Experiencias Internacionales y Nacionales

Estudio para Fortalecer la Estrategia de Educación Cívica y Cultura para el Ejercicio del Derecho a la Protección de Datos Personales por parte de los Titulares

Coordinadora General

Mtra. Susana Cruickshank

Equipo básico de investigadores

Mtro. Víctor Aramburu Cano

Mtro. Andrés Blancas Martínez

Mtra. Cinthya Rocha Santos

México, D.F. 6 de enero del 2016

Índice

I. INTRODUCCIÓN Y JUSTIFICACIÓN

Este estudio se presenta a solicitud de la Dirección General de Prevención y Autorregulación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). La preocupación desde la Dirección General surge ante la evidente ausencia de una cultura del derecho a la protección de datos personales en México. En el informe del extinto IFAI, actual INAI, al Congreso de la Unión del 2013[1] en materia de protección de datos personales, se menciona que el número de denuncias al 2013 fue de 325, de las cuales se resolvieron 297. Para una población de cerca de 120 millones de personas, esta cifra ilustra la ausencia de una ciudadanía consciente de este derecho. Desde la perspectiva de esta Dirección General, se debe impulsar estratégicamente el posicionamiento del derecho a la protección de datos personales y así se ha contemplado en la Planeación Estratégica Institucional, por lo que la estrategia que aquí se propone, será instrumentada como parte de la planeación institucional del INAI. Desde esta consultoría se ha propuesto realizar una estrategia desde la "Teoría de cambio"[2].

Por estrategia (palabra de origen griego referida al "generalato", a las "aptitudes de general") se comprende en este documento un criterio para definir cursos de acción para el logro de los objetivos organizacionales de largo plazo (por oposición a táctica, o criterios para definir acciones orientadas y coordinadas al logro de objetivos de corto plazo, subordinados a los objetivos estratégicos). El concepto de estrategia en la literatura de gestión contemporánea es polisémico. Henry Mintzberg compila al menos diez distintas tradiciones para la interpretación del concepto, de cuyas nociones se retoma la definición de estrategia como un curso de acción definida claramente y de manera coordinada, para seguir en el futuro, un patrón de comportamiento consistente a lo largo del tiempo y enfoque o manera de hacer las cosas.[3]

En esta propuesta se presenta el análisis y revisión de experiencias internacionales en materia de protección de datos personales, que ofrece una oportunidad para identificar las buenas prácticas que puedan ser relevantes para el caso mexicano. Con base en un análisis de gabinete, a partir de documentos oficiales, fuentes primarias confiables y estudios disponibles sobre casos de otros países, se identifican los marcos legal e institucional, así como la estrategia seguida para promover el ejercicio del derecho a la protección de datos personales.

[1] Informe al Congreso de la Unión respecto a la Protección de Datos Personales (en línea) disponible en http://inicio.ifai.org.mx/Otros/Informe%20al%20Congreso%20de%20la%20Uni%C3%B3n%20Respecto%20a%20la%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf

[2] En su forma más básica, una teoría de cambio se explica cómo un grupo de acciones tempranas e intermedias que genera escenarios con resultados de largo alcance. TOC Aspen Institute.

[3] Henry Mintzberg, "The rise and fall of strategic Planning: Reconceiving Roles for Planning, Plans, Planners", The Free Press, United States, 1994.

Asimismo, con base en las entrevistas realizadas a actores homólogos del INAI en otros países se complementa el análisis de gabinete. En lo que se refiere al análisis de instancias nacionales, se identifican las líneas de acción que permiten promover algún derecho para que puedan ser retomadas en esta estrategia.

En cuanto a las entrevistas con funcionarios de otros países, la selección de los casos aquí planteados obedece al criterio de que el país cuente con una política pública expresada en materia de protección de datos personales, a través de marcos legales e institucionales con ese propósito; la selección se refina al considerar casos con similitudes frente a la realidad mexicana, para asegurar un mayor margen de éxito en la implementación de las recomendaciones que se formulen. Como valor adicional se incorporan los resultados de las entrevistas realizadas a actores clave de cada país seleccionado.

Así, a lo largo del documento se revisan las experiencias de Argentina, Australia, Brasil, Chile, Canadá, España, Francia, Reino Unido y Nueva Zelanda que constituyen realidades avanzadas en el terreno de la protección de datos personales. Se integran también, como un apartado adicional, dos casos no contemplados para el análisis, pero que cuentan con elementos que pueden brindar elementos estratégicos: Kosovo y Singapur. El análisis se desarrolla considerando un mapeo de las instituciones responsables del control del ejercicio y aplicación del derecho; se revisan las estrategias seguidas en cada país para hacer efectivo el derecho; se incorporará información proporcionada por actores estratégicos y entrevistados con el justo propósito de identificar los aspectos que inciden positivamente en el ejercicio de la prerrogativa legal, con miras a fortalecer las recomendaciones finales. El mismo ejercicio se realiza para los casos de instituciones mexicanas responsables de garantizar el ejercicio de derechos como se menciona a continuación, y el análisis se complementa con información aportada por servidores públicos con posiciones clave dentro del propio Instituto Nacional de Acceso a la Información, Transparencia y Protección de Datos Personales así como con grupos de derecho con los que el INAI ha tenido acercamiento. Las entrevistas nutren de manera sustantiva la información recopilada en documentos virtuales y físicos y el análisis de las mismas se integra al documento de manera integral[4].

Las principales fuentes e instrumentos de información corresponden a los documentos oficiales de cada país, el resultado sistematizado de cuestionarios semiestructurados a funcionarios clave y, de manera sobresaliente, se destaca la revisión de casos nacionales donde gran parte del éxito radica en la estrategia de promoción del ejercicio de un derecho específico como pueden ser: la Comisión Nacional de Derechos Humanos (CNDH)[5], órgano autónomo coadyuvante del Estado en la consolidación de una cultura de ejercicio, garantía y respeto de los derechos humanos. El Instituto Nacional Electoral (INE), también órgano autónomo, garante del ejercicio de los derechos electorales expresados en la emisión del voto y cuya contribución a la consolidación democrática

[4] También se anexa la sistematización de las mismas.
[5] De la CNDH sólo pudimos obtener datos a partir de su página web, pues no estuvieron dispuestos a dar la entrevista.

es innegable. Respecto a instancias oficiales se revisa el caso de la Procuraduría Federal del Consumidor (PROFECO) y la estrategia comprometida para la formación de una cultura de consumo inteligente. Destaca también el papel de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) responsable de promover y difundir la educación y la transparencia financiera para que las decisiones de los usuarios sean más informadas respecto a los beneficios, costos y riesgos de los productos y servicios ofertados en el sistema financiero mexicano. El caso del propio INAI es materia de este análisis al ser garante del derecho de acceso a la información pública gubernamental.

Se realizaron dos grupos focales, como se estableció en la propuesta técnica, con dos poblaciones: 1) jóvenes entre 22 y 29 años (con la colaboración del IMJUVE) y 2) con representantes de organizaciones de personas enfermas de cáncer (con la colaboración de la Secretaría de Salud). El instrumento se basó en algunas de las preguntas de la encuesta de IPSOS con el fin de corroborar o no las poblaciones objetivo[6].

A continuación se presenta un cuadro resumen de las experiencias de los países revisados a fin de proporcionar una visión integral que es detallada en las siguientes secciones.

Matriz guía para el análisis de experiencias internacionales en materia de protección de datos en posesión de particulares			
País	**Marco Legal**	**Marco institucional**	**Estrategia**
Argentina	• Artículo 43 constitucional • Ley N° 25.326	Dirección Nacional de Protección de Datos Personales	Difusión de la Jurisprudencia; Programa enfocado en niños, adolescentes y padres "Con Vos en la Web"; Acuerdos público-privados; Registro Nacional de Base de Datos.
Australia	• Acta de Privacidad de 1998 • Principios Australianos de Privacidad	Oficina del Comisionado de Información de Australia	Guías en temas diversos como: protección de datos personales, presentación de quejas, reporte de personas desaparecidas. Folletos informativos que abarcan temas de salud,

[6] IPSOS e IFAI, **Encuesta Nacional sobre Protección de Datos Personales a Sujetos Regulados por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y Población en General**, México, 2012

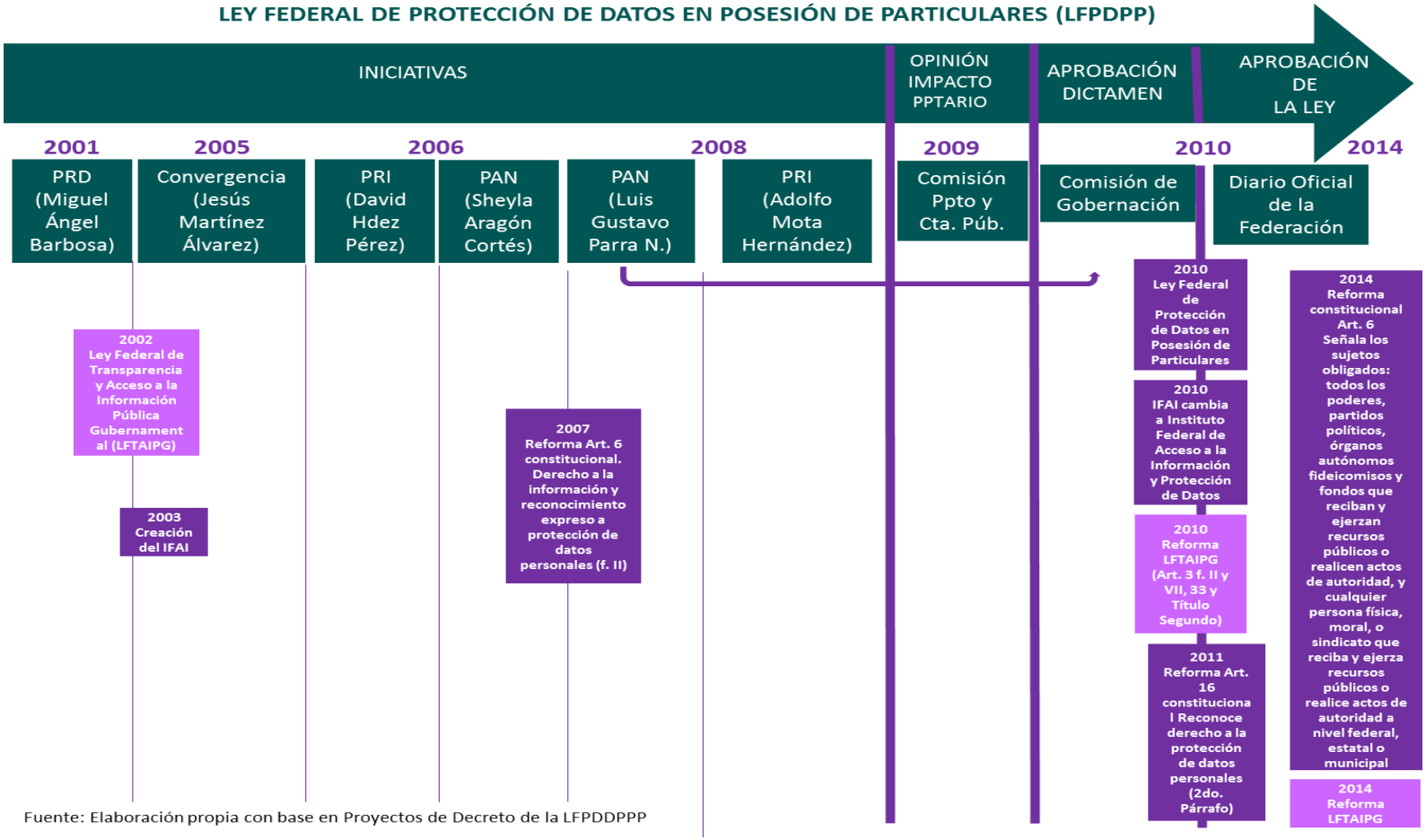
Matriz guía para el análisis de experiencias internacionales en materia de protección de datos en posesión de particulares			
País	**Marco Legal**	**Marco institucional**	**Estrategia**
			crédito, finanzas, tecnología y telecomunicaciones
Brasil	• Constitución Federal, artículo 5, fracciones X y LXXII • Código Civil brasileño, y leyes y regulaciones dirigidas a tipos particulares de relaciones (por ejemplo: el Acta de Internet, Código de Protección al Consumidor y leyes laborales) • Ley 9507/1997 Reglamentaria de Habeas Data • Ley Brasileña de Internet	No existe	No es posible determinarla
Canadá	• 28 leyes federales, provinciales y territoriales	Oficina del Comisionado de Privacidad de Canadá	Guías para la protección de datos y la prevención del robo de identidad a disposición del público en general, especialmente con fines de protección en los servicios financieros; Guías para la protección de datos en diferentes tópicos como el turismo, información biométrica, protección al consumidor, licencias de conducir, información genética y de salud, financiera, seguridad social, entre otras.
Chile	• Constitución de la República de Chile, artículo 19, fracción 4 • Ley 19.628 "Sobre la protección de la vida privada", • Ley 20.285: "Sobre el Acceso a la Información Pública" • Ley 20.575: "Establece el principio del destino en el tratamiento de los datos	No existe	No es posible determinarla

Matriz guía para el análisis de experiencias internacionales en materia de protección de datos en posesión de particulares			
País	**Marco Legal**	**Marco institucional**	**Estrategia**
	personales» • Ley General de Bancos • Ley 19223, "Conductas delictivas relacionadas con la Informática"		
España	• Ley Orgánica de Protección de Datos Personales	Agencia Española de Protección de Datos	Difusión en página web, de documentos, guías, formatos e instructivos acerca del ejercicio de los derechos ARCO; Carta de Servicios de los Organismos y Entes Públicos; Guía para el Ciudadano de 2011; Sede Electrónica para denuncias y reclamaciones.
Francia	• Ley 78-17 de 1978	Comisión Nacional de Informática y Libertades	Las funciones de "informar, orientar y educar" se llevan a cabo principalmente a través de su sitio web, en el cual ponen a disposición de los usuarios un total de 18 guías temáticas que involucran datos personales; Concurso "Operación Privacidad" y Premio Educum dirigido a jóvenes de entre 18 a 25 años.
Reino Unido	• Acta de Protección de Datos de 1988 • Acta de Libertad de Información de 2000 • Regulaciones de Privacidad y Comunicaciones Electrónicas de 2004	Oficina del Comisionado de Información de Reino Unido	La principal herramienta de educación y promoción de prácticas recomendables es su sitio web, organizado en cinco apartados principales: solicitud de información personal, acceso a información pública, quejas y reclamaciones, reclamo de compensaciones, y uso

Matriz guía para el análisis de experiencias internacionales en materia de protección de datos en posesión de particulares			
País	**Marco Legal**	**Marco institucional**	**Estrategia**
			adecuado de información personal.
Nueva Zelanda	• Acta de Privacidad de 1993	Oficina del Comisionado de Privacidad de Nueva Zelanda	Módulos Virtuales de Aprendizaje sobre Privacidad (E-Learning Modules) Semana de la Privacidad; Foros, conferencias y talleres sobre tecnología y privacidad.
FUENTE: Elaboración propia con fuentes de páginas Web oficiales			

La protección de datos personales en posesión de particulares constituye un asunto estratégico en México. En un comienzo, el derecho a la protección de datos estuvo asociado fuertemente al derecho de acceso a la información pública, como se observa en el esquema que da cuenta del surgimiento primario de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en 2002; sin embargo, el derecho a la protección de datos es un derecho autónomo reconocido en la Constitutción Política Mexicana y plasmado en la Ley Federal de Protección de Datos Personales en Posesión de Particulares del 2010 y la normatividad secundaria, y debe ser promovido como tal, con un origen previo en el derecho a la intimidad, como se cita en el marco conceptual de esta estrategia.

LEY FEDERAL DE PROTECCIÓN DE DATOS EN POSESIÓN DE PARTICULARES (LFPDPP)



Fuente: Elaboración propia con base en Proyectos de Decreto de la LFPDDPPP

Contar con instrumentos que permitan implementar y prevenir la violación del derecho a la protección de datos personales, mediante una estrategia de educación cívica para el ejercicio del derecho a la protección de éste, cobra mayor sentido cuando se analizan realidades donde se requiere tener claro que la privacidad es el punto medular en cualquiera de los enfoques sobre la misma aunque se puede privilegiar el dato o la persona.

La protección de datos personales es un tema de interés de los gobiernos que cobra mayor fuerza hacia finales del siglo XX, pero aún en el siglo XXI su desarrollo en regiones como Latino América debe fortalecerse, tanto en sus marcos legales como institucionales para garantizar un adecuado ejercicio del derecho.

Reconocer la necesidad de una estrategia de educación cívica para promover el derecho a la protección de datos no es un asunto menor en un contexto no sólo de interés a nivel internacional por mejorar el tratamiento de los datos en un mundo globalizado y en pleno auge de las TIC, sino que en el contexto nacional, la protección de datos es un derecho asociado a una concepción fundamental para el fortalecimiento de las sociedades democráticas y más aún, si se tiene en cuenta que ambos derechos han dado lugar a modificaciones en la Carta Magna y el marco legal continúa sujeto a un proceso de fortalecimiento para afianzarlos como prerrogativas de la ciudadanía, tanto en la definición de los aspectos legales como en el institucional, al haber transformado de fondo al INAI en un órgano autónomo que lo independiza de su vinculación con el Poder Ejecutivo Federal.

II. MARCO INSTITUCIONAL DE LA ESTRATEGIA

Esta estrategia fue solicitada para cumplir con los objetivos de la Planeación Estratégica que el INAI realizó en marzo del 2015 y cuyos acuerdos fueron publicados en el Diario Oficial del 1 de abril del 2015[7].

Así, la Visión y la Misión del INAI con las que se alinea la estrategia son:

Visión: Ser una Institución Nacional eficaz y eficiente en la consolidación de una cultura de la transparencia, rendición de cuentas y debido tratamiento de datos personales, reconocida por garantizar el cumplimiento y promover el ejercicio de los derechos de acceso a la información y protección de datos personales como base para la participación democrática y un gobierno abierto.

Misión: Garantizar en el Estado mexicano los derechos de las personas a la información pública y a la protección de sus datos personales, así como promover una cultura de transparencia, rendición de cuentas y debido tratamiento de datos personales para el fortalecimiento de una sociedad incluyente y participativa.

Los objetivos son:

1. Garantizar el óptimo cumplimiento de los derechos de acceso a la información pública y la protección de datos personales.
2. Promover el pleno ejercicio de los derechos de acceso a la información pública y de protección de datos personales, así como la transparencia y apertura de las instituciones públicas.
3. Coordinar el Sistema Nacional de Transparencia y Protección de Datos Personales para que los órganos garantes establezcan, apliquen y evalúen acciones de acceso a la información pública, protección y debido tratamiento de datos personales.
4. Impulsar el desempeño organizacional y promover un modelo institucional de servicio púlico orientado a resultados con un enfoque de derechos humanos y perspectiva de género.

[7] Diario Oficial de la Federación del 1º de abril del 2015, disponible en línea en: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/MISION,%20VISION%20Y%20OBJETIVOS%20ESTRATEGICOS%20DEL%20IFAI.pdf

En esta línea y con base en la propuesta técnica, la estrategia de educación sobre el Derecho a la Protección de Datos Personales ha alineado sus objetivos con la Misión y Visión, así como con los objetivos estratégicos institucionales. Además, la estrategia aquí presentada se enmarca en los objetivos 1 y 2 de la misma planeación.

Objetivos de la estrategia:

1. Que los titulares conozcan el derecho que tienen a la protección de sus datos personales.
2. Que los titulares puedan reconocer y valorar adecuadamente los riesgos a los que se enfrentan en el otorgamiento de sus datos personales.
3. Que los titulares puedan tomar decisiones informadas sobre el otorgamiento de sus datos personales a los sujetos obligados.
4. Que los titulares conozcan y utilicen los mecanismos establecidos para hacer valer sus derechos y denunciar los posibles incumplimientos por parte de los sujetos obligados.

III. MARCO JURÍDICO PARA LA ESTRATEGIA

Internacional

Una primera aproximación a la protección de datos, se refiere a la protección en la esfera íntima de la persona y se encuentra enunciada en el ámbito internacional dentro de la Declaración Universal de los Derechos Humanos de 1948, cuyo artículo 12 señala: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Todo persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

La preocupación por la privacidad, se formaliza en el Convenio 108 del Consejo de Europa en 1981, que se divide en 27 artículos agrupados en siete capítulos y cuyo objeto es garantizar el respeto a derechos y libertades fundamentales de toda persona física, sin importar su nacionalidad, con respecto al tratamiento automatizado de sus datos sensibles en el sector público o privado. Más tarde, la Directiva 95/46/CE complementó este Convenio y se abocó a establecer las bases sobre protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.

Por otro lado, la Organización para la Cooperación y el Desarrollo Económico (OCDE) y el Foro de Cooperación Económica Asia Pacífico (APEC por sus siglas en inglés) a través de sus recomendaciones, establecieron la importancia de la regulación del tratamiento de los datos y el aviso de privacidad como aspectos centrales en el marco general de protección de los datos por parte de los sujetos obligados, mientras que para los sujetos del derecho se plantean los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO). Existe un vínculo estrecho entre los derechos ARCO y la consolidación de la tecnología de información y comunicación que facilitan y propician un intercambio y tráfico de datos que debe ser controlado.

Con base en lo anterior, la promoción del derecho para su ejercicio efectivo, cobra una especial importancia pues no basta con desarrollar adecuados y eficaces medios de difusión, sino que se requiere de un plan donde se concrete la estrategia diseñada para fomentar la educación cívica en torno al ejercicio del derecho a la privacidad y la protección de datos personales. Por ello, es necesario establecer una diferencia entre la difusión cuya contribución sin duda es clave para el conocimiento de un derecho, y la estrategia de educación cívica y cultural en torno a ese derecho, expresada en acciones de más largo aliento que permitan profundizar e incrementar la incidencia en los sujetos de derechos llegando a modificar conductas, interiorizar conceptos y en esa medida, transformar comportamientos que redunden en un beneficio para todos, al mejorar una cultura del ejercicio de derecho, a la vez que se reconoce la ley y las implicaciones ante la comisión de una falta, bien pueda ésta deberse a un desconocimiento de la norma o al dolo.

De hecho, el número 14 de los Principios de la Privacidad de la Información de la APEC señala que para la prevención de daños en el manejo de datos personales, deben desarrollarse esfuerzos auto-regulatorios, **campañas de concientización y educación**, leyes, regulaciones más específicas y mecanismos de reforzamiento. Los principios y consideraciones planteados en éste, son un marco que México ha retomado en su legislación del 2011, tanto para los sujetos obligados como para los titulares del derecho. Adicionalmente, México, como integrante de las Naciones Unidas, ha adoptado las directrices para la regulación de los archivos de datos personales informatizados (adoptados mediante la resolución 45/95 de la Asamblea de Naciones Unidas el 14 de diciembre de 1990) que contienen las garantías mínimas que deben prever las legislaciones nacionales en esta materia.

Otro marco referente es la Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995, relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Además de la Carta de los Derechos Fundamentales de la Unión Europea, del año 2000, particularmente en su Artículo 8, en el que se señala sobre protección de datos de carácter personal:

"1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente."[8]

Otro referente son las Directrices de Armonización de la protección de datos en la Comunidad Iberoamericana (adoptados por la Red Iberoamericana de Protección de Datos en el 2007).

Nacional

A nivel nacional, desde 1917, la Constitución Política de los Estados Unidos Mexicanos estableció derechos relativos a la libertad individual, de entre los que destacan la inviolabilidad de correspondencia y domicilio, y más adelante, el secreto a las comunicaciones privadas. En junio del 2009, la Constitución mexicana fue modificada en el Título Primero, Capítulo I sobre los Derechos Humanos y sus Garantías, en el artículo 16:

[8] Carta de los derechos fundamentales de la Unión Europea, (en línea), disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/B.1-cp--Carta-de-los-Derechos-Fundamentales.pdf (Consultada el 23 de septiembre del 2015)

> **"Artículo 16.** Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.
>
> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros."[9]

Después de la Constitución, una primera aproximación a su protección se dio con la aprobación de la Ley Federal de Transparencia y Acceso a la Información Pública en el 2002, al establecer en su artículo 3, lo siguiente:

> Para los efectos de esta Ley se entenderá por…
> II. Datos personales: La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad.

Más tarde, las modificaciones que se hicieron a esta Ley en julio del 2014 en lo que se refiere a lo que se entiende por protección de datos personales y a los sujetos obligados en el Título Primero, Capítulo I de Disposiciones Generales, Artículo 3, fracción XIII y XIV y después en el Capítulo IV de Protección de Datos Personales, artículos del 20 al 26 sobre el trato que deben dar los sujetos obligados a la protección de datos personales.

Además de la legislación señalada, el marco normativo particular para este derecho es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada el 5 de julio del 2010 y cuyos detalles han sido señalados en la introducción, enfocándose a los sujetos obligados y de derecho, así como la definición de los mismos:

> "Artículo 2.- Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:

[9] Diario Oficial de la Federación, 01 de junio del 2009, en línea en: http://dof.gob.mx/nota_detalle.php?codigo=5092143&fecha=01/06/2009

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."

A partir de la LFPDPPP se generó el Reglamento de la misma en diciembre del 2011 que establece y delimita de manera específica los ordenamientos de la Ley.

Finalmente, es menester mencionar que a la fecha, enero del 2016, está en dictaminación en el Senado la Ley General de Datos Personales.

IV. MARCO CONCEPTUAL

A pesar de ser evidente, hay que señalar que el marco normativo y el marco conceptual han ido de la mano en su desarrollo a nivel internacional. En su definición, Hondius[10] refiere a la protección de datos como "aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho individual a la intimidad, respecto del procesamiento manual o automático de datos" y señala que "se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación, o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

A partir de lo anterior, revisaremos en este apartado la evolución conceptual de la protección de datos, desde la revisión del marco de derechos humanos, hacia el desafío de las nuevas tecnologías de la información con respecto a la recolección, procesamiento y transmisión de datos personales. Dentro de esta base, el concepto de la intimidad, en el contexto de la sociedad computarizada, concede derechos a los individuos respecto de sus datos personales como objeto de tratamiento automatizado, e impone obligaciones y deberes de aquellos que controlan y tienen acceso a los ficheros.

El siglo XVIII fue un siglo clave para el desarrollo de la filosofía de los derechos humanos, con su reconocimiento en la Carta de los Derechos del Hombre y del Ciudadano en 1789 en Francia, se dio un reconocimiento universal alcanzando su consolidación como prerrogativas inherentes a todo ser humano[11].

Los derechos individuales —o bien derechos de primera generación— y en particular, el reconocimiento de la libertad personal, incorporan inherentemente el derecho a la intimidad de la persona como una prerrogativa objeto de tutela, ya no sólo en los instrumentos internacionales, sino además, de forma constitucional.

Este derecho ha cobrado importancia considerablemente gracias a que el desarrollo tecnológico ha redimensionado las relaciones entre los individuos, así como su marco de convivencia. Hoy la informática se ha convertido en el símbolo emblemático de la cultura contemporánea.

---

[10] Legal Corp, "El derecho a la protección de los datos personales", 2013, (en línea), disponible en: http://legalcorp.com.sv/index.php?option=com_content&view=article&id=26:el-derecho-a-la-proteccion-de-datos-personales&catid=2:actualidad&Itemid=3 (Consultada el 25 de septiembre del 2015)

[11] Declaración de los derechos del hombre y del ciudadano, 1789, (en línea), disponible en: http://www.juridicas.unam.mx/publica/librev/rev/derhum/cont/30/pr/pr23.pdf (Consultada el 25 de septiembre de 2015)

"Ahora, con el tratamiento, la recolección, el almacenamiento de información que antes sólo podía formar parte de la vida íntima de cada ser humano —o bien, era conocido por un mínimo sector—, ha ido variando paulatinamente su entorno y estructura. Esto es, los datos personales de toda persona se han convertido en una práctica habitual de control y almacenamiento por parte de los sectores tanto públicos como privados"[12].

Es por eso, que el uso y control sobre los datos concernientes a cada persona, debe serle reconocido ya no sólo como una mera prerrogativa, sino además como un derecho protegido y garantizado por mecanismos de protección.

De acuerdo con Aristeo García González "mientras en el ámbito europeo se han preocupado por reconocer y garantizar una protección de datos personales a sus ciudadanos en donde toda aquella información relativa a su persona queda libre de intromisiones salvo el consentimiento del interesado. En otras latitudes, por ejemplo, en algunos países latinoamericanos, ha sido objeto de estudio como un derecho fundamental. Y en el caso particular de México, el reconocimiento de un derecho fundamental a la protección de datos personales apenas ha comenzado"[13]

La historia de los derechos humanos ha pasado por ciertas "generaciones" que se relacionan con los momentos históricos de las sociedades occidentales.

A la fecha se considera el reconocimiento de tres generaciones de derechos que han correspondido a un momento ideológico y social, con características propias. La primera generación de derechos, reconoce las libertades individuales, lo que ha constituido los derechos de defensa de la persona. "En esta fase se configuraron una serie de derechos relativos al aislamiento, tal como lo fue el derecho al honor, a la vida, a la integridad personal, así como el propio reconocimiento a la intimidad de la persona. Derecho que hoy, como consecuencia del desarrollo tecnológico y las nuevas formas de comunicación e información, ha sido necesario reformular en su alcance y contenido"[14].

La segunda generación de derechos humanos, fue influenciada por las luchas sociales del siglo XIX. Estos movimientos reivindicatorios evidenciaron la necesidad de completar el catálogo de derechos y libertades de la primera generación, con una segunda: los derechos económicos, sociales y culturales. El reconocimiento y garantía de estos derechos implicó una acción de los poderes públicos encaminada a garantizar su ejercicio a

[12] García González Aristeo, "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", 2011, (en línea), disponible en: http://www.juridicas.unam.mx/publica/rev/boletin/cont/120/art/art3.htm (Consultado el 25 de noviembre de 2015)
[13] *Ídem*
[14] García González Aristeo, "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", 2011, (en línea), disponible en: http://www.juridicas.unam.mx/publica/rev/boletin/cont/120/art/art3.htm (Consultado el 25 de septiembre de 2015)

través de prestaciones y de servicios públicos. Con la consagración jurídica de tales derechos y políticas se estableció un Estado social de derecho.

Más tarde, como una estrategia reivindicatoria de los derechos humanos, surge una tercera generación de derechos humanos. En ésta, los derechos y las libertades de la tercera generación se presentan con un mayor auge y el reconocimiento del derecho a la intimidad, exige a partir de aquí un reconocimiento a nivel constitucional. Por lo que ahora puede hablarse de un antes y un después de este derecho. El derecho a la protección de datos personales, encontró su fundamento a partir del derecho a la intimidad. El derecho a la intimidad abarca aquello que se considera más propio y oculto del ser humano —entendiéndose por propio y oculto la información que mantiene para sí mismo.

El estudio de García González, señala que es con Warren y Brandeis en 1890, con *The Right to Privacy* cuando se sientan las bases técnico-jurídicas de la noción *Privacy*, contrario a lo que había acontecido con el supuesto teórico en la idea de libertad como autonomía individual defendida por Mill en 1859, que consideraba que los aspectos concernientes al individuo consistían en el derecho a una absoluta independencia, puesto que sobre sí mismo, sobre su cuerpo y mente, el individuo era soberano. Por lo que con Warren y Brandeis, *privacy* implica derecho a la soledad, una facultad "*to be lef alone*", esto es, una garantía del individuo a la protección de su persona y su seguridad frente a cualquier invasión del sagrado recinto de su vida privada y doméstica.

En consecuencia, al proclamarse este derecho, se buscaba proteger las creencias, los pensamientos, emociones y sensaciones de la persona. En 1890, siendo Brandeis juez de la Suprema Corte de los Estados Unidos, en una *dissenting opinion* consideró que frente al gobierno el derecho a la soledad es el más amplio de los derechos y el más estimado por los hombres civilizados. La protección de este derecho frente a cualquier intromisión injustificada del gobierno en la esfera privada del individuo, no importa los medios que se emplean, debía ser considerada una exigencia de la cuarta enmienda de la Constitución americana, por tanto, garantizó a los ciudadanos la seguridad de su persona, de su domicilio y de sus efectos frente a cualquier intromisión indebida.

Sin embargo, dice el autor del estudio, la intimidad como una disciplina jurídica ha perdido su carácter exclusivo individual y privado, para asumir progresivamente una significación pública y colectiva, consecuencia del cauce tecnológico. Entonces, *privacy*, más que un mero sentido estático de defensa de la vida privada del conocimiento ajeno, tiene la función dinámica de controlar la circulación de informaciones relevantes para cada sujeto. Algunos autores se pronuncian en el mismo sentido, señalando que *privacy* no implica sencillamente la falta de información sobre nosotros por parte de los demás, sino más bien el control que tienen las personas sobre la información propia.

"Consecuentemente, frente a la actual sociedad de la información, resulta insuficiente concebir a la intimidad como una derecho garantista (estatus negativo) de defensa frente a cualquier invasión indebida de la esfera privada, sin contemplarla al mismo tiempo, como un derecho activo de control (estatus positivo) sobre el flujo de informaciones que afectan a cada sujeto."[15]

El autor señala que, entre otras cosas, la propia noción de intimidad o privacidad es una categoría cultural, social e histórica, por lo que ahora este concepto ha pasado de una concepción cerrada y estática de la intimidad a otra abierta y dinámica, ya que ahora se contempla la posibilidad de conocer, acceder y controlar las informaciones concernientes a cada persona. Esto es, en la modernidad, el derecho a la intimidad, como el más reciente derecho individual relativo a la libertad, ha variado profundamente, gracias a la revolución tecnológica. Por tanto ha sido necesario ampliar su ámbito de protección, así como el establecimiento de nuevos instrumentos de tutela jurídica.

Se dice que al tratarse de un derecho dinámico que está frente a una sociedad donde la informática se ha convertido en el símbolo emblemático de la cultura, el control electrónico de los documentos de identificación, el proceso informatizado de datos fiscales, el registro de crédito, así como de las reservas de viajes y otros datos importantes de las personas, representan muestras conocidas de la omnipresente vigilancia informática de la existencia habitual de la persona. Cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua e inadvertida que afecta potencialmente incluso a los aspectos más sensibles de su vida privada.

El autor del estudio afirma que la protección de la intimidad frente a la informática no significa impedir el proceso electrónico de informaciones, necesarias en el funcionamiento de cualquier Estado moderno, sino que implica el aseguramiento de un uso democrático de la *Information Technology*. En consecuencia, si un derecho a la intimidad en la vida del ser humano, ha sido viable, un tratamiento y almacenamiento tecnológico de sus datos, también lo puede ser. Por ende, un derecho a la protección de datos personales también debe implicar el reconocimiento de este derecho como fundamental. Por lo que el fenómeno de la intimidad aparece en todas las sociedades.

Hoy, las nuevas tecnologías, al posibilitar la racionalización, simplificación, celeridad y seguridad de las prácticas administrativas y de recopilación de datos, se presentan como una exigencia inaplazable de regulación, que cualquier Estado debe tener en cuenta. Se dice que en las sociedades informatizadas del presente, el poder ya

[15] García González Aristeo, "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", 2011, (en línea), disponible en: http://www.juridicas.unam.mx/publica/rev/boletin/cont/120/art/art3.htm (Consultado el 25 de septiembre de 2015)

no reposa sobre el ejercicio de la fuerza física, sino en el uso de las informaciones que permiten influir y controlar la conducta de los ciudadanos, sin necesidad de recurrir a medios de coacción.

Retomando: el derecho a la intimidad en su ámbito estático, se encuentra reconocido en la mayoría de los países a nivel constitucional. Sin embargo, en cuanto a la intimidad en su ámbito abierto y derivado del desarrollo tecnológico, pueden ser vulnerados otros aspectos de la esfera íntima de la persona, como pueden ser "sus datos personales". Para ello, el derecho fundamental a la intimidad como una concepción cerrada y estática es insuficiente, en virtud de que protege aspectos no vinculados con el desarrollo tecnológico. Y por ende, una concepción abierta y dinámica, esto es, su relación con las nuevas tecnologías significa el reconocimiento ya no sólo de un derecho, sino de nuevos mecanismos de protección, siendo fundamental y necesaria su incorporación en el ámbito constitucional.

Así, el derecho a la intimidad ha pasado de ser una libertad negativa —esto es, una libertad propia del individualismo que exige el respecto a los demás, es decir, un derecho de defensa— a una libertad positiva en donde el individuo cuenta con la facultad de poder controlar toda aquella información que le sea relevante y le concierna a él mismo. Así, en una primera aproximación, cabe señalar que los datos de toda persona deben ser objeto de protección para que éstos puedan ser tratados o elaborados, y finalmente ser convertidos en información, y en consecuencia, sólo ser utilizados para los fines y por las personas autorizadas.

En el marco de la tercera generación de derechos, como hemos mencionado anteriormente, algunos autores señalan que la sociedad tecnológica ha producido una nueva imagen mental del ser humano, que ha sido definido como "hombre artificial". Lo cual no solamente hace referencia al aspecto material de la existencia humana, sino a la dimensión psicológica, en donde un nuevo tipo de hombre que vive en un mundo artificial ha sido producto del mismo ser humano y no de la propia naturaleza. Esto ha significado que el atributo que tradicionalmente se consideraba el dato definitorio de la condición humana, es decir, su inteligencia, ha sido expropiada por las computadoras quienes han sido capaces de desarrollar una "inteligencia artificial". Inteligencia que ha permitido tratar, elaborar y transmitir informaciones, como lo han sido los datos relativos a la persona, lo que en consecuencia ha supuesto la aparición de nuevos derechos y libertades, o bien, el replanteamiento del contenido y función de las existentes. En donde, como se apuntaba, la delimitación conceptual del derecho a la intimidad como facultad de aislamiento, ahora se ha convertido en un poder de control sobre las informaciones que son relevantes para cada sujeto.

A partir de la era tecnológica, a cada individuo le corresponde conocer cuál será el uso de los datos personales que puedan ser objeto de un tratamiento automatizado, y podrá exigir que su almacenamiento y trato sea adecuado para que no se vea vulnerado en su libertad y su dignidad. El ser humano a lo largo de su vida va

dejando una enorme cantidad de datos que se encuentran dispersos en diferentes lugares tanto públicos como privados. Actualmente, con la utilización de nuevos medios tecnológicos, resulta posible agrupar y tratar de interpretar dichos datos, lo que permite crear un perfil determinado del individuo, pudiendo ser objeto de manipulaciones, o de ser interferido en su vida privada con fines ilícitos.

El derecho del ciudadano a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la información, deben ser el contexto en el cual el Estado debe consagrar el derecho fundamental a la protección de datos de carácter personal.

V. EXPERIENCIAS INTERNACIONALES

A continuación se describen casos de países donde la privacidad y protección de datos se encuentra regulada o bien, aplica las disposiciones legales existentes para hacer de este derecho una realidad.

A. Argentina

La protección de datos personales constituye una de las políticas públicas más avanzadas en Argentina, con respecto a la región de latinoamericana. En 2003, sólo tres años después de haberse puesto en operación el marco legal e institucional para la protección de datos personales, el país logró el reconocimiento internacional por parte de la Unión Europea que le otorgó a la normativa argentina la adecuación en los términos de la Directiva 95/46/CE[16], esto significa que no se le aplican las restricciones para la transferencia de datos personales y se permite el libre flujo de los mismos desde la Unión Europea.

