado (si es que lo hay). Nombre del responsable ante el cual se presentó. Domicilio para oír y recibir notificaciones. La fecha en que se dio a conocer la respuesta del responsable. Los actos que motivan su solicitud de protección de datos. Demás elementos que considere necesarios. (Art. 46).	Recurso de revisión (art, 54 LFTAIPG): La dependencia o entidad ante la cual se presentó la solicitud. El nombre del recurrente y del tercero interesado (si lo hay), domicilio o medio para recibir notificaciones. Fecha en que se le notificó o tuvo conocimiento del acto reclamado. El acto que se recurre y los puntos de la petición. La copia de la resolución que se reclama y la notificación que corresponde. Los demás elementos que considere necesarios.
Infracciones	No cumplir con la solicitud del titular para los derechos de ARCO con incumplimiento a la Ley. Actuar con negligencia o dolo en el trámite y respuesta de solicitudes de ARCO. Declarar la inexistencia de datos personales, cuando existen total o parcialmente en la base de datos del responsable. Tratar los datos de forma contraria a los principios establecidos. Omitir en el aviso de privacidad, elementos del artículo 16 de esta Ley. Mantener datos inexactos, no realizar las rectificaciones o cancelaciones cuando afecten los derechos de los titulares. No cumplir con el aviso del art. 64. Incumplir el deber de confidencialidad.	Usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar, total o parcialmente y de forma indebida la información. Actuar con negligencia, dolo o mala fe en la sustanciación de las solicitudes de acceso a la información o en la difusión de la información. Denegar información no clasificada como reservada o no confidencial de manera intencional. Clasificar como reservada información que no cumple con las características de la Ley. Entregar información considerada como reservada o confidencial por la Ley. Entregar de manera intencional información no completa requerida en una solicitud de acceso.

	Cambiar sustancialmente la finalidad del tratamiento. Transferir datos a terceros sin comunicar el aviso de privacidad. Vulnerar la seguridad de bases de datos. Transferir datos fuera de los casos que permite la ley. Recabar o transferir datos sin el consentimiento del titular, cuando éste sea exigible. Impedir la verificación de la autoridad. Recabar información de forma fraudulenta. Hacer uso ilegítimo de los datos cuando el Instituto o los titulares han solicitado el cese. Impedir o afectar el ejercicio de los derechos de ARCO. Contravenir el segundo párrafo del artículo 9 de esta Ley. Incumplir con las obligaciones establecidas por lo previsto en esta Ley. (Art. 63).	No proporcionar la información a que se refiere el punto anterior. (Art. 63 LFTAIPG).
Sanciones	Con base en la naturaleza del dato, la improcedencia del responsable, el carácter intencional, la capacidad económica del responsable y la reincidencia, las sanciones serán (arts. 64 y 65): Multa de 100 a 160 mil días de salario mínimo vigente en el Distrito Federal en los siete primeros casos previstos en las infracciones. Multa de 200 a 320 mil días de salario mínimo vigente en el Distrito Federal, en los casos previstas en las fracciones VIII a XVIII de las infracciones. En caso de que persistan las infracciones citadas se impondrá una multa adicional de 100 a 320 mil días de salario mínimo vigente en el Distrito Federal.	Las sanciones derivadas del incumplimiento de esta Ley, se realizarán en los términos de la Ley Federal de Responsabilidades Administrativas de los Servidores públicos (art. 63 LFTAIPG).
Delitos	De tres meses a tres años de prisión a quien tenga autorización para tratar datos personajes y vulnere su seguridad con ánimo de lucro. Prisión de seis meses a cinco años a quien trate datos personales mediante engaño, con lucro indebido, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos. En el caso de datos sensibles, las penas anteriores se duplicarán.	Las responsabilidades administrativas generadas por el incumplimiento a que se refiere el artículo 63, son independientes de las del orden civil o penal que procedan (art. 64).

Anexo 2. Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Inai, 2014).

Lista de comprobación para los principios de licitud y lealtad		A			B		
		Sí	No	NA	Sí	No	NA
1	¿Conoce la LFPDPPP, su Reglamento y la normativa que deriva de la misma y ha identificado sus obligaciones?	X			X		
2	¿Conoce la normativa que en lo particular regula la actividad en la que se tratan los datos personales y ha identificado aquellas disposiciones que pudieran estar vinculadas con el tratamiento de datos personales?	X				X	
3	¿Ha verificado que en su organización los datos personales se traten conforme a la normativa señalada en las preguntas 1 y 2?	X				X	
4	¿Se asegura de que no se obtengan datos personales a través de medios engañosos o fraudulentos?	X			X		
5	¿Se asegura de que la información proporcionada al titular sobre el tratamiento de sus datos personales, a través del aviso de privacidad, es veraz y completa?	X				X	
6	¿Se asegura que los datos personales son tratados conforme a lo informado y acordado con el titular?	X				X	
7	¿Ha adoptado medidas que permitan verificar el cumplimiento de los principios de licitud y lealtad?	X				X	
Lista de comprobación para el principio de consentimiento							
1	¿Se ha verificado para qué finalidades se requiere el consentimiento, de acuerdo con lo dispuesto por el artículo 10 de la LFPDPPP?	X				X	
2	¿El consentimiento se solicita con relación a finalidades concretas informadas en el aviso de privacidad?	X				X	
3	¿Se ha definido qué tipo de consentimiento se requiere: tácito, expreso o expreso y por escrito?	X				X	
4	¿Se da a conocer el aviso de privacidad previo a la solicitud del consentimiento?	X				X	
5	Cuando los datos se obtienen directamente del titular ¿Se solicita el consentimiento previo a la obtención de los datos personales?	X				X	

6	Cuando los datos se obtienen de manera indirecta, el aviso de privacidad se da a conocer por un medio directo (por ejemplo, correo electrónico o teléfono) y se requiere el consentimiento tácito, ¿se verifica que el titular no haya negado su consentimiento para el tratamiento de sus datos personales?	X				X	
7	Cuando los datos se obtienen de manera indirecta, el aviso de privacidad se da a conocer por un medio indirecto (por ejemplo, correo postal) y se requiere el consentimiento tácito ¿se tiene establecido un procedimiento para esperar el plazo de 5 días hábiles para el tratamiento de los datos personales?			X			X
8	Cuando los datos se obtienen de manera indirecta y se requiere el consentimiento expreso o expreso y por escrito ¿se da a conocer el aviso de privacidad correspondiente, se solicita el consentimiento al titular y se espera a su obtención para el tratamiento de los datos personales?			X			X
9	¿Los medios implementados para la obtención del consentimiento son sencillos y gratuitos y acordes con el tipo de consentimiento que se requiere?	X				X	
10	¿Se cuenta con listados para llevar un control de los titulares que han negado su consentimiento y de las finalidades para las cuales no podrán ser tratados los datos personales?	X				X	
11	¿Se generan pruebas para demostrar el cumplimiento del principio de consentimiento?	X				X	
12	En caso de que haya habido cambios en las finalidades y se requiera el consentimiento ¿se solicita el consentimiento y se da a conocer el nuevo aviso de privacidad?	X				X	
13	¿Se lleva un control sobre el plazo de cinco días hábiles que se debe esperar para el tratamiento de los datos personales cuando esta espera es necesaria?	X				X	
14	¿Ha adoptado medidas que permitan verificar el cumplimiento del principio de consentimiento?	X				X	
Lista de comprobación para el principio de información							
1	¿Cuenta con los avisos de privacidad necesarios, según los tratamientos que se realizan, para informar a los titulares sobre las características principales del tratamiento al que serán sometidos sus datos personales?	X			X		
2	Cuando recaba datos de forma personal o directa ¿da a conocer el aviso de privacidad previo a la obtención de los datos?	X			X		
3	Cuando obtiene datos de forma indirecta, ya sea a través de una transferencia o fuente de acceso público, y el tratamiento implica contacto con el titular ¿da a conocer el aviso de privacidad al primer contacto con este?			X			X
4	Cuando obtiene datos de forma indirecta, ya sea a través de una transferencia o fuente de acceso público, y el tratamiento no implica contacto con el titular, pero tiene datos para contactarlo ¿da a conocer el aviso de privacidad previo al aprovechamiento de los datos personales?			X			X
5	Cuando hay cambio de finalidades ¿da a conocer el aviso de privacidad previo al	X				X	

	aprovechamiento de los datos personales?						
6	¿Toma en cuenta el perfil de los titulares para la redacción del aviso de privacidad? ¿ha verificado que en el aviso de privacidad no se utilicen frases inexactas, ambiguas o vagas? ¿ha verificado que no se incluyan textos o formatos que induzcan al titular a elegir una opción en específico? ¿ha verificado que no se incluyan casillas pre-marcadas? ¿ha verificado que los textos a los que se remitan estén disponibles?	X				X	
7	¿El aviso de privacidad se encuentra ubicado en un lugar visible y de fácil consulta?	X			X		
8	¿Comunica el aviso de privacidad a encargados y terceros siempre que lleva a cabo una remisión o transferencia?	X				X	
9	¿Procura establecer mecanismos para generar evidencia de que se está cumpliendo con el principio de información?	X				X	
10	¿Se ha verificado que el aviso de privacidad en cualquiera de sus modalidades (integral, simplificado o corto) contenga todos los elementos informativos que exige la norma?	X			X		
11	¿Pone a disposición de los titulares el aviso de privacidad integral cuando los datos personales se obtienen de manera personal?	X			X		
12	¿Utiliza el aviso de privacidad simplificado sólo en los casos en que los datos personales se obtienen de manera directa?	X				X	
13	¿Utiliza el aviso de privacidad corto sólo en aquellos casos en los que los datos personales obtenidos son mínimos y el espacio para obtenerlos y dar a conocer el aviso es mínimo y limitado?	X				X	
14	¿Ha verificado que el aviso de privacidad integral esté disponible en el medio que se informó en el aviso de privacidad simplificado o corto?	X				X	
15	¿Los medios ofrecidos para consultar el aviso de privacidad son de acceso gratuito?	X				X	
16	Cuando así ocurre ¿informa en su portal de Internet sobre el uso de tecnologías de rastreo, que a través de estas se obtienen datos personales y la forma en que se pueden deshabilitar?			X			X
17	¿Pone a disposición de los titulares un nuevo aviso de privacidad en los supuestos en que así lo exige la norma?	X			X		
18	¿Ha adoptado medidas que permitan verificar el cumplimiento del principio de información?	X				X	
Lista de comprobación para el principio de proporcionalidad							
1	¿Se asegura de que los datos personales que trata son necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron?	X				X	
2	¿Realiza esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios?	X				X	
3	En el caso de los datos personales sensibles ¿limita el periodo de tratamiento al mínimo necesario?	X				X	
4	Si trata datos personales sensibles ¿ha verificado que dicho tratamiento obedezca a alguno	X				X	