A continuación se describen los marcos legal e institucional, se identifican los sujetos obligados y los sujetos de derecho, se describe la estrategia para definir el enfoque particular sobre el cual se considera necesario profundizar con miras a enriquecer la propuesta que sea útil al interés específico del INAI.[17]

a. Marco Legal

De acuerdo con el sitio oficial de la Dirección Nacional de Protección de Datos Personales, dependiente del Ministerio de Justicia y Derechos Humanos de Argentina**,** el marco legal en la materia en el territorio de Argentina se asienta en los siguientes ordenamientos:

1. Ley 25326.

La Constitución Nacional regula la acción de *habeas data* en el Artículo 43, incisos 1 y 3, incluida en la reforma constitucional de 1994[18]. La Ley 25326 o Ley de Protección de los Datos Personales se promulgó en 2000, definiendo su objeto como: "la protección integral de los datos personales asentados en archivos, registros,

[16] Directiva consultada en línea en : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML
[17] La fuente de información fundamental corresponde al sitio oficial de la instancia responsable en el país http://www.jus.gob.ar/datos-personales/documentacion-y-capacitacion/normativa/normativa-proteccion-de-datos-personales/leyes-y-decretos.aspx (Consultada el 25 de septiembre de 2015).
[18] Torres Natalia, Caso de estudio: Argentina. En Torres Natalia (compiladora). "Acceso a la información y datos personales: una vieja tensión, nuevos desafío", Universidad de Palermo, Centro de Estudios sobre la Libertad de Expresión, s/f.

bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional".

La ley, en su artículo 2, contiene las definiciones básicas. Los datos personales corresponden a la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables. Los datos sensibles son datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. El archivo, registro, base o banco de datos, indistintamente designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso. El tratamiento de datos considera las operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

El responsable del archivo, registro, base o banco de datos es la persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos. Los datos informatizados son los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado. Por titular de los datos se entiende a toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la ley; por usuario de datos se entiende a toda persona pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos. Cuando ocurre la disociación de datos la ley se refiere a todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

Este instrumento normativo contiene una sección que establece los principios para la protección de datos: licitud, calidad de los datos, consentimiento, información, categoría de los datos, datos relativos a la salud seguridad de los datos, confidencialidad, cesión, y transferencia internacional. También contiene un capítulo que regula los derechos de los titulares de los datos a informarse y acceder a la información sobre datos personales que existan en bases de datos públicos o privadas; en esta sección se regulan los derechos a rectificar, actualizar o suprimir datos personales cuando corresponda. El ordenamiento establece las obligaciones para los usuarios y responsables de los archivos, registros y bancos de datos, señalando la obligación de registrarlos por parte de quienes posean este tipo de archivos. La ley prevé aspectos del órgano encargado de controlar la aplicación de

la ley, así como las sanciones administrativas y penales que se aplicarán en caso de incumplimiento. La última sección contiene lo relativo a la acción de protección de datos personales que señala el procedimiento para tomar conocimiento de los datos personales de archivos, registros o bancos de datos públicos o privados, y para los casos en que se presuma alguna irregularidad.

2. Decreto No. 1558/2001.

El Decreto 1558/2001, publicado el 29 de noviembre de 2001, corresponde a la reglamentación de la Ley 25326, que entre otros aspectos crea la Dirección Nacional de Protección de Datos Personales (DNPDP) en el ámbito de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos, como órgano de control de la citada Ley. De acuerdo con el artículo 29 del Decreto su Director tendrá dedicación exclusiva en su función, ejercerá sus funciones con plena independencia y no estará sujeto a instrucciones. La DNPDP se integrará por un Director Nacional, designado por el Poder Ejecutivo Nacional, por un plazo de cuatro años, seleccionado entre personas con antecedentes en la materia. En este decreto se establece también el personal con el que contará la DNPDP, sus fuentes de financiamiento, la integración del Consejo Consultivo que la asesorará, y sus funciones. Asimismo, enfatiza la importancia de alertar la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de sector, en la correcta aplicación de la Ley, para ello las asociaciones de profesionales y organizaciones representantes de responsables o usuarios de archivos, registros, bases o bancos de datos públicos y privados que hayan elaborado códigos éticos, o que pretendan modificarlos deben someterlos a la revisión de la DNPDP quien aprobará el ordenamiento o sugerirá las correcciones necesarias para su aprobación.

El Decreto también contiene los principios relativos a la protección de datos, los derechos de los titulares de los datos, a los usuarios y responsables de archivos, registros y bancos de datos, y prevé las sanciones.

3. Decreto No. 1160/ 2010

El Decreto 1160/2010 se publicó en agosto de 2010 y su fin es modificar el Anexo I del Decreto 1558/2001 con el propósito de que la DNPDP cumpla con la función de investigar y controlar que el tratamiento de los datos personales se realice en los términos de la Ley 25326. El Anexo referido establece el procedimiento para la aplicación de sanciones previstas, y a través de este Decreto se regula con mayores precisiones y simplificaciones la actividad de la DNPDP para la aplicación de sanciones con resguardo de las reglas del debido proceso y del derecho de defensa, así como para que la resolución que impone la sanción administrativa, y la constancia de la misma deberá ser incorporada en el Registro de Infractores a la Ley 25326 a cargo de la DNPDP, para publicarse en su sitio de internet.

4. Ley 26343.

Se publicó en diciembre de 2007 con el propósito de modificar al artículo 47 de la Ley 25326 a fin de establecer que los bancos de datos destinados a prestar servicios de información crediticia deberán eliminar y omitir el asiento, en el futuro, de todo dato referido a obligaciones y calificaciones asociadas de las personas físicas y jurídicas cuyas obligaciones comerciales se hubieran constituido en mora, o si las obligaciones financieras se clasificaran según las normativas del Banco Central de la República de Argentina, durante el periodo del 1 de enero de 2000 al 10 de diciembre de 2003, siempre que las deudas hubieran sido canceladas o regularizadas a la entrada en vigencia de la ley o lo sean en los 180 días posteriores a la entrada en vigor de la misma; la firma de un plan de pagos por parte del deudor o la homologación del acuerdo preventivo extrajudicial es suficiente para la regularización de la deuda.

5. Ley 26951.

La Ley 26.951, promulgada en julio de 2014, crea el Registro Nacional "No Llame". Su objeto es proteger a los titulares o usuarios autorizados de los servicios de telefonía, en cualquiera de sus modalidades, de los abusos del procedimiento de contacto, publicidad, oferta, venta y regalo de bienes o servicios no solicitados (artículos 1 y 3). Los servicios de telefonía comprenden todas las modalidades: telefonía básica, telefonía móvil, servicios de radiocomunicaciones móvil celular, de comunicaciones móviles y de voz IP, así como cualquier otro tipo de servicio similar que a la tecnología permita brindar en el futuro (artículo 4). Al servicio se puede inscribir toda persona física o jurídica titular o usuario autorizado del servicio de telefonía en cualquiera de sus modalidades que manifieste su voluntad de no ser contactada por quien publicite, oferte, venda o regales bienes o servicios (artículo 5). La inscripción al Registro es gratuita y debe ser implementada por medios eficaces y sencillos con constancia de identidad del titular, e igualmente, la baja sólo puede ser solicitada por éste en cualquier momento (artículo 6). La inscripción al Registro es gratuita y debe ser implementada por medios eficaces y sencillos con constancia de identidad del titular, e igualmente, la baja sólo puede ser solicitada por éste en cualquier momento (artículo 6). Se consideran responsables o usuarios de archivos, registros y bancos de datos quienes publiciten, oferten, vendan o regalen bienes o servicios utilizando como medio de contacto los servicios de telefonía en cualquiera de sus modalidades. Se consideran responsables o usuarios de archivos, registros y bancos de datos quienes publiciten, oferten, vendan o regalen bienes o servicios utilizando como medio de contacto los servicios de telefonía en cualquiera de sus modalidades; no podrán dirigirse a (artículo 7). Se implementarán campañas de difusión acerca del funcionamiento del Registro Nacional "No Llame".[19]

6. Decreto No. 2501/2014

[19] Ley 26.343, (en línea), disponible en: http://www.jus.gob.ar/datos-personales/documentacion-y-capacitacion/normativa/normativa-proteccion-de-datos-personales/leyes-y-decretos.aspx (Consultada el 28 de septiembre de 2015).

El Decreto 25/01/2014 se publicó el 6 de enero de 2015 para facultar a la DNPDP a dictar las normas complementarias y procedimientos para una adecuada aplicación de la Ley 26951 referente al Registro Nacional "No llame", y su reglamentación. Al respecto destaca el procedimiento de inscripción al Registro que deberá ser gratuito y simple (artículo 6). Se consideran responsables o usuarios de archivos, registros y bancos de datos quienes publiciten, oferten, vendan o regalen bienes o servicios utilizando como medio de contacto los servicios de telefonía en cualquiera de sus modalidade (artículo 7); señala que las disposiciones no aplican en campañas de bienes públicos, se establecen los horarios razonables para que se efectúen en días hábiles, y la constancia por escrito del consentimiento del titular de los datos para permitir llamadas en caso de estar inscrito en el Registro Nacional "No llame" (artículo 8). Se establecen los pasos para hacer las denuncias (artículo 10) y el procedimiento para tratar los incumplimientos, enfatizando que los sujetos obligados deberán brindar el registro de sus llamadas salientes provisto por la empresa prestadora del servicio de telecomunicación de la que fueran usuarios (artículo 11).

b. Marco Institucional

La Dirección Nacional de Protección de Datos es la instancia responsable de vigilar que se cumpla con la Ley 25326, creada mediante el Decreto 1558/2001, de acuerdo con el artículo 21 de este Decreto la DNPDP se integra por un Director Nacional, designado por el Poder Ejecutivo Nacional, por un plazo de cuatro años, seleccionado entre personas con antecedentes en la materia. Esta instancia es un órgano de control que goza de autonomía funcional y actúa en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación como órgano descentralizado para la efectiva protección de los datos personales.

Entre las funciones principales de la DNPDP se encuentran: estar a cargo el Registro Nacional de las Bases de Datos, instrumento organizado a fin de conocer y controlar las bases de datos; asesorar y asistir a los titulares de datos personales recibiendo las denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos por violar los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos, en este sentido, debe investigar si la base de datos denunciada cumple o no, con los principios que establece la ley y las disposiciones reglamentarias; inscribe archivos, bases o bancos de datos en el Registro Nacional de Bases de Datos, dictamina y sanciona según las disposiciones de la ley; cuenta con el Registro Nacional de Documentos Cuestionados a través del Centro de Asistencia a las Víctimas de Robo de Identidad, cuyo objetivo es registrar y asistir a quienes puedan resultar perjudicados en sus derechos, como consecuencia del robo de información que contiene datos personales.

La DNPDP es miembro de la *Global Privacy Enforcement Network* (Red de Control de Privacidad), creada para fomentar la cooperación entre autoridades internacionales en la materia.

c. Sujetos obligados y sujetos de derecho

De acuerdo con las definiciones del artículo 2 de la Ley 25326, puede considerarse al sujeto obligado como el responsable de archivo, registro, base o banco de datos, que es la persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

En contra parte, el sujeto de derechos, es el titular de los datos que es toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la Ley 25326.

d. Estrategia

La estrategia de la DNPDP para la promoción del derecho sobre la protección de los datos personales incorpora acciones en diversos sentidos: promueve información sobre el marco legal existente en la materia; desarrolla programas específicos para mantener la seguridad en el uso de las tecnologías de información y comunicación (TIC), y favorece los acuerdos público-privados en pro de una cultura de protección de datos. A continuación se abordan con mayor detenimiento estos aspectos.

Difusión de Jurisprudencia.

La DNPDP promueve la cultura de la privacidad y la protección de los datos personales, poniendo a disposición pública para consulta, la Jurisprudencia nacional sobre *Habeas Data*, en su sitio oficial, el material es seleccionado por personal especializado adscrito al Centro de Jurisprudencia, Investigación y Promoción de la Protección de los Datos Personales.

Programa "Con Vos en la Web"[20]

Como refuerzo a la formación en la materia, la DNPDP creó en 2012 el Programa Nacional para la protección de los datos personales de niños, niñas y adolescentes en Internet "Con Vos en la Web[21]", cuyo principal objetivo es fortalecer el conocimiento sobre seguridad de la información en Internet, y concientizar sobre los riesgos y amenazas en la utilización de las nuevas tecnologías TIC, proporcionando herramientas de análisis y respuesta que tiendan a la preservación de la privacidad e intimidad de los usuarios. Con base en este programa se desarrolla un plan de actividades, en forma permanente y conjunta, con UNICEF con lo que se busca propiciar la cooperación técnica para contribuir con el bienestar de la infancia y la adolescencia, promoviendo la protección sus derechos para el pleno desarrollo de sus capacidades.

---

[20] Presidencia de la Nación, "Con vos en la web capacitó 450 alumnos durante el mes de agosto", 2015, (en línea), disponible en: http://www.jus.gob.ar/datos-personales/novedades.aspx (Consultado el 26 de septiembre de 2015)

[21] De acuerdo con el sitio oficial el Berkman Center de la Universidad de Harvard y UNICEF reconocieron al Programa como una de las políticas públicas más exitosas de la región, recibiendo invitación a participar en el evento "Digitally Connected: Towards a Global Community of Knowledge and Practice around Children, Youth, and Digital Media" (Abril, 2014), (en línea), disponible en: http://www.unicef.org/argentina/spanish/monitoring_movilization_28953.htm (Consultado el 26 de septiembre de 2015)

Para alcanzar sus objetivos, el Programa desarrolla distintos tipos de materiales útiles para grupos de diferentes edades. En este sitio web se ponen a disposición guías, manuales, videos tutoriales, consejos, glosarios, juegos y videos; genera espacios de comunicación y participación presenciales tales como talleres para niños y charlas para docentes y padres. Las actividades se llevan adelante en todo el territorio nacional. “Con Vos en la Web” es un programa para niños, adolescentes, padres y docentes que previene sobre los riesgos y la importancia de la protección de la intimidad. A continuación se muestran los recursos utilizados para este propósito.

Grupo	Niños	Adolescentes	Padres	Docentes
Bien o Servicio	Consejos Prevención para juegos on line Seguridad para dispositivos Android	Amenazas: Troyanos • Virus • Keyloggers • Pharming • Sidejacking • Gusanos • Rootkits • Phising • Tabjacking • Botnet	Tendencias web • Informa sobre novedades tecnológicas utilizadas por chicos	Actividades para el aula • Material didáctico para niños y adolescentes que a través del juego concientiza sobre la importancia de la protección
	Verano seguro Consejos para preservar la privacidad on line para vacacionar de forma segura	**Consejos** **Contraseñas seguras** • Consejos para salir a bailar • Celulares • Prevención para juegos on line • Redes WIFI • Spam • Ingeniería social • Seguridad en dispositivos Android	**Guías** • Grooming: consejos para entender y prevenir el acoso a través de internet • Cyberbullying: consejos para entender y prevenir el acoso • Las diez amenazas más peligrosas de internet • Seguridad en redes inalámbricas: Redes WiFi • Reputacion en la web • Sexting	**Recursos** • Manual de protección de datos y nuevas tecnologías • Ley 25326 • Guía de actividades • Guía práctica para adultos
	Juegos On line Consejos para jugar on		• Videos tutoriales para configurar la	**Videos** • Educar en la web

Grupo	Niños	Adolescentes	Padres	Docentes
	line sin poner en riesgo datos personales		privacidad de los perfiles en las redes sociales	
	Videos Abordan temas como: Discriminación Ciberbullying Caperucita ¿agregar extraños a redes sociales?			
Fuente: Elaboración propia con base en http://www.jus.gob.ar/datos-personales/areas-de-la-pdp/con-vos-en-la-web.aspx				

Campus PDP: oferta de cursos

El programa "Con Vos en la Web" se respalda fuertemente en el **Centro de Capacitación, Investigación y Difusión de la Protección de los Datos Personales,** donde operara el Campus Virtual PDP (Campus PDP) diseñado como un espacio de capacitación y difusión de las distintas temáticas involucradas con las tareas de la protección de datos, seguridad de la información, niños y adolescentes y sus relaciones con las nuevas tecnologías, el resguardo del derecho de privacidad e intimidad ante el avance de internet, las amenazas y los riesgos en el uso de las TIC: como evitarlos, la reputación online, los delitos informáticos, protección de datos personales para abogados, entre otros. Así, se constituye una estrategia pedagógica para facilitar el acercamiento de la comunidad a estas temáticas, eliminando las brechas digitales en el país y lugar del mundo con acceso a internet.

De este modo, Campus PDP[22], propicia la creación de redes virtuales de enseñanza y promoción de la protección de datos personales, y el resguardo de la intimidad y privacidad de los mismos, vinculando organismos e instituciones gubernamentales y no gubernamentales, nacionales y del exterior. La oferta de cursos se observa en la siguiente tabla.

[22] Campus Virtual de la Dirección Nacional de Protección de Datos Personales, disponible en: https://capacitacion.jus.gov.ar/dnpdp (Consultada el 28 de septiembre de 2015).

Curso	Temáticas
Protección de datos personales y datos de salud **4 semanas**	Datos sensibles, consentimiento informado, datos de salud
Privacidad en el comercio electrónico **4 semanas**	Riesgos y amenazas en el comercio electrónico, consejos y herramientas de privacidad
Robo de identidad **1 semana más 1 semana de actividades**	Se analizan las diversas modalidades, herramientas de defensa para proteger la identidad a partir del Registro de Documentos cuestionados
Adultos y chicos en la Web, nuevos desafíos	Brinda herramientas para que adultos en general, y padres y docentes en particular incorporen herramientas para acompañar a los jóvenes en el cuidado de sus datos personales en la web
Deep Web	Brinda herramientas para adquirir conocimientos para el uso responsable de las redes sociales, internet y las TIC
Videojuegos y seguridad Web	Curso introductorio para adquirir conocimientos para el uso responsables de las redes sociales, internet y las TIC
Fuente: Elaboración propia con base en http://www.jus.gob.ar/datos-personales/documentacion-y-capacitacion/campus-virtual-pdp/oferta-de-cursos-2015.aspx (consultada el 3 de octubre de 2015)	

Ejercicio de derechos / Denuncias de incumplimientos[23]

Existen algunas variantes para el ejercicio de derechos que involucran datos personales:

- **Derecho de acceso**

Si un sujeto de derechos desea conocer qué datos hay sobre su persona en una base datos, puede ejercer el derecho de acceso previsto en el art. 14 de la ley 25.326.

[23]Presidencia de la Nación, "Ejerce tus derechos. Denuncia un incumplimiento", 2015, (en línea), disponible en: http://www.jus.gob.ar/datos-personales/ejerce-tus-derechos/denuncia-un-incumplimiento.aspx (Consultado el 26 de septiembre de 2015)

- **Derecho de rectificación, actualización o supresión**

Si sus datos no están actualizados, o requieren rectificación, supresión (datos falsos, incompletos, erróneos o desactualizados) o sometimiento a confidencialidad, puede ejercer los derechos previstos en el art. 16 de la ley 25.326.

- **Derecho al olvido – Información crediticia**

Si el usuario todavía figura informado negativamente en una base de datos de prestación de servicios de información crediticia por un plazo superior a cinco años (5) desde la mora, puede ejercer el derecho de supresión de sus datos.

- **Documentos cuestionados**

Si su documento de identidad fue extraviado, hurtado o por cualquier motivo ha salido de la esfera de su control, comuníquese con las empresas de información comercial (Veraz, Nosis, Fidelitas etc.), para informarles dicha circunstancia (deberá contar con la denuncia pertinente), así evitará su utilización fraudulenta.

Si un sujeto de derechos desea conocer qué datos hay sobre su persona en una base datos, o presentar una denuncia ante la DNPDP, puede ejercer el derecho de acceso previsto en la ley 25.326 con las siguientes previsiones:

- La solicitud de derecho de acceso sólo podrá ser efectuada en forma personal.
- El derecho de acceso podrá solicitarse en forma gratuita con intervalos no inferiores a seis meses, salvo causa justificada. La solicitud debe dirigirse directamente ante el organismo público o privado, empresa o profesional de que presume o tiene la certeza que posee sus datos.
- Para que la DNPDP pueda iniciar el control pertinente deberán haber transcurrido 10 días corridos desde la solicitud de acceso, y también aportar alguno de los siguientes documentos:
    - La negativa del responsable del banco de datos a facilitar la información solicitada.
    - Copia recepcionada de la solicitud de acceso, a fin de acreditarlo.
    - Cualquier documento enviado por el responsable del banco de datos.

Entre los requisitos necesarios para presentar una denuncia ante la DNPDP, sobre cualquier tema vinculado, se requiere presentar un escrito con los siguientes datos:

- Lugar y fecha.
- Nombres, apellido, indicación de identidad (DNI, CUIL, CUIT) y domicilio real y constituido del interesado y, de así considerarlo, un número telefónico que facilite el contacto.
- Relación de los hechos y, si lo considera pertinente, la norma en que el interesado funde su derecho.
- La petición concretada, en términos claros y precisos.

- Ofrecimiento de toda prueba que pueda corroborar los hechos denunciados, acompañando la documentación que obre en su poder o, en su defecto, su mención con la individualización posible, expresando lo que de ella resulte y designando el archivo, oficina pública o lugar donde se encuentren los originales.
- Firma del interesado o de su representante legal o apoderado.
- La presentación debe hacerse por triplicado.

B. Australia

En Australia la preocupación por la protección de datos personales es un asunto atendido por la autoridad gubernamental desde la década de los ochenta. Los marcos legal e institucional así como la estrategia, se presentan con base en la información obtenida de la fuente oficial del país que corresponde a la Oficina del Comisionado Australiano de Información[24].

a. Marco Legal

1. Ley o Acta Federal de Privacidad

La protección de datos personales en Australia se compone de una mezcla de instrumentos normativos de carácter federal y estatal. El Acta Federal de Privacidad de 1988 (Privacy Act 1988) y sus 13 Principios Australianos de Privacidad (APPs por sus siglas en inglés) aplican a las entidades del sector privado con un volumen de negocios de al menos 3 millones de dólares australianos, así como a todos los gobiernos de la Commonwealth y a las agencias gubernamentales del territorio de la capital del país.

El Acta Federal de Privacidad se modificó con la enmienda para la Mejora de Protección de la Privacidad en 2012 que entró en vigor en marzo de 2014. La enmienda fortaleció significativamente las facultades del Comisionado de Privacidad para realizar evaluaciones de cumplimiento de la privacidad tanto para las agencias gubernamentales como para algunas organizaciones del sector privado; garantizar el cumplimiento de la Ley de Privacidad modificada y, por primera vez, introducir multas por incumplimiento, incumplimiento grave y reiterado de los APP's.

Algunas de las **evaluaciones** realizadas por la Oficina el Comisionado de Privacidad entre 2014 y 2015 son:

- Evaluación de los controles de seguridad de acceso en el sistema de salud en línea del Hospital San Vicente de Sydney
- Evaluación sinóptica de los datos de pasajeros del Aeropuerto Internacional de Melbourne
- Evaluación de la Ley de Justicia y Seguridad de la Commonwealth
- Evaluación de las políticas de privacidad en línea (Principio de Privacidad 1)
- Evaluación del Western Sydney Medicare

Otros cambios en el Acta Federal de Privacidad (AFP) se refieren a disposiciones nuevas en los **informes de créditos** que incluyen: la presentación de informes de crédito más amplios, un proceso de corrección y quejas

[24]Australian Government, Office of the Australian Information Commissioner, disponible en: http://www.oaic.gov.au/ (Consultada el 30 de septiembre de 2015)

simplificado y mejorado; introducción de sanciones civiles por incumplimiento de algunas disposiciones de informes de crédito; y el requisito para los proveedores de crédito de ser miembros de un plan de resolución de conflictos de forma externa. Esta nueva disposición da poder a la Oficina del Comisionado de Información de Australia para manejar las quejas relacionadas con la privacidad a través de esquemas de resolución de conflictos de forma externa.

Asimismo, el AFP incluye nuevas disposiciones sobre **Códigos de Prácticas sobre Privacidad de la Información**, al respecto la Oficina del Comisionado ha presentado directrices para ayudar a las agencias y organizaciones a desarrollar un Código bajo la nueva ley[25].

2. Otra legislación

Cada uno de los estados y territorios de Australia, (a excepción de Australia Occidental y Australia del Sur) cuentan con su propia legislación en materia de protección de datos, aplicable a las agencias del gobierno y las empresas privadas que tienen interacción con ellas. Estas leyes son:

- Ley de Privacidad de la Información 2014 (Territorio de la Capital Australiana) que es específica para regular la información personal manejada por los organismos del sector público
- Ley de Información de 2002 (Territorio del Norte)
- Ley de Protección de la Privacidad y de Datos Personales de 1998 (Nueva Gales del Sur)
- Ley de Privacidad de la Información de 2009 (Queensland)
- Ley de Protección de Información Personal de 2004 (Tasmania), y
- Ley de la Privacidad y Protección de Datos de 2014 (Victoria).

También hay otras leyes estatales y federales que se refieren a la protección de datos, algunas enfocadas a actividades muy específicas, por ejemplo:

- Ley de Telecomunicaciones 1997 (Commonwealth)
- Ley Nacional de Salud 1953 (Commonwealth)
- Ley de Registros de Salud y de Privacidad de la Información 2002 (Victoria)
- Ley de Registros de Salud 2001 (Victoria)
- Ley de Vigilancia de los Lugares de Trabajo 2005 (New South Wales)
- Ley de Crímenes 1914 que protege los antecedentes penales.

[25] Australian Government, Office of the Australian Information Commissioner, "Our regulatory approach", (en línea), disponible en: http://www.oaic.gov.au/about-us/our-regulatory-approach/all/ (Consultada 30 de septiembre de 2015)

- Ley de Financiamiento 2006 con aspectos relacionados con el lavado de dinero y contra el terrorismo
- Ley de Propiedad Personal 2009

3. Los 13 Principios de la Privacidad en Australia[26]

El AFP se refiere en general a la protección de la información personal de un individuo; los 13 principios de la privacidad incluidos en esta Ley establecen normas, derechos y obligaciones para el manejo, tenencia, acceso y corrección de datos personales, incluida información sensible. Los principios son:

1. Transparencia en la administración de datos personales.
2. Anonimato y seudonimia
3. Recolección de información personal.
4. Recepción de información no solicitada.
5. Notificación sobre la recolección de información.
6. Uso o revelación de información personal
7. Marketing directo
8. Envío transnacional de información personal
9. Adopción, uso o divulgación de identificadores relacionados con el gobierno
10. Calidad de la información personal recolectada
11. Seguridad de la información personal
12. Acceso a información personal
13. Corrección de la información personal.

La información personal corresponde a información u opinión acerca de un individuo identificado, o razonablemente identificable con independencia de que la información u opinión sea cierta o no, o si la información u opinión está registrada en forma material o no.

Los datos personales sensibles corresponden a información u opinión acerca de: origen racial o étnico, opiniones políticas, pertenencia a una asociación política, creencias o afiliaciones religiosas, creencias filosóficas, pertenencia a una asociación profesional o comercial, pertenencia a un sindicato, orientación o prácticas sexuales, antecedentes penales que también es información personal, información de salud, información genética, información biométrica utilizada con el propósito de la identificación o verificación biométrica automatizada, y plantillas biométricas.

[26] Australian Government, Office of the Australian Information Commissioner "APP guidelines", (en línea), disponible en: http://www.oaic.gov.au/agencies-and-organisations/app-guidelines/ (Consultada 30 de septiembre de 2015)

b. Marco Institucional

La Oficina del Comisionado de Información en Australia es responsable regulador de la protección de datos. Su actividad se divide en dos grandes ramas:

- Resolución de disputas. Responsable del manejo de casos y las investigaciones con relación al cumplimiento de del Acta Federal de Privacidad. También es responsable de la provisión de información en línea.
- Regulación y Estrategia. Proporciona asesoramiento y orientación sobre el AFP y la Ley de Libertad de Información, analiza y redacta presentaciones sobre la legislación propuesta, lleva a cabo las auditorías y observaciones sobre las preguntas y propuestas que pueden tener un impacto en la privacidad, la libertad de información y la política de información del gobierno. Esta rama también apoya con la atención, comunicación y relaciones públicas con las empresas, y juega un papel fundamental en la sensibilización acerca de la privacidad, y los derechos y responsabilidades en torno a la protección de información.

La Oficina del Comisionado cuenta con dos Comités Externos para asesorarse: el Comité Asesor de Información y el Comité Asesor de Privacidad, éste se compone de ocho miembros, nombrados por el Gobernador General y su papel es asistir y asesorar al Comisionado de Información a través de:

- Proporcionar asesoramiento sobre la privacidad y la protección de la información personal
- Proporcionar información estratégica para proyectos clave realizados por la Oficina del Comisionado de Información Australiano
- Fomentar asociaciones de colaboración entre las principales partes interesadas para promover aún más la protección de la privacidad individual
- Promover el valor de la vida privada a la comunidad australiana, empresas y el gobierno
- Apoyar a la Oficina en la rendición de cuentas a las partes interesadas externas.

c. Sujetos obligados y sujetos de derecho

El Acta Federal de Privacidad 1988 regula la forma en que se maneja la información personal. En ese sentido, el sujeto de derecho es el individuo, y a través de ella el individuo posee un mayor control sobre la forma en que se maneja su información al permitirle: saber que se está recogiendo información personal, cómo se va a utilizar, y con quién será compartida; tiene la opción de no identificarse o de usar un seudónimo en ciertas circunstancias; pedir el acceso a su información personal (incluyendo información sobre su salud): dejar de recibir información

sobre marketing directo; solicitar la corrección de su información personal; presentar una queja sobre una entidad cubierta por la Ley de Privacidad, si se considera que se ha manejado mal su información personal.

Las entidades del sector privado a las que aplica la Ley pueden ser: individuos, corporativos, sociedades, asociaciones no incorporadas y fideicomisos. Los sujetos obligados son las agencias australianas de gobierno (incluyendo la isla de Norfolk), así como todos los negocios y organizaciones sin fines de lucro, o con una facturación anual de más $3 millones de dólares. Además de algunos operadores de pequeñas empresas con una facturación menor a esa cifra, también son sujetos obligados los siguientes:

- Los proveedores de servicios de salud del sector privado, entre los que se cuenta a:
    - Los proveedores tradicionales de servicios de salud, como hospitales privados, médicos, farmacéuticos y aliados profesionales de la salud
    - Terapeutas complementarios, como los neurópatas o quiroprácticos
    - Gimnasios y clínicas de pérdida de peso
    - Centro de cuidado infantil, escuelas empresas privadas e instituciones de educación superior privadas
- Empresas que venden o compran información personal
- Corporativos de información crediticia
- Proveedores de servicios contratados para la Commonwealth
- Asociaciones de trabajadores registrados o reconocidos en virtud de la Ley 2009 sobre Trabajo Justo
- Empresas que han optado por el AFP
- Empresas que están relacionadas con un negocio que será cubierto por el AFP

Los operadores de pequeñas empresas particulares son cubiertos por el AFP y al respecto se cuentan:

- Actividades de las entidades o agentes autorizados relativas a la presentación de informes Contra el Lavado de Dinero o contra el Terrorismo
- Actos y prácticas relacionadas con bases de datos de arrendamiento residencial
- Actividades relacionadas con la realización de una votación o acción de protección

Otro grupo de sujetos obligados abarca a personas o instituciones que manejan:

- Información crediticia del consumidor –incluidos los órganos de información de crédito, proveedores de crédito (incluye lo servicios públicos de energía y agua, y los proveedores de telecomunicaciones,
- Expediente fiscal (número de archivo para pago de impuestos,)

- La información personal contenida en el Registro de la Propiedad o Valores Personales,
- Información sobre los años de condena en el marco del Plan de Condenas de la Commonwealth,
- Registros de información de salud conforme a la Ley de registros electrónicos de salud.

d. Estrategia

Difusión de Recursos para el ejercicio del derecho a la privacidad

La Oficina del Comisionado de Información Australiana ofrece una serie de recursos informativos para ayudar al público en general, así como a organizaciones del sector privado y los organismos gubernamentales de Australia y la Isla de Norfolk, a entender el AFP. En la página web se encuentran: Guías de privacidad (27); hojas informativas de privacidad (56), recursos para las agencias (5), recursos para empresas (16) y recursos de entrenamiento (guía para evaluación de impacto de la privacidad y presentación de obligaciones en materia de privacidad).

Las guías se refieren a temas variados, y específicamente paras los individuos se identifican:

- Protección de información personal,
- Quejas de privacidad: cómo manejarlas,
- Notificación de violación de datos: guía para el manejo de brechas de seguridad de la información personal,
- Reporte de personas desaparecidas,
- Principios de Privacidad en Australia.

Las hojas informativas de privacidad abarcan temas como salud y sanidad en línea, crédito y finanzas, tecnología y telecomunicaciones. Entre las dirigidas a los individuos se identifican:

- Consejos para proteger la privacidad
- Presentación de una queja de privacidad
- Proveedores de crédito
- Marketing directo y su informe de crédito
- Fraude y su informe de crédito
- Cuándo se borrará la información en su informe de crédito
- Corrección de un informe de crédito
- Quién puede acceder a un informe de crédito
- Acceso de emergencia y su registro de la salud en línea
- Medicare y su registro de salud en línea

- Los jóvenes y el sistema de registro de la sanidad electrónica
- Consentimiento y manejo de la información personal en su registro de salud en línea
- Conciliación de las quejas de privacidad
- La protección de la información del contribuyente
- Fotocopiadoras digitales: recogida y almacenamiento de datos personales
- Publicidad comportamental en línea
- Emergencias y desastres
- Actividad ilegal y aplicación de la ley
- Exploración de ID en clubes y pubs
- Uso y divulgación de la información genética
- Información sobre salud y capacidad deteriorada

Ejercicio de derechos / Denuncias de incumplimientos

Ofrece información en línea sobre el procedimiento para la presentación de una queja ante la Oficina del Comisionado de Información respecto al manejo de los datos personales[27] de parte de las agencias gubernamentales y las organizaciones del sector privado obligadas por el AFP. Se señala la gratuidad del trámite aunque si se decide la intervención de abogado el costo es a cuenta del individuo. El quejoso debe acudir primero a la agencia u organización que violentó su derecho a la privacidad y, en caso de que la respuesta no le satisfaga, puede acudir a presentar su queja por escrito, en línea, ante la Oficina de Comisionado. Se establece el procedimiento para la presentación, los requisitos que debe cubrir y cómo se tratará la información aportada en el proceso de resolución de su queja. Las quejas aplican contra agencias gubernamentales de Australia y organizaciones del sector privado (empresas y sin fines de lucro). Se manifiesta que el individuo puede ejercer su derecho de solicitar a la Corte Federal de Australia la revisión de una decisión o determinación de la Oficina del Comisionado.

[27] La queja puede presentarse también por: el manejo de los registros de salud en línea, identificadores de salud, información genética, seguro de enfermedad, regímenes de prestaciones farmacéuticas; el manejo de algunos antecedentes penales (penas extinguidas), el manejo de información personal en el Registro de Bienes Muebles de Valores; y datos de coincidencia sobre los números de identificación fiscal y su uso.

C. Brasil[28]

La Carta Magna de Brasil contiene principios generales referentes a la protección de datos, y aunque cuenta con disposiciones legales en torno al *Habeas data* (1997) además de la que regula aspectos como el internet, no cuenta con un marco legislativo específico en la materia, y está pendiente de desarrollar un marco institucional encargado de vigilar la aplicación y ejercicio del derecho.

a. Marco Legal

El país no cuenta con una ley de protección de datos, sin embargo hay principios generales al respecto en la Constitución Federal, en particular en el artículo 5, fracciones X y LXXII; en el Código Civil brasileño, y leyes y regulaciones dirigidas a tipos particulares de relaciones (por ejemplo: el Acta de Internet, Código de Protección al Consumidor y leyes laborales) sectores específicos (instituciones financieras, industria de la salud, telecomunicaciones entre otras); y actividades profesionales particulares (medicina y derecho). Adicionalmente hay leyes sobre tratamiento y salvaguarda de documentos e información, manejados por entidades gubernamentales que tienen implicaciones sobre la privacidad.[29] El código Civil en su artículo 21 también establece el derecho a la privacidad.

La Constitución Federal de Brasil establece que:

- La intimidad, vida privada, honor e imagen de las personas son inviolables
- La confidencialidad de correspondencia y comunicación electrónica está protegida, y
- Todos tienen asegurado el acceso a la información, si bien la confidencialidad de la fuente debe ser salvaguardada como algo necesario en el ejercicio de la actividad profesional.

La Ley 9507/1997 Ley Reglamentaria de *Habeas Data*, regula el derecho de acceso a informaciones, disciplinas, y el procedimiento de *Habeas Data*.[30] Esta Ley faculta a la ciudadanía a presentar denuncias ante el Tribunal

---

[28] Saltor Carlos, "La Protección de Datos Personales: Estudio Comparativo Europa-América con especial análisis de la situación de Argentina", Universidad Complutense de Madrid, 2013 (en línea), disponible en: http://eprints.ucm.es/22832/1/T34731.pdf
Red Iberoamericana de Protección de Datos, "Cuadro Comparativo: Desarrollos Normativos Nacionales en Materia de Protección de Datos", 2004, (en línea), disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/iberoamerica/common/pdfs/cuadro_comparativo_de_normativas_15-6-2004_22_07_05.pdf

[29] Data Protection Laws in the World, DLA-PIPER en http://dlapiperdataprotection.com/#handbook/world-map-section (Consultada el 2 de octubre de 2015)

[30] University of Alicante Intellectual Property & Information Technology, "Ley 9507/1997, de 12 de Noviembre de 1997, Ley Reglamentaria de Habeas Data, Regula el Derecho de Acceso a Informaciones, Disciplinas, y el Procedimiento del Habeas Data", 1997, (en línea),

Constitucional contra cualquier entidad que posea una base de datos, para buscar amparo judicial, para conocer o solicitar la corrección o remoción de sus datos personales. Pero aún no se cuenta con una autoridad encargada de velar por la protección de datos personales.

El debate en torno a la construcción de un marco legal ha pasado recientemente por un periodo de máxima efervescencia en la nación, destacando:

- La propuesta del Senado de la Ley 330/2013 que busca establecer principios, derechos y obligaciones para el uso y tratamiento de la información personal en Brasil, así como su transmisión.
- En noviembre de 2012, el Congreso Brasileño promulgó la Ley contra crímenes informáticos, que criminaliza los actos de *hackeo,* o invasión de dispositivos electrónicos para intentar obtener, adulterar o destruir información sin el consentimiento del propietario del dispositivo.
- En junio de 2014, la Ley Brasileña de Internet tomó fuerza, estableciendo principios generales, derechos y obligaciones para su uso. Hace previsiones relevantes respecto al almacenamiento, su tratamiento y revelación de datos recolectados en línea.
- Se encuentra en curso la discusión en el Senado de una enmienda al Código Brasileño de los Consumidores para establecer como práctica abusiva la oferta de productos o servicios no solicitados a través de medios electrónicos o por teléfono.

b. Marco Institucional

No cuenta con una instancia responsable de la protección de datos. Sin embargo, los juicios por violación de privacidad, pueden tratarse por la vía de los procedimientos administrativos o acciones civiles individuales que pueden ser iniciados por el individuo, la autoridad pública (por ejemplo la Procuraduría del Consumidor) o asociaciones de defensa de intereses colectivos. La Ley Brasileña del Internet también establece multas para los infractores de la privacidad y del derecho a la intimidad.

Asimismo, debe destacarse la existencia del *Habeas data* como un medio previsto en la Constitución Federal, que es utilizado para lograr acceder a la información personal contenida en registros y bases de datos de entidades gubernamentales para su corrección.

c. Sujetos obligados y sujetos de derecho

El *Habeas data* hace a todos los brasileños sujetos del derecho al permitirles recurrir ante los tribunales para lograr la visualización de los datos de registros públicos y privados en los que se incluyen los datos personales,

---

disponible en: http://www.uaipit.com/es/legislacion/2344/Ley-9507/1997--de-12-de-Noviembre-de-1997--Ley-Reglamentaria-de-Habeas-Data--Regula-el-Derecho-de-Acceso-a-Informaciones--Disciplinas--y-el-Procedimiento-del-Habeas-Data--

así como permitirles la rectificación de datos inexactos u obsoletos o que den lugar a alguna conducta discriminatoria.

Con base en lo anterior, se puede señalar que los sujetos obligados son todas las personas e instancias que posean datos personales.

d. Estrategia

El análisis de la estrategia cívica de promoción del derecho en este caso, requiere de profundizar la revisión sobre los procesos mediante los cuales los individuos ejercen su derecho a la privacidad ante los tribunales. Así, puede inferirse la posibilidad de que se logre una visualización de alcance limitado a la difusión o bien, que ella se encuentre sectorizada. No es visible en línea ninguna estrategia por parte de las instancias públicas.