	de los supuestos permitidos por la norma?						
5	¿Ha adoptado medidas que permitan verificar el cumplimiento del principio de proporcionalidad?	X				X	
Lista de comprobación para el principio de finalidad							
1	¿Las finalidades para las que se tratan los datos personales están previstas en el aviso de privacidad y, en su caso, fueron consentidas por el titular?	X				X	
2	¿Se incluyen en el aviso de privacidad todas las finalidades para las cuales se tratan los datos personales? ¿las finalidades son determinadas, es decir, claras, objetivas y que no den lugar a confusión?	X				X	
3	¿En el aviso de privacidad se distingue claramente las finalidades secundarias de las primarias?	X				X	
4	¿Tiene implementados mecanismos para que el titular pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias? ¿se informa en el aviso de privacidad sobre esos mecanismos? ¿Están disponibles para que el titular, en su caso, manifieste su negativa antes de que sus datos personales se traten para las finalidades secundarias?	X			X		
5	Cuando el aviso de privacidad se da a conocer a través de un medio indirecto, como el correo postal ¿informa al titular en el aviso de privacidad, que tiene cinco días hábiles para manifestar su negativa para el tratamiento de su información para finalidades secundarias? ¿tiene implementado mecanismos para no tratar los datos personales antes de que concluya dicho periodo?			X			X
6	¿Ha verificado que en sus procedimientos no se condicione el tratamiento para finalidades primarias, a que el titular consienta las finalidades secundarias?	X				X	
7	¿Solicita el consentimiento de los titulares para el tratamiento de sus datos personales para finalidades nuevas, que no fueron prevista de origen en el aviso de privacidad? O bien ¿ha verificado que alguna ley o reglamento permitan específicamente dicho tratamiento?	X				X	
8	¿Ha adoptado medidas que permitan verificar el cumplimiento del principio de finalidad?		X			X	
Lista de comprobación para el principio de calidad							
1	¿Ha adoptado medidas para procurar que los datos personales que trata sean exactos, completos, pertinentes, actualizados y correctos?	X				X	
2	¿Actualiza o corrige los datos personales cuando cuenta con evidencia objetiva que así lo justifique?	X				X	
3	¿Ha establecido el plazo de conservación de los datos personales? ¿considera en este plazo los tres elementos esenciales: (i) tiempo necesario para llevar a cabo las finalidades, (ii) cumplimiento de aspectos legales, administrativos, contables, fiscales, jurídicos e históricos, y (iii) periodo de bloqueo (plazos legales y contractuales para demostrar posibles responsabilidades)?	X				X	

4	En su caso ¿elimina los datos personales relacionados con incumplimiento de obligaciones contractuales en un plazo de 72 meses, contados a partir de la fecha en que se presente el mencionado incumplimiento?		X			X	
5	¿Bloquea los datos personales previo a su supresión, en el momento en que ello se requiere? ¿se asegura de que ninguna persona trate los datos personales que se encuentran en periodo de bloqueo?	X			X		
6	¿Se suprimen los datos personales una vez que concluyó el plazo de conservación? ¿tiene establecido procedimientos seguros para la eliminación de los datos personales?	X				X	
7	¿Tiene documentados los procedimientos de conservación, bloqueo y supresión de los datos personales?		X			X	
8	¿Cuenta con evidencia de que los datos personales se conservan, bloquean y suprimen atendiendo el principio de cancelación o en respuesta a una solicitud de ejercicio del derecho de cancelación?		X			X	
9	Cuando ello se requiere ¿informa a los encargados que manejan bases de datos a su nombre, sobre las modificaciones realizadas a los datos personales?	X				X	
10	¿Ha adoptado medidas que permitan verificar el cumplimiento del principio de calidad?		X			X	
Lista de comprobación para el principio de responsabilidad							
1	¿Ha adoptado medidas para procurar que los datos personales que trata sean exactos, completos, pertinentes, actualizados y correctos?	X				X	
2	¿Actualiza o corrige los datos personales cuando cuenta con evidencia objetiva que así lo justifique?	X				X	
3	¿Ha establecido el plazo de conservación de los datos personales? ¿considera en este plazo los tres elementos esenciales: (i) tiempo necesario para llevar a cabo las finalidades, (ii) cumplimiento de aspectos legales, administrativos, contables, fiscales, jurídicos e históricos, y (iii) periodo de bloqueo (plazos legales y contractuales para demostrar posibles responsabilidades)?	X				X	
Lista de comprobación del deber de confidencialidad							
1	¿Tiene implementadas medidas para garantizar la confidencialidad de los datos personales que trata?	X				X	
2	¿Se asegura de que sus empleados, encargados o terceros guarden confidencialidad respecto de los datos personales a los que tienen acceso?	X				X	
3	¿Prevé sanciones en caso de incumplimiento del deber de confidencialidad?	X				X	
Lista de comprobación de la relación responsable-encargado							
1	¿La relación con el encargado está establecida mediante un instrumento jurídico que permita comprobar su existencia, alcance y contenido?	X				X	
2	¿Los acuerdos con el encargado se basan en lo previsto en el aviso de privacidad en el que se definieron las condiciones del tratamiento?	X				X	
3	¿En el instrumento jurídico que se establecen las condiciones de la relación con el	X				X	