Ejercicio de derechos / Denuncias de incumplimientos

- A pesar de carecer de una institución encargada de velar por la protección de la privacidad y de los datos personales, la Constitución Federal de Brasil establece la inviolabilidad de la intimidad, la vida privada, honor e imagen de las personas. Asimismo, la confidencialidad en la correspondencia y comunicación electrónica se encuentra salvaguardada.

- En el marco de la Ley 9507/1997 se faculta a la ciudadanía a presentar denuncias, directamente ante el Tribunal Constitucional brasileño, en contra de cualquier entidad que posea una base de datos, ya sea para buscar amparo judicial, para conocer o solicitar la corrección o remoción de sus datos personales. No obstante, no existen indicios que sugieran que el procedimiento de presentación de una denuncia por un ciudadano, sea sencillo y accesible.

D. Canadá

Canadá cuenta con la Office of the Privacy Commisioner of Canada, pero también cuenta con autoridades provinciales y territoriales que se mencionan en este apartado[31].

a. Marco Legal

En Canadá hay 28 estatutos federales, provinciales y territoriales sobre la privacidad, que gobiernan la protección de información personal en los sectores privado y público. Canadá tiene dos leyes federales de la privacidad: la Ley de Privacidad que cubre las prácticas de manejo de información personal por parte de los departamentos y agencias del gobierno, y la Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA, por sus siglas en inglés) que aplica al sector privado.

La información personal incluye cualquier información sobre un individuo identificable, no se encuentran específicamente definidos los datos o información sensible.

La Ley de Privacidad tuvo efectos a partir de 1983; a través de ella se obliga a 250 departamentos y agencias de gobierno federal a respetar la privacidad, al limitar la recolección, uso y transferencia de información personal. Esta ley da a los individuos el derecho al acceso y corrección de información personal en posesión de organizaciones gubernamentales. Esta ley sólo aplica a las instituciones del gobierno federal, para el manejo de toda la información personal que el gobierno recoge, utiliza y divulga, sobre las personas o sus empleados federales; no aplica a partidos ni representantes políticos.

La Ley de Protección de Información Personal y Documentos Electrónicos o PIPEDA, establece normas básicas de cómo las organizaciones del sector privado recogen, usan o revelan información personal en el curso de las actividades comerciales a través de Canadá. También se aplica a la información personal de los empleados de obras regulados por el gobierno federal, empresas, organizaciones o empresas (regulados por el gobierno federal como son bancos, aerolíneas y empresas de telecomunicaciones).

La PIPEDA no aplica en una organización que opera totalmente dentro de una provincia que cuenta con una legislación que ha sido considerada sustancialmente similar a ésta, a menos que la información cruce las fronteras provinciales o nacionales. Las provincias de Alberta, Columbia Británica y Quebec tienen legislación general para el sector privado considerada sustancialmente similar. Por otra parte, Ontario, Nueva Brunswick, y Terranova y Labrador cuentan con legislación sobre privacidad aplicable sólo para información en materia de

[31] La información sistematizada en las siguientes secciones proviene de:
Office of the Privacy Commissioner of Canada, disponible en: https://www.priv.gc.ca/index_e.asp
DLA PIPER, "Data protection laws of the world, World Map", 2015, disponible en: http://dlapiperdataprotection.com/#handbook/world-map-section

salud que se ha declarado sustancialmente similar, pero sólo respecto a la custodia de información sanitaria. En estos casos las leyes se denominan: Ley de Protección de Información Personal en Salud de Ontario; Ley de Acceso y Privacidad de la Información de Salud Personal de Nuevo Brunswick; y Ley de Información Personal sobre salud de Terranova Labrador. En otras provincias se han creado sus leyes de privacidad de información en salud, pero no se consideran sustancialmente similares a PIPEDA, por lo que ésta es la ley que se aplica.

De esto modo, los estatutos de privacidad que regulan al sector privado de Canadá son:

- Ley de Protección de Datos Personales y Documentos Electrónicos (PIPEDA)
- Ley de Protección de Datos Personales (PIPA Alberta)
- Ley de Protección de Datos Personales (PIPA British Columbia)
- Ley de la Protección de Datos Personales y Prevención del Robo de Identidad (PIPITPA, aún no entra en vigor)
- Ley sobre la Protección de Datos Personales en el Sector Privado (Ley de Privacidad de Quebec) y
- Los Estatutos Canadienses de Privacidad que aplican colectivamente

Adicionalmente, hay una legislación que dispone aspectos relativos a la protección de información personal, por ejemplo;

- La Ley Federal Bancaria, que contiene disposiciones que regulan el uso y divulgación de información financiera personal por las instituciones financieras reguladas por el gobierno federal.
- Legislación relativa a la presentación de informes de crédito al consumo, la cual existen en la mayoría de las provincias. Ella impone límites a las agencias y da a los consumidores el derecho de acceso y a solicitar la corrección de la información.
- Leyes provinciales de cooperativas de crédito que suelen tener disposiciones relativas a la confidencialidad de la información respecto a las operaciones de los miembros.
- Leyes provinciales que contienen cláusulas de confidencialidad relativas a la información personal recopilada de los profesionistas.

b. Marco Institucional

Cada provincia y territorio en Canadá tiene un Comisionado o Defensor del Pueblo encargado de supervisar la legislación provincial y territorial de privacidad. Así, la protección de datos personales en Canadá está a cargo de diversas instancias.

- Oficina del Comisionado de Privacidad de Canadá (responsable de vigilar la aplicación de PIPEDA)

- Oficina del Comisionado de Información y Privacidad de Alberta (responsable de vigilar la aplicación de la Ley de Protección de Información Personal –PIPA por sus siglas en inglés- en Alberta)
- Oficina del Comisionado de Información y Privacidad de British Columbia (responsable de vigilar la aplicación de la Ley de Protección de Información Personal –PIPA por sus siglas en inglés- en BC), y
- Comisión de Acceso a la Información de Quebec (responsable de vigilar la aplicación de la Ley de Privacidad en Quebec)

El Comisionado de la Privacidad de Canadá es un oficial del Parlamento que reporta directamente a la Casa de los Comunes y al Senado; tiene facultades para: investigar quejas, conducir auditorías, ejecutar acciones de persecución bajo dos leyes federales; informar públicamente sobre las prácticas del manejo de información personal de las organizaciones del sector público y privado; apoyar, realizar y publicar investigaciones sobre cuestiones de privacidad; y promover la conciencia pública y comprensión de las cuestiones de privacidad.

c. Sujetos obligados y sujetos de derecho

De acuerdo con la PIPEDA los sujetos obligados son:

- Organizaciones del sector privado que desarrollan actividades en Canadá en las provincias o territorios de Manitoba, Nuevo Brunswick, Terranova y Labrador, Territorios del Noroeste, Nueva Escocia, Nunavut, Ontario, Isla del Príncipe Eduardo, Saskatchewan, o Yukon, pero no su manejo de información de los empleados.
- Organizaciones del sector privado que desarrollan actividades en Canadá cuando la información personal que recopilada, usada o divulgada cruce las fronteras provinciales o nacionales, pero no su manejo de información de los empleados.
- Organizaciones reguladas por el gobierno federal que ejerzan la actividad comercial en Canadá, como la bancaria, líneas aéreas, teléfonos o radiodifusión, incluyendo el manejo de la información de salud y la información de los empleados.

Los sujetos de derechos son todas las personas que cuentan con información personal en Canadá.

d. **Estrategia**

Difusión en página web

Guía para personas: protección de la privacidad

La estrategia canadiense para la promoción del derecho de protección de la privacidad considera acciones para: instituciones federales, empresas e individuos. En particular para estos últimos se diseñó la **Guía para personas: protección de la privacidad**, e incluye un instrumento de información para prevenir el robo de identidad.

Robo de identidad. Se informa a los individuos sobre el riesgo del robo que puede permitir el cobro de cheques, vaciar cuentas bancarias, estafar a la compañía de la tarjeta de crédito, hipotecar bienes, falsificación de cheques y tarjetas. En su página web proporciona consejo para reducir el robo, entre ellos:

- Evitar compartir información personal que circule libremente. Al respecto aconseja preguntar expresamente para qué se pide la información y cómo se va a utilizar.
- No compartir el número de seguro, en particular en los informes de crédito y las bases de datos informáticas.
- **Tarjetas de crédito.** Para este punto específico la Oficina del Comisionado de Privacidad aconseja aspectos del uso de crédito vía internet, el monitoreo del correo para la entrega de estados de cuenta; revisión de informe de crédito anual.
- **Correo impreso**. En la recepción de correo en un buzón doméstico se debe asegurar un mecanismo seguro para el almacenaje, recogerlo de inmediato, triturar o destruir elementos con nombre y dirección, aprobación previa de tarjeta de crédito.
- **Teléfono.** No proporcionar información bancaria por teléfono y verificar la autenticidad de llamadas que solicitan información de tarjetas de crédito.
- **Monedero.** Portar sólo identificaciones personales como licencia de conducir y no llevar pasaporte, certificado de nacimiento, número de seguro. No permitir que se fotocopien los documentos de identidad a menos que exista una necesidad real y la certeza de la protección de sus datos.
- **Operaciones online**. Ofrece consejos para proteger ordenador y dispositivo móvil que son fuente de información personal concentrada.

Además de consejos prácticos en estos terrenos se ofrecen guías para garantizar a privacidad en diferentes tópicos como por ejemplo: turismo, información biométrica, protección al consumidor, licencias de conducir, información genética, información sobre salud, información financiera personal, violaciones a la privacidad,

radiofrecuencia, tecnología, información inalámbrica, seguridad social, privacidad en el centro de trabajo, y privacidad de la juventud, entre otros.

Además, en la página oficial web del Comisionado de Privacidad de Canadá existen diversos materiales de aprendizaje sobre protección de datos personales. Cuenta con informes, publicaciones, guías, presentaciones, videos y otras herramientas como Apps para Android dirigidos específicamente a jóvenes y protección de datos en redes sociales de internet[32].

Ejercicio de derechos / Denuncias de incumplimientos

Cómo presentar una queja de privacidad[33]

En el orden federal, los derechos a la privacidad están protegidos por dos leyes distintas:

- El Acta de Privacidad, que contempla a las instituciones del gobierno federal.
- El Acta de Protección de Información Personal y Documentos Electrónicos (PIPEDA), que contempla a un gran número de organizaciones del sector privado.

Debido a que los distintos territorios y provincias canadienses cuentan con varias leyes e instituciones responsables de observar el cumplimento de las mismas, como los comisionados y ombudsman provinciales y territoriales, el primer paso para presentar una queja es determinar la instancia correcta ante la cual presentar la denuncia. Para ello se pone a disposición de los interesados, a través del sitio web oficial, una Hoja de Datos Básicos sobre la Privacidad de Canadá (Fact Sheet: Privacy Legislation in Canada)[34].

El proceso para presentar una queja, ya sea contra una institución pública federal o contra una organización privada, es bastante similar y consta de tres modalidades:

1. Llenar la "Forma para Quejas en línea".
2. Descargar la forma llenada electrónicamente, imprimirla y enviarla por correo postal.
3. Descargar, imprimir la forma de quejas, llenar a mano y enviarla por correo postal.

Cualquier opción elegida es libre de costos y la Oficina del Comisionado a la Privacidad no se compromete a tiempos definidos para emitir respuestas a sus investigaciones.

---

[32] Office of the Privacy Commissioner of Canada, "Presentation Packages for Parents and Teachers", 2012, (en línea), disponible en: https://www.priv.gc.ca/youth-jeunes/pp/index_e.asp y "Guidance and Information", 2014, (en línea), disponible en: https://www.priv.gc.ca/information/guide-info/index_e.asp (Consultadas 1 de octubre de 2015)

[33] Office of the Privacy Commissioner of Canada, "How to File a Privacy Complaint", 2015, (en línea), disponible en: https://www.priv.gc.ca/complaint-plainte/index_e.asp

[34] Office of the Privacy Commissioner of Canada, "Fact Sheets", 2015, (en línea), disponible en: https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp

Es importante señalar que en entrevista con Melanie Millar- Chapman, Gerente de Investigación (Research Manager) en la Oficina del Comisionado de Privacidad de Canadá, ella nos informó que entre los objetivos de la Oficina del Comisionado de Privacidad de Canadá (OPC) se encuentran tanto proteger como promover los derechos a la privacidad. Para tales efectos, las actividades que involucran comunicación y difusión apoyan tales misiones tanto de manera directa como indirecta.

En palabras de la Sra. Melanie Millar-Chapman[35], el área encargada de Comunicaciones centra sus esfuerzos en promover que tanto individuos como organizaciones estén informados de sus derechos a la privacidad, o de sus responsabilidades, en el caso de estas últimas.

Los programas de comunicación y difusión son tanto activos y reactivos, entendiéndose estos últimos como todas aquellas actividades que involucren responder quejas y solicitudes de información de individuos y organizaciones, ya sea a través de su centro de atención telefónico o por otros medios electrónicos. Durante el año 2014 se atendieron más de nueve mil llamadas telefónicas[36].

El siguiente cuadro muestra la incidencia temática de las quejas totales atendidas en el marco de PIPEDA, es decir, bajo el acta que regula el manejo de los datos personales en posesión de privados:

PIPEDA 2014 – Quejas recibidas por sector o industria		
Sector	**Número de quejas**	**Proporción porcentual del total de quejas**
Alojamiento/ Bienes raíces	19	5%
Entretenimiento	4	1%
Financiero	81	20%
Industria de Seguros	21	5%
Internet	72	18%

[35] Research Manager; ver sección de Anexos y Formatos de Entrevista
[36] Entrevista con la Gerente de Investigación de la Oficina del Comisionado de Privacidad de Canadá, Melanie Chapman-Millar, ocurrida el día 2 de Diciembre de 2015 (en anexos).

PIPEDA 2014 – Quejas recibidas por sector o industria		
Sector	**Número de quejas**	**Proporción porcentual del total de quejas**
Otros sectores	24	6%
Profesionales	9	2%
Ventas	25	6%
Servicios	23	6%
Telecomunicaciones	52	13%
Transporte	72	18%
Total	402	100%

Entre los medios activos que emplean se encuentran las acciones de investigación y difusión de guías, las cuales tienen por principal herramienta el sitio web de la OPC, que en 2014 recibió más de dos millones de visitas[37]. Otra práctica que utilizan para tener cercanía con el público general, es la conducción de encuestas anuales y bianuales que versan acerca del grado de conocimiento de los entrevistados sobre temas relacionados a derechos y responsabilidades concernientes a privacidad.

Otra práctica acostumbrada por la OPC, es la organización periódica de conferencias, talleres y eventos sobre temas de privacidad, mismos que fungen como vehículo para alcanzar a públicos mayores de interesados. Entre los grupos prioritarios que han identificado para la instrumentación de campañas específicas, se encuentran los menores de edad, adultos mayores y pequeñas empresas, esto en el entendido de que ambos grupos etarios y empresas nuevas suelen ser un blanco de estafadores, comercio insistente y fraudes electrónicos. En lo que se refiere a redes sociales, la OPC actualmente cuenta con un blog y administra cuentas en Twitter y Youtube.

[37] Entrevista con la Gerente de Investigación de la Oficina del Comisionado de Privacidad de Canadá, Melanie Chapman-Millar, ocurrida el día 2 de Diciembre de 2015 (en anexos)

E. Chile

Chile ha logrado un desarrollo relevante en materia legal de protección de datos personales, incluso fue de los primeros países latinoamericanos en generar una normativa al respecto, sin embargo al igual que Brasil no ha promovido la conformación de un ente específicamente dedicado a la vigilancia de la aplicación del derecho.

a. Marco Legal

La protección de datos personales se encuentra prevista en diversas leyes específicas, esto es, se encuentra dispersa en algunas leyes conexas o complementarias[38] como son:

- Constitución de la República de Chile, artículo 19, fracción 4 asegura "el respeto y la protección de la vida pública y privada de la persona y de su familia. Cualquier persona que por acción u omisión arbitraria o ilegal sufre una privación, perturbación o amenaza a este derecho puede presentar una Acción de Amparo Constitucional.
- Ley 19.628 "Sobre la protección de la vida privada", comúnmente conocida como "Ley de Protección de Datos de Carácter Personal" (LPDCP) define y se refiere al tratamiento de la información personal en bases de datos públicas y privadas[39].
- Ley 20.285: "Sobre el Acceso a la Información Pública": adelanta el principio de Transparencia en la Función Pública, el derecho individual del acceso a la información de los órganos de la Administración Pública, así como los procedimientos y excepciones de los mismos.
- Ley 20.575: "Establece el principio del destino en el tratamiento de los datos personales»: incorpora normas adicionales cuando se trata de información personal relacionada con aspectos económicos o deuda.
- Ley General de Bancos, cuyo artículo 154 establece el secreto bancario: sostiene que, salvo ciertas excepciones, todos los depósitos son secretos, y la información relacionada se puede dar solo para el dueño de la cuenta o representante designado.
- Ley 19223, "Conductas delictivas relacionadas con la Informática": establece sanciones para quienes violan e ilegalmente acceden y / o utilizan la información disponible en las bases de datos electrónicas.

Bajo la LPDCP la información personal se refiere a cualquier información concerniente a la persona natural, independientemente de si es identificada o identificable. Con esta misma norma, la información sensible se

[38] DLA PIPER, "Data protection laws of the world, World Map", 2015, disponible en: http://dlapiperdataprotection.com/#handbook/world-map-section (Consultada el 2 de octubre de 2015)
[39] Última modificación: 17 de febrero 2012.

refiere a las características físicas o morales, a hechos o circunstancias de su vida privada e intimidad, tales como hábitos personales, origen racial, ideología u opinión política, credo religioso, condiciones de salud mental y física, y vida sexual.

La información personal sólo puede ser tratada sin mediar consentimiento escrito del propietario de la información o cuando se presentan alguna de las siguientes condiciones: autorización por ley, recolección por medio de fuentes de acceso público, y si es información de carácter económico, financiero, bancario o comercial, siempre y cuando el tratamiento de la información cumpla con los requisitos específicos establecidos en la ley.

b. Marco Institucional

No hay una autoridad específica para la protección de datos por lo que estos asuntos se resuelven en las cortes chilenas: Jueces de jurisdicción civil; Cortes de Apelación y Suprema Corte. Los primeros representan la instancia inicial ante una violación a la Ley de Protección de Datos de Carácter Personal o Ley de Protección de la Vida Privada. Las Cortes de Apelación son la instancia para presentar las acciones constitucionales, que incluye los alegatos por violaciones al derecho constitucional de la Privacidad. La Suprema Corte atiende apelaciones que involucran violaciones constitucionales, que incluyen peticiones del ciudadano para remover, modificar o bloquear información o datos personales de una base de datos pública o privada y que le es negada.

c. Sujetos obligados y sujetos de derecho

De acuerdo con la LPDCP, la "persona responsable" es la persona física, persona jurídica, o entidad pública que decide el tratamiento de datos personales; es responsable de asegurar que los datos personales están protegidos en conformidad con los requisitos legales aplicables; debe responder también a las consultas de cualquier persona respecto de sus datos personales, así como su modificación, supresión o bloqueo, etcétera. Si no hay respuesta, (es) que debe ser proporcionada por la persona responsable dentro de dos días hábiles, la persona afectada puede iniciar un procedimiento civil ante las autoridades correspondientes (el correspondiente las autoridades).

d. Estrategia

El ejercicio de los derechos ARCO en Chile requiere de la contratación de un abogado que actúe ante Tribunales cuyo costo es a cargo del interesado. La Fundación chilena “Protección de Datos Personales”[40] promueve la existencia de una autoridad independiente que proteja del abuso por desconocimiento de la ley. De este modo la Fundación pone a disposición del público tres modelos de solicitud para que las personas puedan solicitar su acceso a datos, la cesión de datos y la eliminación de los mismos.

[40] Fundación Protección de Datos Personales, disponible en :http://protecciondedatospersonales.cl/ (Consultada el 15 de octubre de 2015)

Así, el análisis de la estrategia cívica de promoción del derecho para la realidad chilena, requiere de profundizar la revisión sobre los procesos mediante los cuales los individuos ejercen su derecho a la protección de sus datos. La observación sobre la estrategia cívica en este caso debe ser completada con entrevistas que abarquen a más de una instancia gubernamental e incorpore posiblemente, a autoridades judiciales.

Ejercicio de derechos / Denuncias de incumplimientos

La protección de datos personales en Chile se encuentra prevista tanto en la Constitución de la República como en diversas leyes complementarias. No obstante, como en el caso de Brasil, no se cuenta con una institución encargada de velar por la protección de tales derechos. Sin embargo, los asuntos que se presenten en tal materia se resuelven en las distintas cortes chilenas: Jueces de Jurisdicción Civil, Cortes de Apelación y en la Suprema Corte de Chile.

F. España

La protección de datos en España se encuentra regulada por la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) de cuya aplicación se encarga la Agencia Española de Protección de Datos (AEPD)[41].

a. Marco Legal

La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) es el instrumento rector de la protección de datos en el territorio español. Contiene los derechos ARCO: de acceso, rectificación, cancelación y oposición. Establece el derecho a que todo individuo, al momento de la recogida de datos personales, sea informado previamente de modo expreso, preciso e inequívoco de la existencia de un fichero, la posibilidad de ejercitar sus derechos y del responsable del tratamiento. A través del derecho de acceso el ciudadano puede conocer y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento. El derecho de rectificación permite corregir errores, modificar los datos inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento. La cancelación posibilita que se supriman los datos inadecuados o excesivos sin perjuicio del deber de bloqueo recogido en la LOPD. Con el derecho de oposición el afectado puede impedir que se lleve a cabo el tratamiento de sus datos de carácter personal o se cese el mismo.

La LOPD contiene también el derecho de información que es previo al tratamiento de los datos personales. Este implica que si se van a registrar y tratar los datos de carácter personal, es necesario informar previamente a los interesados a través del medio que se utilice para la recogida, de modo expreso, preciso e inequívoco respecto: i) de la existencia de un fichero o tratamiento de o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; ii) del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; iii) de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; iv) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, y v) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Un dato de carácter personal, de acuerdo con la LOPD es cualquier información que permite identificar o hacer identificable a una persona. En ese sentido el derecho fundamental a la protección de datos reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos.

[41] El desarrollo de los apartados posteriores se sistematiza con base en la información del sitio oficial de la AEPD Agencia Española de Protección de Datos, disponible en http://www.agpd.es/portalwebAGPD/index-ides-idphp.php (Consultada el 15 de octubre de 2015)

b. Marco Institucional

La Agencia Española de Protección de Datos es la autoridad estatal de control independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos; garantiza y tutela el derecho fundamental a la protección de datos de carácter personal de los ciudadanos. La AEPD, aunque creada en 1992, comenzó a funcionar en 1994 como un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con completa independencia de las Administraciones Públicas en el ejercicio de sus funciones, cuenta con presupuesto propio y plena autonomía funcional. Se relaciona con el Gobierno a través del Ministerio de Justicia[42]. La Agencia tutela al ciudadano en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición cuando no han sido adecuadamente atendidos. Asimismo, garantiza el derecho a la protección de datos investigando y sancionando aquellas actuaciones que puedan ser contrarias a la ley. El cuadro siguiente muestra algunos datos del desempeño de la AEPD.

Agencia Española de Protección de Datos: datos clave de desempeño en 2014	
Área de desempeño	**Registro**
Reclamaciones de tutela de derechos	2,099
Denuncias	10,074
Resoluciones de inspección	11,222
Ficheros inscritos	3,746,930
Consultas de ficheros	10,443,827
Operaciones de inscripción de ficheros	584,258
Autorización de transferencias internacionales	1,232
Consultas telefónicas, escritas y presenciales	99,524
Visitas a la web	5,706,488
Fuente: Elaboración propia con base en: http://www.agpd.es/portalwebAGPD/LaAgencia/index-ides-idphp.php **Consultada el 22 de octubre de 2015**	

[42] Agencia Española de Protección de Datos, "Conoce la Agencia", 2014, (en línea), disponible en: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/index-ides-idphp.php (Consultada el 15 de octubre de 2015)

c. Sujetos obligados y sujetos de derecho

Los sujetos obligados son las empresas y organismos públicos, que son a su vez los responsables de los ficheros (bases de datos) de datos personales. Los sujetos de derecho es la ciudadanía en general.

d. Estrategia

Difusión en página web

A través de su portal web oficial, la AEPD pone a la disposición de los usuarios de internet y la ciudadanía en general, una serie de documentos y guías que fungen como instrumentos para informar a los ciudadanos acerca de sus derechos y de los servicios que presta la Agencia. Explica de manera esquemática cómo se ejercen los derechos ARCO, ante qué circunstancias, acompañando la explicación de formatos, guías e instructivos específicos para hacerlo real. Todos se ejercen de manera personal.

Asimismo, informa sobre la existencia de derechos relacionados con algún campo específico para fortalecer la protección de los datos personales como los relacionados con la publicidad o los que derivan del uso y registro en sistemas de información de carácter regional en la Comunidad Europea que permiten controlar el cruce de las fronteras, la transferencia de datos personales y la prevención del terrorismo. Así, la AEPD informa sobre:

1. Derechos de exclusión de guías de teléfonos. Se ofrecen formatos para: i) ejercicio de derechos de exclusión de la utilización de los datos para fines de publicidad y prospección comercial, y ii) ejercicio de derecho de exclusión en los repertorios telefónicos de acceso público
2. Derechos a no recibir publicidad no deseada. La persona se inscribe en el fichero de exclusión publicitaria en el sitio web para evitar recibir publicidad e entidades con las que no se mantiene ni ha mantenido ninguna relación[43]; se continúa recibiendo publicidad de empresas a las que sí se autorizó utilizar los datos. Si a los 10 días sigue recibiendo publicidad se puede recurrir a la AEPD
3. Derechos de los abonados y usuarios de servicios de telecomunicaciones. Este derecho descansa en la Ley 32/2003 del 3 de noviembre, General de Telecomunicaciones para mantener anónimos los datos de las personas una vez que no sean necesarios, entre otros derechos.
4. Derechos de los destinatarios de servicios de comunicaciones electrónicas. En este renglón aplica la Ley 34/2004 del 11 de julio, de Servicios de la Sociedad de Información y de Comercio Electrónico (artículos 20, 21 y 22) a fin de que, entre otros, al comprar en línea la persona con la que se realicen sea identificable, tener claridad sobre ofertas promociones, concursos y sorteos, no recibir de información que oculte la identidad de quien la envía, no recibir publicidad no solicitada, revocar el consentimiento en cualquier

[43] Listas Robinson de Exclusión Publicitaria, disponible en: www.listarobinson.es (Consultada el 15 de octubre de 2015)

momento; los prestadores de servicios podrán utilizar dispositivos para almacenar datos siempre que antes hayan informado al usuarios sobre la utilización.

- **Otros derechos.** La AEPD también puede tutelar derechos relacionados con la protección de datos, por ejemplo:

- Derecho de acceso al Sistema Schengen. El Sistema está a cargo de la Comisaría General de la Policía Judicial, Unidad de Cooperación Internacional; a través de él se permite a los países miembros de la Unión Europea registrar información sobre la descripción de las personas derivada del control en fronteras, aduanas y la policía.
- Derechos de acceso, rectificación y cancelación en relación con el acuerdo TFTP que habilita la transferencia financiera a Estados Unidos. Este acuerdo fue firmado entre la Unión Europea y Estados Unidos (EU) con base en el Programa de Seguimiento de la Financiación del Terrorismo, conocido como Acuerdo TFTP, en agosto de 2010. Mediante este acuerdo se habilita el intercambio de información entre Europa y EU en el contexto de la lucha contra el terrorismo. Los artículos 15 y 16 del Acuerdo permiten a los ciudadanos acceder a la información, rectificarlos y en su caso, la posibilidad de eliminarlos o bloquearlos para impedir el acceso a los mismo.
    - La AEPD pone a disposición de los individuos formularios para su ejercicio: formulación de verificación de identidad, formulación de derecho de acceso, formulación de ejercicio de derechos de rectificación o cancelación, y formulario de autorización a la AEPD.
- Derechos de indemnización. En caso de que los interesados sufran daño por incumplimiento de la LOPD por parte del responsable, en sus bienes o derechos, tendrán derecho a una indemnización de conformidad con la Ley. Cuando se trate de ficheros de titularidad pública la responsabilidad se exigirá de conformidad con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas. En caso de ficheros de titularidad privada, la acción se ejercitará ante los órganos de jurisdicción ordinaria.
- Derechos de consulta al RGPD. Toda persona tiene derecho a conocer la existencia de tratamiento de datos personales, sus finalidades y la identidad del responsable del tratamiento, recabando la información del Registro General de Protección de Datos, que es público y gratuito.

Carta de servicios de la AEPD

La Carta de Servicios es un documento que constituye el instrumento a través del cual los Órganos, Organismos y Entes Públicos y otras Entidades de la Administración General del Estado informan a los ciudadanos y usuarios sobre los servicios que tienen encomendados, sobre los derechos que les asisten en relación con aquellos y sobre los compromisos de calidad en su prestación.

El derecho fundamental a la protección de datos: guía para el ciudadano (2011)

Es un instrumento que informa al ciudadano de los aspectos centrales para la protección de sus datos: qué son los datos, cuándo se pueden solicitar datos, cómo se tratan los mismos, los derechos ARCO, qué hacer en caso de que no se hayan respetado los datos, posibilidad de tratar datos de otras personas, qué saber del tratamiento de datos para niños, internet, información sobre solvencia, y recursos y publicaciones de la AEPD. Otras guías puestas a disposición por la AEPD son:

- Guía sobre el uso de las cookies 2013
- Guía de Videovigilancia
- Guía para clientes que contraten servicios de Cloud Computing 2013
- Guía sobre seguridad y privacidad de las tecnologías
- Guía de protección de datos en las relaciones laborales 2009
- Derechos de niños y niñas – deberes de padres y madres: guía de recomendaciones 2008

- **Guía del responsable de ficheros (2008).** Este instrumento ofrece al responsable del fichero información sobre: el deber de notificar los ficheros, requisitos para el ámbito público y privado, ficheros no automatizados, qué hacer al recoger datos, datos especialmente protegidos, atención a los derechos de los ciudadanos, comunicar datos a terceros, transferencias internacionales, medidas de seguridad y notificaciones a la AEPD.

- **Menores.** La página de la AEPD ofrece información dirigida a los niños, especialmente para mejorar la seguridad ante la utilización de dispositivos electrónicos como tabletas y teléfonos inteligentes, así como las redes sociales. Ofrece actividades lúdicas que promueven la seguridad de los niños.

- En esta misma sección se proporciona información a los maestros sobre el marco legal de la protección de datos y fichas didácticas para promover la seguridad en el uso del internet, proteger la identidad en redes sociales, concienciar sobre el uso de la imagen en la web, correo electrónico, mensajería instantánea y chat, conocer las prácticas comerciales y publicitarias utilizando el internet, concienciar a menores sobre ciberbullying, sexting y grooming.

- Existe también un Convenio Marco de Colaboración firmado el 13 de octubre de 2015 entre el Ministerio de Educación, cultura y Deporte y la Agencia Española de Protección de Datos para el impulso de la formación y sensibilización de los menores de edad en materia de privacidad y protección de datos, en particular en Internet.

- **Derecho al olvido.** La AEPD orienta a las personas de cómo aplicar el derecho al olvido que básicamente consiste en evitar que los motores de búsqueda arrojen datos personales que el propietario no desea que sean públicos.

Ejercicio de derechos / Denuncias de incumplimientos

Con el título de Presentación de Denuncias y Reclamaciones[44]

La AEPD pone a disposición de los ciudadanos su plataforma electrónica denominada "Sede Electrónica" la cual facilita el acceso a los servicios públicos de la Agencia, entre los cuales se encuentran la presentación de denuncias y reclamaciones.

Cuando un responsable (público o privado) de ficheros de datos personales no haya atendido una solicitud ciudadana en los plazos marcados por la ley, la LOPD contempla la posibilidad de que el ciudadano reclame la asistencia de la Agencia Española de Protección de Datos para que el ejercicio de sus derechos sea efectivo, mediante la presentación de una Reclamación de Tutela de Derechos.

La Reclamación contempla tres tipos de casos: de Acceso, de Rectificación y de Oposición.

A través de la Sede Electrónica se puede acceder, previo registro que exige información básica de identificación ciudadana -como es el DNI de la persona- a los formatos denominados "Certificado Electrónico" y "Soporte en Papel". Ya sea que se trate de una Denuncia (de SPAM u otros casos) o una Reclamación, la Sede Electrónica contiene los formularios en línea para la recepción y atención de las mismas.

[44] Agencia Española de Protección de Datos, "Solicitud de presentación de una reclamación de tutela de derechos", 2014, (en línea), disponible en: https://sedeagpd.gob.es/sede-electronica-web/vistas/formReclamacionDerechos/reclamacionDerechos.jsf (Consultada el 15 de octubre de 2015)

G. Francia

Francia cuenta con la Comisión Nacional de Informática y Libertades, cuya página oficial es la fuente de la información sistematizada.[45]

a. Marco Legal

La protección de datos en Francia tiene su origen en la Ley No. 78-17 de 1978 en materia de tecnología de la información, archivos de datos y libertad civil. Los datos personales corresponden a cualquier información relativa a la persona física o que pueda determinarla directa o indirectamente, por referencia a un número de identificación o uno o más factores específicos como el nombre, número de registro, teléfono, etcétera. Los datos sensibles pueden revelar directa o indirectamente origen étnico o racial, opiniones políticas, filosóficas o religiosas, afiliación a un sindicato, y la concerniente a la salud o vida sexual.

b. Marco Institucional

La Comisión Nacional de Informática y Libertades[46] (CNIL) es un órgano administrativo independiente cuya misión es asegurar la aplicación de la legislación en materia de protección de datos. De sus 17 miembros 12 son electos o designados por las asambleas o las jurisdicciones a las cuales pertenecen; eligen a su presidente entre sus miembros, no reciben instrucción de ninguna autoridad. Los ministerios, autoridades públicas, directores de empresas públicas o privadas no pueden oponerse a su acción. El presidente del CNIL recluta libremente a sus colaboradores, el presupuesto de la institución proviene de los recursos del Estado, y sus decisiones pueden ser recusadas en la jurisdicción administrativa

c. Sujetos obligados y sujetos de derecho

Los sujetos obligados son todos los que posean un fichero o base de datos personales. La página de la CNIL ofrece ayuda para orientar a quienes están obligados a declarar, para ello pone a disposición un formulario que permite determinar si se está obligado. Así, son sujetos obligados las colectividades territoriales, establecimientos financieros o de seguros, empresas privadas, profesionistas independientes, asociaciones, administración u organismo público, particulares, establecimientos o profesionales de la salud y propietarios de viviendas sociales.

Los sujetos de derecho son todos los individuos o personas físicas. .

[45]Comisión Nacional de Informática y Libertades, disponible en: http://www.cnil.fr/ (Consultada el 20 de octubre de 2015)
[46] Comisión Nacional de Informática y Libertades, "Role and responsabilities", (en línea), disponible en: http://www.cnil.fr/english/the-cnil/role-and-responsibilities/ (Consultada el 20 de octubre de 2015)

d. Estrategia

Difusión en página web

Propiamente, la CNIL no cuenta con una estrategia cívica única y definida en esos términos, sino que a través de su sitio web ofrece una variedad de material y recursos de difusión al servicio de los usuarios. Entre las principales funciones de la CNIL se encuentran "el informar, el orientar y el educar"[47], y para ello cuentan con información al alcance de los usuarios de internet, la cual incluye por lo menos 18 guías[48] referentes a diversos temas en los que se involucran datos personales.

1. La CNIL en breve
2. Guía de estudio de impacto sobre la privacidad: cómo llevarlo a cabo
3. Guía de estudio de impacto sobre la vida privada: modelos y bases de conocimiento
4. Guía de estudio de impacto sobre la vida privada: medidas para tratar los riesgos sobre las libertades y la vida privada
5. Guía telefónica
6. Medidas para progresar hacia la igualdad de oportunidades
7. Guía de comunicación política
8. Guía la publicidad si la veo
9. Guía para los abogados
10. Guía para los profesionales de la salud
11. Guía de enseñanza
12. Guía de seguridad de datos personales
13. Guía del derecho de acceso
14. Guía para los empleados y sus salarios
15. Guía de los gobiernos locales
16. Guía de investigación y enseñanza superior
17. Banca de crédito: ¿estás fichado?
18. La guía de la CNIL

[47] Comisión Nacional de Informática y Libertades, "Role and responsabilities", disponible en: http://www.cnil.fr/english/the-cnil/role-and-responsibilities/ (Consultada el 20 de octubre de 2015)

[45] Comisión Nacional de Informática y Libertades, "Guidelines", disponible en: http://www.cnil.fr/documentation/guides/ responsibilities/ (Consultada el 20 de octubre de 2015)

Concurso Operación Privacidad

Es un concurso dirigido a jóvenes particularmente expuestos a situaciones inadecuadas como subir fotos al internet, se asume que el desconocimiento de la ley puede hacer incurrir en un acto ilícito por lo que es necesario apoyar a este grupo de edad para que aprenda las mejoras prácticas en internet.

Este concurso se realizó por segunda ocasión en octubre de 2015 en conjunto con la CNIL y el Colectivo de la Educación para el lanzamiento digital en la segunda edición de Premio Educum. Los participantes pueden ser jóvenes de 18 a 25 años para que envíen videos, aplicaciones, juegos, kits, materiales de impresión para la elaboración de su proyecto. Se realizan talleres para la presentación del concurso y se apoya a los jóvenes en la realización de sus proyectos. El concurso es apoyado por el Ministerio de Educación Nacional y el Departamento de Juventud y Deporte.

Temas relativos a la protección de datos. La protección de datos abarca áreas temáticas que se difunden mediante las siguientes guías[49]:

- Seguros. La regulación del uso de los datos luego de la contratación.
- Banca de crédito. Protección de datos aplicada a los asuntos financieros: ficheros de bancos, obligaciones de los profesionales, medios de pago y aspectos fiscales.
- Gobiernos locales. Informatización de servicios ofrecidos a los ciudadanos, videovigilancia y geolocalización.
- Consumo, pub y spam. Los clientes son blancos pero no víctimas ¿cómo luchar contra el abuso?
- Viajes y transporte. Vigilancia en las rutas, controles de refuerzo en los aeropuertos, geolocalización, cómo tomar en cuenta los límites de la seguridad sin traspasar el anonimato.
- Educación. Pedagogía de la protección de datos, obligaciones de las escuelas y numeralia.
- Internet y telefonía. Redes sociales, teléfonos celulares, motores de búsqueda, cómo sistematizar los datos personales.
- Vivienda. Regulación de la utilización de datos personales por el sector de vivienda y la energía.
- Policía, seguridad y Justicia.
- Salud. Datos de salud, datos sensibles sometidos a la prueba de "salud numérica" carta de vida, expediente médico, expediente farmacéutico, médico en la web.
- Trabajo. Reclutamiento, control de horario, utilización del internet y la mensajería, geolocalización, videovigilancia, salarios y empleadores y la gestión de los datos personales en el trabajo.
- Vida cívica. Comunicación política, lista electoral, voto electrónico y vida asociativa.

[49] Comisión Nacional de Informática y Libertades, "Guidelines", disponible en: http://www.cnil.fr/documentation/guides/ responsibilities/ (Consultada el 20 de octubre de 2015)

- Videovigilancia en el espacio público, el trabajo y en los lugares privados.

Ejercicio de derechos / Denuncias de incumplimientos

El sitio web de la CNIL cuenta con una sección denominada “Quejas en Línea” (Plainte en ligne), la cual permite a los usuarios la presentación de quejas concernientes a los siguientes temas:

- Internet
- Comercio
- Empleo
- Telefonía
- Banca y crédito
- Otros Casos

Al seleccionar el tema concerniente a la preocupación del usuario, se despliegan varios subtemas para cada categoría, los cuales proveen un menú de opción múltiple con mayor grado de especificidad.
El usuario elige los pormenores de la naturaleza de su queja y al final el sitio web produce un documento membretado por la CNIL en formato PDF cuya instrucción es imprimirlo y enviarlo por correo a la persona física o moral responsable de la posesión de los datos personales. La CNIL lleva a cabo un seguimiento de las quejas registradas a través de esta modalidad.

H. Reino Unido

El Reino Unido cuenta con uno de los esquemas legal e institucional de protección de datos y/o de la privacidad más avanzado. Tiene un organismo dedicado a la vigilancia de este derecho a la vez que ha ido articulando y fortaleciendo su esquema legal de protección para lograrlo[50].

a. Marco Legal

El Acta de Protección de Datos de 1998 (Data Protection Act 1998) regula protección de Datos. El Acta define Ocho Principios de Protección de Datos que obliga personas físicas y morales. Otra normatividad relacionada incluye el Acta de Libertad de Información (Freedom of Information Act) y a las Regulaciones en materia de Privacidad y Comunicaciones Electrónicas (Privacy and Electronic Communications Regulations). De manera esquemática, la legislación de la protección de datos se establece en la siguiente serie de normativas[51]:

1. Data Protection Act de 1998, transposición de la Directiva 95/46/CE del Parlamento Europeo y del Consejo. Se trata de la ley de mayor relevancia en la materia y que establece los fundamentos jurídicos para manejar información en el Reino Unido, ya que proporciona los instrumentos para que los ciudadanos se sientan más arropados en cuanto a datos personales se refiere.
2. Consumer Protection (Distance Selling) Regulations de 2000 es la transposición de la Directiva europea 1997/7/EC[52] y en ella se especifican, entre otros, los siguientes parámetros: la información necesaria para formalizar un contrato, los servicios que se han de prestar, el derecho a cancelar una petición o el pago por tarjeta de crédito.
3. Freedom of Information Act de 2000, que otorga a los ciudadanos y a las organizaciones el derecho a solicitar información sobre los datos que poseen instituciones públicas de Inglaterra, Gales e Irlanda del Norte y de instituciones privadas de Escocia.
4. Electronic Signature Regulations de 2002, transposición de la Directiva 1999/93/EC del Parlamento Europeo y en la que el art. 5 se centra exclusivamente en la protección de datos, si bien no constituye el tema central de dicha regulación.

---

[50] La información se tomó de la página oficial de The Information Commisioner Office, consultada en línea en: https://ico.org.uk/ (Consultada el 15 de octubre del 2015)

[51] María Cristina Toledo Báez, "Aproximación a la protección de datos personales en España, Inglaterra y Francia como ejercicio de derecho comparado previo a una traducción", 2010, (en línea), disponible en: http://www.eumed.net/rev/cccss/07/mctb.htm (Consultada el 20 de octubre de 2015).

[52] Consultada en línea en: http://www.eu-consumer-law.org/consumerstudy_part2e_en.pdf

5. Privacy and Electronic Communications (EC Directive) Regulations de 2003, que constituye la transposición de la Directiva 2002/58/CE.

6. Environmental Information Regulation de 2004, transposición de la Directiva 2003/4/EC, y similar en esencia a la Freedom of Information Act, sólo que atañe únicamente a datos relativos a información medioambiental.

b. Marco Institucional

La Oficina del Comisionado de Información (Information Commisioner's Office) que ejerce sus funciones en Inglaterra y Gales, es un organismo independiente que funge como la autoridad encargada de defender los derechos de información privada contemplados en el Acta de Protección de Datos de 1998 así como también el Tribunal de Información (Information Tribunal)[53]:

- Con la aprobación de la nueva Ley de protección de datos de 1998, así como con la aprobación de la Ley de Libertad de Información de 2000 (Freedom of Information Act, FOIA) (110), el Registrador y el Tribunal de Datos pasaron a ser, respectivamente, el Comisionado y el Tribunal de Información.
- El Comisionado es un oficial independiente nombrado por la Reina y encargado de controlar, por un lado, la aplicación de la legislación sobre protección de datos personales y, por otro lado, la relativa a la libertad de información prevista en la FOIA, en la que se regula el acceso a los datos personales que obran en manos de los poderes públicos.
- Su obligación principal es promover las buenas prácticas entre los responsables de los tratamientos de datos personales y controlar el cumplimiento de la legislación sobre protección de datos. Es nombrado por un periodo de cinco años, pudiendo ser reelegido por tres veces consecutivas, aunque en la práctica suele estar dos periodos consecutivos.
- El Comisionado es un órgano independiente que responde ante el Parlamento y no ante el Ministro, y ejerce las funciones que le son asignadas por Ley.
- El Comisionado cuenta, desde 2003, con tres Oficinas Regionales (Irlanda del Norte, Escocia y Gales), que se encargan del tratamiento de datos en sus respectivas regiones.
- En enero de 2008 se aprobó un Documento de organización y funcionamiento de este Comisionado, en el que se regula además su relación con el Gobierno. Junto al Comisionado, existe un Tribunal «especial», el Tribunal de Información.
- Las reglas por las que se rige el funcionamiento de este Tribunal, que estaban previstas en la Ley de protección de datos inglesa, se han modificado para introducir los cambios técnicos necesarios para que

[53] Mónica Arenas Ramiro, Profesora Ayudante Doctor Universidad de Alcalá de Henares, "La protección de datos personales en los países de la Unión Europea" file:///Users/normacastaneda/Downloads/02-arenas%20(3).pdf (Consultada el 22 de octubre de 2015)

este Tribunal pueda ocuparse también de los recursos presentados contra la FOIA, que entró en vigor en enero de 2005.

- Es el Gobierno el que dota al Tribunal de los medios materiales y personales necesarios para el desempeño de sus funciones, por lo que en principio no cuenta con personal ni con domicilio fijo, aunque en la práctica tiene a su cargo personal de apoyo y suele situarse en Londres.

c. Sujetos obligados y sujetos de derecho

En lo que respecta a los titulares y obligados por el derecho a la protección de datos personales, en todos los ordenamientos jurídicos europeos se considera que son titulares todas las personas físicas, incluyéndose a los menores (a los que se les otorga un tratamiento especial) y excluyéndose en la mayoría de los casos a las personas fallecidas. En cambio, es en relación con la titularidad de las personas jurídicas donde existen diferencias entre unos ordenamientos jurídicos y otros. También es doctrina compartida por dichos ordenamientos que los obligados por el derecho a la protección de datos personales ya no son sólo los poderes públicos sino también los particulares y, en especial, las empresas que se encargan de gestionar bancos de datos personales.

d. Estrategia

Difusión en página web

Entre las funciones principales de la ICO se incluyen el "educar e influenciar, promover prácticas recomendables y facilitar información y asesoramiento", para el adecuado cumplimiento de lo anterior, su principal herramienta es su sitio web y los recursos informativos y de contacto que ponen a disposición de los usuarios.
El apartado principal destinado al público contiene los siguientes sub-apartados:

- Solicitud de información personal bajo el Acta de Protección de Datos
- Acceso a la información en posesión de un organismo público
- Presentar queja o preocupación acerca de alguna organización
- Reclamo de compensaciones
- Revisar que la información personal se encuentro bajo un uso adecuado

Asimismo, la ICO publica en su sitio web diversas guías para personas físicas y morales; cuentan con links de acceso a mecanismos de denuncia, e informan acerca de eventos y seminarios presenciales o en línea.[54]

[54] Information Commissioner's Office, "Events and webinars", 2015, (en línea), disponible en: https://ico.org.uk/about-the-ico/news-and-events/events-and-webinars/ (Consultada el 22 de octubre)

Ejercicio de derechos / Denuncias de incumplimientos[55]

A través de su sitio web, la Oficina del Comisionado para la Información, pone a disposición de los usuarios un apartado para reportar aquellas prácticas de manejo de información por parte de organizaciones, que pudiesen incurrir en vulneración de derechos de los ciudadanos.

Las categorías dispuestas en la página son las siguientes:

- Llamadas y mensajes molestos: Por teléfono, mensaje o correo electrónico.
- Acceso o reutilización de información: Ya sea información privada o información solicitada a organismos públicos.
- Cómo ha sido manejada mi información personal: Cuando exista preocupación sobre el manejo de información personal por parte de una organización.
- Resultados de búsquedas por internet: Cuando un proveedor de motor de búsqueda por internet no ha procedido a remover ligas de información de las personas, a pesar de haberles sido solicitado tal cosa.
- Cookies: Si existe preocupación por parte del usuario, acerca del uso que alguien más pueda darle a sus cookies.
- Quejas y cumplidos acerca de la ICO: En caso de que el usuario se encuentre insatisfecho con el trabajo de la Oficina del Comisionado para la Información.

Cada una de las categorías anteriores, al ser seleccionadas, despliegan subtemas que abarcan las posibles preocupaciones de los usuarios, y que eventualmente dan acceso a un portal denominado "Snap Surveys"[56], por medio del cual se llenan los pormenores de la queja del usuario y se le da seguimiento.

[55] Bajo el título de Reporte de preocupaciones (Concerns)
Information Commissioner's Office, "Report a concern", 2015, (en línea), disponible en: https://ico.org.uk/concerns/ (Consultada el 22 de octubre)

[56] Information Commissioner's Office, "Report your concerns about nuisance calls and messages", 2015, (en línea), disponible en: https://www.snapsurveys.com/swh/surveylogin.asp?k=138312369469 (Consultada el 22 de octubre)

I. Nueva Zelanda

Nueva Zelanda cuenta con la Privacy Commisioner Te Mana Matapono Matatapu[57].

a. Marco Legal

De acuerdo con el Dictamen 11/2011 relativo al nivel de protección de datos personales de Nueva Zelanda[58], la principal norma de protección de datos en este país es la Ley sobre la intimidad (Privacy Act) de 1993, muy influida por las Directrices de la OCDE sobre la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales de 1980. También se cuenta con un sistema de monitoreo del cumplimiento de Doce Principios de Privacidad y de Cuatro Principios del Registro Público de Privacidad, todos ellos incluidos en el Acta de Privacidad.

Existen tres códigos de buenas prácticas en materia de intimidad que se han elaborado con arreglo al artículo 46 de la Ley y se aplican específicamente y con requisitos más exigentes a los datos médicos, la información sobre telecomunicaciones y los datos de notificación del acreedor.

También existen leyes en materia de libertad de información, spam, sanciones penales por determinadas violaciones de la intimidad, cancelación de antecedentes penales, vigilancia, conservación de datos médicos, registros públicos y discriminación. Asimismo existen disposiciones relacionadas con el derecho a la intimidad como las normas sobre el secreto recogidas en la Ley electoral de 1993 que protegen la intimidad del votante.

Nueva Zelanda cuenta con dos leyes sobre libertad de información que contienen disposiciones sobre el derecho a la intimidad:

- La Ley de información oficial (Official Information Act) regula los organismos de la administración central y el sector público.
- La Ley de reuniones e información oficial de la administración local (Local Government Official Information and Meetings Act) de 1987 regula la administración local.

Ambas, contienen disposiciones para proteger la intimidad en los casos en que se pretende difundir información oficial y sobre la obligación de motivar las decisiones administrativas que afectan a las personas físicas.

---

[57] La información aquí proporcionada proviene fundamentalmente de su página oficial:
Privacy Commissioner Te Mana Matapono Matatapu, disponible en: https://privacy.org.nz (Consultada el 22 de octubre)

[58] Grupo de trabajo del artículo 29 sobre protección de datos, "Dictamen 11/2011 relativo al nivel de protección de datos personales en Nueva Zelanda", 2011, (en línea), disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp182_es.pdf (Consultada el 22 de octubre)

La Ley no distingue entre datos sensibles y no sensibles, considera que todos los datos son sensibles en potencia y, por tanto, están sujetos a las mismas normas de protección. Las categorías de datos establecidas en el artículo 8 de la Directiva se rigen por la Ley de Derechos Humanos de 1993. Como la normativa neozelandesa de protección de datos es anterior a la Directiva UE, está basada en el enfoque de las directrices de la OCDE.

b. Marco Institucional

La Oficina del Comisionado para la Privacidad de Nueva Zelanda (Office of the New Zealand Privacy Commissioner) se instituyó para administrar el Acta de Privacidad de 1993. El Comisionado tiene la encomienda de proteger la información personal de los neozelandeses en poder tanto de organismos públicos como privados.

Entre otras funciones, la oficina del Comisionado administra un sistema de quejas y emite Códigos de Práctica o Reglas para diversos sectores, así como campañas de educación en materia de datos personales.[59]

El Comisariado ha emitido diversas directrices, folletos e informaciones que especifican los derechos y las obligaciones de las organizaciones y las personas, así como notas sobre casos anónimos de quejas concretas. En ellos imparte orientaciones sobre la aplicación práctica de los principios de intimidad. Por otra parte, la jurisprudencia sobre derechos humanos contiene directrices e interpreta los diversos aspectos de la Ley sobre la intimidad[60].

c. Sujetos obligados y sujetos de derecho

La Ley regula toda la información personal en cualquier forma o soporte. Se aplica a la totalidad de los sectores público y privado, con pocas excepciones por motivos de interés público específico.

La Ley define los datos personales como «información sobre una persona identificable» entendiendo por persona el individuo físico vivo, e incluye información sobre la inscripción del fallecimiento en el registro civil.

[59] Privacy Commissioner Te Mana Matapono Matatapu, "Introduction", 2013, (en línea), disponible en: https://www.privacy.org.nz/about-us/introduction/ (Consultada el 22 de octubre)

[60] Grupo de trabajo del artículo 29 sobre protección de datos, "Dictamen 11/2011 relativo al nivel de protección de datos personales en Nueva Zelanda", 2011, (en línea), disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp182_es.pdf (Consultada el 22 de octubre)

d. Estrategia

Difusión en página web

Entre los instrumentos que utilizan para la promoción del derecho a la privacidad y protección de datos personales se incluye:

- Una plataforma virtual denominada "Elearning Privacy Training Modules" (Módulos de Entrenamiento sobre Privacidad en Línea)

Actividades presenciales

1. La organización de una "Semana de la Privacidad", la cual tiene lugar una vez al año y en la cual se promueve la importancia de la privacidad a través de una serie de eventos y materiales.
2. La organización de Foros y Conferencias sobre Tecnología y Privacidad (Technology & Privacy Forums)
3. El Comisariado para la intimidad dispone de amplia información en su sitio Web y publica un boletín trimestral y notas sobre casos anónimos de investigaciones concretas.
4. El Comisionado organiza sesiones de formación regularmente y talleres en todo el país destinados a los responsables de protección de la intimidad y otros interesados, y participa en la Semana Asia-Pacífico de protección de la intimidad que se celebra anualmente.
5. El Comisariado realiza estudios cada cierto tiempo para determinar el conocimiento y la eficiencia de la acción del Comisario.

Asimismo, la Ley sobre la intimidad exige que cada organismo público o privado tenga al menos una persona responsable de protección de la intimidad. Estas personas son responsables de fomentar el cumplimiento por su organismo de los principios de protección de la información; de tramitar las solicitudes de acceso; de trabajar con el Comisionado para la intimidad en caso de investigación; y de garantizar de cualquier otra manera el respeto por su organismo de la Ley sobre la intimidad. Existen varias redes de responsables de protección de la intimidad que cubren todo el país y se reúnen periódicamente.

Se promociona también la "Semana de la Privacidad[61]" que se lleva a cabo cada año en diferentes fechas. Durante la semana de la privacidad se elige una mascota y se generan diferentes actividades con diversos actores. Seminarios, foros, actividades para organismos obligados y para titulares de los derechos. ej. Se

[61] Privacy Commissioner Te Mana Matapono Matatapu, "Privacy Week", 2013, (en línea), disponible en: https://privacy.org.nz/forums-and-seminars/privacy-week/ (Consultada el 22 de octubre)

propone colocar como pantallas en las computadoras de oficinas, protectores de pantalla con mensajes sobre la importancia de la privacidad de los datos personales, publicar artículos en boletines internos sobre la privacidad de los datos personales, etc.

Ejercicio de derechos / Denuncias de incumplimientos

Bajo el título de ¿Cómo presentar una queja? Las dos formas que existen para presentar una queja ante la Oficina del Comisionado para la Privacidad de Nueva Zelanda son:

- En línea, directamente en el sitio web y en una interfaz que aparece para el llenado de datos como identificación de la persona que emite la queja y la organización de la cual se queja, así como una descripción de lo ocurrido.
- Bajando la "Forma de Quejas" que se encuentra en línea, imprimirla, llenarla a mano y enviarla a través de correo postal a la Oficina.

Se menciona en el sitio web que la forma más expedita de resolver una queja es bajo la modalidad en línea, y que para ambos casos habrán de responderse las siguientes seis preguntas:

- ¿Se ha puesto en contacto directamente con la organización en relación a su queja?
- Datos de identificación de la persona que emite la queja.
- Datos de la organización y/o personas de las cuales desea quejarse.
- Motivos de la queja: Qué, Cuándo, Qué información personal, Quién, y Cuánto tiempo después se percató de lo ocurrido.
- ¿Cómo ha sido afectado por tal malversación de su información personal?
- ¿De qué manera se beneficiaría usted con la resolución de esta queja?

La Oficina del Comisionado para la Privacidad se compromete, sin definir tiempos de respuesta, a darle seguimiento a las quejas recibidas por ambos medios.

J. Organizaciones aliadas en la protección de datos personales en las experiencias internacionales

Instituciones Promotoras del Derecho a la Protección de Datos Personales y Organismos Aliados			
País	**Institución**	**Órgano(s)**	**Actividades**
Argentina	Dirección Nacional de Protección de Datos Personales[62]	UNICEF Iniciativa "Educar" del Ministerio de Educación, el "Programa Conectar Igualdad" de ANSES, con la Fundación Sadosky, del Ministerio de Ciencia, Tecnología e Innovación Productiva, y con NIC Argentina, servicio público del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto, Programa Núcleos de Acceso al Conocimiento/ Puntos de Acceso Digital, de la Secretaría de Comunicaciones del Ministerio de Planificación Federal, Inversión Pública y Servicios, así como con el Ministerio de Economía a través del Programa Impulso Argentino.	Programa "Con Vos en la Web" de colaboración para proteger los derechos a la privacidad y la seguridad de niños, niñas y adolescentes usuarios de internet. Promover la cooperación entre el sector público y privado para la elaboración de prácticas y procedimientos respetuosos de la privacidad de las personas.
Australia	Oficina del Comisionado de Información de Australia[63]	Proveedores de Servicios de Salud que incluyen a practicantes y especialistas médicos, hospitales privados, farmacias, psicólogos, fisioterapeutas, dentistas, asilos de ancianos, radiólogos, gimnasios, clínicas de	Colaboran estrechamente en la elaboración y en el cumplimiento de la "Guía de Privacidad Médica" (Health Privacy Guidance) Son al mismo tiempo "sujetos obligados" que colaboran en el contenido de la guía.

[62]Presidencia de la Nación, disponible en: http://www.jus.gob.ar/datos-personales.aspx (Consultada el 30 de octubre de 2015)
[63] Australian Government, Office of the Australian Information Commissioner, disponible en: http://www.oaic.gov.au/ (Consultada 30 de septiembre de 2015)

Instituciones Promotoras del Derecho a la Protección de Datos Personales y Organismos Aliados			
País	**Institución**	**Órgano(s)**	**Actividades**
		control de peso, bancos de sangre, entre otros.	
Canadá	Oficina del Comisionado de Privacidad de Canadá,[64]y Oficinas Regionales de Alberta y British Columbia	Cuentan con un documento titulado: "Memorándum de entendimiento en relación a la cooperación y colaboración con las Políticas de Privacidad del Sector Privado, Aplicación y Educación Pública[65]", compuesta por las Oficinas de Privacidad Central y Regionales	Colaborar y coordinarse para arribar a puntos en común en términos de aplicación de su normatividad, políticas de privacidad, definición y desarrollo de iniciativas de educación pública, así como el intercambio de información en los términos de sus competencias.
España	Agencia Española de Protección de Datos[66] / Plan Estratégico 2015-2019	Administraciones Educativas (INTEF), Fiscalía y Fuerzas y Cuerpos de Seguridad del Estado, Unidades Tecnológicas de la Policía y la Guardia Civil, y el Ministerio de Educación y Comunidades Autónomas. Ministerio de Sanidad Instituto Nacional de Administración Pública (INAP), Autoridades Autonómicas de Protección de Datos, el Defensor del Pueblo, Consejo de	Para la protección de menores de edad. Para la protección de datos relacionados con los tratamientos llevados a cabo en el sector sanitario. Para mejorar las medidas de prevención en relación con los tratamientos de datos que llevan a cabo las Administraciones Públicas.

[64] Office of the Privacy Commissioner of Canada, disponible en :https://www.priv.gc.ca/index_e.asp (Consultada 30 de septiembre de 2015)
[65] Office of the Privacy Commissioner of Canada, "Memorandum of Understanding", disponible en: https://www.priv.gc.ca/au-ans/prov/mou_e.asp (Consultada 30 de septiembre de 2015)
[66] Agencia Española de Protección de Datos, disponible en: http://www.agpd.es/portalwebAGPD/index-ides-idphp.php (Consultada el 15 de octubre de 2015)

Instituciones Promotoras del Derecho a la Protección de Datos Personales y Organismos Aliados			
País	**Institución**	**Órgano(s)**	**Actividades**
		Transparencia y Buen Gobierno, Consejo General del Poder Judicial, Consejo General del Poder Judicial, Fiscalía General del Estado, Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), y la Oficina para la Ejecución de la Reforma de la Administración (OPERA) y el Ministerio de Fomento Comisión de Estrategia TIC	Completar la digitalización de la Agencia.
Francia	Comisión Nacional de Informática y Libertades[67]	Consejo Nacional de Abogados	Desarrollar acciones formativas en la Ley de Protección de Datos y la promoción de la función de las libertades correspondientes. La organización posible de controles conjuntos, solicitudes de inversión para articular textos

[67] Comisión Nacional de Informática y Libertades, disponible en: http://www.cnil.fr/ (Consultada el 20 de octubre de 2015)

Instituciones Promotoras del Derecho a la Protección de Datos Personales y Organismos Aliados			
País	**Institución**	**Órgano(s)**	**Actividades**
		Servicio Interministerial de Archivos de Francia (SIAF) Asambleas de Cámaras Francesas de Comercio e Industria	normativos producidos por alguna de las dos instituciones. Programas de capacitación, sensibilización, información y formación. Elaboración de guías prácticas para la capacitación de agentes de las cámaras.
Reino Unido	Oficina del Comisionado de Información[68]	Departamento de Educación, Sistema de Salud y Bienestar Social, Departamento de Salud, Colegio Policial, Sociedades Crediticias, entre otros. Ofcom, PhonepayPlus, La Autoridad de Competición y Mercados y la Autoridad de Conducta Financiera	Elaboración de Guías para el cumplimiento de las disposiciones legales en materia de privacidad, para los sectores de Educación, Salud, Policía, justicia y fronteras y Finanzas, respectivamente. Elaboración de guiás con consejos para el uso seguro y confidencial de teléfonos inteligentes y otros aparatos de telecomunicaciones.
Nueva Zelanda	Oficina del Comisionado de Privacidad de Nueva Zelanda[69]	La Oficina aprueba los denominados AISAs (Approved Information Sharing Agreements) Acuerdos aprobados para el intercambio de información, mismos que fungen como una	Actualmente existen tres AISAs aprobados: • Entre la Agencia Tributaria (Inland Revenue) y el Departamento de Asuntos Interiores.

[68] Information Commissioner's Office, disponible en: https://ico.org.uk/ (Consultada el 22 de octubre)
[69] Privacy Commissioner Te Mana Matapono Matatapu, disponible en: https://privacy.org.nz (Consultada el 22 de octubre)

Instituciones Promotoras del Derecho a la Protección de Datos Personales y Organismos Aliados			
País	**Institución**	**Órgano(s)**	**Actividades**
		herramienta para que diversas instituciones de gobierno puedan proveer de servicios públicos efectivos y eficientes, a través del intercambio de información, sin por ello vulnerar los derechos de los particulares.	• Entre la Agencia Tributaria y la Policía de Nueva Zelanda. • Entre los Ministerios de Desarrollo Social, Justicia, Salud, y Educación, y la Policía de Nueva Zelanda, con la finalidad de mejorar los servicios públicos enfocados en “niñez vulnerable”.

VI. OTRAS EXPERIENCIAS POSITIVAS

K. Kosovo

En Kosovo, la Agencia Nacional de Protección de Datos Personales, en cooperación con el Ministerio de Educación, Ciencia y Tecnología realizó en el 2014 el proyecto denominado 'My Privacy'[70] (Mi privacidad).
Este proyecto tuvo el objetivo de concienciar al público, centrándose en los jóvenes (estudiantes de secundaria) sobre la privacidad mediante una campaña de protección de datos personales. La campaña se centró en la realización de actividades coordinadas con el Ministerio de Educación, respectivamente, con los departamentos de las diez escuelas secundarias seleccionadas en ciertos municipios: Gjilan, Ferizaj, Partesh, Shtime, Suharekë, Prizren, Drenas, Peje, Prishtinë y Mitrovice.

La primera etapa del proyecto consistió en la distribución de un folleto cuyo contenido fue ayudar a los estudiantes para informarse con más precisión acerca de su privacidad en tres dimensiones: la familia, la escuela y el Internet.

La segunda fase del proyecto tuvo que ver con los discursos de los supervisores nacionales organizados por grupos de enfoque seleccionados con el objetivo de aumentar su conocimiento sobre sus derechos a la privacidad, la forma en que pueden proteger su privacidad y así sucesivamente.

La etapa final del proyecto se caracterizó por una competencia de pruebas similares, en la que durante una semana la mitad de los estudiantes seleccionados de diez escuelas trabajaron en algún área artística, mientras que la segunda mitad de ellos en escritura académica (ensayo) sobre el tema: “Mi vida privada”.

Las dos escuelas restantes quedaron al final de la primera vuelta de esta semana, mientras que dos ganadores de cada escuela fueron dados a conocer después de la segunda semana y fueron recompensados con dotaciones y regalos simbólicos por parte de la Agencia Nacional de Protección de Datos Personales.

Los premios a los estudiantes mejor evaluados en el nivel nacional se otorgaron el 28 de enero de 2014, Día Europeo de Protección de Datos Personales.

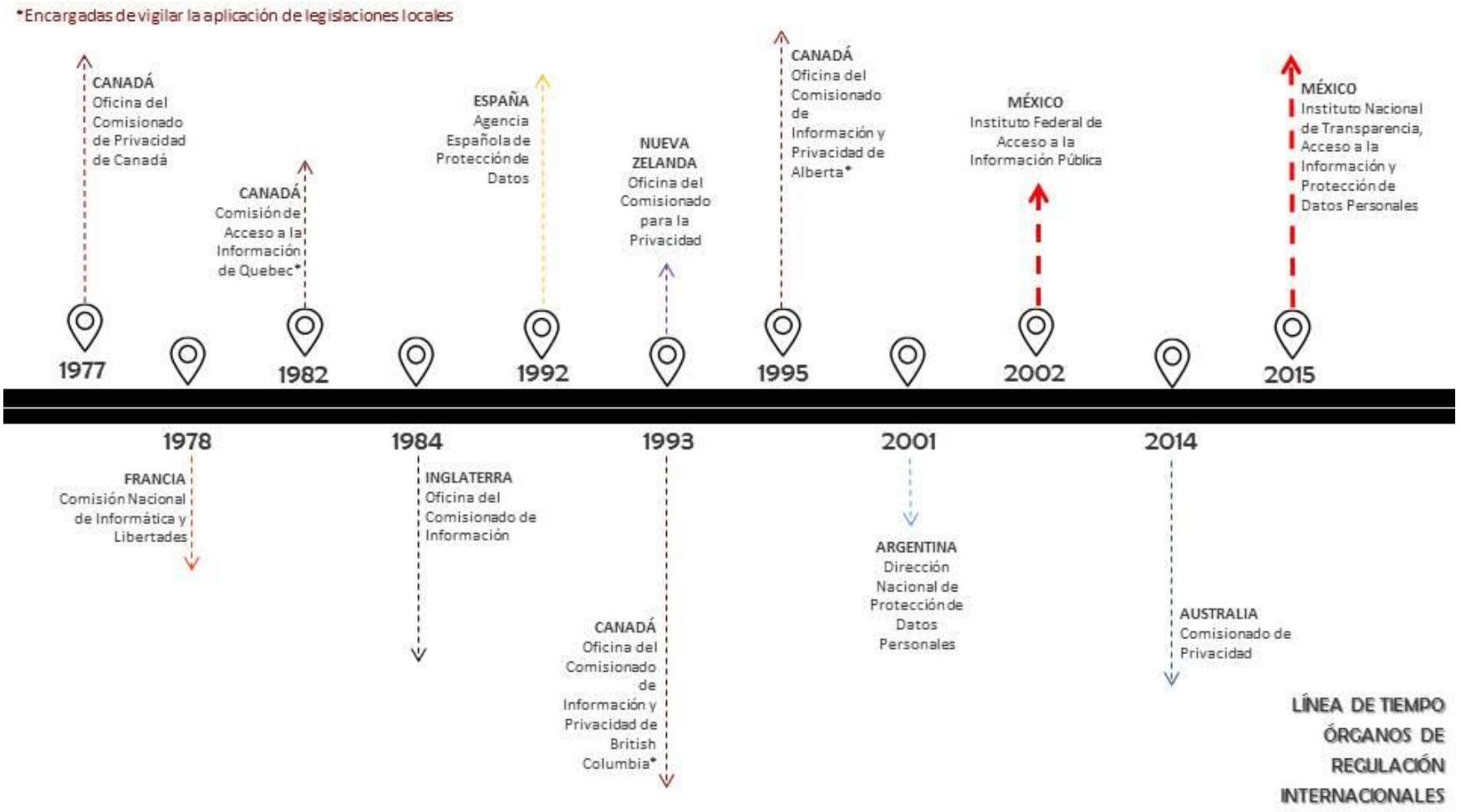
[70] National Agency for Personal Data Protection, ““My Privacy” - Awareness Campaign with Schools Commenced”, 2013, (en línea), disponible en: http://www.amdp-rks.org/web/?page=2,10,128#.VilFyvkrLIU (Consultada el 22 de octubre de 2015)

L. Singapur

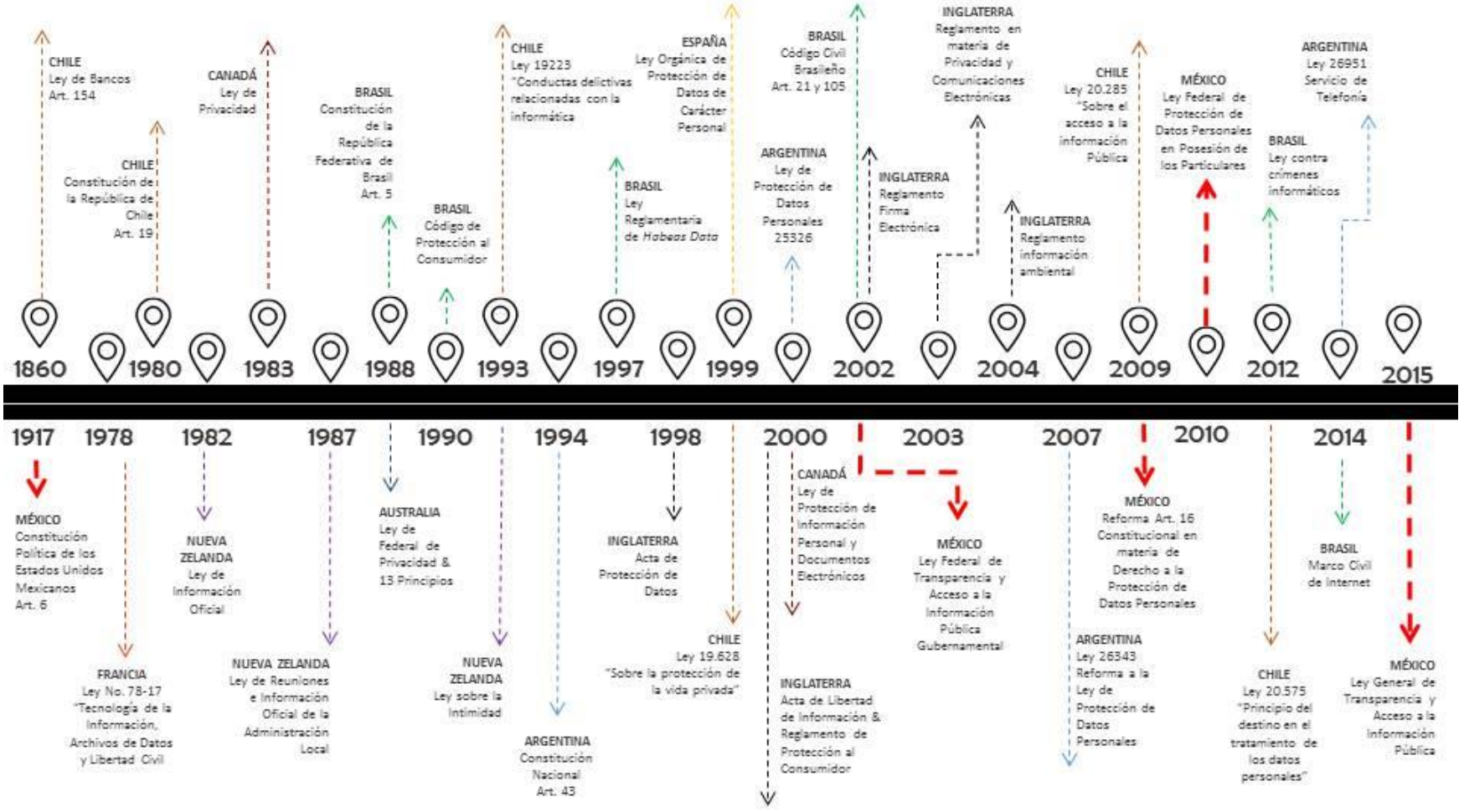
La Comisión de Protección de Datos de Singapur (Personal Data Protection Comission)[71] cuenta también con la difusión de materiales de aprendizaje sobre la protección de datos personales: un programa de aprendizaje interactivo en línea, guías, manuales, posters y videos tanto para sujetos obligados como para titulares de derecho.

[71] Personal Data Protection, disponible en: https://www.pdpc.gov.sg/home (Consultada el 22 de octubre de 2015)

Línea de Tiempo Órganos de Regulaciones Internacionales.



Línea de Tiempo de Instrumentos Jurídicos



VII. EXPERIENCIAS NACIONALES

A nivel nacional existen instancias que promueven los derechos como una piedra angular para el logro de objetivos institucionales. A continuación se analizan los casos del INAI, la CNDH, CONDUSEF, INE y PROFECO.

El siguiente es un cuadro resumen de las experiencias de las instancias revisadas a fin de proporcionar una visión integral que es detallada en las siguientes secciones:

Matriz guía para el análisis de experiencias nacionales en materia de estrategias de educación en defensa de derechos					
Entidad	**Marco Legal**	**Marco institucional**	**Estrategia**	**Población potencial y objetivo**	**Actores clave (Enfoque de la entrevista)**
Nacional	Ley General de Transparencia y Acceso a la Información Pública Ley Federal de Transparencia y Acceso a la Información Pública	INAI	Instrumentos de difusión	Todos los mexicanos y extranjeros que se encuentren en territorio nacional	CONDUSEF INE SEP SHCP
Nacional	Ley de la Comisión Nacional de los Derechos Humanos	CNDH	Medios y campañas de difusión y educación	Todos los mexicanos y extranjeros que se encuentren en territorio nacional	INAPAM, Secretaría de Salud, Secretaría de Educación Pública, INMUJERES; Secretaría de Gobernación, Poder Judicial, CONAPRED, Poder Legislativo, DIF, Organizaciones de la Sociedad Civil, entre otros.
Nacional	Ley de Protección y Defensa al Usuario de Servicios Financieros	CONDUSEF	Elaborar, difundir y promover información de utilidad para los usuarios de servicios	Usuarios, a cualquier persona que utilice o por cualquier causa tenga algún derecho frente a la Institución Financiera como	CONSEFIN (Consejería en Seguros y Fianzas), Bancos, y con las Cámaras empresariales para la difusión.

	Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros		financieros.	resultado de la operación o servicio prestado.	
Nacional	Ley General de Instituciones y Procedimientos Electorales	INE	Estrategia Nacional de Educación Cívica para el Desarrollo de la Cultura Política Democrática 2011-2015.	Los ciudadanos que en territorio nacional o extranjero, ejerzan sus derechos político-electorales	SEP, DIF, IMJUVE, Cámara de Diputados, los Congresos Locales, el PNUD, OSC, gobiernos estatales.
Nacional	Ley Federal de Protección al Consumidor	PROFECO	Productos informativos que promueven los derechos de los consumidores	Consumidores	CONAPRED,INAPAM, INFONAVIT, Bancos e IFTL.
FUENTE: Elaboración propia con datos de las págs. web oficiales					

A. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)

Según su página web institucional, el derecho de acceso a la información favorece la transparencia en el gobierno y la rendición de cuentas de todos los servidores públicos, lo cual promueve una mejora de la eficiencia de las instituciones federales y la calidad de sus servicios.

A partir del 12 de junio del 2002, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental obliga a todas las dependencias y entidades del gobierno federal a dar acceso a la información contenida en sus documentos, respecto, entre otras cosas, a su forma de trabajo, al uso de los recursos públicos, sus resultados y desempeño. Esto con base en la reforma constitucional al artículo 16, de junio del 2008 y publicada el 1 de junio del 2009[72].

Cualquier persona puede solicitar información a las instituciones federales y obtenerla en forma rápida y sencilla, sin necesidad de identificarse, ni justificar el uso que dará a la misma. Además, esta Ley garantiza el derecho de las personas a la vida privada, al obligar a las instituciones a proteger los datos personales que tienen en sus archivos o bases de datos.

De esta forma, distingue la información gubernamental, que es pública, de la información sobre las personas, que es confidencial. La Ley, aprobada en junio del año 2002, es producto de la participación de grupos de la sociedad que llevaron una iniciativa propia del Ejecutivo Federal al Congreso y los legisladores, quienes la aprobaron en forma unánime. Con base en la Ley, fue creado el Instituto Federal de Acceso a la Información Pública (IFAI),un organismo autónomo encargado de garantizar a todas las personas el acceso a la información pública y la protección de sus datos personales que posee el gobierno federal.[73]

a. Marco Legal

Es a partir de mayo de 2015 que el antes Instituto Federal de Acceso a la Información y Protección de Datos, cambia de nombre a Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, sustentando este cambio en la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).

---

[72] Consultado en línea en : http://info4.juridicas.unam.mx/ijure/fed/9/17.htm?s=

[73] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Marco Normativo", (en línea), disponible en: http://inicio.inai.org.mx/SitePages/marcoNormativo.aspx (Consultada el 22 de octubre de 2015)

Fundamentalmente se promueven dos derechos desde el INAI: El acceso a la información pública y la protección de datos personales.

Actualmente conviven la LGTAIP y la LFTAIPG. La primera, promulgada el 5 de mayo de 2015, amplía las atribuciones de la Ley Federal incluyendo para la obligación de transparencia y acceso a la información a cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las Entidades Federativas y los municipios. Es decir, con la Ley se amplía el número de sujetos obligados y en ese sentido el Instituto elaborará un nuevo padrón. Un aspecto a destacar de la LGTAIP es la creación del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, que estará coordinado por el Instituto y al cual concurren también los organismos garantes de las entidades federativas, el Instituto Nacional de Estadística y Geografía, la Auditoría Superior de la Federación y el Archivo General de la Nación.

En este apartado hablaremos de las estrategias realizadas por el extinto IFAI y el actual INAI en materia de educación para el derecho de acceso a la información pública.

La LFTAIPG, según su Art. 1, tiene la finalidad de 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.

Y la LGTAIP en su Artículo 1., dice: **"**La presente Ley es de orden público y de observancia general en toda la República, es reglamentaria del artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia y acceso a la información. Tiene por objeto establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las Entidades Federativas y los municipios".

b. Marco Institucional

Con base en elementos de identidad institucional, como son la Misión, Visión y Objetivos, el INAI fundamenta su actuación de la siguiente manera: "Misión: Garantizar en el Estado mexicano los derechos de las personas a la información pública y a la protección de sus datos personales, así como promover una cultura de transparencia,

rendición de cuentas y debido tratamiento de datos personales para el fortalecimiento de una sociedad incluyente y participativa"[74].