	encargado se contemplan, al menos, las obligaciones del artículo 50 del Reglamento de la LFPDPPP?						
4	¿Ha quedado establecida la obligación del encargado de solicitar la autorización del responsable para realizar subcontrataciones que involucren el tratamiento de datos personales?	X				X	
5	¿Los servicios de cómputo en la nube que tiene contratados o que pretende contratar cumplen con los requisitos del artículo 52 del reglamento de la LFPDPPP?			X			X
6	¿Verifica que el encargado cumpla con sus obligaciones en torno a la protección de los datos personales?	X				X	
Lista de comprobación con el deber de seguridad							
1	¿Cuenta con un inventario de bases de datos?		X			X	
2	¿Determina las funciones y obligaciones de las personas que traten datos personales?	X				X	
3	¿Realiza un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos?	X				X	
4	¿Establece las medidas de seguridad aplicables a los datos personales e identifica aquellas implementadas de manera efectiva?		X			X	
5	¿Realiza el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales?		X			X	
6	¿Cuentan con un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha		X			X	
7	¿Llevan a cabo revisiones o auditorías?		X			X	
8	¿Capacitan al personal que efectúa el tratamiento?	X				X	
9	¿Notifican al titular en caso de vulneración de seguridad?	X				X	
Lista de comprobación de las transferencias							
1	Cuando no se actualiza alguna de las causales del artículo 37 de la LFPDPPP ¿solicita el consentimiento de los titulares para la transferencia?	X				X	
2	¿Informa en el aviso de privacidad que realiza transferencias, a quién y para qué finalidades?	X				X	
3	Cuando se requiere ¿incluye en el aviso de privacidad la cláusula para solicitar el consentimiento del titular?	X				X	
4	¿Realiza transferencias exclusivamente para las finalidades que establece el aviso de privacidad y a los terceros ahí señalados?	X				X	
5	¿Se asegura de comunicar a los terceros receptores el aviso de privacidad y las condiciones en las que el titular sujetó el tratamiento de sus datos personales?	X				X	
6	¿Cuenta con evidencia de que las transferencias se realizaron de acuerdo con lo que señala la norma?	X				X	
7	Cuando la transferencia es nacional ¿la formaliza mediante instrumento jurídico que permita	X				X	

	demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales?						
8	Cuando usted es el responsable receptor de datos personales ¿utiliza los datos recibidos exclusivamente para los fines que se establecieron en el aviso de privacidad y que, en su caso, consintió el titular? O bien, si desea tratar los datos para nuevas finalidades ¿solicita el consentimiento y pone a disposición del titular el aviso de privacidad?	X				X	
9	Cuando se trata de transferencias internacionales ¿transfiere los datos exclusivamente cuando el tercero receptor asume las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales?	X				X	
10	Cuando se trata de transferencias internacionales ¿las formaliza mediante instrumento jurídico que prevea al menos las mismas obligaciones para el tercero receptor, a las que se encuentra sujeto el responsable que transfiere los datos personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales?	X				X	

Anexo 3. Guía de preguntas

Fecha: _____ Hora: _____ Folio: _____

Organización: _____

Entrevistado: _____

Cargo: _____

Introducción

Estimado entrevistado:

Agradecemos su participación y confianza en esta investigación.

La entrevista es para conocer más sobre la implementación de políticas de protección de datos personales en las organizaciones.

Queremos hacer de su conocimiento que será grabado en audio. Usted puede estar completamente seguro de que su identidad y la de su organización serán estrictamente confidenciales. La información que usted provea únicamente será utilizada para los fines de esta investigación. Le pedimos que conteste a cada pregunta con total honestidad.

Su colaboración es muy importante para realizar exitosamente esta investigación, muchas gracias por su ayuda.

A continuación, procederemos a la entrevista.

1. ¿Cuál fue el motivo principal por el que la organización cumple con la ley?
2. Las multas de la ley van desde los 100 a los 320 mil días de salario mínimo (vigentes en la Ciudad de México). ¿Las sanciones establecidas en la ley generan temor para que la organización a cumpla con los procedimientos y se abstenga de cometer una infracción?
3. ¿La organización habría cumplido con la Ley si no existieran las multas? ¿Cuál sería la razón?
4. ¿La organización ha recibido alguna inspección por parte de una autoridad/superior para verificar el cumplimiento de la protección de datos personales? ¿Cómo ha sido?
5. ¿Sería importante que evalúen a la organización con periodicidad para verificar el cumplimiento con la protección de datos personales?
6. ¿El monitoreo por parte de una autoridad como el Inai afectaría las actividades con respecto al uso que hace de los datos personales en la organización?

7. ¿La organización ha recibido alguna inspección por parte de una autoridad/superior para verificar el cumplimiento de la protección de datos personales? ¿Cómo ha sido?
8. ¿Sería importante que evalúen a la organización con periodicidad para verificar el cumplimiento con la protección de datos personales?
9. ¿El monitoreo por parte de una autoridad como el Inai modificaría las conductas con respecto al uso que hace de los datos personales en la organización?
10. ¿En quién recayó la decisión de implementar la ley en su organización para proteger los datos personales?
11. ¿La dirección propicia el cumplimiento con la protección de los datos personales en la organización?
12. ¿Alguna vez han hecho algo como comprar bases de datos para contactar a posibles usuarios o le han ofrecido dinero a cambio de una base de datos que pertenece a la organización? Si no, ¿qué haría en el supuesto de que ocurriera?
13. ¿Considera que la organización protegería los datos personales si no existieran las sanciones de la ley? ¿Por qué?
14. ¿La organización realiza programas de capacitación para incrementar el conocimiento sobre las reglas del uso de los datos personales?
15. ¿Estar capacitado sobre cómo usar los datos personales tiene algún impacto en el tratamiento que se hace de ellos en la organización?
16. ¿Qué prácticas implementa la organización para garantizar la protección de los datos personales con las TIC?
17. ¿Han tenido alguna fuga de información como archivos o bases de datos desde computadoras o el servidor que haya afectado a la organización? ¿Cómo lo han resuelto?
18. ¿Es importante para la organización que sus clientes confíen que sus datos personales están seguros? ¿Sus clientes están preocupados por el uso de sus datos personales?
19. ¿Qué tipo de actividades realizan en la organización para que sus clientes sepan que sus datos estarán seguros?
20. ¿Realizan actividades como llamar o enviar correos electrónicos a sus prospectos sin su consentimiento?