La primera parte de la Misión resalta la importancia de garantizar el acceso a la información pública gubernamental. La segunda parte de la Misión se refiere a la protección de la información personal. Finalmente, la tercera parte de la Misión trata sobre la promoción de la cultura de transparencia y rendición de cuentas y en el fortalecimiento de una sociedad incluyente y participativa.

Visión: **"**Ser una Institución Nacional eficaz y eficiente en la consolidación de una cultura de transparencia, rendición de cuentas y debido tratamiento de datos personales, reconocida por garantizar el cumplimiento de la normativa de la materia y promover el ejercicio de los derechos de acceso a la información y protección de datos personales como base para la participación democrática y un gobierno abierto".

"Objetivos: 1. Garantizar el óptimo cumplimiento de los derechos de acceso a la información pública y la protección de datos personales 2. Promover el pleno ejercicio de los derechos de acceso a la información pública y de protección de datos personales, así como la transparencia y apertura de las instituciones públicas. 3. Coordinar el Sistema Nacional de Transparencia y de Protección de Datos Personales, para que los órganos garantes establezcan, apliquen y evalúen acciones de acceso a la información pública, protección y debido tratamiento de datos personales y 4. Impulsar el desempeño organizacional y promover un modelo institucional de servicio público orientado a resultados con un enfoque de derechos humanos y perspectiva de género."

Además, en materia específica de acceso a la información pública, el portal del INAI ofrece el acceso al INFOMEX, herramienta virtual que permite la búsqueda de la información pública en todas las instancias gubernamentales por ahora y a más tardar en un año, a partir de la promulgación de la LGTAIP, en todas las instancias que la Ley contempla como sujetos obligados.

c. Sujetos obligados y sujetos de derecho

Según la LFTAIPG en su Art. 3, Fracción XIV, son Sujetos obligados de esta Ley:

a) El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República;

[74] Diario Oficial de la Federación del 01 de abril de 2015. Consultado en línea en: http://dof.gob.mx/nota_detalle.php?codigo=5387578&fecha=01/04/2015

b) El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos;

c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal;

d) Los órganos constitucionales autónomos;

e) Los tribunales administrativos federales, y

f) Cualquier otro órgano federal.

Por otra parte, según lo establece en el **Art. 1** la LFTAIPG, su finalidad es garantizar el acceso de "toda persona" a la información pública en posesión de los sujetos mencionados anteriormente, por lo cual se entenderá como sujetos de derecho de esta Ley, a todas las personas cuyos datos personales se encuentren en posesión de los sujetos obligados, así como a cualquier persona que haga una solicitud de información en el marco de la Ley.

En la Ley General de Transparencia y Acceso a la Información Púbica, son Sujetos Obligados, según su **Artículo 23.** Son sujetos obligados a transparentar y permitir el acceso a su información y proteger los datos personales que obren en su poder: cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en los ámbitos federal, de las Entidades Federativas y municipal."

En su **Artículo 122.,** la Ley señala que**: "**Cualquier persona por sí misma o a través de su representante, podrá presentar solicitud de acceso a información ante la Unidad de Transparencia, a través de la Plataforma Nacional, en la oficina u oficinas designadas para ello, vía correo electrónico, correo postal, mensajería, telégrafo, verbalmente o cualquier medio aprobado por el Sistema Nacional".

d. Estrategia

Entre los esfuerzos que ha llevado a cabo el Instituto para la promoción de la transparencia, el acceso a la información pública gubernamental, se encuentra la utilización de diversos instrumentos de difusión que se listan a continuación[75]:

[75] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Publicaciones", (en línea), disponible en: http://inicio.ifai.org.mx/SitePages/Publicaciones.aspx (Consultada el 22 de octubre de 2015)

- **Trípticos y Guías Prácticas**
  - ✓ Transparencia, Acceso a la Información, Protección de Datos y Sociedad Civil
  - ✓ Acceso o corrección de datos personales en poder de la Administración Pública Federal
  - ✓ Elaborar una Solicitud de Información
  - ✓ Falta de Respuesta a una Solicitud de Información Pública (Positiva Ficta)
  - ✓ Elaborar un Recurso de Revisión

- **Carteles de Difusión**
  - ✓ Protege tu Privacidad
  - ✓ La Información Gubernamental es Información Pública
  - ✓ 10 Consejos útiles para el uso de internet
  - ✓ Cuadernos de Transparencia

En formato PDF, se encuentran disponibles en la página institucional en formato PDF, así como en versión de Audiolibros, los siguientes 19:

- ✓ Corrupción: de los ángeles a los índices
- ✓ ¿Qué es la rendición de cuentas?
- ✓ Estado y transparencia: un paseo por la filosofía política
- ✓ La transparencia como problema
- ✓ Lo íntimo, lo privado y lo público
- ✓ Leyes de Acceso a la Información en el Mundo
- ✓ Transparencia y Partidos Políticos
- ✓ Economía Política de la Transparencia
- ✓ Transparencia y democracia: claves para un concierto
- ✓ Medios de comunicación y la función de transparencia
- ✓ La transparencia y los derechos laborales
- ✓ Transparencia y vida universitaria
- ✓ Transparencia: ruta para la eficacia y legitimidad en la función policial
- ✓ Moral y transparencia: Fundamento e implicaciones morales de la transparencia
- ✓ Transparencia y Política de competencia

- ✓ El acceso a la información como un derecho fundamental: La reforma al artículo 6° de la Constitución mexicana
- ✓ Transparencia y seguridad nacional
- ✓ El Acceso a la información en la sociedad de consumo: de la comida chatarra a los productos milagro

- **Coediciones**

En colaboración con distintas agrupaciones y organizaciones nacionales e internacionales, el INAI pone a disposición de los usuarios de su sitio web institucional, un conjunto de libros electrónicos en formato PDF; a fecha de octubre 2015, se encuentran disponibles los siguientes 23:

- ✓ Transparencia Focalizada
- ✓ Libro de Redes Sociales
- ✓ Guía para la Acción Pública. Los sitios Web Accesibles
- ✓ Propuestas para una Efectiva Transparencia Presupuestaria
- ✓ Transparencia, acceso a la información tributaria y el secreto fiscal
- ✓ Una policía más fuerte, una policía más transparente. Insumos para aprender de la experiencia
- ✓ Guía para el ejercicio del derecho de acceso a la información
- ✓ Código Buenas Prácticas
- ✓ Razones y Significados
- ✓ Hacia una democracia de contenidos
- ✓ Estudio en Materia de Transparencia OSOS
- ✓ El Poder de la Transparencia: Nueve derrotas a la opacidad
- ✓ Transparencia, rendición de cuentas y construcción de confianza en la sociedad y el Estado mexicanos
- ✓ Políticas de Transparencia: ciudadanía y rendición de cuentas
- ✓ El derecho de acceso a la información en México: un diagnóstico de la sociedad
- ✓ Right of access to information in Mexico: a diagnosis by society
- ✓ Transparencia: libros, autores e ideas
- ✓ El Poder de la Transparencia: Seis derrotas a la opacidad
- ✓ Manual de Acceso a la Información, Transparencia y Rendición de Cuentas
- ✓ Transparencia y Acceso a la Información de las Organizaciones Civiles
- ✓ La Transparencia en la República: un recuento de buenas prácticas
- ✓ Democracia, Transparencia y Constitución: Propuestas para un debate necesario

- **Memorias y Eventos**

En esta sección se pone a disposición de los usuarios del sitio institucional, 9 documentos en formato PDF, que contienen las memorias de eventos en los que estuvo involucrado el INAI:

- ✓ Semana Nacional de la Transparencia (Del 2004 al 2009)
- ✓ IV Encuentro Iberoamericano de Protección de Datos Personales
- ✓ III Conferencia Internacional de Comisionados de Acceso a la Información
- ✓ 1er. Certamen Nacional de Ensayo México entra en la era de la transparencia

- **Carteles en lenguas indígenas**

Se cuenta con al menos 9 Carteles de difusión acerca de información gubernamental de utilidad, en lenguas indígenas:

- ✓ Maya
- ✓ Náhuatl
- ✓ Zapoteco
- ✓ Purépecha
- ✓ Tsotsil
- ✓ Mexicano de Guerrero
- ✓ Chinanteco
- ✓ Tlapaneco
- ✓ Cuicateco

- **Cuadernos Metodológicos**

Además de poner a disposición del público una serie de manuales internos referentes a sistemas institucionales y manejo de archivos y trámites, se incluyen los siguientes archivos en formato PDF:

- ✓ El ABC de la Transparencia
- ✓ El ABC de los Datos Personales
- ✓ El ABC de los Archivos

- **Otras Publicaciones**

En esta sección se incluyen los siguientes 7 documentos en formato PDF:

- ✓ La promesa del Gobierno Abierto
- ✓ Mexico: Transparency and access to information
- ✓ Cartilla Nacional de Derechos
- ✓ Diagnóstico sobre la situación archivística de las dependencias y entidades de la Administración Pública Federal: 2007
- ✓ Guía Práctica para la gestión de las unidades de enlace y comités de información en las dependencias y entidades de la APF Tomo I
- ✓ Guía Práctica para la gestión de las unidades de enlace y comités de información en las dependencias y entidades de la APF Tomo II
- ✓ Compilación Jurídica de los otros sujetos obligados por la ley federal de transparencia y acceso a la información pública gubernamental

Además se tienen diferentes convenios con instituciones gubernamentales, organismos de la sociedad civil e instituciones académicas con el fin de dar a conocer la herramienta del INFOMEX mediante talleres de capacitación.

B. Comisión Nacional de Derechos Humanos (CNDH)

Respecto de sus antecedentes directos, el 13 de febrero de 1989, dentro de la Secretaría de Gobernación, se creó la Dirección General de Derechos Humanos. Un año más tarde, el 6 de junio de 1990 nació por decreto presidencial una institución denominada Comisión Nacional de Derechos Humanos, constituyéndose como un Organismo desconcentrado de dicha Secretaría. Posteriormente, mediante una reforma publicada en el Diario Oficial de la Federación el 28 de enero de 1992, se adicionó el apartado B del artículo 102, elevando a la CNDH a rango constitucional y bajo la naturaleza jurídica de un Organismo descentralizado, con personalidad jurídica y patrimonio propios, dándose de esta forma el surgimiento del llamado Sistema Nacional No Jurisdiccional de Protección de los Derechos Humanos.

Finalmente, por medio de una reforma constitucional, publicada en el Diario Oficial de la Federación el 13 de septiembre de 1999, dicho Organismo Nacional se constituyó como una Institución con plena autonomía de

gestión y presupuestaria, modificándose la denominación de Comisión Nacional de Derechos Humanos por la de Comisión Nacional de los Derechos Humanos.[76]

a. Marco Legal

Ley de la Comisión Nacional de los Derechos Humanos

En su art. 1, se determina el ámbito de competencia de la CNDH a todo el territorio nacional y respecto de los mexicanos y extranjeros que se encuentren en el país.

En el art. 2, se define a la Comisión como un organismo que cuenta con autonomía de gestión y presupuestaria, personalidad jurídica y patrimonio propios, y cuyo objeto esencial es la protección, observancia, promoción, estudio y divulgación de los derechos humanos que ampara el orden jurídico mexicano.

En el art. 3 se establece su competencia para conocer quejas relacionadas con presuntas violaciones a los derechos humanos cuando éstas fueren imputadas a autoridades y servidores públicos de carácter federal, con excepción de los del Poder Judicial de la Federación.

b. Marco Institucional

El Manual de Organización General, es el documento en el que se enmarca el ámbito de responsabilidad y competencia del organismo: atribuciones, estructura orgánica, objetivos y funciones de los Órganos y Unidades Administrativas a que se refiere el Reglamento Interno; así como el organigrama que muestra la estructura de organización, los niveles jerárquicos y grados de autoridad, con el objeto de disponer de una herramienta de trabajo que contribuya al cabal cumplimiento de la misión y objetivos esenciales de la Comisión Nacional de los Derechos Humanos.

En 1992, la protección y defensa de los derechos humanos fue elevada a rango constitucional. Con fecha 13 de septiembre de 1999 se reformó el artículo 102, apartado B constitucional, en él se le da a la Comisión Nacional de los Derechos Humanos el carácter de organismo autónomo. Su objetivo esencial desde entonces es la **protección, observancia, promoción, estudio y divulgación de los Derechos Humanos** previstos en el orden jurídico mexicano.

Entre sus atribuciones se encuentran las siguientes acciones de educación : “Elaborar y ejecutar programas preventivos en materia de derechos humanos” y “Formular programas y proponer acciones en coordinación con

[76] Comisión Nacional de los Derechos Humanos, “Antecedentes”, 2015, (en línea), disponible en: http://www.cndh.org.mx/Antecedentes (Consultada el 23 de octubre de 2015)

las dependencias competentes que impulsen el cumplimiento dentro del territorio nacional de los tratados, convenciones y acuerdos internacionales signados y ratificados por México en materia de derechos humanos".

c. Sujetos obligados y sujetos de derecho

Son sujetos de observación por parte de la Comisión, las autoridades y servidores públicos de carácter federal, con excepción de los del Poder Judicial de la Federación, relacionados con presuntas violaciones a los derechos humanos.

Se identifica, a partir del Art. 1, como sujetos de derechos humanos, todos los mexicanos y extranjeros que se encuentren en territorio nacional.

d. Estrategia

La Comisión Nacional de Derechos Humanos, para la defensa y promoción de los derechos humanos en todo el territorio nacional, se ha valido de diversos medios y campañas de difusión y educación en la materia de su competencia.

Las diversas campañas[77] informativas que se han llevado a cabo, se han organizado en los siguientes cinco temas:

a) Tus Derechos Humanos

Los subtemas incluidos en este apartado son:

- ✓ Adultos Mayores (1 Spot TV, 1 Spot Radio y 1 Impreso)
- ✓ Amigo Migrante (2 Spots TV, 2 Spots Radio y 2 Impresos)
- ✓ Cartilla de los Derechos y Deberes de las personas (1 Spot TV, 1 Spot Radio y 6 Impresos)
- ✓ Derechos a la salud (1 Spot TV, 1 Spot Radio y 1 Impreso)
- ✓ Derechos de los jóvenes (2 Spots TV –uno en versión maya-, 1 Spot Radio y 1 Impreso)
- ✓ Derechos de las mujeres (1 Spot TV, 1 Spot Radio y 1 Impreso)
- ✓ Derechos de los niños (1 Spot TV, 1 Spot Radio y 1 Impreso)
- ✓ Derechos de los pueblos indígenas (2 Spots TV, 2 Spots Radio, uno de ellos con versiones adicionales en Maya, Mixe, Mixteco, Náhuatl, Otomí, Purépecha y Tseltal, 1 Impreso y 1 Cartel)
- ✓ Discapacidad (1 Spot TV, 1 Spot Radio y 1 Cartel)

[77] Comisión Nacional de los Derechos Humanos, "Campañas", 2015, (en línea), disponible en: http://www.cndh.org.mx/Campanas (Consultada el 23 de octubre de 2015)

- ✓ Los Derechos de las niñas y los niños (2 Spots TV, 2 Spots Radio y 2 Carteles)
- ✓ Paisano (1 Spot TV, 1 Spot Radio y 1 Impreso)
- ✓ Personas con discapacidad (1 Spot TV, 1 Spot Radio y 1 Impreso)
- ✓ Tus derechos humanos nuestra razón de ser (1 Spot TV, 1 Spot Radio y 2 Carteles)
- ✓ VIH Sida (1 Spot TV, 1 Spot Radio y 1 Impreso)

b) Información sobre CNDH

Los subtemas de este apartado son:

- ✓ Cambiamos (1 Spot TV, 1 Spot Radio y 1 Cartel)
- ✓ 20 Aniversario (1 Spot TV, 1 Spot Radio y 1 Cartel)

c) Cultura de la Legalidad

- ✓ Sobre este tema se han difundido 2 Spots de TV, 2 Spots de Radio y 2 Impresos

d) Províctima

- ✓ Províctima (2 Spot TV, 2 Spot Radio y 2 Impresos)
- ✓ Víctima del delito (1 Spot TV, 1 Spot Radio y 1 Impreso)

e) Trata de personas

- ✓ Contra la trata de personas (1 Spot TV, 1 Spot Radio y 1 Impreso)
- ✓ Trata de personas (1 Spot TV, 1 Spot Radio y 1 Impreso)

C. Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF)[78]

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros fue creada el 18 de enero de 1999 en el marco de la Ley de Protección y Defensa al Usuario de Servicios Financieros. Es una institución pública dependiente de la Secretaría de Hacienda y Crédito Público, dedicada tanto a orientar, informar y promover la Educación Financiera, como a atender y resolver las quejas y reclamaciones de los usuarios de servicios y productos financieros.

a. Marco Legal

- **Ley de Protección y Defensa al Usuario de Servicios Financieros**

Según su Artículo. 1, su objeto es la protección y defensa de los derechos e intereses del público usuario de los servicios financieros, que prestan las instituciones públicas, privadas y del sector social debidamente autorizadas, así como regular la organización, procedimientos y funcionamiento de la entidad pública encargada de dichas funciones.

En el título II, capítulo I de las Facultades de la CONDUSEF, se lee en el numeral XIV que una de sus facultades es ”Proporcionar información a los Usuarios relacionada con los servicios y productos que ofrecen las Instituciones Financieras, y elaborar programas de difusión con los diversos beneficios que se otorguen a los Usuarios”, también se lee en el XVI “Informar al público sobre la situación de los servicios que prestan las Instituciones Financieras y sus niveles de atención, así como de aquellas Instituciones Financieras que presentan los niveles más altos de reclamaciones por parte de los Usuarios. Esta información podrá incluir la clasificación de Instituciones Financieras en aspectos cualitativos y cuantitativos de sus productos y servicios”.

- **Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros**

Éste determina funciones de la Comisión, así como estructura interna y funciones. La Dirección General de

[78] Secretaría de Hacienda y Crédito Público, Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, disponible en: http://www.condusef.gob.mx/ (Consultada el 23 de octubre de 2015)

Educación Financiera es quien se encarga de la función asignada en la CONDUSEF de transmitir de manera preventiva a los usuarios la información que ayude a ejercer sus derechos como usuarios de servicios financieros.

Otros instrumentos legales en los que se enmarca la CONDUSEF son:

- Ley para la Transparencia y Ordenamiento de los servicios Financieros
- Reglamento de supervisión de la CONDUSEF

b. Marco Institucional

En el Artículo 15 del "Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros" se establecen las funciones de la Dirección General de Educación Financiera, con el ejercicio de las siguientes atribuciones:

"Actuar como enlace con las instituciones financieras, dependencias y entidades de la Administración Pública Federal y organismos internacionales, en asuntos relacionados con el ejercicio de sus atribuciones;

a) Ser el enlace de la Comisión Nacional y fungir como Secretario Técnico del Comité de Educación Financiera que preside la Secretaría;

b) Difundir los precios, comisiones y características de los servicios y productos financieros, con la finalidad de apoyar a los Usuarios en la toma de decisiones y fomentar la competencia entre Instituciones Financieras;

c) Integrar, mantener actualizado y difundir el Buró de Entidades Financieras;

d) Fracción adicionada DOF 02-06-2014

e) Realizar, coordinar y publicar investigaciones y estudios sobre productos y servicios financieros, educación financiera y protección a los Usuarios;

f) Diseñar e instrumentar propuestas y estrategias que faciliten a la población en general, la comprensión de las características de los servicios y productos financieros que se ofrecen en el mercado;

g) Desarrollar y, en su caso, coadyuvar junto con otras instituciones públicas y privadas en la realización de acciones y proyectos que contribuyan al fomento de la educación financiera;

h) Establecer y mantener relaciones con instituciones educativas, financieras, medios de comunicación, autoridades y organismos públicos y privados, y organismos internacionales, con la finalidad de fomentar la educación financiera;

i) Establecer los mecanismos de colaboración con las Instituciones Financieras para elaborar y difundir los programas y contenidos en materia de educación financiera;

j) Proponer a las autoridades competentes, programas y contenidos en materia de educación financiera;

k) Coordinar y ejecutar el Programa anual de publicaciones de la Comisión Nacional;

l) Diseñar y administrar herramientas web que difundan información o contenidos en materia de educación financiera;

m) Administrar y actualizar el Sitio Web de Cuadros Comparativos de servicios y productos financieros de la Comisión Nacional;

n) Coordinar el Consejo Editorial de la revista "Proteja su Dinero";

o) Elaborar investigaciones, entrevistas, crónicas, reportajes y otros productos periodísticos para la revista "Proteja su Dinero";

p) Planear y coordinar la realización de eventos para difundir y promover la educación financiera entre la población;

q) Participar y promover la realización de foros nacionales e internacionales cuyo objeto sea acorde con el de la Comisión Nacional, a fin de facilitar el intercambio de experiencias;

r) Planear y ejecutar los programas de difusión y comunicación social de la Comisión Nacional;

s) Establecer y mantener vínculos con los distintos medios de comunicación, a fin de promover entrevistas con los servidores públicos de la Comisión Nacional para la difusión de los servicios y acciones relevantes del Organismo;

t) Organizar y supervisar entrevistas y conferencias de prensa, así como emitir boletines informativos en las materias competencia de la Comisión Nacional;

u) Evaluar las campañas informativas de la Comisión Nacional;

v) Elaborar y difundir de publicaciones institucionales, campañas informativas y cualquier otro material que contribuya al fomento de la educación financiera;

w) Dar seguimiento a la información divulgada por los medios de comunicación acerca de las actividades de la Comisión Nacional, informando de ello a las unidades administrativas de la misma;

x) Coordinar la distribución de las publicaciones desarrolladas por la Comisión Nacional para el cumplimiento de sus fines"

c. Sujetos obligados y sujetos de derecho

Según se define en el art. 2 de la Ley, en sus fracciones I y IV:

Son sujetos obligados las Instituciones Financieras, sociedades controladoras, instituciones de crédito, sociedades financieras de objeto múltiple, sociedades de información crediticia, casas de bolsa, especialistas bursátiles, fondos de inversión, almacenes generales de depósito, uniones de crédito, casas de cambio, instituciones de seguros, sociedades mutualistas de seguros, instituciones de fianzas, administradoras de fondos para el retiro, PENSIONISSSTE, empresas operadoras de la base de datos nacional del sistema de ahorro para el retiro, Instituto del Fondo Nacional para el Consumo de los Trabajadores, sociedades cooperativas de ahorro y préstamo, sociedades financieras populares, sociedades financieras comunitarias, y cualquiera otra sociedad que requiera de la autorización de la SHCP o cualesquiera de las Comisiones Nacionales para constituirse y funcionar como tales y ofrecer un producto o servicio financiero a los Usuarios.

Se entienden como sujetos de derecho o usuarios, a cualquier persona que utilice o por cualquier causa tenga algún derecho frente a la Institución Financiera como resultado de la operación o servicio prestado.

d. Estrategia

Dado que entre sus compromisos figura el "Fomentar la Educación Financiera entre la población", la CONDUSEF elabora, difunde y promueve información de utilidad para los usuarios de servicios financieros. Algunos de estos documentos e instrumentos son:

- **ABC de la Educación Financiera**[79]

  - ✓ Se trata de una guía interactiva, esquemática y a color, en la cual se incluye definiciones prácticas de 164 conceptos, instituciones, gestiones, entre otros recursos, con la finalidad de ser una herramienta de apoyo para la toma de mejores decisiones por parte de los ciudadanos.
  - ✓ Cuenta con 82 págs., y se encuentra disponible en formato PDF en la web institucional.

- **Comunicados de Prensa**[80]

  - ✓ Reflejan o describen circunstancias o temas de coyuntura correspondientes a cada momento en que han sido redactados, resultando de tal manera, de gran utilidad para conocer antecedentes de la actividad financiera del país.
  - ✓ Desde 2010 se han publicado cerca de 600 Comunicados de Prensa, mismos que son accesibles a través de la página institucional.

- **Estudios y Evaluaciones**

Desde 2013 se han publicado 32 estudios y evaluaciones, de los cuales 7 han sido durante el presente año, mismos que versan acerca de temáticas diversas como:

- ✓ Reclamaciones imputables a un posible robo de identidad 2011-2015 1er semestre
- ✓ Balance sobre las Acciones de Defensa al Usuario 2do trimestre 2015
- ✓ Cláusulas Abusivas
- ✓ Evolución de las Reclamaciones Imputables a un Posible Fraude
- ✓ Evolución de las Reclamaciones 2011, 2012, 2013 y 2014
- ✓ Balance sobre las Acciones de Defensa al Usuario 1er Trimestre 2015
- ✓ Actualización Banca Múltiple y Banca de Desarrollo Enero-Diciembre 2014

Además, en entrevista el Mtro. Torres Góngora, Director de la Dirección de Educación Financiera, señaló que el evento más importante del año para ellos es la *Semana de la Educación Financiera*. Fundamentalmente trabajan

[79] Educación Financiera y Condusef, "A, B, C De Educación Financiera", 2009, (en línea), disponible en: http://www.condusef.gob.mx/PDF-s/mat_difusion/abc_09.pdf (Consultada el 23 de octubre)

[80] Secretaría de Hacienda y Crédito Público, Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, "Comunicados de Prensa", 2015, (en línea), disponible en: http://www.condusef.gob.mx/index.php/prensa (Consultada el 23 de octubre de 2015)

con Cámaras empresariales y con jóvenes, pero su población objetivo son todas las personas usuarios de los servicios financieros.

D. Instituto Nacional Electoral (INE) [81]

El Instituto Nacional Electoral es el organismo público autónomo encargado de organizar las elecciones federales, es decir, la elección del Presidente de la República, Diputados y Senadores que integran el Congreso de la Unión, así como organizar, en coordinación con los organismos electorales de las entidades federativas, las elecciones locales en los estados de la República y la Ciudad de México.

Entre sus fines destaca el "Llevar a cabo la promoción del voto y coadyuvar a la difusión de la cultura democrática".

a. Marco Legal

En 1990, como resultado de las reformas realizadas a la Constitución en materia electoral, el Congreso de la Unión expidió el "Código Federal de Instituciones y Procedimientos Electorales" (COFIPE) y dio lugar a la creación del Instituto Federal Electoral (IFE), a fin de contar con una institución imparcial que diera certeza, transparencia y legalidad a las elecciones federales.

"La reforma constitucional en materia política-electoral, publicada el 10 de febrero de 2014 rediseñó el régimen electoral mexicano y transformó el Instituto Federal Electoral (IFE) en una autoridad de carácter nacional: el Instituto Nacional Electoral (INE), a fin de homologar los estándares con los que se organizan los procesos electorales federales y locales para garantizar altos niveles de calidad en nuestra democracia electoral. Además de organizar los procesos electorales federales, el INE se coordina con los organismos electorales locales para la organización de los comicios en las entidades federativas."[82]

Así, la Ley General de Instituciones y Procedimientos Electorales refiere en su Artículo. 1, que es una Ley de orden público y de observancia general en el territorio nacional y para los Ciudadanos que ejerzan su derecho al sufragio en territorio extranjero.

[81] Instituto Nacional Electoral, disponible en: http://www.ine.mx/portal/ (Consultada el 17 de octubre de 2015)
[82] Instituto Nacional Electoral, "Historia del Instituto Federal Electoral", (en línea), disponible en: http://www.ine.mx/archivos3/portal/historico/contenido/menuitem.cdd858023b32d5b7787e6910d08600a0/ (Consultada el 17 de octubre de 2015)

Tiene por objeto establecer las disposiciones aplicables en materia de instituciones y procedimientos electorales, distribuir competencias entre la Federación y las entidades federativas en estas materias, así como la relación entre el Instituto Nacional Electoral y los Organismos Públicos Locales.

b. Marco Institucional

El INE es un organismo autónomo que depende de manera general del Congreso de la Unión. Su estructura se compone por los órganos centrales:

- Consejo General
- Presidencia del Consejo General
- Junta General Ejecutiva
- Secretaría Ejecutiva
- Contraloría General

Direcciones Ejecutivas

- Dirección Ejecutiva del Registro Federal de Electores
- Dirección Ejecutiva de Prerrogativas y Partidos Políticos
- Dirección Ejecutiva de Organización Electoral
- Dirección Ejecutiva del Servicio Profesional Electoral Nacional
- Dirección Ejecutiva de Capacitación Electoral y Educación Cívica
- Dirección Ejecutiva de Administración

Unidades Técnicas

- Coordinación Nacional de Comunicación Social
- Coordinación de Asuntos Internacionales
- Unidad Técnica de Servicios de Informática
- Dirección Jurídica
- Dirección del Secretariado
- Unidad Técnica de Planeación
- Unidad Técnica de Igualdad de Género y No Discriminación
- Unidad Técnica de lo Contencioso Electoral
- Unidad Técnica de Fiscalización
- Unidad Técnica de Vinculación con los Organismos Públicos Locales

- Unidad Técnica de Transparencia y Protección de Datos Personales

Órganos Delegacionales

Juntas Locales y Distritales

Es a la Dirección Ejecutiva de Capacitación Electoral y Educación Cívica a quien le corresponde según el **Artículo 58** de la Ley General de Instituciones y Procedimientos Electorales (LEGIPE):

a) Elaborar, proponer y coordinar los programas de educación cívica que desarrollen las juntas locales y distritales ejecutivas.
b) Promover la suscripción de convenios en materia de educación cívica con los Organismos Públicos Locales sugiriendo la articulación de políticas nacionales orientadas a la promoción de la cultura político-democrática y la construcción de ciudadanía.
c) Vigilar el cumplimiento de los programas y políticas a los que se refieren los dos incisos anteriores.
d) Diseñar y proponer estrategias para promover el voto entre la ciudadanía.
e) Diseñar y promover estrategias para la integración de mesas directivas de casilla y la capacitación electoral.
f) Preparar el material didáctico y los instructivos electorales.
g) Orientar a los ciudadanos para el ejercicio de sus derechos y cumplimiento de sus obligaciones político-electorales.
h) Llevar a cabo las acciones necesarias para exhortar a los ciudadanos que se inscriban y actualicen su registro en el Registro Federal de electores y para que acudan a votar.
i) Asistir a las sesiones de la Comisión de Capacitación Electoral y Educación Cívica sólo con derecho de voz.
j) Diseñar y proponer campañas de educación cívica en coordinación con la Fiscalía Especializada para la prevención de delitos electorales.

En el **Artículo 49** del Reglamento Interior del Instituto Nacional Electoral señala, entre otras, las siguientes atribuciones:

a) Elaborar, proponer, y coordinar los programas de capacitación electoral y de educación cívica que se desarrollen, tanto a nivel central como a través de las Juntas Locales y Distritales.
b) Planear, dirigir y supervisar la elaboración de las políticas y programas de educación cívica y capacitación electoral y educación cívica que desarrollarán las Juntas Locales y Distritales.

c) Presentar a la Junta los programas de capacitación electoral y educación cívica y vigilar su ejecución.
d) Evaluar periódicamente el cumplimiento de los programas autorizados para la Dirección, tanto en el nivel central como en los niveles delegacional y subdelegacional.
e) Diseñar y promover estrategias para la integración de mesas directivas de casilla y la capacitación electoral a nivel local y federal.
f) Dirigir y supervisar la investigación, análisis y la preparación de material didáctico que requieren los programas de capacitación electoral y educación cívica.
g) Diseñar e instrumentar las campañas de difusión institucionales y, en su caso, coordinarse para ello con las instancias que por el objeto o contenido de la campaña sean competentes.
h) Orientar a los ciudadanos para el ejercicio de sus derechos y cumplimiento de sus obligaciones político-electorales.
i) Coordinar la elaboración de análisis, estudios, investigaciones y bases de datos sobre temas de capacitación electoral, educación cívica y cultura política democrática, dirigidos a fomentar el conocimiento y difusión de estas temáticas y construir una ciudadanía más participativa y mejor informada.
j) Diseñar, proponer e implementar campañas de educación cívica en coordinación con la Fiscalía Especializada para la Prevención de Delitos Electorales.
k) Identificar y establecer mecanismos de colaboración con institutos políticos, organizaciones civiles, instituciones académicas y de investigación, así como de educación superior o especializada, para coadyuvar al desarrollo de la vida democrática.
l) Diseñar y organizar encuentros y foros académicos que contribuyan a la difusión de la educación cívica y la cultura democrática.
m) Planear, ejecutar, dirigir y supervisar los programas de divulgación desarrollo y fortalecimiento de la cultura política democrática y los referentes a la comunicación educativa, con el objeto de impulsar la cultura democrática.
n) Diseñar y proponer estrategias para promover el voto entre la ciudadanía.
o) Diseñar y proponer las estrategias de capacitación electoral y educación cívica a nivel nacional.

c. Sujetos obligados y sujetos de derecho

Se establece en el **art. 2**, incisos a al d, de la Ley, que ésta reglamenta las normas constitucionales relativas a:

a) Los derechos y obligaciones político-electorales de los ciudadanos;
b) La función estatal de organizar las elecciones de los integrantes de los Poderes Legislativo y Ejecutivo de la Unión;

c) Las reglas comunes a los procesos electorales federales y locales, y

d) La integración de los organismos electorales

Por tanto, se identifica como sujetos obligados de la Ley, al Instituto Nacional Electoral y los Organismos Públicos Locales, quienes en el ámbito de su competencia, dispondrán lo necesario para asegurar el cumplimiento de la Ley.

Y, como sujetos de derecho, a los ciudadanos que en territorio nacional o extranjero, ejerzan sus derechos político-electorales.

d. Estrategia

El Instituto cuenta con una "Estrategia Nacional de Educación Cívica para el Desarrollo de la Cultura Política Democrática"[83] (ENEC) 2011-2015, a través de la cual se diseñan e implementan una serie de proyectos y acciones dirigidos a la construcción de ciudadanía democrática y a la creación de condiciones para el ejercicio integral de los derechos de las y los mexicanos. Éste tiene una extensión de 135 páginas, y se encuentra disponible en formato PDF en la página web institucional. Dicha estrategia complementa la estrategia de educación con la de difusión y de comunicación en el derecho al voto.

La entrevista con Jacinto Vaquero, Director de Educación Cívica del INE, nos permitió conocer que la nueva estrategia se hizo con base en el Informe del país sobre la calidad de la ciudadanía en México, encuesta muy robusta cuyo eje principal se realizó con 11 mil entrevistas cara a cara. El Diagnóstico alertó que hay cosas que cambiar dentro de la nueva estrategia, *"es decir no tenemos que cambiar rotundamente, no hay que dar un giro de 180 grados sino lo que el diagnóstico nos confirma es que el planteamiento que hicimos es el correcto y más bien tenemos que buscar nuevas maneras, formas innovadoras de intentar atender los problemas y queda claro ahora que los problemas no son problemas que el Instituto pueda resolver por sí mismo, sino que tienen que ver con una responsabilidad que tienen todas las instituciones del Estado mexicano."*

La ENEC fue elaborada por la Dirección Ejecutiva de Capacitación Electoral y Educación Cívica en enero de 2011. El trabajo del Instituto se orientó en tres líneas estratégicas:

- La implementación de prácticas y políticas orientadas a la construcción de ciudadanía.

[83] Instituto Nacional Electoral, "Estrategia Nacional de Educación Cívica", (en línea), disponible en: http://www.ine.mx/archivos2/portal/DECEYEC/EducacionCivica/estrategiaNacional/ (Consultada el 17 de octubre de 2015)

- Generación y socialización de información sobre prácticas y condiciones determinantes para la construcción de ciudadanía.
- Desarrollo e implementación de procesos educativos que promuevan el aprecio por lo público y contribuyen a generar capacidad de agencia de las y los ciudadanos.

El siguiente cuadro muestra de forma esquemática los "Objetivos y Líneas Estratégicas" de la Estrategia Nacional de Educación Cívica 2011-2015.

Estrategia Nacional de Educación Cívica

Objetivos Estratégicos	Líneas Estratégicas	Programas	Proyectos
Objetivo I Contribuir al Diseño e implementación de prácticas y políticas públicas que favorezcan la construcción de ciudadanía en México	Línea Estratégica I Impulso de Políticas Públicas para la construcción de Ciudadanía	Programa 1 Impulso a prácticas sociales y políticas para la construcción de ciudadanía	Proyecto 1.1 Fomento de Practicas y políticas en equidad y desarrollo
		Programa 2 Monitoreo ciudadano para la actuación prodemocrática	Proyecto 2.1 Informe país sobre la calidad de la ciudadanía en México
			Proyecto 2.2 Informes especiales sobre temas de agencia pública para la construcción de ciudadanía y calidad de la democracia
Objetivo II Generar y socializar información relevante sobre prácticas y condiciones determinantes de la construcción de la ciudadanía, la cual contribuirá a la deliberación y acción Publica	Línea estratégica II Generalización de información sobre prácticas y condiciones determinantes para la construcción de ciudadanía	Programa III Sistema Nacional de Información para la Construcción de Ciudadanía	Proyecto 3.1 Construcción de indicadores de calidad de la ciudadanía
			Proyecto 3.2 Sistematización de prácticas sociales y políticas para la construcción de ciudadanía
			Proyecto 3.3 Sistematización de estrategias y modelos educativos de formación ciudadana
Objetivo III Desarrollar e implementar procesos y medios educativos eficaces que promuevan el aprecio por lo público y contribuyan a generar la capacidad de agencia de las y los ciudadanos	Línea estratégica III educación en y para la participación	Programa 4 Programa nacional de formación cívica para la participación y la convivencia política democrática	Proyecto 4.1 Formación Ciudadana para adultos
			Proyecto 4.2Formacion ciudadana para jóvenes
			Proyecto 4.3 Convivencia democrática en escuelas de educación básica
			Proyectos 4.4 Formación ciudadana para la participación electoral
		Programa 5 Programas de formulación ciudadana para la incidencia de políticas publicas	Proyecto 5.1 Formación de promotores ciudadanos para la incidencia en políticas públicas
			Proyecto 5.2 Formación de liderazgos democrático y deliberación del sistema de partidos políticos

Fuente: Instituto Nacional Electoral

Corroboramos que entre los instrumentos que utiliza el Instituto para llevar a cabo la ENEC, se cuentan:

- **Spots de Radio y TV**
    - Promoción de la Cultura Democrática
    - Promoción de la Participación Ciudadana en Procesos Electorales Locales 2014
    - Actualización al Padrón Electoral
    - Promoción de la Participación Ciudadana en el Proceso Electoral Federal 2014-2015
    - Redes sociales como medios alternativos

- **Materiales Gráficos**
    - Campaña Institucional 2013 IFE
    - Elecciones 2012 IFE: "Yo decido qué quiero para México"
    - Campaña Institucional 2007-2010 IFE
    - Perifoneo
    - Posters
    - Volanteo
    - Espectaculares
    - Gobelas

- **Seminarios**
    - Seminario sobre la Reforma Electoral 2007
    - Seminario Avance Tecnológico y e-Democracia

- **Concursos y eventos**

Constantemente el Instituto organiza una serie de eventos y concursos para enriquecer y fomentar una interacción directa con la ciudadanía:

- ✓ 10° Congreso Nacional de Organismos Públicos Autónomos de México (OPAM)
- ✓ Convocatoria del Concurso Nacional de Ideas, Plan Maestro Conjunto Tlalpan INE
- ✓ Convocatorias para la designación de las y los Consejeros Presidentes y las y los Consejeros Electorales de los Organismos Públicos Locales 2015

- **Investigación sobre democracia y materia electoral**[84]

Elaboración de "Estudios e Investigaciones" acerca de estos temas:

- ✓ Capacitación electoral
- ✓ Participación ciudadana
- ✓ Educación cívica
- ✓ Cultura política democrática
- ✓ El Informe País
- ✓ Estudios Censales

El trabajo de difusión en radio y televisión es sujeto a los tiempos oficiales; se utilizan algunos otros medios alternativos, todo esto es complementario a la educación cívica.

Las campañas de difusión del INE se han enfocado básicamente en el derecho de las personas mayores de 18 años que tienen credencial para votar, que es una credencial que se ha vuelto el medio de identificación por excelencia. Se comenzó a promover otro tipo de valores y derechos políticos con estrategias de educación cívica y de formación de ciudadanos.