Anexo 4. Aviso de Privacidad Integral del Caso 1

Aviso de privacidad para padres de familia y alumnos
XXX, en lo sucesivo XXX, con domicilio fiscal XXX, Puebla, Pue., México, y página de internet XXX, es responsable del uso y protección de sus datos personales, necesarios para la prestación de servicios educativos en cumplimiento a lo establecido por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, y al respecto hacemos de su conocimiento lo siguiente.
Para XXX resulta necesaria la recopilación de ciertos datos personales para llevar a cabo las operaciones propias del servicio educativo dentro del marco legal y de seguridad necesario para proteger sus datos personales y cumplir con las finalidades descritas en este aviso de privacidad con objeto de otorgarle pleno control y decisión sobre la información que nos proporciona.

¿Para qué fines utilizaremos sus datos personales?
Para otorgar nuestro servicio educativo, XXX podrá utilizar los datos personales proporcionados por el titular, padre de familia o de quien ejerce la patria potestad para los siguientes fines:

- Proceso de admisión,
- Proceso de enseñanza para los niveles de Preescolar, Primaria, Secundaria y Preparatoria conforme a los programas educativos registrados con reconocimiento y validez oficial de estudios ante autoridades educativas nacionales e internacionales, lo cual incluye el fortalecimiento de la formación integral del alumnado en aspectos psicológicos, físicos, sociales y éticos,
- Control de acceso a los planteles escolares para fines de seguridad,
- Para cuidar la salud del alumnado y establecer comunicación con los contactos autorizados,
- Trámite de solicitudes de beca,
- Emisión y registro de facturación,
- Reportes a autoridades administrativas, educativas y fiscales en cumplimiento de las disposiciones vigentes,
- Proporcionar informes para efectos legales a las autoridades competentes.

Conforme a lo establecido por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, con la firma en el Contrato por Servicios Educativos base de la relación jurídica, el padre de familia o quien ejerce la patria potestad manifiesta su conformidad y consentimiento expreso con el documento denominado Condiciones Generales - Ciclo Escolar 2016 -2017 y con el presente Aviso de Privacidad para padres de familia y alumnos para el tratamiento de los datos del titular incluyendo los

patrimoniales y financieros proporcionados en trámites de beca o en la solicitud de sus derechos de Acceso, Rectificación, Cancelación y Oposición (derechos ARCO).
De manera adicional, podremos utilizar su información personal para las siguientes finalidades secundarias que no son condicionales para el servicio educativo solicitado, pero que nos permiten y facilitan brindarle una mejor atención:

- Listas de espera para prospectos de ingreso al XXX,
- Registro de ex alumnos para mantener contacto, conocer su trayectoria y proporcionarle beneficios especiales como parte de la comunidad XXX,
- Seguridad dentro y fuera de los planteles escolares, en viajes de estudio, o en eventos escolares en los que el alumno participe como parte de su formación académica,
- Reportes e informes para efectos de disciplina o para la emisión de constancias de participación,
- Uso de imágenes (video y fotografía) para fines de promoción y los que deriven de las relaciones institucionales del XXX en redes sociales y en diferentes medios de comunicación y transmisión de datos,
- Mercadotecnia o publicidad.

En caso de que no desee que sus datos personales sean tratados para estos fines secundarios, Usted cuenta con un plazo de cinco días hábiles contados a partir de la fecha de la firma del Contrato por Servicios Educativos con Fundación Colegio Americano de Puebla para solicitarlo directamente al área de Datos Personales mediante el envío de un correo electrónico dirigido a XXX y llenar el formulario correspondiente. Para el caso de imágenes, deberá llenar el Aviso para no hacer uso de imágenes, el cual deberá entregar directamente en la oficina de datos personales para ser incluido en los listados de exclusión.
En caso de no manifestar su negativa, transcurrido ese plazo XXX asumirá que cuenta con su consentimiento tácito.
La negativa para el uso de sus datos personales para estas finalidades secundarias no podrá ser un motivo para que le neguemos los servicios educativos.

¿Qué datos personales recabamos?
Para llevar a cabo las finalidades descritas en el Aviso de Privacidad para padres de familia y alumnos, es indispensable que sus datos sean completos, veraces, exactos y actuales. En caso de que no sean correctos o sea necesario actualizarlos le solicitamos atentamente lo notifique de acuerdo con lo establecido en el presente aviso de privacidad.
XXX puede recabar por teléfono, correo electrónico, página web y de manera directa del titular, padre de familia o de quien ejerce la patria potestad los siguientes datos personales:

- Datos de identificación: nombre completo, lugar y fecha de nacimiento, nacionalidad, calidad migratoria, Clave Única de Registro de Población (CURP), dirección, colonia o fraccionamiento, ciudad, código postal, teléfonos, información migratoria, profesión, ocupación, correos electrónicos de contacto.
- Datos laborales del padre de familia o responsable legal: ocupación, título o profesión, nombre de la empresa o institución, dirección de la empresa o institución, puesto, teléfono directo o extensión, correo institucional.