Se han realizado algunos diagnósticos a lo largo de la vida de lo que fue el IFE , ahora del INE, sobre cómo es que la ciudadanía se comporta en términos de participación, si sabe, si conoce sus derechos, si no los conoce, y si los conoce, si los ejerce, si se organiza para ejercerlos, por ejemplo.

Desde su perspectiva, el tiempo es muy limitado para dar a conocer los servicios del Instituto a la ciudadanía, para que realmente utilicen los servicios del Instituto.

Los escasos recursos son otro gran reto, y en esto también se refiere al tiempo en radio y televisión. Por ello se han implementado algunos medios alternativos cuando se tienen campañas para promover el voto o para promover que los ciudadanos sean funcionarios de casilla.

La innovación es el principal recurso ante la escasez en ese sentido la estrategia que se hizo de educación cívica lo que pretende es tener una conciencia más clara del papel del ciudadano y lo público *"y entonces invertir menos dinero en difusión cada que viene una elección y más bien tener ciudadanos conscientes de que tienen una*

[84] Instituto Nacional Electoral, "Investigación sobre democracia y materia electoral", (en línea), disponible en: http://www.ine.mx/archivos2/portal/DECEYEC/EducacionCivica/materiales/estudiosEncuestas/ (Consultada el 17 de octubre de 2015)

responsabilidad con el Estado, con el país, con sus conciudadanos y entonces que sea una cosa automática y no tener que estar teniendo que convencer cuando viene cada elección."

"¿Cómo llegamos al ciudadano? Pues con una estrategia promoción del voto que está en el área de educación cívica apoyada con la difusión. Es siempre un apoyo a lo que hemos tratado de darle mayor visión estratégica es al tema de la formación cívica."

Es decir, trabajar directamente con la sociedad a través de nuestra estructura territorial más allá de la difusión, por lo que la Estrategia se ejecuta a nivel territorial mediante la estructura que tiene el INE en los 300 distritos.

Por otro lado, algunos de los factores que no favorecen en la promoción del derecho, son las problemáticas detectadas o la molestia de la gente con el sistema político o a la política institucional en su conjunto.

La visión estratégica ahora del INE es hacer un gran acuerdo nacional en el que éste llame a las instituciones del estado mexicano a hacerse cargo de garantizar los derechos, no solo los políticos, sino todos los derechos que tienen las personas a través de la atención de sus problemáticas. Por ello la tarea de educación cívica se vuelve muy importante porque a partir de ello, es que se espera que haya un cambio de la cultura política.

e. Aliados

Las instituciones con las que trabaje el INE, son entre otras SEP, DIF, IMJUVE, la Cámara de Diputados, los Congresos Locales, el PNUD y organizaciones de la sociedad civil. El INE cuenta con una gran gama de instituciones con las que se alía para fusionar recursos no sólo económicos, sino para intercambiar experiencias que les ayude a ir abordando las tareas de formación.

f. Grupos prioritarios

La formación de derechos políticos de las mujeres en comunidades, *"lo que hacemos es fortalecer y empoderar a las mujeres dándoles un material que tenemos, lo que hacemos es que el INE tiene desde el IFE un modelo de participación con perspectiva de género que tiene que ver con participación democrática, entonces realizamos una capacitación a estas organizaciones de mujeres para que impartan ese taller y la idea es esa, empoderar a la mujer, lo que hemos logrado es que en algunas comunidades empiezan a participar en los órganos políticos, se están formando síndicas o regidoras, estamos apostando a que sean presidentas municipales, que vayan participando en la vida política de la comunidad y creo que ese es uno de los proyectos más exitosos que hemos tenido y esa es la idea que incidamos…"*

Otro éxito es el de los resultados de la Consulta Infantil y Juvenil, los cuales se llevaron a la Cámara de Diputados después del 2012, los resultados de esa consulta se volvieron un insumo importante para la nueva Ley de Niñas, Niños y Adolescentes, entonces el INE ha ido aportando en distintos ámbitos para distintos públicos.

Desde el punto de vista de la instrumentación operación, una lección es que de alguna manera la estrategia definió no sólo los conceptos, el marco conceptual, sino que definió los proyectos que se realizarían con mucho detalle a lo largo de los cinco años, entonces *"de repente la estrategia a veces se convirtió en una suerte de camisa de fuerza porque lo que no se te había ocurrido en el momento en que se diseñó a mediados del 2010 de repente no cabía…"*

Se pudieron hacer los ajustes y las reformas, lo cual no fue sencillo, otra lección aprendida en la instrumentación es que país cambia, *"cada año es un país distinto están pasando cosas que nos obligan a hacer ajustes."*

El INE a decir de los servidores públicos entrevistados, es que fue muy ambicioso con demasiados proyectos, se quiso abarcar a todos los públicos con muchos proyectos, *"se tiene que ir más despacio con menos proyectos, más arropados y mejor pensados."*

E. Procuraduría Federal del Consumidor (PROFECO)[85]

La PROFECO surge en 1976 en el marco de la Ley Federal de Protección al Consumidor. Surge como la institución encargada de defender los derechos de los consumidores, prevenir abusos y garantizar relaciones de consumo justas. Entre sus objetivos figuran:

- Proteger y defender los derechos de las y los consumidores.
- Generar una cultura de consumo responsable
- Proporcionar información oportuna y objetiva para la toma de decisiones de consumo
- Implementar métodos de atención pronta y accesible a la diversidad de consumidoras y consumidores mediante el uso de tecnologías de la información.

[85] Procuraduría Federal del Consumidor, disponible en: http://www.profeco.gob.mx/ (Consultada el 18 de octubre de 2015)

a. Marco Legal

Se enmarca fundamentalmente en la Ley Federal de Protección al Consumidor.

Su objeto es promover y proteger los derechos y cultura del consumidor y procurar la equidad, certeza y seguridad jurídica en las relaciones entre proveedores y consumidores.

b. Marco Institucional

La PROFECO es un organismo que se inserta en la Secretaría de Economía. En el marco institucional se encuentran la Misión, visión y objetivos:

Misión:

"Somos una institución que protege y promueve los derechos de las y los consumidores, garantizando relaciones comerciales equitativas que fortalezcan la cultura de consumo responsable y el acceso en mejores condiciones de mercado a productos y servicios, asegurando certeza, legalidad y seguridad jurídica dentro del marco normativo de los Derechos Humanos reconocidos para la población consumidora."

Visión

"Ser una Institución cercana a la gente, efectiva en la protección y defensa de las personas consumidoras, reconocida por su estricto apego a la ley, con capacidad de fomentar la igualdad, la no discriminación, la participación ciudadana, y la educación para un consumo responsable."

Objetivos:

- Proteger y defender los derechos de las y los consumidores.
- Generar una cultura de consumo responsable.
- Proporcionar información oportuna y objetiva para la toma de decisiones de consumo.
- Implementar métodos de atención pronta y accesible a la diversidad de consumidoras y consumidores mediante el uso de tecnologías de la información.

La entrevista permitió conocer cómo se organiza la PROFECO internamente para operar la estrategia de educación al consumidor. La Coordinación de Educación y Divulgación se integra por dos direcciones, la de educación y la de divulgación, mismas que trabajan de manera coordinada en la elaboración de contenido y la difusión de los mismos mediante diferentes herramientas. No existe un documento público que se denomine "estrategia", ésta es parte de la planeación institucional anual y es interna. Anualmente se revisan resultados y

algunas veces se mantienen líneas de acción, otras se cambian, dependiendo los análisis y evaluaciones que realizan tanto de manera interna como externa.

c. Sujetos obligados y sujetos de derecho

Se entiende por sujetos obligados al "Proveedor", definidos en el art. 2, fracción II, como la persona física o moral en términos del Código Civil Federal, que habitual o periódicamente ofrece, distribuye, vende, arrienda o concede el uso o disfrute de bienes, productos y servicios.

Por su parte, es sujeto de derecho, el "Consumidor", definido en el mismo art., fracción I, como la persona física o moral que adquiere, realiza o disfruta como destinatario final bienes, productos o servicios. Se entiende también por consumidor a la persona física o moral que adquiera, almacene, utilice o consuma bienes o servicios con objeto de integrarlos en procesos de producción, transformación, comercialización o prestación de servicios a terceros, únicamente para los casos a que se refieren los artículos 99 y 117 de la LFPC.

d. Estrategia

En este apartado hacemos un análisis de la estrategia desde los elementos encontrados en la página electrónica complementando con la entrevista realizada el 10 de noviembre del 2015 al Licenciado Yuri Calzada Elrich, Director de Educación para el Consumo de la PROFECO.

La PROFECO, a través de su Coordinación General de Educación y Divulgación (CGED), y en observancia la (LFPC, art. 1, fracción II) se encarga de fomentar una cultura de consumo inteligente y responsable por medio de la difusión y la enseñanza para que los ciudadanos estén informados.

Para cumplir con su objetivo, la coordinación crea productos informativos que promueven los derechos de los consumidores y los pasos para el consumo responsable (antes consumo inteligente) y lleva a cabo acciones preventivas como la educación, la organización y la capacitación de consumidores. La PROFECO cuenta con promotores en todos los estados de la República mediante los cuales se llevan a cabo los talleres de educación que imparte el organismo.[86] A decir del entrevistado, el concepto de consumo responsable es relativamente nuevo, antes le llamaban consumo inteligente, pero "ese término no dejaba bien parado al consumidor" y por eso cambiaron al concepto a "consumo responsable".

[86] Procuraduría Federal del Consumidor, "Quiénes somos", 2015, (en línea), disponible en: http://www.profeco.gob.mx/n_institucion/q_somos.asp (Consultada el 18 de octubre de 2015)

La CGED cuenta con producción propia de televisión, radio e internet y, desde hace más de tres décadas, elabora contenidos que ayudan a mejorar la economía familiar y a tomar decisiones de consumo inteligente, como la **Revista del Consumidor**, la publicación emblemática de Profeco.[87]

Los instrumentos y medios de los que se vale Profeco para difundir información de su competencia a la ciudadanía, son:

- **Revista del Consumidor**
  - ✓ Ha sido publicada desde hace 37 años y circulada en puestos de periódicos y locales cerrados de todo el país.
  - ✓ La Revista informa sobre temas actuales de consumo, el resultado de los estudios de calidad, los comparativos de precios y sobre los derechos de los consumidores.
  - ✓ La Revista cuenta con cuentas de Facebook, Twitter y Youtube, a través de las cuales se difunde contenido.
- **Brújula de compra**
  - ✓ Se trata de un Boletín Electrónico en línea, en el cual se publican diversos artículos para orientar las decisiones de compra de los usuarios.
  - ✓ Algunos temas son: Comparativos de precios de diferentes productos, recomendaciones para cuidar las finanzas personales en épocas de alto consumo, resultados de encuestas, información sobre diferentes conceptos económicos empleados en la vida diaria, etc.
- **Educación y Organización de Consumidores**

Profeco cuenta con el **Programa de Educación para el Consumo**, mismo que imparte a los grupos de consumidoras y consumidores y a la población en general, en todo el país y consta de los siguientes 12 temas:

- ✓ Consumo y consumismo
- ✓ Publicidad, moda y diseño
- ✓ Esfera individual, el consumidor
- ✓ Esfera social, la sociedad
- ✓ Esfera medioambiental, consumo sustentable
- ✓ Ley Federal de Protección al Consumidor y los Derechos del Consumidor
- ✓ Profeco y sus servicios
- ✓ La información

[87] Procuraduría Federal del Consumidor, "Educación y Divulgación", 2015, (en línea), disponible en: http://www.profeco.gob.mx/educ_div/educ_div.asp (Consultada el 18 de octubre de 2015)

- ✓ Los riesgos
- ✓ Los contratos
- ✓ El resarcimiento
- ✓ Organización y acciones colectivas

- **Monitoreo de Tiendas Virtuales**

  - ✓ Se trata de un monitoreo y publicación de resultados quincenal, efectuado para verificar que los sitios mexicanos que ofrecen venta en línea cumplan con los elementos necesarios para proteger los derechos de los consumidores, tales como medidas de seguridad para proteger datos personales y financieros, medios de contacto para presentar una reclamación o solicitar aclaraciones, entre otros.

- **Elaboración de Encuestas y Sondeos**

  - ✓ Profeco difunde los resultados de encuestas y sondeos realizados en el boletín Brújula de compra, en la Revista del Consumidor y en Internet.

- **Trabajo conjunto con Asociaciones de Consumidores**

  - ✓ Profeco ofrece asesoría y acompañamiento a los interesados en formar agrupaciones u organizaciones de Asociaciones de Consumidores y otras Organizaciones de la Sociedad Civil.

Además de lo anterior, la estrategia de educación incluye el desarrollo de decálogos dirigidos a jóvenes para comprar casa y el decálogo para el consumidor de tequila. Se tiene un museo itinerante para los niños, con varios momentos y se está preparando lo mismo para jóvenes.

e. Aliados

Tanto CONAPRED como INAPAM, son aliados para la población con la que trabajan, en este caso población vulnerable. También INFONAVIT y los Bancos son aliados para cierto grupo poblacional. Están llegando estrategias para la población joven, para que sepan ubicar vicios ocultos de los organismos financieros.

Con la entrada en vigor de la reforma de telecomunicaciones se estableció una colaboración con el IFTL, porque es uno de los sectores que más quejas tiene y se creó en la Profeco la subprocuraduría de telecomunicaciones,

en este marco se han hecho esfuerzos como “yo soy usuario” mediante el cual los usuarios de telecomunicaciones pueden poner una queja en el portal.

f. Grupos prioritarios

En PROFECO tienen claro que toda la población en México es su población objetivo, pues todos y todas los mexicanos somos consumidores. Sin embargo trabajan estrategias dirigidas a ciertos grupos poblacionales. Han dedicado muchas líneas de acción a niños y niñas, como la currícula escolar con la inclusión del tema de consumo responsable en la educación básica y el museo itinerante. Para el 2016 se está preparando una estrategia intensa dirigida a los jóvenes entre 18 y 30 años. Antes se habían dedicado a la niñez y a los adultos entre 30 y 50 años. Reconocen que su alcance ha crecido, pero no se tiene un porcentaje aproximado.

g. Eventos periódicos sistematizados, premios, etc.

Cada año se trabaja fuertemente frente a las temporadas de alto consumo: San Valentín, cuaresma, navidad, Buen Fin. Se incluye el aviso de que no se compre pescado importado por ejemplo, incluimos desde el aspecto nutricional, el apoyo a los pescadores mexicanos y el cuidado del bolsillo familiar.

VIII. LÍNEAS ESTRATÉGICAS PROPUESTAS: POBLACIÓN OBJETIVO Y GRUPOS PRIORITARIOS

La Estrategia de Educación Cívica y Cultura (EECyC) a través de la cual se busca promover el ejercicio del derecho a la privacidad y la protección de datos personales por parte de los titulares de datos, se encuadra en la normatividad nacional en la materia, la cual está citada en el marco jurídico de esta estrategia.

La identificación de la población objetivo y dentro de ésta los grupos prioritarios a los cuales se dirigirá la EECyC, el alcance del análisis y la propuesta para la educación cívica, parten de los siguientes criterios:

- **Los riesgos que los individuos tienen al otorgar sus datos personales a los sujetos obligados,**
- **Vulnerabilidad de los individuos**
- **Número de titulares**
- **La capacidad de éstos para posicionar el derecho y**
- **El costo – efectividad de la misma**.
- **La fuerza y la importancia del mercado**

Riesgo de los Individuos

La OECD reconoce en la *Recomendación del Consejo sobre Política y Gobernanza Regulatoria*[88] que la regulación (o las políticas públicas) se desarrolla como una medida o solución a problemas detectados, de forma que el diseño de la regulación (política o estrategia) debe tener su origen en los riesgos que tiene por objetivo reducir.[89] Sin embargo, la OECD también reconoce que una regulación (política o estrategia) debe ser implementada solamente cuando existe evidencia del riesgo y sus consecuencias; así como cuando la evaluación del costo-beneficio de la regulación es positiva.[90] De esta forma, una posible alternativa siempre es la inacción, ya que implementar acciones o políticas sin evidencia no solamente puede tener poco o nulo efecto, sino generar otros efectos que afecten a otro grupo de interés o tenga mayores consecuencias sobre el mismo.

[88] Documento: Recomendación del Consejo sobre Política y Gobernanza Regulatoria. Organización para la Cooperación y el Desarrollo Económico, OCDE, 2012. Consultado en línea en : http://www.oecd.org/gov/regulatory-policy/Recommendation%20with%20cover%20SP.pdf

[89] *Idem*

[90] *La MIR en el contexto de la política y gobernanza regulatoria.* Taller de Elaboración de MIR con Análisis de Riesgos. Ciudad de México, Junio de 2014. Presentación consultada en http://es.slideshare.net/OECD-GOV/2-spfloresrariamexicojunio2014

La *Recomendación del Consejo sobre Política y Gobernanza Regulatoria, también* señala que los gobiernos deben "…exigir a los reguladores desarrollar, implementar y revisar estrategias de cumplimiento de la regulación frente a criterios basados en riesgo"[91]. Y la Comisión Federal de Mejora Regulatoria define el riesgo como *la probabilidad de que un evento adverso ocurra, multiplicado por el daño que causaría en caso de materializarse. El riesgo es simplemente la pérdida esperada y suele identificarse con mayor frecuencia en situaciones que afectan a la vida, la salud, el entorno, las finanzas y la vida cotidiana.*[92]

En las consideraciones previstas en la ley sobre los sujetos obligados y las definiciones sobre datos personales, debe resaltarse que la protección de los datos personales puede tener incidencia o contribuir al cumplimiento de objetivos en torno a la prevención de delitos como: secuestro, pederastia, extorsión, robo de identidad, los cuales se tipifican y sancionan a través de otros marcos jurídicos e instancias legales. En ese sentido, la EECyC cobra mayor importancia, pues por un lado se busca cubrir el objetivo primario de la educación en el derecho a la protección de datos personales de los sujetos del derecho, y por otro, su implementación puede favorecer la modificación, en sentido positivo, en el registro de algunos delitos directamente relacionados con el manejo de los datos personales por parte de los sujetos obligados.

El fin último es lograr que los individuos sean conscientes del derecho a la privacidad y la protección de datos personales, por lo que su concretización exige de un planteamiento que atienda a los titulares mediante abordajes diferenciados fundados en una noción de riesgo que ponga en claro los grupos o datos con mayor prioridad para la consolidación de una cultura de la privacidad.

De forma más específica, se ha considerado al riesgo como la probabilidad de utilización de los datos personales de forma no autorizada por parte de los sujetos obligados, de forma que pueda afectar el entorno personal, social, económico o profesional de los titulares del derecho, en los límites de su privacidad[93].

Las experiencias internacionales revisadas en materia de protección de datos diseñan líneas de acción o actividades pensadas para la población en general, para ciertos grupos demográficos, y para usuarios de sectores de servicios particulares como los financieros, los de salud y de telecomunicaciones. En tal sentido, puesto que la EECyC busca que los titulares conozcan el derecho que tienen a la protección de datos personales, pero al mismo tiempo que reconozcan y valoren adecuadamente el riesgo al que se enfrentan en el otorgamiento de datos personales, es menester que estén en posibilidad de tomar decisiones informadas sobre el otorgamiento

[91] *Idem*
[92] Beneficios económicos de la regulación basada en riesgos: caso de dispositivos médicos. Consultada en http://www.oecd.org/gov/regulatory-policy/48658862.pdf
[93] Retoma elementos de Davara Rodríguez, citado en INAI (2004) Estudio sobre Protección de Datos, México, 2004, consultado en línea en: http://inicio.ifai.org.mx/Estudios/prot_datos.pdf, así como de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

de sus datos personales a los sujetos obligados, y en caso de ser necesario, que utilicen los mecanismos establecidos para hacer valer sus derechos y denunciar los posibles incumplimientos por parte de los sujetos obligados. Para lograr lo anterior es necesario dirigir la estrategia a poblaciones objetivo diferenciadas, que sean atendidas mediante intervenciones focalizadas y diseñadas de acuerdo con ciertas características de la población objetivo.

Nuevamente, estas acciones o políticas deben ser evaluadas bajo un criterio de evidencia y riesgo para determinar si existe un beneficio positivo. Además, se ha tomado en cuenta en esta estrategia el criterio de costo-efectividad, pues las acciones propuestas para la promoción del derecho a la privacidad, no deben implicar necesariamente un alto costo, ya que podría incrementarse la inviabilidad en términos económicos, políticos y/o técnicos; se plantean acciones que pueden implicar un bajo costo con un alto impacto. Además de éste, los criterios aquí planteados, son los planteados en la propuesta técnica y mencionados al comienzo de este apartado, a saber: por la exposición al riesgo, por la vulnerabilidad de los individuos, el número de titulares, por la posibilidad de que estos titulares a su vez promuevan el ejercicio del derecho y por la fuerza e importancia del mercado.

Con base en los elementos anteriores, en el presente documento se integra un planteamiento general sobre la importancia de definir adecuadamente a la población objetivo, se identifica a los grupos o tipos de titulares que se proponen como población objetivo y por grupos prioritarios para la estrategia. Al final, se presentan los aliados posibles en la implementación de la EECyC. La definición de grupos prioritarios se hace en un primer momento por grupo demográfico, considerando los riesgos principales a los que se encuentra expuesto así como su capacidad de posicionamiento y réplica del derecho en un espacio más amplio, para que, en un segundo momento se dé paso a la cuantificación de la población objetivo y su importancia en la economía. Por supuesto, se tiene considerado que estos aspectos permitirán definir la (s) instancia (s) y la (s) estrategia (s) a través de las cuales se atenderá a la población objetivo.

Vulnerabilidad de los individuos

Existen distintas concepciones sobre el término de vulnerabilidad, de acuerdo con distintos ámbitos de atención. Por ejemplo, la Oficina de las Naciones Unidas para la Reducción de Riesgo de Desastres (UNISDR) señala que la vulnerabilidad es la incapacidad de resistencia cuando se presenta un fenómeno amenazante o la incapacidad para reponerse después de que ha ocurrido un desastre. Esta definición se asocia ante riesgos de desastres naturales; sin embargo, se puede extrapolar la definición a otros ámbitos como los riesgos en un sentido más

amplio.[94] Otra definición de la Federación Internacional de Sociedades de la Cruz Roja señala a la capacidad disminuida de una persona o grupo de personas para anticiparse, hacer frente y resistir los efectos de un peligro natural o causado por la actividad humana, y para recuperarse de los mismos. En este concepto ya se aborda a la vulnerabilidad de forma más cercana a la actividad humana y por lo tanto a la definición que pudiera utilizarse para el INAI.[95]

En este documento, se utilizará un concepto relacionado con la incapacidad de las personas para anticiparse, hacer frente y resistir los efectos derivados de actividades humanas relacionadas con el uso y mal manejo de datos personales, ya sea por su manejo o robo.

Número de titulares

Este rubro consiste básicamente en la población potencial que está expuesta a un riesgo relacionado con el mal uso de sus datos personales. Es decir, la población que se vincula a un sector en particular o que pertenece a un grupo de población identificado con riesgo de exposición sobre datos personales.

Capacidad para posicionar el derecho

En este rubro se hace referencia a la capacidad que tienen las personas dentro de un sector o un grupo identificado con riesgo asociado al mal uso de sus datos personales, y que pueden identificar una posible vulneración al derecho de privacidad de datos personales, pero que también puedan ayudar a la transmisión de la identificación del derecho a otras personas y la denuncia en caso de que se identifique alguna situación de riesgo latente o de facto.

Costo efectividad de la estrategia en el sector o población

En este rubro se analizará qué estrategia por tipo de sector o grupo podría tener un mayor beneficio positivo en términos del costo y la efectividad de su implementación. Este rubro se analizará de forma cualitativa, al igual que en los casos anteriores en función de que no existen datos que permitan analizar posibles estrategas ya emprendidas sobre dichas poblaciones.

Importancia del mercado

Finalmente, se analizará la importancia del mercado como uno de los determinantes para definir y priorizar la estrategia de protección del derecho de datos personales. En este caso se utilizará un criterio económico para los sectores. En el caso de los grupos de población este rubro no se considera el criterio económico de primera mano pero una posible aproximación podría ser el valor del PIB per cápita por el número de titulares. Si bien es

[94] Consultado en http://www.unisdr.org/2004/campaign/booklet-spa/page8-spa.pdf.
[95] Consultado en http://www.ifrc.org/es/introduccion/disaster-management/sobre-desastres/que-es-un-desastre/que-es-la-vulnerabilidad/

una medida que no es comparable con la importancia del mercado, refiere a un valor monetario en un periodo de tiempo.

Importancia para el impulso del derecho a la protección de datos

La identificación de la población objetivo constituye uno de los aspectos básicos del diseño de instrumentos de política pública. Una vez que se ha definido adecuadamente el problema a resolver, se requiere caracterizar, a partir de criterios socioeconómicos, demográficos, o de ubicación territorial, al grupo de personas que lo padecen,[96] y hacia las cuales se dirigirán los esfuerzos institucionales, como transferencias de recursos, apoyos en especie o bienes y servicios, con la intención de modificar sus condiciones de manera positiva. Esta síntesis sin embargo, guarda una complejidad mayor cuando se está frente a la intención de desarrollar un plan de educación cívica cuyo propósito es fortalecer el ejercicio de un derecho que, por definición, abarca a toda la población del país, como lo es el de la protección de datos personales, ya sea por el riesgo de que se utilicen con fines comerciales o por riesgos a la integridad de la persona por utilizar sus datos para fines ilícitos o se afecte la esfera más íntima de la persona.

La identificación de la población objetivo es esencial por partida doble: tanto por las definiciones formales en el diseño del instrumento, como porque el reconocimiento correcto de la misma permitirá diseñar las herramientas *ad hoc* que permitan garantizar su participación como el recurso más eficaz para fortalecer una cultura de protección de la privacidad desde la posición de los titulares del derecho.

Así, las posibilidades de éxito en el conocimiento y ejercicio del derecho dependen más que nunca de una estrategia innovadora que desde su origen logre permear, por distintos medios y formas, en todos los individuos, los que la promueven y que la deben hacer propia. Aunque el derecho es general, es necesario promoverlo mediante instrumentos que consideren un enfoque diferenciado, de acuerdo con características específicas de la población: por grupo de edad, por el número de titulares, por la sensibilidad de los datos, o por el tipo de servicios utilizados y que impliquen un mayor riesgo a la privacidad. La Estrategia de Educación Cívica y Cultura del INAI entonces requiere incluir un su planteamiento a diversas poblaciones objetivo, más aún cuando la implementación de la EECyC necesita del involucramiento de las personas, sea porque está en condiciones de mayor vulnerabilidad de que su privacidad sea violentada, por ejemplo los usuarios de servicios financieros o de telecomunicaciones, o porque el posicionamiento del derecho y su ejercicio puede garantizar mayores resultados

[96] Con base en Lineamientos generales para la elaboración de diagnósticos de cuyos resultados se obtienen propuestas de atención a programas de desarrollo social, numeral 6.2 que contiene la definición de población objetivo y su caracterización, publicado en el Diario Oficial de la Federación el 7de mayo de 2009. Consultar en línea en : http://dof.gob.mx/nota_detalle.php?codigo=5089652&fecha=07/05/2009

en el largo plazo, si se adopta desde etapas tempranas e incluso como parte de su formación educativa, por ejemplo los niños y jóvenes.

De este modo, como ya hemos mencionado, uno de los aspectos más sensibles en la definición de la población objetivo se vincula con el riesgo, que es un aspecto clave en el estudio y la definición de herramientas para la protección de datos y más que nada, para identificar a la población objetivo a la que se deben dirigir las acciones.

La noción de riesgo en la protección de datos personales

En materia de privacidad, se ha considerado al riesgo como la probabilidad de utilización de los datos personales de forma no autorizada por parte de los sujetos obligados, que pueda afectar el entorno personal, social, económico o profesional de los titulares del derecho en los límites de su privacidad[97].

Si bien aún está sometida a revisión, y no expresa un criterio concluyente puesto que datos no sensibles en un contexto sí pueden serlo en otro, únicamente con fines ilustrativos el INAI desarrolló una metodología de análisis de riesgo que conjunta tres variables posibles que afectarían la percepción del valor de los datos personales para un atacante: Beneficio, Accesibilidad y Anonimidad, conocida como metodología BAA.[98]

1) **Beneficio para el atacante**. Aquellos datos personales que representen mayor beneficio tienen más probabilidad de ser atacados (por ejemplo, beneficio económico por venderlos o usarlos).

2) **Accesibilidad para el atacante.** Aquellos datos personales que sean de fácil acceso tienen mayor probabilidad de ser atacados (por ejemplo, miles de personas pueden acceder a la vez a una base de datos a través de un sitio web, pero sólo unas cuantas lo podrían hacer a un archivero).

3) **Anonimidad del atacante.** Aquellos datos personales cuyo acceso represente mayor anonimidad tienen más probabilidad de ser atacados (por ejemplo, internet es un medio más anónimo que presentarse físicamente en las instalaciones de una empresa).

La metodología BAA de análisis de riesgos, facilita a los responsables una aproximación a la identificación y priorización de la información que requiere protección; considerando los tipos de datos personales, la sensibilidad de los mismos, y el número de titulares, para determinar el valor del riesgo de los datos que representa para un

[97] Retoma elementos de Davara Rodríguez, citado en INAI (2004) Estudio sobre Protección de Datos, México, 2004, así como de la Ley.
[98] Instituto Federal de Acceso a la Información y Protección de Datos Personales, Metodología de Análisis de Riesgo BAA, 2013, p. 2-4 consultado en línea en : http://inicio.ifai.org.mx/DocumentosdeInteres/Metodologia_de_Analisis_de_Riesgo_BAA_nuevo_aviso.pdf

atacante. La siguiente tabla clasifica los datos personales en cuatro categorías por nivel de riesgo inherente; esta sistematización permite mejorar la seguridad y contribuir a la mitigación del riesgo.

Clasificación de riesgo de los datos personales[1/]	
Nivel de riesgo	**Tipo de datos personales**
Riesgo inherente bajo **Información general de una persona física identificada o identificable**	Datos de identificación y contacto o información académica o laboral, tal como nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo y lugar de trabajo, idioma o lengua, escolaridad, cédula profesional, información migratoria
Riesgo inherente medio	
Datos que permiten conocer la *ubicación física* de la persona	Dirección física, información relativa al tránsito de las personas dentro y fuera del país, y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más. Por ejemplo: dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etcétera
Datos que permitan inferir el *patrimonio* de una persona	Saldos bancarios, estados y/o números de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, finanzas sueldos y salarios, servicios contratados. Incluye el número de tarjeta bancaria de crédito y/o débito
Datos de *autenticación* de los usuarios	Contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, identificaciones oficiales, inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona
Datos *jurídicos*	Antecedentes penales, amparos, demandas, contratos, litigios y

Clasificación de riesgo de los datos personales[1/]	
Nivel de riesgo	**Tipo de datos personales**
	cualquier otro tipo de información relativa a una persona que se encuentra sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa
Riesgo inherente alto **Datos personales sensibles de acuerdo con la ley**	Incluyen datos de salud, se refieren a la información médica que documente el estado de salud física y mental, pasado, presente o futuro, información genética, origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, referencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular
Riesgo inherente reforzado **Los *datos de mayor riesgo* son los que de acuerdo a su naturaleza derivan en mayor beneficio para un atacante**	Información adicional de tarjeta bancaria: considera el número de la tarjeta de crédito y/o débito combinado con cualquier dato relacionado o contenidos en la misma como fecha de vencimiento, códigos de seguridad, datos de la banda magnética o número de identificación personal (PIN)
Las *personas de alto riesgo* son aquellas cuya profesión, oficio o condición están expuestas a una mayor probabilidad de ser atacadas debido al beneficio económico o reputacional que sus datos personales pueden representar para un atacante	Líderes políticos, religiosos, empresariales, de opinión y cualquier persona considerada como personaje público. Cualquier persona cuya profesión esté relacionada con la impartición de la justicia y la seguridad nacional. El tratamiento de los datos de personas de alto riesgo involucra que la base de datos contiene nombres de figuras públicas que pueden ser reconocidas a primera vista, así como información personal donde se infiera o se relacione explícitamente con su profesión, puesto o cargo en combinación con datos de identificación como nombre, domicilio, entre otros.

Clasificación de riesgo de los datos personales[1/]	
Nivel de riesgo	**Tipo de datos personales**
[1/] Con base en: Instituto Federal de Acceso a la Información y Protección de Datos Personales (2013) Metodología de Análisis de Riesgo BAA. Al respecto se remarca la aclaración del INAI respecto a que las categorías se desarrollaron exclusivamente para la aplicación de la metodología, pero no pueden ser consideradas como un criterio emitido por el Instituto; más aún cuando el pleno del INAI no ha emitido criterios institucionales al respecto, además de que se asume que ciertos datos personales que pudieran no ser sensibles, pueden llegar a serlo dependiendo del contexto en que se trate la información.	

Complementariamente, de acuerdo con las "Recomendaciones en materia de seguridad de datos personales" emitidas por el INAI, se entiende al "riesgo como una combinación de la probabilidad de que un incidente ocurra y de sus consecuencias desfavorables; de modo tal que al determinar el riesgo en un escenario específico de la organización, se pueda evaluar el impacto y realizar un estimado de las medidas de seguridad necesarias para preservar la información personal" [99].

Las recomendaciones del INAI parten de la definición sobre datos personales sensibles de la LFPDPPP e identifican los factores que permitan determinar las medidas de seguridad para su control o mitigación.

> "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 éste. 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".

A. Factores para determinar las medidas de seguridad

I. El riesgo inherente por tipo de dato personal;
II. La sensibilidad de los datos personales tratados;
III. El desarrollo tecnológico; y
IV. Las posibles consecuencias de una vulneración para los titulares

Adicionalmente, el responsable debe procurar tomar en cuenta los siguientes elementos:

I. El número de titulares;
II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;

[99] En Diario Oficial de la Federación, 30 de octubre de 2013, publicado por el IFAI "Recomendaciones en materia de seguridad de datos personales, 12 pp., p.2. consultado en línea en: http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013

III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y

IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.

Las experiencias internacionales en materia de protección de datos incorporan metodología basadas en el análisis de riesgos para la identificación y definición de medidas de seguridad. En la siguiente tabla se condensan diferentes nociones sobre el concepto, así como ciertos aspectos relevantes presentados en algunos países revisados para efectos de este estudio, y que cuentan con fuerte marco legal e institucional en materia de protección de datos.

Concepto de riesgo en experiencias internacionales					
Concepto	**INAI (México)[1/]**	**AEPD (España)[2/]**	**CNIL (Francia)[3/]**	**ICO (Reino Unido)[4/]**	**CIP (Ontario, Canadá)[5/]**
Qué es el riesgo	Una combinación de la probabilidad de que un incidente ocurra y de sus consecuencias desfavorables[1/]	Probabilidad de que una amenaza se materialice aprovechando una vulnerabilidad de los sistemas de información o, la probabilidad de que ocurra un incidente que cause un impacto con un determinado daño en los sistemas de información	Escenario que describe un evento temido o indeseable y todas las amenazas que lo harían posible. Es estimado en términos de severidad y probabilidad.	Es un evento o causa que provoca incertidumbre en los resultados de las operaciones de la ICO.	Los riesgos de privacidad son principalmente de operación, definidos como aquellos con probabilidad de causar alguna pérdida o daño ya sea directo o indirecto; suelen ser resultado de: procesos y sistemas internos inadecuados o inútiles; a problemas relacionados al recurso humano que labora en una organización; y, a eventos externos. También se pueden relacionar con riesgos atribuibles a proveedores externos de la organización (outsourcing), ya que se trata de un área a menudo descuidada.
Aspectos relevantes relacionados con el enfoque de riesgo utilizado en cada país	El IFAI recomienda a los sujetos obligados la adopción de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP) basad en el ciclo PHVA (Planear-Hacer-Verificar-Actuar) El análisis y medidas de seguridad implementadas deben enfocarse en la protección de datos personales contra daño, pérdida, alteración, destrucción o el uso , acceso o tratamiento no autorizado, y vulneraciones Al determinar el riesgo en un escenario específico por la organización, se puede evaluar el impacto y realizar un estimado de las medidas de seguridad para preservar la información personal	Los **riesgos** pueden ser de dos tipos: El primero afecta a las personas cuyos datos son tratados; se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización fraudulenta de los mismos. El segundo es que la organización no haya implantado una correcta política de protección de datos, haberlo hecho con descuido, sin mecanismos de planificación, implantación, verificación y corrección eficaces.	El nivel de riesgo es estimado en términos de severidad y probabilidad. La severidad representa la magnitud de un riesgo; depende del nivel de identificación de ciertos datos personales con el nivel de consecuencias de los impactos potenciales. La probabilidad representa la factibilidad de que un riesgo ocurra; depende del nivel de las vulnerabilidades con que cuenta una estructura de apoyo al enfrentar el nivel de capacidades de las fuentes de riesgo. Los riesgos deben ser identificados y estimados en términos de severidad, para aquellos cuya severidad es alta, se deben identificar las amenazas que los podrían hacer posibles y estimar la probabilidad de ocurrencia.	Los riesgos representan oportunidades y amenazas. **Opciones para tratar con los riesgos** **Tolerar**: Si no es posible reducir un riesgo en un área específica (o si hacerlo sería desproporcionado) se puede tolerar, no hacer nada. **Tratar**: Reducir el riesgo de manera sensible identificando acciones mitigadoras **Transferir**: Transferencia a otras organizaciones, utilizando aseguradoras o trasladando un área determinada de trabajo. **Terminar**: Poner fin a un determinado proyecto en el cual la mitigación de los riesgos sea imposible o inviable desde la perspectiva de costo-beneficio.	Una efectiva administración de riesgos de privacidad es de naturaleza eminentemente preventiva, se esfuerza por eliminar los riesgos de privacidad antes de que ocurran. Se puede lograr con el diseño efectivo de medidas protectoras de la privacidad apoyadas en tecnología y procesos que logren consolidarse en un modo operativo estándar de la organización en cuestión.

Fuente: Elaboración propia con base en las siguientes fuentes

[1/] "Recomendaciones en materia de seguridad de datos personales ", publicado en el Diario Oficial de la Federación el 30 de Octubre de 2013. Consultado en : http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013

[2/]"Guía para una Evaluación de Impacto en la Protección de Datos Personales", de la Agencia Española de Protección de Datos, 2014, 72 pp, pág 21-22. Consultada en línea en: **https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf**

[3/] Commission Nationale de l´Infromatique et des Libertés (2012) Methodology for privacy risk management. How to implement the Data Protection Act, Francia, 31 pp. Consultado en : http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

[4/] ICO (2011) Políticas y Procedimientos de Administración de Riesgos, Versión 1.1.8 Enero de 2011, p. 10 Consultado en línea en : https://ico.org.uk/media/about-the-ico/policies-and-procedures/1903/ico_risk_management_policy_and_procedures.pdf

[5/] **Comisionado de Información y Privacidad de Ontario, Canadá (2010) Administración de Riesgos de Privacidad: Construyendo la protección de privacidad como un marco de administración de riesgos para asegurar que los riesgos de privacidad sean tratados por *default*", 27 pp.** Consultado en línea en **https://www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf**
)

De este modo puede observarse que, en general, la noción de riesgo entraña la concepción de un evento cuya materialización no se desea; consiste en un acontecimiento no deseable que puede ocurrir el cual depende de dos aspectos que al combinarse pueden acarrear consecuencias de grado variado, se trata de ***severidad o impacto*** y ***probabilidad de ocurrencia.***

En ese sentido, la estimación del nivel de riesgo se convierte en un aspecto central para la protección de los datos personales. En términos de la CNIL, la agencia francesa de protección de la privacidad, el Nivel de Riesgo = Severidad + Probabilidad. A partir de esta consideración desarrolla la siguiente matriz sobre diferentes grados de riesgo.