- Datos de facturación: Registro Federal de Contribuyentes (RFC), nombre o razón social de la empresa o institución, y domicilio fiscal, municipio, estado, código postal y correo electrónico para envío del comprobante fiscal digital por internet (CFDI).
- Datos bancarios como número de cuenta o tarjeta con la que efectúa el pago de cuotas.
- Datos patrimoniales en caso de trámite de beca para la realización de estudio socio-económico, situación financiera de la familia, comprobante de ingresos reciente del padre o madre, número de familia, nombre y número del alumno, calificaciones, grado y nivel, fotografía, acta de nacimiento.
- Datos del alumno: lugar y fecha de nacimiento, edad, nacionalidad, calidad migratoria, Clave Única de Registro de Población (CURP), escuela de procedencia, último grado cursado, grado y ciclo al que se desea inscribir, boleta de calificaciones, diplomas y certificados del alumno, constancia de estudios.
- Datos de familia, o contacto en caso de emergencia incluyendo del médico tratante proporcionando nombre, dirección y teléfono fijo o celular.

Además de los datos personales mencionados anteriormente, para las finalidades informadas en el presente Aviso de Privacidad para padres de familia y alumnos podremos recabar los siguientes datos personales considerados como sensibles por la Ley, que requieren de especial protección como son:

- Datos de salud: tipo de sangre, alergias, enfermedades crónicas, cuidados especiales, hábitos alimenticios, estatura, peso y talla.
- Datos psicológicos para dar seguimiento al desarrollo de los alumnos por parte de las(os) Consejeros escolares.
- Hospital público a referir, Instituto Mexicano del Seguro Social (IMSS), Instituto de Seguridad y Servicio Social de los Trabajadores al Servicio de los Poderes del Estado de Puebla (ISSSTEP) o Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE) y clínica de adscripción.
- Hospital privado a referir, nombre, dirección y teléfono del médico tratante.
- Contactos de emergencia: nombre y teléfonos de familiares.
- Datos financieros para la emisión, en su caso, de Comprobantes Fiscales Digitales por Internet (CFDI's).

Con la autenticación mediante el nombre de usuario y contraseña, y el llenado del formulario de Datos de Familia en la sección Mis Hijos disponible en el portal XXX, Usted otorga su consentimiento expreso para el tratamiento de sus datos sensibles y financieros conforme a los términos y condiciones el presente Aviso de Privacidad para padres de familia y alumnos.

¿Con quién compartimos su información personal y para qué fines?

Le informamos que sus datos personales pueden ser compartidos dentro y fuera del país con las siguientes personas, empresas, organizaciones o autoridades distintas a nosotros, para los siguientes fines:

Destinatario de los datos personales	Finalidad

Destinatario de los datos personales	Finalidad
Secretaría de Educación Pública (SEP), Benemérita Universidad Autónoma de Puebla (BUAP), Organización de Bachillerato Internacional (IB)	Reconocimiento de estudios con validez oficial y en cumplimiento a requerimientos de información
Auditores y autoridades fiscales, Secretaría de Gobernación por asuntos migratorios, Juzgados de lo familiar a requerimiento expreso, Ministerios públicos a requerimiento expreso	Para cumplir con requerimientos de información por parte de autoridades oficiales
Compañías aseguradoras, hospitales, médicos, proveedor de fotografías y credenciales para acceso a planteles	Cuidado de la salud y seguridad
Hoteles, agencias de viaje, aerolíneas	Logística de viajes de estudio
Asociación de Colegios Americanos de México (ASOMEX), escuelas, institutos y universidades, asociaciones de árbitros	Realización de eventos académicos y escolares (culturales, artísticos y torneos deportivos)

Para las transferencias marcadas con asterisco requerimos de su consentimiento.

Con relación a las transferencias que requieren su consentimiento, ponemos a su disposición el mecanismo que se indica en el siguiente párrafo para que, en su caso, nos lo otorgue. Le recordamos que, si después de leer este aviso de privacidad para padres de familia y alumnos no nos otorga su consentimiento, dichas transferencias no se podrán realizar, quedando inhabilitado el alumno para poder participar en eventos culturales, artísticos y torneos deportivos, así como en viajes de estudio.
Para el caso de las transferencias mencionadas con anterioridad relacionadas con la participación del alumno en eventos académicos y escolares (culturales, artísticos y torneos deportivos) o con la realización de los viajes de estudio, deberá entregar en las oficinas de la Dirección Técnica organizadora la Carta Autorización del Padre de Familia o de quien ejerce la patria potestad y la Hoja Médica que en su caso se le solicite en donde conste su autorización expresa y por escrito previo a la realización del evento.
Con la firma del Contrato por Servicios Educativos manifiesta estar de acuerdo con el presente Aviso de Privacidad para padres de familia y alumnos en lo que respecta a la transferencia de datos con relación al cuidado de la salud y seguridad física del alumno.
En caso de no contar con estos datos hacemos constar que no estaríamos en posibilidad de brindarle ciertos servicios para cumplir con nuestros fines.

¿Cómo puede acceder, rectificar o cancelar sus datos personales, u oponerse a su uso?
Usted tiene derecho a acceder a sus datos personales que poseemos, y a los detalles del tratamiento de los mismos (Acceso). Asimismo, es su derecho solicitar la corrección de su información personal en caso de que esté desactualizada, sea inexacta o incompleta (Rectificación), o que la eliminemos de nuestros registros o bases de datos cuando considere que no se requieren para

alguna de las finalidades descritas en el presente Aviso de Privacidad para padres de familia y alumnos (Cancelación) u oponerse al uso de sus datos personales para fines específicos (Oposición). Estos derechos se conocen como derechos ARCO.
El procedimiento y requisitos para el ejercicio de sus derechos ARCO, se informa a continuación:
Para el ejercicio de cualquiera de los derechos ARCO, en el portal XXX. Usted tiene disponible el Aviso de Privacidad para padres de familia y alumnos, el formato "Solicitud de derechos ARCO y/o Revocación del consentimiento" que deberá completar e imprimir adjuntando la documentación en él indicada que acredite su identidad como titular, padre de familia o de quien ejerce la patria potestad, y presentarla:

1. Mediante el envío al correo electrónico XXX, indicando como asunto “Derechos ARCO y/o Revocación del consentimiento”, o bien,
2. Acudiendo al área de Datos Personales ubicada en XXX Puebla, Pue. en horario de 8 a 14 horas de lunes a viernes a entregar su documentación completa y en donde también le podrán orientar en el llenado de su solicitud.

¿A través de qué medios puede acreditar su identidad el titular, padre de familia o quien ejerce la patria potestad?
El mecanismo que se ha implementado para el ejercicio de sus derechos es a través de la “Solicitud de derechos ARCO y/o Revocación del consentimiento”, adjuntando los documentos en él solicitados que acrediten la identidad del titular, padre de familia o de quien ejerce la patria potestad.

¿Qué información y/o documentación deberá contener la solicitud?
Su solicitud deberá contener:

1. Nombre del titular, padre de familia o de quien ejerce la patria potestad y número de familia, datos de identificación como: fecha de nacimiento, Registro Federal de Contribuyentes (RFC), domicilio, teléfono y correo electrónico para comunicarle la respuesta a su solicitud.
2. Adjuntar copia simple de los documentos que acrediten la identidad del titular, padre de familia (credencial de elector, cédula profesional, pasaporte, cartilla el servicio militar o documento migratorio) y en el caso de quien ejerce la patria potestad, documento que acredite la representación legal del titular (instrumento notarial en donde consten sus facultades y credencial de elector).
3. Descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y
4. Cualquier otro elemento o documento que pueda aportar para facilitar la localización de los datos personales.

En ciertas circunstancias XXX podrá solicitarle los documentos en original para cotejo.
Si la solicitud del titular, padre de familia o de quien ejerce la patria potestad no es clara, es errónea o incompleta, XXX podrá solicitarle información adicional durante los siguientes 5 días hábiles y el solicitante tendrá 10 días hábiles para atender el requerimiento. De no dar respuesta, la solicitud se tendrá por no presentada.

¿En cuántos días le daremos respuesta a su solicitud?
XXX comunicará en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud de acceso, rectificación, cancelación u oposición y/o revocación del consentimiento, y la documentación completa, la determinación adoptada. Si la solicitud es procedente, se hará efectiva dentro de los 15 días hábiles siguientes a la fecha en que se haya comunicado la respuesta anterior.
Los plazos antes referidos podrán ser ampliados una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

¿Por qué medio le comunicaremos la respuesta a su solicitud?
XXX comunicará al titular, padre de familia o a quien ejerce la patria potestad al correo electrónico que indique en la "Solicitud de derechos ARCO y/o Revocación del consentimiento" la respuesta a su solicitud en los plazos indicados con anterioridad. Sin embargo, XXX tiene la facultad de negar el ejercicio de los derechos ARCO cuando:

- La identidad del titular, padre de familia o de quien ejerce la patria potestad no se acrediten debidamente.
- No se encuentren los datos personales en la base de datos.
- Se lesionen derechos de terceros a criterio de los abogados del XXX.
- La rectificación, cancelación u oposición haya sido realizada previamente.
- Exista impedimento legal o resolución de autoridad que restrinja estos derechos.

¿En qué medios se pueden reproducir los datos personales que, en su caso, solicite?
Cuando se trate de solicitudes de acceso a datos personales, la entrega procederá previa validación del formato de "Solicitud de derechos ARCO y/o Revocación del consentimiento", y de los documentos que acrediten la identidad del solicitante, padre de familia o quien ejerce la patria potestad según corresponda para posteriormente poner a disposición sus datos solicitados mediante la expedición de copias simples.
Ponemos a sus órdenes los siguientes formularios o sistemas para facilitar el ejercicio de derechos ARCO:
En el portal XXX sección Aviso de Privacidad para padres de familia y alumnos, se encuentra disponible el formato "Solicitud de derechos ARCO y/o Revocación del consentimiento".
Para mayor información sobre el procedimiento, ponemos a disposición los siguientes medios:
Enviando un correo electrónico a XXXo acudiendo al área de Datos Personales ubicada en XXX Puebla, Pue. en horario de 8 a 14 horas de lunes a viernes o llamando al teléfono XXX para recibir orientación sobre el llenado de la solicitud.

Revocación del consentimiento
Usted puede revocar el consentimiento que, en su caso, nos haya otorgado para el tratamiento de sus datos personales. Sin embargo, es importante que tenga en cuenta que no en todos los casos podremos atender su solicitud o concluir el uso de forma

inmediata, ya que es posible que por alguna obligación legal requiramos seguir tratando sus datos personales. Asimismo, deberá considerar que, para ciertos fines, la revocación de su consentimiento implicará que no le podamos seguir prestando el servicio que solicitó, o la conclusión de su relación con nosotros.
Para revocar su consentimiento deberá acceder al portal del XXX sección Aviso de Privacidad para padres de familia y alumnos, para obtener y completar el formato en el apartado "Solicitud de derechos ARCO y/o Revocación del consentimiento".
El procedimiento y requisitos para la revocación del consentimiento, es el señalado para ejercer los derechos ARCO mediante el llenado del formato de solicitud y presentación de la documentación que acredite la identidad del titular, padre de familia o de quien ejerce la patria potestad.

¿Cómo puede limitar el uso o divulgación de su información personal?
Con objeto de que pueda limitar el uso y divulgación de su información personal, le ofrecemos los siguientes medios:
Usted podrá dejar de recibir mensajes para promocionar nuestros servicios y oferta educativa por teléfono y correo electrónico o postal enviando un correo electrónico al área de Datos Personales a la dirección, XXX con el asunto "Limitación de uso o divulgación".
XXX elaborará Listados de exclusión por aquellos titulares de quienes no se desee que sus datos sean tratados para ciertas finalidades descritas en el Aviso de Privacidad para padres de familia y alumnos vigente, o en caso de que no se desee recibir publicidad de nuestra parte.