Respuestas ante el nivel de riesgo	
Nivel de riesgo	**Qué hacer**
Riesgos con severidad y probabilidad altas	Deben ser evitados o reducidos absolutamente a través de la implementación de medidas de seguridad orientadas a reducir tanto la severidad como la probabilidad. Idealmente, se debe tener cuidado para asegurar que este tipo de riesgos sean atendidos inclusive por medio de medidas independientes de prevención (acciones tomadas previamente a un evento perjudicial), protección (acciones tomadas durante el evento perjudicial) y recuperación (acciones tomadas posteriormente al evento perjudicial).
Riesgos con alta severidad y baja probabilidad	Deben ser evitados o reducidos a través de la implementación de medidas de seguridad que reduzcan ya sea su severidad o su probabilidad. El énfasis debe darse a las medidas de prevención
Riesgos con baja severidad y alta probabilidad	Deben ser reducidos a través de la implementación de medidas de seguridad que reduzcan su probabilidad. El énfasis debe darse en las medidas de recuperación.
Riesgo con severidad y probabilidad bajas	Deben asumirse, especialmente si el tratamiento de otros riesgos conduce a su tratamiento
Fuente: Elaboración propia con base en Commission Nationale de l´Infromatique et des Libertés (2012) Methodology for privacy risk management. How to implement the Data Protection Act, Francia, 31 pp. p.19http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf	

La concretización del riesgo puede depender en cierto sentido de la capacidad y/o características del sujeto, el costo-efectividad de la concretización misma, así como de la vulnerabilidad a que esté expuesta la información. Algunos riesgos generales pueden traducirse en[100]:

- Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales.
- Pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el responsable del tratamiento.
- Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas, en particular, cuando se producen pérdidas de datos personales.
- Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por una deficiente gestión de la privacidad.
- Falta de conocimiento experto sobre protección de datos y canales de comunicación con los afectados.

Asimismo, algunas de las fuentes de riesgo pueden incluir:[101]

- Personas que pertenecen a la organización: funcionarios, encargados de manejar sistemas de información y bases de datos personales.
- Personas externas a la organización: sujetos de derecho, proveedores, organizaciones de la sociedad civil, dependencias de gobierno, actividad humana en general.
- Fuentes no humanas: virus cibernéticos, desastres naturales, materiales inflamables, epidemias, etcétera.

Existe también la noción de ***riesgo residual***, el cual puede ser entendido como la posibilidad de daño o perjuicio que subsiste después de haber suministrado medidas de control y prevención; en otras palabras se conforma por aquella porción de riesgo imposible de erradicar por completo, de las actividades de una organización. La determinación sobre este tipo de riesgos también se basa en los niveles de severidad y probabilidad.

Puede considerarse, para el caso mexicano, que en algunos casos, la EECyC se debe plantear a partir del riesgo residual, por ejemplo en el sector salud donde existen controles sólidos asociados a las previsiones legales en torno al manejo de los expedientes médicos y las sanciones por su utilización indebida; el expediente es un

[100] . "Guía para una Evaluación de Impacto en la Protección de Datos Personales", de la Agencia Española de Protección de Datos, 2014, 72 pp, 23-23 p. en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
[101] CNIL, Metodología para la administración de riesgos de privacidad 2012, p. 7. En http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

documento que condensa información de la salud de las personas y su manejo se encuentra protegido por la legislación en la materia. No obstante, con base en la consideración sobre el número de titulares que congregaría el sector salud es indispensable plantear a estos usuarios dentro de las prioridades de la población objetivo, si bien, puedan diseñarse intervenciones de carácter general como ocurre en otras realidades en las que ellas se dan paralelamente con acciones enfocadas en sectores clave (como el de salud), con un nivel de riesgo específico (financiero o de telecomunicaciones) o por potenciar la posibilidad de posicionar el derecho a la protección de datos (niñez y juventud).

La variedad de criterios que pueden estar detrás de la definición de estrategias, líneas de acción y objetivos de la EECyC, facilita un abordaje diferenciado, y probablemente tiene una contribución para fortalecer las acciones que desde otro ámbito legal, se desarrollen para la atención de algún servicio como lo es el de la salud que ya se ha comentado. Asimismo, es altamente probable que el desarrollo de una cultura de protección de datos tenga una incidencia directa o indirecta en el comportamiento de algunos indicadores relacionados con la prevención de delitos, sin embargo, no debe perderse de vista que la aspiración de la EECyC debe materializarse con base en un marco jurídico propio, si bien puede contribuir en otros ámbitos de política pública, y que en todo momento se debe implementar con base un conjunto de facultades específicas que constituyen el telón de fondo, que no puede ser rebasado, para el diseño y ejecución de acciones específicas por parte de la instancia responsable, garante y con facultades precisas en torno a la protección de datos personales. Así, la educación en torno al ejercicio de un derecho no implica la extensión de facultades para el INAI, pues de hecho aún pensando en una EECyC con enfoque amplio, el instituto no necesariamente está en plenas posibilidades de garantizar la protección[102].

B. Experiencias Internacionales

Las experiencias internacionales revisadas en materia de protección de datos diseñan líneas de acción o actividades pensadas para la población en general, para ciertos grupos demográficos, y para usuarios de sectores de servicios particulares como los financieros, los de salud y de telecomunicaciones. En tal sentido, puesto que la EECyC busca que los titulares conozcan el derecho que tienen a la protección de datos personales, pero al mismo tiempo que reconozcan y valoren adecuadamente el riesgo a los que se enfrentan en el otorgamiento de datos personales, es menester que estén en posibilidad de tomar decisiones informadas sobre el otorgamiento de sus datos personales a los sujetos obligados, y en caso de ser necesario, que utilicen los mecanismos establecidos para hacer valer sus derechos y denunciar los posibles incumplimientos por parte de

[102] Piénsese por ejemplo en la comisión de delitos que se perpetran a raíz de la posesión de datos por parte de particulares.

los sujetos obligados. Para lograr lo anterior es necesario dirigir la estrategia a poblaciones objetivo diferenciadas que sean atendidas mediante intervenciones focalizadas y diseñadas de acuerdo con ciertas características de la población objetivo.

Además del riesgo, en esta EECyC, se han tomado en cuenta criterios de costo-efectividad, pues las acciones propuestas para la promoción del derecho a la privacidad, no deben implicar necesariamente un alto costo, ya que podría incrementarse la inviabilidad en términos económicos, políticos y/o técnicos; se plantean acciones que pueden implicar un bajo costo con un alto impacto. También se toman en cuenta los criterios planteados en la propuesta técnica, a saber: por la vulnerabilidad de los individuos, por el número de titulares, por la posibilidad de que estos titulares a su vez promuevan el ejercicio del derecho, por su capacidad de influencia en la opinión pública y por la fuerza e importancia del mercado.

Con base en los elementos anteriores, en el presente documento se integra un planteamiento general sobre la importancia de definir adecuadamente a la población objetivo, tomando en consideración una noción de riesgo, se identifica a los grupos o tipos de titulares que se proponen como población objetivo prioritaria para la estrategia. Al final, se presentan los aliados posibles en la implementación de la EECyC.

Como ya se ha mencionado, uno de los aspectos más sensibles en la definición de la población objetivo se vincula con el riesgo, que es un aspecto clave en el estudio y la definición de herramientas para la protección de datos y más que nada, para identificar a la población objetivo a la que se deben dirigir las acciones.

La definición de grupos prioritarios se hace en un primer momento por grupo demográfico, considerando los riesgos principales a los que se encuentra expuesto así como su capacidad de posicionamiento y réplica del derecho en un espacio más amplio, para que, en un segundo momento se dé paso a la cuantificación de la población objetivo. Por supuesto, se tiene considerado que estos aspectos permitirán definir la (s) instancia (s) y la (s) estrategia (s) a través de las cuales se atenderá a la población objetivo.

La delimitación de los niveles de riesgo tiene un reconocimiento implícito a ciertos campos en los que es posible identificar una mayor probabilidad de ocurrencia de desprotección de la privacidad como: los usuarios de servicios financieros, de salud y los de telecomunicaciones. Las experiencias revisadas a nivel internacional permiten constatar una preocupación en el mismo sentido, a pesar de que el enfoque o los instrumentos de atención puedan diferenciarse entre sí. Asimismo, es claro el reconocimiento respecto a la importancia de promover el ejercicio del derecho en grupos etéreos como la niñez y la juventud, ya que se apuesta a obtener mayores resultados si la promoción se dirige hacia personas en etapas tempranas de la vida para lograr una cultura de protección a la privacidad en el largo plazo.

En Argentina una buena parte de los esfuerzos institucionales se concentran en la niñez y la juventud a través del Programa "Con vos en la web"[103], impulsado también a través de la iniciativa presidencial "Conectar Igualdad"[104], que fortalece el conocimiento sobre seguridad de la información al usar el internet; asimismo, concientiza sobre los riesgos y amenazas en la utilización de las nuevas tecnologías de la información. El programa cuenta con un conjunto de actividades desarrolladas de manera permanente con el apoyo de la UNICEF. Adicionalmente, las guías y manuales que se encuentran en la web están pensados para personas en ciertos grupos de edades o con ocupaciones que permiten propiciar la difusión del derecho, por ejemplo los maestros, los padres de familia y profesionistas dedicados a la defensa legal. Por supuesto, también está el enfoque concentrado en atender a sectores como el financiero, a partir de una preocupación en torno al robo de identidad para evitar fraudes. De acuerdo con la entrevista que esta consultoría realizó al personal clave de la Dirección Nacional de Protección de Datos Personales, la forma en que se van incorporando o definiendo nuevas herramientas o áreas temáticas de interés en el terreno de la protección de datos, es a partir de las quejas presentadas por la población, atendiendo al sector específico del que provienen, o por la demanda de información particular que hace la ciudadanía.

En el caso de Australia se desarrolla un conjunto de instrumentos que están enfocados a prevenir riesgos en ciertos sectores como los ya mencionados, en el campo de la salud incorpora a los servicios en línea y los registros electrónicos en este sector, así como los datos de los contribuyentes. Canadá y en general los países revisados: Nueva Zelanda, Reino Unido, España y Francia, guardan similitudes en los sectores priorizados así como en la identificación de poblaciones donde el derecho puede estar mejor posicionado, por supuesto con algunos matices como por ejemplo al utilizar la tarjeta de crédito, la provisión del número de seguridad social, seguridad al portar información personal que, en Australia por ejemplo, abarca la posibilidad de mantener el anonimato y no proporcionar el nombre. También es posible observar un interés por el riesgo de compartir información que puede propiciar un excesivo o abusivo uso de la misma con fines publicitarios o de comercialización, en este caso Argentina cuenta con el Registro "No Llame Más" para evitarlo y España pone a disposición del público información para que la gente sepa qué hacer para que sus datos dejen de ser utilizados con fines de publicidad y comerciales. En casos como el de Francia y Nueva Zelanda se promueven acciones de carácter masivo para promover el derecho como el concurso de la privacidad y la semana de la privacidad respectivamente. El primero, es decir, el concurso se enfoca en jóvenes y pretende concientizarlos en torno a los riesgos de manejar información en internet, particularmente al compartir fotos. La semana de privacidad busca promover, con el apoyo de diferentes socios, tanto gubernamentales como privados, la importancia de la

[103] Presidencia de la Nación, "Con vos en la web capacitó 450 alumnos durante el mes de agosto", 2015, (en línea), disponible en: http://www.jus.gob.ar/datos-personales/novedades.aspx (Consultado el 26 de septiembre de 2015)
[104] Un programa que ha permitido entregar una *notebook* a cinco millones de niños argentinos.

Conectar Igualdad, disponible en: http://www.conectarigualdad.gob.ar/ (Consultada el 20 de noviembre de 2015)

protección de los datos. Entre otras acciones destacan las dirigidas a capacitar a la ciudadanía o bien, a acercar información para sensibilizarla en torno a este tema, es particularmente importante el "E-learning Privacy Training Modules" y la Privacy Awaraness Week en Nueva Zelanda y Australia respectivamente; la oferta de cursos en Inglaterra y Argentina es muy amplia. En el caso de Brasil que no cuenta con una instancia reguladora, y es necesario recurrir a los tribunales para que se protejan, es posible identificar un avance importante en términos legislativos para la seguridad en el internet.

A partir del análisis de los instrumentos diseñados para la promoción del derecho a la protección de datos personales en diferentes países, observamos que la definición de la población objetivo se da en distintos niveles, con base en el riesgo, en sectores en que éste se agudiza de manera sensible, y con base en la posibilidad de la construcción y posicionamiento de una cultura de derecho a la protección de datos personales si se difunde entre ciertos grupos en particular. Por ello las naciones tienen variados instrumentos con un alcance en distinta profundidad puesto que en tanto se promueve el derecho de manera general, se diseñan herramientas enfocadas a un grupo particular de acuerdo con las principales problemáticas detectadas.

De conformidad con algunas fuentes consultadas[105] en torno a la protección de datos personales, el tema incluye en su abordaje la revisión de la legislación aprobada en diversos países, lo que hace posible identificar los sectores de principal interés para las autoridades, aunque también se identifica un énfasis con algún enfoque en particular, sea del sector financiero, el uso de tecnologías de la información o las redes sociales, aun así es necesario fortalecer el abordaje de la protección de datos con base en un diseño sustentado en la definición de poblaciones objetivo específicas. En el caso de Inglaterra se identifican reglas especiales para el uso de las telecomunicaciones, correo electrónico y marketing directo por teléfono y fax, pero por otro lado, la privacidad es considerada como un derecho humano a partir de una revisión de diferentes experiencias ubica diferentes campos temáticos como centro de interés en la protección de datos por ejemplo en: los mercados financieros y de consumidores, las infracciones a la seguridad en redes sociales como Facebook o los sistemas de votación electrónica y de vigilancia, la creciente comunicación no solicitada, y el riesgo de "descontextualización" de la información en las redes sociales. En el estudio de Noriswadi 2013, se señala que el mayor interés se centra en las tecnologías y el uso del internet con base en la revisión de experiencias en Estados Unidos, el Reino Unido, Malasia y la experiencia europea.

[105] Jay Rosemary y Clarke Jane, "Data Protection Compliance in the UK. A pocket guide", 2008, second edition, Pinsent Masons, IT Governance Publishing, United Kingdom. (documento en PDF)
Gutwirth Serge, Poullet Yves, De Hert Pal (editors) "Data protection in a profiled world", 2010, Bruselas Bélgica
Noriswadi Ismail, Lee Yong Cieh Edwing (editors) "Beyond data protection. Strategic case studies and practical guidance", 2013, Berlín. Germany.

La identificación de la población objetivo para la protección de los datos personales puede identificarse en otros casos, como el canadiense, a partir de 2015, mediante la definición de campos temáticos con base en la literatura, medios de comunicación y reporte académicos; con base en una serie de grupos focales, durante diciembre de 2014, en las ciudades de Vancouver, Toronto, Montreal y Halifax, a partir de preguntas estructuradas. También se realizaron encuentros con "*stakeholders*", así como con 150 representantes de la academia, sociedad civil, grupos de consumidores, del sector privado y el gobierno, incluyendo oficinas de territorios provinciales con normatividad propia en materia de protección de datos[106]. De acuerdo con los temas propuestos, se identifican diferentes campos temáticos.

1. **Economía de la información personal**

   Se trata de visualizar un modelo de negocios no declarado en torno a la utilización de los datos personales con fines de comercializarlos, es decir se utilizan los contactos, los tópicos de interés, y las experiencias de navegación con fines de venta; en suma el interés es que se observe que la información personal está convirtiéndose en un negocio.

2. **Servicios de gobierno y vigilancia**

   Se plantea la preocupación por una mayor utilización de tecnologías en el gobierno para aumentar el intercambio de información entre diferentes niveles de gobierno y organizaciones del sector privado, como una manera de modernizar los servicios a los canadienses.

3. **La protección de los canadienses en un mundo sin fronteras**

   El objetivo se dirige a que se observe a la economía global como una red integrada donde la información personal puede moverse rápidamente en el mundo, incluyendo países que no cuentan con protecciones adecuadas o son muy débiles, lo que representa un peligro para los canadienses.

4. **Reputación y privacidad**

   El tema busca hacer conciencia sobre la forma en que los usuarios construyen directamente su propia privacidad en el internet, a partir de la publicación de fotos, comentarios en línea, etcétera.

5. **El cuerpo como información**

   Existe una mayor información sobre los "cuerpos" de las personas en la red, que es proveída a través de dispositivos que pueden digitalizarse y conectarse fuera de línea sin que el propietario lo sepa, lo cual puede tener un impacto decisivo en la privacidad con efectos adversos.

6. **Fortalecimiento de la rendición de cuentas y la salvaguarda de la privacidad**

[106] Office of the Privacy Commissioner of Canada, "The OPC Privacy priorities 2015-2020. Mapping a course for greater protection", 2015 Consultado en línea en : https://www.priv.gc.ca/information/pub/pp_2015_e.pdf)

Las organizaciones se encuentran obligadas a almacenar y procesar adecuadamente y de manera responsable la información que manejan, como una práctica de gestión que se actualice, y mantenga continuamente nuevas formas de proteger la privacidad brindando las garantías de seguridad eficaz en un mundo en el que proliferan las amenazas de pérdida, robo o mal uso de la información, este es un aspecto sobre el cual los gobiernos deben rendir cuentas.

El Parlamento Europeo[107] plantea la utilización de un enfoque en la protección de datos a partir de la consideración de una mayor vulnerabilidad de algunos grupos, por ejemplo a los niños y las víctimas de crímenes. También forzó algunos cambios para el transporte aéreo y el intercambio de datos bancarios como un compromiso a preservar la privacidad en un contexto de mayor uso del internet. En particular, las áreas de interés en la protección de datos, que está estrechamente relacionado con los derechos civiles, del Parlamento Europeo son las siguientes:

1. **Mejor protección a las víctimas.** El Parlamento impulsa la prevención del abuso en línea, la persecución de los delincuentes, la eliminación de la pornografía infantil, promoviendo nuevas penalidades que incluyen castigos más severos; también promueve la atención a la lucha contra el tráfico de niños y la protección a las víctimas de sus agresores, evitando que la víctima deba cambiarse de residencia y que sea extensiva esta medida que aplica sólo en casos de violencia de género a la víctima de cualquier crimen.
2. **Protección de la privacidad, información personal y libertad en el internet.** Se requiere poner límites a la colecta masiva de información personal compartida en redes sociales, motores de búsqueda, y otros proveedores de servicios en línea.
3. **Derechos para los solicitantes de asilo y en la vigilancia de las fronteras.** El Parlamento señala que deben existir procedimientos sencillos y comunes, así como plazos adecuados para el manejo de las solicitudes de asilo y apoyo a los países que enfrentan una afluencia de solicitantes muy marcada.

Como puede verse, la importancia de la población objetivo es fundamental en la promoción del derecho de protección de datos. Ella puede seleccionarse con base en un enfoque centrado en el sector con un mayor riesgo de vulnerabilidad a la violación del derecho, o bien puede enfocarse exclusivamente en un grupo de edad específico, tal como ocurre en otras realidades que cuentan con políticas, programas e instrumentos de niños o jóvenes. Estos abordajes también pueden complementarse con acciones que utilizan un enfoque desde la

[107]European Parliament, disponible en: http://www.europarl.europa.eu/elections-2014/en/press-kit/civil-liberties-data-privacy-protecting-the-vulnerable (Consultada el 19 de noviembre de 2015)

vulnerabilidad de un grupo social, lo que sin duda contribuye a contar con una EECyC que abarque a la mayor parte de los individuos.

En el caso de México, a través del INAI se promueven acciones hacia la concienciación en torno al derecho a la privacidad[108] que se complementan con acciones sustantivas del Instituto, a partir de la aplicación de procedimientos, solicitudes y recursos como: (i) procedimiento de verificación; (ii) procedimiento de protección de derechos; (iii) procedimiento de imposición de sanciones; (iv) solicitudes de acceso y corrección de datos personales recibidas por la Administración Pública Federal (APF); así como (v) recursos de revisión sustanciados por el INAI en relación con solicitudes de acceso y corrección de datos personales en posesión de la APF. Estos elementos también pueden considerarse en el diseño de la EECyC, pues a final de cuentas son indicadores claros sobre la toma de conciencia en torno a un derecho por parte de los individuos. Si se cobra conciencia de la posesión del derecho a la protección de datos personales y a la privacidad, es posible esperar la aplicación de un mayor número de procedimientos hacia particulares o instancias gubernamentales, a iniciativa de los titulares del derecho.

De acuerdo con el Informe al Congreso de la Unión respecto a la Protección de Datos Personales, rendido por el INAI en 2014, en la norma en materia de protección de datos personales, si se trata de particulares, de dependencias o entidades de la APF, se registran tres tipos de expedientes: de orientación, cuando el INAI no es competente para conocer el asunto; de investigación preliminar, cuando la denuncia se desprende de presuntas violaciones a la LFPDPPP, a la LFTAIPG o a la normatividad en la materia (para contar con elementos necesarios parar iniciar un procedimiento de verificación); y de verificación, en función de las determinaciones del Pleno respecto al inicio de dicho procedimiento.

Con base en la LFPDPPP, las sanciones son impuestas una vez que culmina un procedimiento de imposición de sanciones en el cual el responsable tiene la oportunidad de desvirtuar, mediante pruebas, que es falso el hecho imputado. La sanción se origina como resultado de la inconformidad de un titular después de un procedimiento de protección de derechos ARCO, o bien como resultado de un procedimiento de verificación. En el caso del procedimiento de protección de derechos ARCO, el INAI promueve la conciliación; este procedimiento tiene su

[108] Destacan por ejemplo, la emisión de la ***Guía Práctica para generar el aviso a la privacidad; Recomendaciones para la designación de la persona o departamento de datos personales, Guía práctica para ejercer el derecho a la protección de datos personales, y Guía práctica para la atención de solicitudes de ejercicio de los derechos ARCO***, cuyos objetivos son proporcionar a los titulares de los datos personales la información básica para el ejercicio del derecho de protección de datos personales, así como facilitar al responsable del tratamiento de los datos personales el cumplimiento de las obligaciones previstas en la Ley y Reglamento; la puesta a disposición del aviso de privacidad; la designación de la persona o departamento de datos personales, y la atención de solicitudes de derechos ARCO. Al respecto, véase IFAI (2014) Informe a Congreso de la Unión respecto a la Protección de Datos Personales, p. 106. Consultado en línea en : http://inicio.ifai.org.mx/Informes%202014/Informe%20de%20labores%202014.pdf

origen en una solicitud de protección que un titular de datos presenta ante el INAI en virtud de no haber recibido respuesta por parte del responsable o por estar inconforme con la que le hubiera proporcionado con motivo de la solicitud para hacer efectivos sus derechos ARCO.

C. Definición de Población Objetivo y Grupos Prioritarios

Los objetivos de una Estrategia de Educación Cívica y Cultura sobre el Derecho a la Protección de Datos Personales por parte de los titulares con base en la propuesta técnica hecha son:

1. Que los titulares conozcan el derecho que tienen a la protección de sus datos personales.
2. Que los titulares puedan reconocer y valorar adecuadamente los riesgos a los que se enfrentan en el otorgamiento de sus datos personales.
3. Que los titulares puedan tomar decisiones informadas sobre el otorgamiento de sus datos personales a los sujetos obligados.
4. Que los titulares conozcan y utilicen los mecanismos establecidos para hacer valer sus derechos y denunciar los posibles incumplimientos por parte de los sujetos obligados.

La estrategia de educación para protección de datos personales que se propone es estratificada por grupos demográficos y sectoriales de industria. Esta identificación está basada en los segmentos que se considera que pueden ser más riesgosos en el uso de información de datos personales. Para ello, se recurrió a la experiencia de México y otros países sobre los principales sectores que se atienden.

En efecto, las experiencias internacionales revisadas y documentadas en el apartado correspondiente, permiten establecer una orientación en diversas direcciones para la protección de datos personales; en la selección de los grupos y sectores de los países destacó la consideración a un potencial riesgo de vulneración a la privacidad, el señalamiento de algún sector con base en las quejas presentadas por los poseedores del derecho o el interés por posicionarlo en sectores y grupos específicos. De este modo, en la estrategia que se propone, la selección de grupos y sectores se realizó atendiendo a los criterios establecidos en los Términos de Referencia y mencionados ya en el apartado anterior, pero también en el interés mostrado en otras realidades con una mayor raigambre o antigüedad en la política de protección de datos personales.

a. Sectores priorizados en Otros Países

Menores de edad

Entre las experiencias revisadas destaca un interés en la población infantil y en la juventud. En el caso específico de Argentina, para la Dirección Nacional de Protección de Datos Personales, el interés en este grupo de población se apoya en la convicción de que los niños constituyen un grupo en torno al cual es posible lograr el interés de otros actores como los padres y maestros; el programa "Con Vos en a Web", que ya ha sido referido, articula acciones dirigidas a estos tres grupos, colocando a los niños como el actor central. También se reconoce que niños y jóvenes tienen mayores habilidades digitales por lo que posicionar el derecho a la privacidad se vuelve tarea menos complicada frente a otros grupos de edad; así, como se señaló, la difusión sobre este derecho entre menores, se ha impulsado aprovechando la política pública enfocada a disminuir la brecha digital a través del Programa "Conectar Igualdad" (mencionado en el apartado correspondiente) que ha entregado más de cinco millones de notebooks a los niños en ese país, mediante los cuales se hizo llegar información en materia de protección de datos personales.

En el caso de España también se ubican líneas de acción claramente relacionadas con la atención al grupo de población de menores de edad, a los cuales se llega especialmente a través de los padres y madres. La Agencia Española de Protección de Datos ofrece una guía para el ciudadano que es orientadora sobre el tratamiento de datos de niños y niñas, y se pone a disposición del público la guía de recomendaciones enfocadas en que los padres tomen conciencia sobre sus obigaciones con relación a la protección de datos personales de los menores de edad. Los niños y niñas son así uno de los grupos de población de atención especial al que, como en Argentina, también se dirigen acciones sustentadas en las habiidades digitales; de manera más específica, para los menores se ofrecen orientaciones dirigidas a mejorar la seguridad ante el uso de dispositivos electrónicos (teléfonos y tabletas) y las redes sociales. También a través de los maestros se promueve la seguridad en el uso del internet, la protección de la identidad en redes sociales, el uso de la imagen en la web, y protección contra el ciberbullying, sexting o grooming.

Sector Financiero

La protección de los datos en el sector financiero constituye un campo de interés general en las realidades revisadas en particular por el incremento de operaciones en internet. Por ejemplo, la Office of the Privacy Comissioner de Canadá especifica recomendaciones para el uso de crédito a través del internet, el monitoreo para la entrega de los estados de cuenta, la revisión de informes y de crédito anual. Asimismo, el robo de identidad es un aspecto de interés pues su ocurrencia está directamente relacionada con la comisión de delitos financieros, por lo que la protección de datos se orienta a proteger desde el cobro de cheques, al robo de fondos

en cuentas bancarias, prácticas de estafa en tarjetas de crédito, hipoteca de bienes, o falsificación de cheques y tarjetas. En el caso de Argentina también destacan las acciones y medidas enfocadas a la protección de datos personales para evitar el robo de identidad cuyo principal efecto es la comisión de fraudes. La Office of the Australian Information Comissioner obliga a la protección de datos a corporativos de información creditica, y en el caso de Francia se orienta sobre la protección de datos en la Banca de Crédito en particular para asuntos de registros bancarios, medios de pago y las obligaciones de los profesionales.

Salud

En la experiencia de Australia, la protección de datos en el sector salud es particularmente llamativa porque abarca desde proveedores tradicionales de servicios de salud como hospitales privados, médicos, farmacéuticos y hasta aliados profesionales de la salud como pueden ser terapeutas, quiroprácticos y clínicas de pérdida de peso; asimismo, se incluyen servicios de salud en línea. Por otro lado en Canadá la protección de la privacidad alcanza a la información genética, de salud y biométrica. En el caso de Francia la salud se plantea como un tema central pues se consideran como datos sensibles el expediente médico, el expediene farmacéutico y la información que se haya compartido con el médico mediante la web.

Telecomunicaciones

Los proveedores de telecomunicaciones están incluidos como sujetos obligados a la protección de datos en países como Australia, Canadá y España, en esta última se ofrece información específica sobre los derechos de los abonados y usuarios de servicios de telecomunicaciones que permite mantener anónimos los datos de las personas en cuanto dejan de ser necesarios. En el Reino Unido la protección de datos en el sector de telecomunicaciones es clave por lo que su agencia de protección a la privacidad tiene, como parte de su política la guía para el uso seguro de teléfonos inteligentes y otros aparatos de telecomunicaciones.

Comercio electrónico

El comercio electrónico es un tema común en la agenda de las agencias responsabes de la protección de datos personales, por ejemplo, en España se cuenta con la Ley de Servicios de la Sociedad y de Comercio Electrónico (mencionada en el apartado corresponidente) que protege las compras en línea y promueve que la persona con la que se realizan se vuelva identificable, propicia que el comercio de este tipo se de en condiciones de claridad en cuanto a ofertas, promociones, concursos y sorteos y que la procedencia de la publicidad pueda ser identificable. La Agencia Española que protege los datos se enfoca en difundir derechos de exclusión de guías de teléfono y el derecho de no recibir publicidad no deseada. En Argentina, la protección de datos en la práctica del

comercio electrónico ha generado el Registro “No llame más” con fines similares, pues busca limitar la práctica de diseminar datos personales a partir de compras en forma electrónica.

Por otro lado, como se ha identificado con la experiencia internacional, es necesario dirigir una estrategia a la industria de las telecomunicaciones, el comercio electrónico, el sector salud y los servicios financieros. Si bien existen otras industrias más grandes, no es evidente que en otras la transmisión de datos personales constituya un riesgo potencial mayor a las presentadas, de forma que se deba atender con prioridad.

b. Grupos Identificados para su atención en México

Por grupos demográficos

Menores de edad

Al grupo de menores de edad se puede dividir en dos sub-grupos, los niños y niñas de 6 a 11 años y los jóvenes de 12 a 17 años. Esta clasificación es importante porque en el primer grupo, no se considera que los titulares del derecho tengan la capacidad de tomar un juicio adecuado sobre el nivel de riesgo que puede existir al proporcionar sus datos personales en algún sitio físico o electrónico. Por lo tanto, los receptores principales de las acciones que se utilizarían para mitigar los riesgos son los padres o tutores. En el caso de los adolescentes, se asume que los riesgos ya pueden ser identificados por ellos mismos, de forma que las acciones podrían estar dirigidas a ellos mismos y de forma complementaria a los padres. Además, se considera que los adolescentes tienen una mayor exposición al riesgo porque la supervisión de los padres es menor que en el grupo anterior.

En ambos casos, los principales riesgos asociados a la entrega de datos personales y su potencial uso no autorizado para fines comerciales, se vinculan por el uso y exposición a internet, ya que es en estas situaciones donde los niños, niñas y jóvenes pueden entregar información personal. En otros contextos, la exposición al riesgo disminuye porque los adolescentes en este rango de edad, normalmente no contratan servicios de forma directa —en menor medida estos grupos contratan servicios bancarios, pero si lo hacen, es bajo la supervisión de un adulto. Por ejemplo; el “11º Estudio sobre los hábitos de los usuarios de Internet en México 2015” señala que el 47% de los niños inicia su exposición al Internet de los 6 a los 11 años y el 15% de los 12 a los 17 años. También se menciona que el 43% de los niños inicia el contacto con Internet de los 3 a los 6 años; no obstante, en esta edad el riesgo de transmisión de datos personales es menor por la supervisión de los padres y la poca autonomía para la manipilación de esta herramienta. En la misma encuesta se menciona que la penetración de

internautas de seis o más años ha crecido considerablemente. Por ejemplo, en 2006 la penetración del Internet en la población mayor a seis años era del 21% y en 2014 fue del 51%.

Por otro lado, de acuerdo con el INEGI, en 2014, el 42.2% de los niños de 6-11 años de edad y el 79.9% de 12-17 son usuarios de Internet.[109]

Por industrias

Las personas también pueden estar expuestas a distintos niveles de riesgo por el uso y contratación de algunos servicios. Por ejemplo, existe riesgo de que falle el resguardo de sus datos personales por el uso de servicios financieros (bancarios, seguros, etc.), de telecomunicaciones, médicos, videojuegos en línea, uso de internet para fines recreativos y comerciales, entre los más importantes. A continuación se presenta una breve descripción de las industrias que pueden tener un nivel de riesgo en la protección de datos personales.

Industria financiera

Se consideran como parte del universo de empresas pertenecientes a la industria financiera los bancos, sociedades financieras de objeto múltiple, aseguradoras, afores, sociedades corporativas de ahorro y crédito popular, sociedades financieras populares, y las sociedades financieras comunitarias.

En esta industria existen al menos dos riesgos inherentes a la actividad de los usuarios de servicios financieros: el primero es por el uso inadecuado o ilegal de información personal y financiera que resguardan estas instituciones y el segundo es por el uso de plataformas tecnológicas a través de internet para el uso de la información financiera de los usuarios. En el primer caso, el riesgo se considera bajo, ya que estas industrias están ampliamente reguladas y los costos de la venta de esta infomación podrían ser altos. Este es el caso para instituciones financieras grandes; sin embargo, no se debe descartar el riesgo para instituciones de crédito de menor tamaño, donde incluso el ingreso derivado de la venta de datos personales puede ser importante. El riesgo por el uso de plataformas o portales bancarios en internet podría considerarse un riesgo de nivel bajo, por contar con alta seguridad tecnológica.

En este sector existe un organismo regulador específico que es la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) que vigila el cumplimento de las obligaciones de las empresas que pertenecen a dicho sector en varios temas específicos. Sin embargo, la Ley de Protección y Defensa al Usuario de Servicios Financieros prohíbe la distribución de los datos personales y financieros con

[109] "Estadísticas a propósito del Día Mundial del Internet (17 de mayo)". Datos Nacionales, consultado en http://www.inegi.org.mx/saladeprensa/aproposito/2015/internet0.pdf

fines mercadotécnicos o publicitarios[110] y también faculta a la CONDUSEF al establecimiento de un registro de usuarios que no deseen que su información sea utilizada para fines comerciales o de mercadotecnia.

En México alrededor del 39% de la población urbana se encuentra bancarizada y sólo alrededor del 6% de la población rural lo está[111]. Además, del 39% de la población urbana bancarizada, el 78% utiliza internet y su uso se encuentra relacionado con la diversidad y movilidad de los medios de acceso; siendo el teléfono celular el dispositivo preferido al momento de conectarse a internet[112]. Esto es considerado un factor de alto riesgo.

Salud

En este documento se considerará al universo de servicios de salud pública y privada como la población usuaria de servicios de salud. En ésta se incluye hospitales, clínicas, consultorios, médicos particulares, entre otras instalaciones. Además, esto también puede incluir servicios de seguros médicos a través de instituciones financieras especializadas.

El principal riesgo asociado a este sector es derivado de la venta de información personal a terceros que pueda ser utilizada para fines comerciales o laborales. Sin embargo, un riesgo potencial en este sector se origina por la divulgación de información personal altamente sensible que pueda ser utilizada para su discriminación en algún ámbito de su vida. Como en el caso de instituciones financieras, en instituciones grandes el riesgo es menor que en instituciones de menor tamaño o de médicos que conservan información personal. En este sector es importante mencionar que es necesario distinguir entre la transmisión de información con fines puramente comerciales de aquella que puede tener un beneficio médico, la cual es relevante mantener y que las acciones derivadas de este documento no desinhiban una práctica médica con beneficios reales. De hecho la Comisión Europea reconoce la importancia de la protección de datos en el sector salud pero también la transmisión de información con fines médicos. De tal forma, las directivas de la Comisión Europea sobre la protección de datos abordan las particularidades del sector con reglas específicas.[113] Además, se ha identificado que los antecedentes médicos tienen un valor de mercado importante.[114]

---

[110] Ley de Protección y Defensa al Usuario de Servicios Financieros. Artículo 8, Párrafo 4. Consultado en http://www.diputados.gob.mx/LeyesBiblio/pdf/64.pdf

[111] Proteja su dinero "Descubre los hábitos de los usuarios bancarizados en internet", 2014, (en línea), disponible en: http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/servicios-financieros/462-a-un-solo-clic (Consultada el 15 de noviembre del 2015)

[112] *Ídem.*

[113] Directiva de Protección de Datos 95/46/EC, consultada en http://ec.europa.eu/health/data_collection/data_protection/in_eu/index_en.htm#fragment3

[114] http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

El sector salud también es uno ampliamente regulado por diversas instancias de salud en México como la Secretaría de Salud, la Comisión Federal para la Protección de Riesgos Sanitarios (COFEPRIS), Comisión Nacional de Arbitraje Médico (CONAMED) y en este caso fundamentalmente por la NOM-024-SSA3-2012, entre otras normas. Por esta razón, se parte de un riesgo considerado bajo en instituciones grandes y a medida que el tamaño de dichas organizaciones o empresas se reduce, el riesgo es mayor —pues se pueden utilizar los datos para fines comerciales.

En este sector existe un segmento en el cual se puede observar un traslape de los usuarios del sector salud con el sector financiero. Este grupo se refiere a las personas que contratan servicios de seguros de gastos médicos.

Telecomunicaciones

Se considera ususarios del servicio de telecomunicaciones a aquellos que cuenten con algún dispositivo de comunicación en una o dos vías. Por ejemplo, la telefonía celular es un medio de dos vías mientras que la televisión abierta es un medio de una sola vía. En este caso se va a considerar solamente a los subsectores que se basan en comunicación de dos vías, dado que son los que tienen riesgo de transmisión de datos personales. Por ejemplo, para contar con señal de televisión abierta o de radio no se requiere la transmisión de ningún dato personal, ni el uso de estas tecnologías propicia de forma masiva la transmisión de esta información.

El sector de las telecomunicaciones es otro sector regulado desde hace varios años por la Comisión Federal de Telecomunicaciones (COFETEL) y actualmente por el Instituto Federal de Telecomunicaciones (IFT). La regulación en el sector es estricta y supervisada constantemente en diversos ámbitos, incluido el económico, técnico y social. La regulación tiene, entre otros objetivos, reducir el riesgo de que las empresas utilicen su potencial poder de mercado para dañar a los consumidores. A pesar de que la regulación es estricta, es de esperar que los beneficios económicos sean relevantes; esto, aunado al riesgo de perder la concesión por actividades no permitidas, hace que la probabilidad de que las empresas tengan incentivos en utilizar la información de forma ilegal sean bajos.

En este sector existe un número importante de personas que puede utilizar diversos servicios y no es adecuado contabilizar dos veces a un mismo usuario. Como no existe información que indique cuántos usuarios tienen al menos alguno de estos dispositivos, y evitar varias duplicidades, una aproximación a la definición de la población objetivo asumirá un error de exclusión contabilizando solamente a la población de usuarios más grande. Aún así, la definición incluye un error de inclusión amplio, debido a que las personas que están expuestas a que sus datos personales sean vulnerables de transacciones comerciales no son todos los usuarios de estos servicios, sino los titulares de las líneas telefónicas o de los contratos de servicios. Esto es porque los usuarios que no son titulares de los contratos de servicio no transfieren sus datos personales a las compañías involucradas.

Comercio electrónico

Por comercio electrónico se entiende a todas aquellas plataformas electrónicas en las que se tenga una interacción de datos empresa-cliente la cual no necesariamente involucra un pago monetario asociado, ya que existen diversos servicios que no tienen costo directo para los usuarios, pero que existe una transmisión de datos personales; por ejemplo, las plataformas de redes sociales se consideran en este apartado como proveedoras de servicios sin costo. En cambio los servicios tradicionales incluyen a todas las compras por internet que pueden incluir transacciones financieras (boletos de eventos, aerolíneas, servicios de transporte, etc.) En esta industria también existen al menos dos riesgos diferenciados: uno se refiere al uso de los datos personales por parte de las empresas que venden productos y servicios. El segundo se refiere al riesgo que se deriva por la exposición de los datos personales en plataformas a través de Internet y que pueden ser obtenidos de forma ilícita por terceros para usarlos también con estos fines.