Uso de tecnologías de rastreo en nuestro portal de internet
Le informamos que en nuestra página de internet XXX utilizamos "cookies", "web beacons" y otras tecnologías a través de las cuales es posible monitorear su comportamiento como usuario de internet, así como brindarle un mejor servicio y experiencia al navegar en nuestra página. Las "cookies" son archivos que almacenan información en el disco duro o navegador del usuario permitiendo que las páginas "web" lo reconozcan y sepan que ya han sido visitadas con anterioridad y las "web beacons" son archivos que permiten conocer de manera personalizada los accesos a los sitios de internet.
Los datos personales que recabamos a través de estas tecnologías, los utilizaremos para los siguientes fines:

- Inscripción del alumno en nuestro sistema escolar y de cobranza
- Proceso de facturación
- Verificación y confirmación de identidad de familias y alumnos

Las "cookies", "web beacons" y otras tecnologías pueden ser deshabilitadas excepto aquellas que sean necesarias para el propio funcionamiento de la página de internet o sistema de que se trate.
Para conocer cómo hacerlo, puede consultar la sección de ayuda del navegador de su preferencia.
Asimismo, le informamos que su información personal será compartida con las siguientes áreas y procesos internos de XXX únicamente para llevar a cabo las actividades propias al servicio educativo con los siguientes fines:

Destinatario de los datos personales	Finalidad
Admisiones	Asignación de número de familia y de alumno y control escolar
Áreas académicas	Registro y control de alumnos y reportes a organizaciones para reconocimiento de validez oficial de estudios, listas de alumnos por grupo
Contabilidad	Para registro de cuotas, cobranza y control de facturación
Relaciones Institucionales	Para fines de promoción y los que deriven de las relaciones institucionales de XXX, publicación de imágenes (video y fotografía) en redes sociales y en diferentes medios de comunicación
Informática	Para programación del proceso escolar, elaboración de grupos por grados, cobranza, becas otorgadas, control de facturación emitida, respaldo y resguardo de datos e información
Centro de medios	Listas de grupos y grados para control de biblioteca
Recursos Humanos	Para contratación y cobertura de seguro educativo y escolar
Educación deportiva y artística	Para integración de equipos y lista de participantes a torneos y logística de viajes en eventos escolares (artísticos y deportivos)
Auditores externos y autoridades oficiales	A requerimiento de autoridad mediante escrito debidamente fundamentado
Médicos y hospitales	Para brindar atención médica de emergencia y cuidados especiales necesarios

XXX dentro de un marco legal y de seguridad necesarios protege sus datos personales con objeto de otorgarle pleno control y decisión sobre la información que nos proporciona.

¿Cómo puede conocer los cambios en el Aviso de Privacidad para padres de familia y alumnos?

XXX se reserva el derecho de efectuar en cualquier momento modificaciones o actualizaciones al presente Aviso de Privacidad para padres de familia y alumnos, en atención a disposiciones legales, políticas internas o nuevos requerimientos para la prestación de nuestros servicios y oferta educativa. A través de una circular XXX le mantendrá informado y para conocer el detalle y la última fecha de actualización le sugerimos consultar periódicamente nuestro Aviso de Privacidad para padres de familia y alumnos accediendo a la página XXX.

Anexo 5. Aviso de Privacidad del Caso 2

Con fundamento en los artículos 15 y 16 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares hacemos de su conocimiento que XXXXXXXX, con domicilio en XXXXXXX es responsable de recabar sus datos personales, del uso que se le dé a los mismos y de su protección.

Su información personal será utilizada para las siguientes finalidades: proveer los servicios y productos que ha solicitado; notificarle sobre nuevos servicios o productos que tengan relación con los ya contratados o adquiridos; comunicarle sobre cambios en los mismos; elaborar estudios y programas que son necesarios para determinar hábitos de consumo; realizar evaluaciones periódicas de nuestros productos y servicios a efecto de mejorar la calidad de los mismos; evaluar la calidad del servicio que brindamos, y en general, para dar cumplimiento a las obligaciones que hemos contraído con usted.

Para las finalidades antes mencionadas, requerimos obtener los siguientes datos personales:

- Nombre completo
- Edad
- Estado civil
- Sexo
- Teléfono fijo y/o celular
- Correo electrónico
- Firma autógrafa
- Dirección
- Nivel de escolaridad
- RFC y/o CURP
- Nivel de ingreso

Con base en la ley en materia de protección de datos personales en posesión de particulares, los siguientes datos son considerados sensibles:

- Padecimientos de salud

Es importante informarle que usted tiene derecho al Acceso, Rectificación y Cancelación de sus datos personales, a Oponerse al tratamiento de los mismos o a revocar el consentimiento que para dicho fin nos haya otorgado.

Para ello, es necesario que envíe la solicitud en los términos que marca la Ley en su Art. 29 a NOMBRE DE LA PERSONA RESPONSABLE, responsable de nuestro Departamento de Protección de Datos Personales, ubicado en DOMICILIO, o bien, se comunique al teléfono XXXXX o vía correo electrónico a XXXXX@hotmail.com, el cual solicitamos confirme vía telefónica para garantizar su correcta recepción.

Importante: Cualquier modificación a este Aviso de Privacidad podrá consultarlo en DIRECCIÓN DE PÁGINA WEB.

Fecha de actualización: 19/02/2013