En esta definición de usuarios de comercio electrónico también se debería incluir a las personas que utilizan aplicaciones de internet en computadoras, tabletas electrónicas, teléfonos celulares, etc. Ya sea que se tenga que pagar por ellas o no pero que solicitan información de datos personales. En este caso, el sector también puede presentar duplicidades con usuarios de servicios bancarios por internet o contabilizar usuarios que utilizan plataformas que no necesariamente solicitan información de datos personales.

c. Análisis de sectores y grupos de población

Como ya fue mencionado, la justificación de las industrias seleccionadas, así como los grupos demográficos se basa en seis criterios: 1) el riesgo de los individuos, 2) la vulnerabilidad, 3) el número de titulares, 4) la capacidad de posicionar el derecho, 5) el costo-efectividad de la estrategia y 6) la importancia del mercado.

Número de titulares

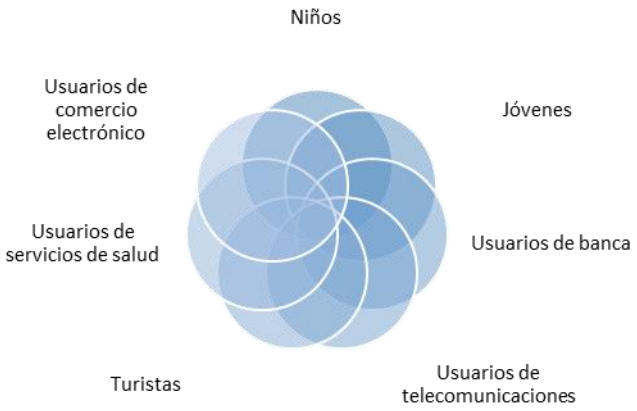
En relación con el número de titulares o la población objetivo de cada sector es necesario reconocer que existen duplicidades porque no se cuenta con información de los titulares sobre los servicios utilizados; en cambio, existe una estimación del número de usuarios totales. Por ejemplo, se cuenta con información del número total de celulares pero no de personas que usan el servicio y que cuentan con uno o más celulares.

Es importante mencionar que la caracterización anterior de grupos demográficos o los usuarios de algunos bienes de industrias específicas hace que las poblaciones objetivo se empalmen; es decir, es frecuente que un individuo sea parte de varios grupos. Por ejemplo; jóvenes con dispositivos de telefonía celular que lo utilizan como medio de acceso para las aplicaciones de internet, incluidas la banca electrónica. Este problema de las distintas poblaciones debería inducir un ejercicio que elimine a los agentes duplicados para tener un conteo más

preciso. El problema que se acaba de mencionar se puede observar en un diagrama de Venn que se presenta a continuación:

Poblaciones con riesgo de exposición de datos personales

(Superposición de poblaciones)



El problema de la duplicidad entre sectores no se puede eliminar con la información actual, razón por la cual se utilizó el sub-sector con el mayor número de titulares. A continuación se presenta una cuantificación sobre la población de cada sector.

Telecomunicaciones y comercio electrónico

En el sector de las telecomunicaciones se encuentran los usuarios de telefonía celular, telefonía fija, internet en diversos dispositivos, televisión abierta y televisión por cable. Definir a la población objetivo del sector de las telecomunicaciones y del comercio electrónico bajo este enfoque es complicado porque no se tiene información precisa sobre el número de personas que utilizan uno o más servicios. En cambio, hay estadísticas por sub-sector y en muchos de los casos se refiere al número de subscripciones en lugar de usuarios, lo que genera una duplicidad en la contabilidad de la población objetivo. Esta falta de información hace que definir la prioridad para enfocar la estrategia de atención de la educación de datos personales bajo este enfoque sea limitada, aunque proporciona cierta dimensión de los usuarios.

Las telecomunicaciones y los servicios de comercio electrónico cada vez están más interrelacionados y es común que las empresas tengan presencia en varios sectores. Es decir, los usuarios de telefonía fija y/o celular utilizan internet a través del servicio en casa o en dispositivos móviles. Ya sea por tamaño, riesgo o la condición de multi-sectorialidad, las telecomunicaciones son un elemento fundamental en la política de protección de datos. Por

ejemplo, el uso de celulares hace que la información del número telefónico sea constantemente solicitado, y posteriormente que sea contactado con ofertas de bancos, tiendas departamentales, etc.

Los subsectores que se consideran en este estudio entonces se refieren a la teléfonía celular (al segundo trimestre del 2015 las suscripciones de telefonía móvil fueron de 103.4 millones)[115], teléfonía fija (al segundo trimestre del 2015 se cuentan con 21.1 millones de líneas en todo el territorio nacional),[116] el servicio de internet (al segundo trimestre del 2015, había contratadas en México 13.68 millones de suscripciones a banda ancha fija[117]), y/o la televisión (al segundo trimestre del 2015, el número de suscripciones de televisión restringida fue de 16.98 millones, mientras que el número de suscripciones de televisión restringida por cable fue de 7.7 millones[118]).

El comercio electrónico es también un mercado complejo, no sólo para definir, sino también para acotar una estrategia. En este documento se define este sector como cualquier interacción en la que exista un intercambio de información cliente-empresa por medio de plataformas electrónicas. En una aplicación de un celular móvil, por ejemplo, se puede contener información exhaustiva sobre un individuo: correo electrónico, información sobre la tarjeta de crédito, fecha de nacimiento, ubicación geográfica, nombre, edad, etc. En consecuencia, es importante fortalecer una cultura sobre la protección de datos personales y el acceso a la información. En Canadá se tiene una estrategia específica para evitar el robo de identidad, donde se habla de "hacer campañas" para que la gente comience a monitorear las transacciones del uso de crédito vía internet.

En este sector, los usuarios de banda ancha móvil para el segundo trimestre de 2015 sumaron 54.6 millones de usuarios. Esto implica, de acuerdo con el IFT que existen 45 suscripciones por cada 100 habitantes en México. En cambio, los servicios de banda ancha fija sumaron para el mismo periodo 13.7 millones de suscripciones.[119]

Los usuarios de internet han crecido de forma sustancial en los últimos años. Por ejemplo, en 2001 solamente 7 millones de personas tenían acceso al Internet y para 2013, la cifra subió a 51.1 millones.[120] Si bien estos usuarios pueden tener acceso a internet, no todos ingresan datos personales a través de esta plataforma.

[115] Instituto Federal de Telecomunicaciones, "Líneas de Telefonía Móvil", 2015, (en línea), disponible en: http://cgpe.ift.org.mx/2ite15/tel_moviles.html#3.1 (Consultada el 15 de noviembre del 2015)
[116] Instituto Federal de Telecomunicaciones, "Líneas de Telefonía Fija", 2015, (en línea), disponible en: http://cgpe.ift.org.mx/2ite15/tel_fijas.html (Consultada el 15 de noviembre del 2015)
[117] Instituto Federal de Telecomunicaciones, "Televisión Restringda", 2015, (en línea), disponible en: http://cgpe.ift.org.mx/2ite15/tel_fijas.html#2.3.1 (Consultada el 15 de noviembre del 2015)
[118] *Ídem*
[119] Instituto Federal de Telecomunicaciones (IFT). Segundo Informe Trimestral Estadístico, consultado en: http://cgpe.ift.org.mx/
[120] Instituto Federal de Telecomunicaciones (IFT). Segundo Informe Trimestral Estadístico, consultado en: http://cgpe.ift.org.mx/

Algunos usuarios ingresan sus datos para contratar estos servicios con empresas de telecomunicaciones y otros solamente utilizan internet en pequeños negocios por lo que no transfieren información personal a empresas proveedoras. De estos usuarios, un subconjunto utiliza redes sociales y otros realizan actos de comercio electrónico en donde ingresan datos personales que deben estar protegidos y donde existe un riesgo potencial.

De acuerdo con una investigación que realizó la Asociación Mexicana de Internet (AMIPCI), dentro de los usos que las personas le destinan al internet, 71% lo utilizan por el correo electrónico, 64% para búsquedas de información, 40% lo usan para redes sociales, 25% para videojuegos, 9% por electrodomésticos, 8% por smart phones, 8 % para tabletas electrónicas, y 5% para otros usos.[121] De éstos, los servicios con mayor riesgo potencial son el uso del correo electrónico, el uso de redes sociales y los videojuegos. En este tipo de plataformas es importante difundir y reconocer qué tipo de empresas pueden ser riesgosas y qué tipo de información conocer para tener esto en cuenta. Incluso, la forma en que se conectan al internet es importante, ya que de los usuarios, 64% lo hace a través de conexiones públicas.

Destaca en el *11º estudio sobre los hábitos de los usuarios de internet en México 2015* que el 7% del total de encuestados no se encuentra inscrito en ninguna red social y de éstos, el 52% lo hace por la protección de sus datos personales.[122]

El comercio electrónico también ha tenido una evolución importante. Por ejemplo; en 2015, $162.1 miles de millones de pesos se movieron por este medio —de acuerdo con la AMIPCI.[123] Este estudio de 2015, señala por ejemplo que el 75% de los usuarios de internet realizaron una compra por este medio en los últimos tres meses de 2015. De la misma forma, 57% de los usuarios de internet realizaron una compra en sitios internacionales —principalmente en Estados Unidos (64%) y Asia (36%). De los patrones de consumo destaca que el 75% de los compradores usan mayoritariamente su tarjeta de crédito o débito (95%). Sin embargo, su mayor preocupación sobre la seguridad es el resguardo de la información de las tarjetas en los sitios de internet (77%). A pesar de la alta tasa de uso de tarjetas de crédito, el 44% continúa realizando métodos que no requieran conexión a internet. En el mismo estudio se entrevistaron a los comercios que tienen plataformas electrónicas y el 29% de éstos, no contaban con un servicio de análisis o prevención de riesgos.

[121] Estudio sobre los hábitos de los usuarios de internet en México 2014, Asociación Méxicana de Internet (AMPICI). Consultado en https://amipci.org.mx

[122] 11º estudio sobre los hábitos de los usuarios de internet en México 2015, Asociación Mexicana de Internet (AMIPCI). Consultado en https://www.amipci.org.mx/images/AMIPCI_HABITOS_DEL_INTERNAUTA_MEXICANO_2015.pdf

[123] Estudio sobre el Comercio Electrónico en México 2015, Asociación Mexicana de Internet (AMIPCI). Consultado en https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf

En esta industria, el segmento de los usuarios de telefonía móvil en 2015 suman 103 millones personas, de acuerdo con el IFT.[124] Este representa el mayor número de usuarios en alguno de los sub-segmentos considerados en telecomunicaciones o comercio electrónico.[125]

Salud

El almacenamiento de información relacionado a la salud es otro tema de datos personales importante. Las bases de datos a las que tienen acceso las instituciones de gobierno, hospitales privados e incluso las farmacias cuentan con información de la frecuencia del uso de medicamentos, hasta el registro de distintas enfermedades.

En el caso australiano, ya se consideran dentro del marco legal como sujetos obligados los proveedores de servicios de salud del sector privado, entre los que se cuenta a hospitales privados, médicos, farmacéuticos y aliados profesionales de la salud. Como este ejemplo, la mayoría de los casos internacionales.

La población de México que tiene acceso a servicios de salud privada es baja. En la tabla siguiente se puede observar a las personas que tienen acceso a este tipo de servicios por edad para el periodo de 2013. En general se observa que el 77% del total de beneficiarios recibe servicios de salud. De este 77%, solamente el 1% cuenta con servicios privados. Se destaca que la estrategia de educación para estos usuarios se debería enfocar en las instituciones privadas y públicas, se contempla a la Secretaría de Salud y las instancias del Instituto Mexicano de Seguro Social (IMSS) y del Instituto de Seguridad y Servicios Sociales para los Trabajadores del Estado (ISSSTE), como espacios para la educación a usuarios[126].

Con estos criterios se puede utilizar la siguiente tabla para identificar que los usuarios o beneficiarios de los servicios de salud con más de 20 años, que pueden ser en un primer momento los receptores de la información sobre protección de datos personales. Es importante reconocer que en este grupo de edad existen titulares y beneficiarios[127]; sin embargo, en este momento no es posible distinguir entre ellos de forma precisa. En 2013 existían 552 mil personas con servicios privados de salud que pueden presentar algún riesgo por la divulgación de sus datos personales, lo que podría considerarse como la población objetivo de este segmento.

---

[124] Instituto Federal de Telecomunicaciones (IFT). Segundo Informe Trimestral Estadístico, consultado en: http://cgpe.ift.org.mx/2ite15/tel_moviles.html#3.1

[125] Bajo este enfoque existe duplicidad porque se contabiliza más de una vez a las personas con más de un celular.

[126] INEGI, Encuesta Nacional de Empleo y Seguridad Social, 2013, ENESS, Tabulados Básicos 2014. (En línea) disponible en *www3.**inegi**.org.mx/sistemas/**tabuladosbasicos**/LeerArchivo.aspx?... (* Consultada el 15 de noviembre del 2015)

[127] Ejemplo: Un titular puede ser un padre que contrata un seguro de gastos médicos mayores y su hijo ser un benefciario de la póliza. Si bien los datos personales de ambos están involucrados, el titular es quien los transmite a través de algún mecanismo. Es el mismo caso en telecomunicaciones, un padre solicita una línea de teléfono o servicio de Internet a pesar de que el beneficiario puede ser una persona distinta.

En 2013 existían 552 mil personas con servicios privados de salud y alrededor de 91 millones de personas con servicios de salud pública, que pueden presentar algún riesgo por la divulgación de sus datos personales, lo que podría considerarse como la población objetivo de este segmento.

Afiliados a los sistemas de salud

Años	Población	Sin Afiliación	Total	IMSS	ISSSTE	Seguro Popular	Otra Pública	Otra Privada	No Especifico
Total	**118 563 412**	**26 960 893**	**91 540 602**	**40 000 144**	**6 174 281**	**41 145 824**	**3 372 089**	**848 264**	**61 917**
0 a 9 años	20 983 035	4 136 736	16 841 183	6 261 886	736 705	9 185 433	524 687	132 472	5 116
10 a 19 años	22 964 500	5 275 269	17 674 999	6 702 777	975 375	9 193 885	639 383	163 579	14 232
20 a 29 años	18 798 604	5 704 505	13 077 706	6 741 191	528 732	5 297 772	390 368	119 643	16 393
30 a 39 años	16 647 264	3 885 203	12 751 727	5 875 577	796 802	5 475 901	452 899	150 548	10 334
40 a 49 años	15 112 902	3 444 965	11 660 802	5 227 034	966 202	4 810 740	516 006	140 820	7 135
50 a 59 años	11 159 949	2 373 716	8 782 707	3 923 171	1 058 580	3 328 687	383 966	88 303	3 526
60 a 69 años	6 914 937	1 217 301	5 695 630	2 786 039	636 736	1 978 995	259 127	34 733	2 006
70 años y más	5 945 919	908 513	5 034 481	2 471 176	472 184	1 871 082	205 653	14 386	2 925
No especificado	36 302	14 685	21 367	11 293	2 965	3 329	0	3 780	250

Fuente: INEGI, Encuesta Nacional de Empleo y Seguridad Social. 2013, ENESS, Tabulados Básicos. 2014, consultado en http://www.inegi.org.mx/est/contenidos/proyectos/encuestas/hogares/modulos/eness/eness2013/default.aspx.

Usuarios de servicios financieros

El sector financiero es una de las industrias más importantes en términos de protección a la información para fines comerciales por el número de usuarios que utilizan estos servicios. Debido a su importancia, en algunos casos internacionales ya se plantean estrategias específicas en relación a temas financieros. El caso de Australia incluye disposiciones nuevas en su Ley Federal de Privacidad, se incluyen disposiciones nuevas para informes de créditos. Dentro de las campañas para prevenir robos de identidad, se incluye la publicidad para no proporcionar información bancaria por teléfono y verificar autenticidad de llamadas que solicitan información de tarjetas de crédito.

La población objetivo de este sector suma aproximadamente 24.9 millones de usuarios que corresponden al grupo o sub-sector más grande y que corresponde a los ahorradores de instituciones formales[128]. Es importante mencionar que puede haber traslapes entre usuarios y servicios, es el problema que se presenta en los casos representado en el diagrama de Venn para distintos sectores. En este caso, se reconoce que existe un error en la población objetivo debido a que hay usuarios que no ahorran pero que utilizan otros servicios financieros, pero se considera más adecuado evitar la duplicidad.

En México se realiza la Encuesta Nacional de Inclusión Financiera (ENIF) que está enfocada en adultos de 18 a 70 años e incluye tanto al sector formal como el informal —este segmento de población suma 70.3 millones de personas en México para la versión del 2012. El objetivo de esta encuesta es generar información estadística del acceso y el uso de servicios financieros entre los mexicanos para que sea posible diseñar políticas públicas que promuevan la inclusión financiera. De acuerdo con la ENIF, 24.9 millones de los adultos son usuarios del ahorro formal (35.5%) y 30.7 millones de personas son usuarios del ahorro informal[129].

Las personas que utilizan productos formales, el 60.5% utiliza los servicios bancarios para el pago de su nómina y 46.6% para ahorrar. En cambio, las personas con ahorro informal no utilizan necesariamente medios que pongan en riesgo su información personal; tales como las tandas u otros medios a través de la familia. En cambio, hay cajas de ahorro informales que representan un riesgo menor ya que la población que utiliza estos medios representa el 14.7% de los ahorradores no formales y pocas veces ponen en riesgo sus datos personales en sistemas digitalizados públicos.[130]

[128] INEGI, Encuesta Nacional de Inclusión Financiera (2012), consultada en http://www.cnbv.gob.mx/Inclusi%C3%B3n/Documents/Folleto%20Resultados%20ENIF2012.pdf
[129] Idem
[130] Ídem

Por el lado del crédito, solamente 19.3 millones de personas tienen acceso al crédito formal (27,5%) y 23.6 millones acude a la informalidad para solicitar un préstamo (33.7%). De las personas que acuden a las instituciones de crédito formal, 72% lo solicita con una institución departamental y el 33% por medio de una tarjeta bancaria.[131]

En el caso de los seguros financieros, la encuesta refleja que 15.4 millones de personas utilizan estos servicios, que representa el 22% de los usuarios de los servicios financieros. Finalmente, los usuarios de cuentas de ahorro para el retiro son 19.5 millones de personas que representan el 27.8% del total de usuarios[132].

Niños y Jóvenes

Llevar a cabo una campaña intensiva de protección de información para los niños y jóvenes, representa una oportunidad grande para un cambio de paradigma que puede traer amplios beneficios. Si bien los beneficios pueden ser percibidos como de mediano o largo plazo, también los hay de corto plazo. Es una variable de preocupación el resultado de la encuesta de IPSOS en donde "mientras más joven, es más fácil que la gente proporcione sus datos personales sin hacer más preguntas" [133]. Esto incluye los grupos entre 12 y 17 años, así como entre 18 y 35. Se percibe, además un relajamiento en los jóvenes de los potenciales riesgos del mal uso de información personal. Incluso se puede hablar de un desinterés en el grupo de jóvenes al observar que "las personas entre 18 y 35 años tuvieron como primera respuesta que no saben cuál es la empresa o institución que les solicitan datos". Por otro lado, "a una menor proporción de gente entre 12 y 17 años, le preocupa mucho lo que pase después de una compra o trámite con datos personales". Es decir, entre los grupos de edad encuestados, los más jóvenes no tienen interés en lo que pasa después de una compra que implica datos personales.

Esta falta de cultura de protección de la información personal, llama a una estrategia focalizada al sector más joven de la población. Además de traer beneficios concretos de corto plazo, para el buen uso de su información, invertir en una campaña para la niñez y la juventud logrará impulsar esta cultura en el largo plazo, ya que se tienen externalidades positivas conforme los jóvenes comiencen a ser más conscientes de este tema. Hay otro tema importante que se relaciona con estos dos grupos: el uso de internet. Es frecuente que los sitios de internet

[131] Ídem
[132] Ídem.
[133] IPSOS e IFAI, "Encuesta Nacional sobre Protección de Datos Personales a Sujetos Regulados por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y Población en General", 2012, México. http://inicio.ifai.org.mx/EncuestaNacionaldeProtecciondeDatosPersonales2012/01ReportePoblacion.pdf

constantemente pidan información personal o acceden a plataformas donde éstos almancenan dicha información[134]. Esto agudiza la necesidad de generar estrategias de concientización.

De acuerdo con INEGI, en México durante el 2014 la población infantil de 0 - 17 años sumó 40.2 millones de personas (19.7 millones de niñas y 20.5 de niños)[135]. Sin embargo, la prioridad para elaborar una estrategia de educación sobre la protección de los datos personales debería estar acotada en primer lugar en la niñez con edad escolar y que asisten a algún centro de educación. Tomando en cuenta que el grado escolar es importante para que la estrategia tenga un impacto significativo. Potencialmente, esta estrategia puede iniciar en la educación básica (nivel primaria y secundaria), en donde los alumnos pueden tener mayor madurez para comprender la importancia de la protección de datos. Posteriormente, los alumnos de educación preparatoria y los primeros años de universidad también son un segmento importante para implementar la estrategia de educación.

Los alumnos de educación básica (primaria) que están en un rango entre 6 y 11 años de edad, que en 2014, según la CONAPO había 13.4 millones de niños dentro de este rango, son un segmento en donde la estrategia podría difundirse en las escuelas primarias a través de información a los padres o tutores. Para el segmento de 12 a 17 años, los niños sumaron en 2014, 13.4 millones, (8.1 mil niños más que en el segmento anterior) y también los centros ecolares son el principal espacio de promoción del Derecho a la Protección de Datos Personales. Sin embargo, de acuerdo con la Secretaría de Educación Pública, en el ciclo escolar 2013-2014 había 6, 571,858 niños y niñas inscritos en la educación secundaria y 4, 682,336 en la educación preparatoria, que es el nivel de instrucción que corresponde a dichas edades. De tal forma, la población potencial de este grupo podría considerarse en 26.8 millones de niños que corresponden al grupo de edad de 6 a 17 años.

La estrategia de educación se puede emprender al menos de dos formas o bajo dos esquemas, uno es incorporando el tema dentro de la currícula y temarios escolares (que se observa es una estrategia a mediano y largo plazo), y otro es a través de ciclos con campañas de educación por medio de talleres, seminarios, conferencias. La relevancia de esta decisión afecta la definición de la población objetivo de la niñez en educación secundaria, ya que al incorporarse en una materia, la población objetivo es el número de alumnos en un grado escolar, a diferencia de las acciones de educación informal que pueden incluir a toda la población de este nivel de escolaridad. Por ello, la estrategia más importante y para implementar en la primera etapa con esta población, es a través de talleres, seminarios o conferencias de capacitación.

[134] Por ejemplo, plataformas o aplicaciones en las que se solicitan datos generales sobre su identificación y ubicación.
[135] INEGI, "Estadísticas a propósito del Día del Niño (30 de abril)", 2015, México (En línea) disponible en http://www.inegi.org.mx/saladeprensa/aproposito/2015/ni%C3%B1o0.pdf (Consultada el 31 de noviembre del 2015)

Riesgo de los individuos

El INAI cuenta con una definición de riesgo que ya se utiliza en los conceptos de protección de datos personales. Sin embargo, esta definición presenta complicaciones para su cuantificación, ya sea por las variables que utiliza como por su disponibilidad, tal es el número de entradas o interacciones de un usuario sobre una plataforma. *Una definición más directa para medir el riesgo es la probabilidad de que un individuo asociado a un sector o grupo presente un problema con sus datos personales o como lo define la* Comisión Federal de Mejora Regulatoria "*la probabilidad de que un evento adverso ocurra, multiplicado por el daño que causaría en caso de materializarse... El riesgo es simplemente la pérdida esperada y suele identificarse con mayor frecuencia en situaciones que afectan a la vida, la salud, el entorno, las finanzas y la vida cotidiana"*[136]. De esta forma es necesario conocer cuántos individuos han presentado una queja relacionada con el mal uso de su información y el total de titulares que existe en dichos sectores. El riesgo se obtiene dividiendo al número de personas que han presentado una queja sobre el número de titulares de cada sector o grupo.

Sin embargo, la cuantificación precisa de estas dos variables es compleja y no se cuenta con datos o estadísticas suficientes que reflejen el nivel de riesgo que pueda presentar un determinado usuario de algún servicio o tipo de población. Por otro lado, la información que está disponible es muy general y hace que existan duplicidades entre las poblaciones de cada sector o tipo de usuario.

La variable de exposición al riesgo o la ocurrencia de que los datos personales sean utilizados para fines comerciales o ilícitos es compleja de obtener o aproximar. Esto es porque en muchos de los casos, los afectados no saben que su información ha sido vulnerada o aún sabiendo, no realizan ninguna acción en contra de dicha situación. También es complicada la medición, dada la interacción de una persona en distintas plataformas, servicios, etc., en las que se originó el problema con los datos. La variable más cercana en relación con la exposición al riesgo de las personas por el uso no autorizado y con fines comerciales o ilegales de sus datos personales es probablemente el número de denuncias sobre este hecho —a pesar de que es una limitante porque no se conoce cuántas personas fueron vulneradas y no lo saben o no lo denunciaron. El INAI lleva la contabilidad de las denuncias que sumaron en 2014, 558 casos.[137].

Las denuncias en el 2014 representaron 558 que podrían considerarse bajas en relación con la población del país. Estas denuncias no puede identificarse a nivel sectorial, razón por la cual no es posible utilizar esta variable

[136] Beneficios económicos de la regulación basada en riesgos: caso de dispositivos médicos. Consultada en http://www.oecd.org/gov/regulatory-policy/48658862.pdf

[137] *Informe de Labores 2014. Instituto Federal de Acceso a la Información y Protección de Datos* (IFAI), consultado en línea el 01 de diciembre del 2015 en http://inicio.ifai.org.mx/Informes%202014/Informe%20de%20labores%202014.pdf en

para identificar prioridades de atención en esta categoría de análisis. Por otro lado, el número registrado podría implicar tres causas: la primera es que la población no tiene conocimiento de que su derecho ha sido vulnerado; que la persona que conoce el hecho no realiza una denuncia; o simplemente que no existe un problema relevante en términos del número de personas afectadas. En cualquier caso, una política o estrategia debe considerar la evidencia y en todo caso, aplicar una política que tenga un costo-beneficio neto positivo.

Otro problema con esta situación es que los individuos presentan una queja ante una institución distinta al INAI, por ejemplo, la que regula el sector. En el caso de los servicios financieros, muchos que han sido vulnerados en sus datos personales acuden a la CONDUSEF o a la institución bancaria pero no al INAI. Este puede ser el caso de las personas que sufrieron el robo de identidad. Este problema es uno de los que debe atender el INAI pero en coordinación con otras instituciones de cada sector para indentificar violaciones sobre datos personales, y puede investigar el indebido tratamiento de datos personales vinculados con el robo de identidad. De hecho, el INAI es la autoridad que debe garantizar el derecho a la protección de datos personales, aunque no está facultado para investigar de forma directa el robo de identidad, ya que esta función le corresponde a una autoridad penal.

Otras variables para medir el riesgo se refieren a los procedimientos de protección de derechos, los cuales tienen su origen en una denuncia pero tampoco se cuenta con información detallada por sector para ordenar su importancia. En cualquier caso, esta variable reportó 50 en 2012, 57 en 2013[138] y 123 en 2014[139] solicitudes o reclamaciones de protección de datos, cifra que también se considera baja.

Al no contar con un indicador transversal que refiera al número de quejas relacionadas con la vulneración de los datos personales, no es posible obtener una medida de riesgo que sea comparable en todos los sectores. Sin embargo, se buscaron indicadores sectoriales que refieran a un nivel de riesgo a pesar de que no fueran equivalentes.

La CONDUSEF en 2014 reportó 2,753,936 reclamaciones que pueden identificarse como un posible fraude en tarjeta de crédito o débito[140]. Este problema de fraude se origina por el mal uso de datos personales, entre otra información. Sin embargo, este problema de robo de identidad acumula la totalidad de problemas relacionados

[138] *Informe al Congreso de la Unión respecto a la Protección de Datos Personal* presentado por el IFAI: http://inicio.ifai.org.mx/Otros/Informe%20al%20Congreso%20de%20la%20Uni%C3%B3n%20Respecto%20a%20la%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf

[139] Ídem

[140] Anuario Estadístico de la CONDUSEF, consultado en http://www.condusef.gob.mx/PDF-s/estadistica/anuario_2014.pdf

con el mal uso de datos personales; por ejemplo, con fines comerciales. En el primer semestre de 2014, las reclamaciones imputables al robo de identidad fueron 20,168 y para 2015 sumaron 28,258.[141]

Más aún, como grupo de edad, para los jóvenes de 18 a 35 años, el banco es el lugar donde más se pide información personal, mismo patrón para los mayores de 36 años, donde además, es importante mencionar que en la encuesta de IPSOS, se incluye a las afores como institución privada que más pide información[142]. Con esto se presentan dos ejes de importancia: el nivel de riesgo que implica el mal uso de información personal en la industria financiera, y la estrategia de recopilación intensa de información que tienen las instituciones financieras.

En el sector de telecomunicaciones se buscó información sobre clonación de aparatos celulares, que puede relacionarse con el robo de datos personales. Sin embargo, esta información no se publica por ninguna institución pública o privada. De hecho, no se tuvo una estadística confiable relacionada con el número de denuncias relacionadas con el mal uso de datos personales. La estadística que más se aproxima es el reporte sobre el número de teléfonos celulares que corresponde a 341,740 pero para el periodo de 2013.[143] La cifra no se publicó para el 2014.

Para el caso del sector salud y el de niños y jóvenes no se ubicó un indicador que tuviera una referencia al riesgo sobre los datos personales.

Vulnerabilidad

Como ya fue mencionado, la vulnerabilidad es la situación en la cual una persona no puede hacer frente a un riesgo latente y una vez ocurrido, no tiene medios para reducir o eliminar sus efectos. En el caso de datos personales, se podría decir que la persona no tendría la capacidad de identificar el riesgo de que puedan hacer mal uso de sus datos y tampoco pueda tener mecanismos para corregir los daños potenciales.

En el caso del sector de las telecomunicaciones y el comercio electrónico, se puede mencionar que efectivamente existe un potencial de riesgo importante debido al uso de plataformas donde se intercambia información constante y no existen medios para que un usuario pueda saber si sus datos personales fueron vulnerados por ese medio. Si bien muchas de las empresas dentro del sector de telecomunicaciones están ampliamente reguladas y existen sanciones importantes si no aseguran la información de sus usuarios, el riesgo

[141] Reclamaciones imputables al robo de identidad 2011-2015 (1er semestre), consultado en http://www.condusef.gob.mx/PDF-s/Comunicados/2015/com71_reclamaciones-robo-identidad.pdf
[142] Según la encuesta de Ipsos y según los grupos focales realizados en este estudio, los datos personales que se solicitan en bancos son: Nombre, edad, dirección, teléfono, ocupación, ingresos, correo electrónico, grado de estudios, identificación con fotografía.
[143] Anatel 2014, Estudio e Investigación para el Desarrollo de Nuevas Medidas Tecnológicas que Permiten Inhibir y Combatir la Utilización de Equipos de Telecomunicaciones para la Comisión de Delitos.

también parte de los propios usuarios de las plataformas. Por ejemplo, pueden existir usuarios de internet que buscan violentar los candados de seguridad para obtener información de otros consumidores para distintos fines ilícitos.

En términos de la definición de vulnerabilidad, en este sector, un grupo importante de usuarios no tendría la capacidad de identificar un riesgo latente para toda la interacción que realiza en sistemas de telecomunicaciones ni tampoco medios efectivos para reducir los efectos. Por ejemplo, desde la venta de sus datos para fines comerciales hasta el uso de su información para delitos contra la salud o la integridad, los usuarios no tienen canales para reducir las afectaciones que se pueden derivar. En el caso de la venta de datos para fines comerciales, los usuarios pueden encontrar pocos medios para que la información ya no sea utilizada y cuando existen problemas relacionados con la salud y la integridad los efectos son prácticamente no resarcibles. En este sentido, el sector de las telecomunicaciones presenta un nivel de vulnerabilidad importante y que debe ser atendido.

El sistema financiero es otro sector en donde existe un alto riesgo para que los datos personales sean utilizados de forma ilegal y que puede tener efectos en el patrimonios de los usuarios. Si bien las personas pueden ser afectadas patrimonialmente por el robo de su identidad por la exposición a los medios de pago físicos o electrónicos, también es frecuente que los titulares identifiquen el daño y este pueda resarcirse, al menos para una parte importante de los usuarios. Por ejemplo, el usuario es capaz de identificar en buena medida el daño a su patrimonio y las instituciones financieras proveen seguros que permiten cubrir los daños económicos por el robo de identidad. Esto es posible en las instituciones bancarias formalemente establecidas y más grandes del país. Sin embargo, a medida que éstas instituciones de crédito o ahorro son más pequeñas, estas pueden presentar mayor vulnerabilidad. De tal forma, la vulnerabilidad en este sector debe reducirse para el riesgo residual que enfrentan los usuarios de estos servicios.

En el caso de los servicios de salud, el riesgo de que se utilice la información de pacientes para fines comerciales y para la discriminación de personas en distintos ámbitos (laboral, educativo, personal, etc.) es latente y tampoco se cuentan con los medios suficientes para que los daños puedan ser eliminados. Esto es para el caso de que lo datos sean utilizados con fines comerciales. A pesar de lo anterior, existen instituciones que trabajan para cuidar la integridad de los pacientes como es la CONAMED.

Finalmente, el grupo de niños y jóvenes presenta una vulnerabilidad importante porque el riesgo de transmisión de información sin cuidado sobre la identificación y localización de los mismos, es alto. Además este grupo está particularmente expuesto en sectores donde también existe un riesgo potencialmente alto como es el internet y el comercio electrónico.

Capacidad para posicionar el derecho

La industria de las telecomunicaciones se observa como una plataforma importante que puede posicionar los derechos relacionados con los datos personales. Esto se considera de esta forma por el posicionamiento del internet y los dispositivos de comunicación que existe entre la población. De hecho, las herramientas basadas en el internet tienen un alto grado de aceptación. Por ejemplo, ya se realizan campañas electorales, campañas de difusión de información, estrategias comerciales, etc. El potencial de la herramienta es tan importante que puede posicionar información que es presentada de forma adecuada, en poco tiempo y con una relativa baja inversión. Por ejemplo, en Estados Unidos y México se han observado experiencias en donde las campañas políticas basadas en plataformas tecnológicas han tenido muy buenos resultados.

En el sector salud, el potencial de posicionar los derechos sobre los datos personales es importante pero difícilmente alcance la efectividad por el uso de plataformas electrónicas. Esto se debe a que una campaña de posicionamiento enfocada en este grupo sin el uso de herramientas tecnológicas utilizaría medios tradicionales. Esto significa que se utilizarían muchos recursos para diseminar este tipo de proyecto para alcanzar de forma individual o grupos pequeños. Una parte relevante de este sector es que el interés de los usuarios se puede ver reflejado en mayor medida al incluir no solamente datos de identificación sino de salud.

En el sector financiero se considera que la capacidad para posicionar el derecho es relevante debido a las afectaciones potenciales que pueden derivarse. Sin embargo, este derecho ya se ejerce de forma indirecta a través de los daños percibidos por los usuarios de este sector. Es decir, al identificar los daños financieros sobre el mal uso de datos personales y someter una queja ante instituciones financieras, ejercen una acción sobre el mal uso de sus datos.

En el caso de los niños y los jóvenes, se considera que tiene potencialmente alta capacidad para diseminar el derecho, sin embargo es posible que la inversión en ellos sea a mediano plazo. Si bien este grupo de edad tiene poca consciencia sobre el derecho, si se logra posicionar la utilidad del derecho y sus potenciales efectos pueden ser materialmente un grupo diseminador de conductas y conocimiento muy relevantes. No obstante, la mejor forma de hacer que este grupo interactue es a través de redes sociales. Como se mencionó con anterioridad, el 42.2% de los niños de 6-11 años de edad y el 79.9% de 12-17 son usuarios de Internet.[144]

Costo efectividad de la estrategia

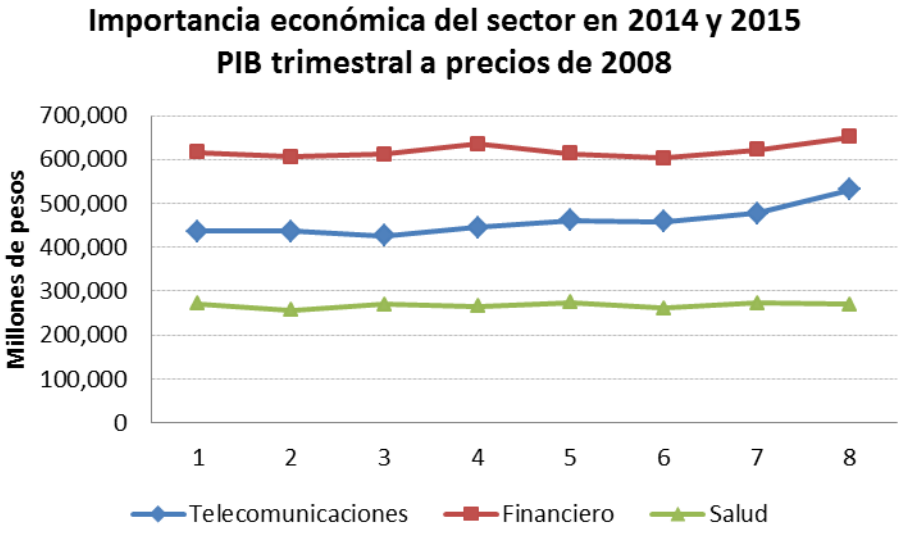
En este documento no es posible hacer una valoración sobre la razón de costo-efectividad que potencialmente tendría una estrategia a utilizar en cada grupo para definir sus prioridades. Sin embargo, es posible distinguir

[144] "Estadísticas a propósito del Día Mundial del Internet (17 de mayo)". Datos Nacionales, consultado en http://www.inegi.org.mx/saladeprensa/aproposito/2015/internet0.pdf

entre dos grandes estrategias de difusión del derecho. La estrategia que utiliza plataformas electrónicas que es principalmente interactiva y la que utiliza medios tradicionales a través de folletos, talleres, cursos, etc. pero que es en una sola vía. En este caso, la primer estrategia se prevee con una efectividad alta en relación con su costo, además de que la penetración de la difusión puede ser muy rápida. En la industria de las telecomunicaciones se utilizaría esta estrategia. Por el contrario, una estrategia tradicional su costo efectividad sería baja en relación con el tiempo invertido, debido a los nuevos patrones de comunicación. En todo caso se podrían utilizar como campañas alternativas o de reforzamiento. Para la industria del sector financiero, de salud y en grupos de escolares, esta es probablemente la más utilizada. Sin embargo, también se pueden combinar con plataformas tecnológicas para que su efectividad sea mayor ante grupos focalizados.

Importancia del mercado

El valor económico del mercado también es relevante para definir las prioridades de atención a la estrategia de protección de datos personales. En la gráfica siguiente se puede observar la evolución del Producto Interno Bruto trimestral para el 2014 y el 2015 de los sectores: Información en medios masivos (excepto la edición de libros y revistas); los servicios financieros y de seguros y de los servicios de salud y asistencia social. Como se puede observar, el sector financiero es el mas importante, seguido de las telecomunicaciones y el de salud. En el caso de los niños y jóvenes no se considera este criterio.



Fuente: Elaboración propia con datos del PIB que publica el INEGI

D. Análisis de los criterios

En esta sección se pretende observar a todos los criterios en un solo punto de vista para definir la prioridad de la estrategia. Para ello se presenta la siguiente tabla con la posición de cada variable analizada.

Prioridades en la selección de estrategias				
	Telecomunicaciones	**Salud**	**Niños, niñas y jóvenes**	**Financiero**
Número de titulares	103 millones Lugar 1	91 millones Lugar 2	426.9 millones Lugar 3	24.9 millones Lugar 4
Riesgo	No disponible	No disponible	2.7 millones	No disponible
Vulnerabilidad	Alta sin controles en algunos segmentos	Alta con controles	Alta sin controles	Alta con controles y mecanismos para resarcir daños
Posicionamiento del derecho	Muy alta	Media	Alta	Media
Costo efectividad	Alta	Baja	Baja	Baja
Relevancia económica	Lugar 2	Lugar 3	No disponible	Lugar 1

De acuerdo con la tabla anterior, se propone que el primer lugar en la atención de la estrategia para la difusión del derecho sobre protección de datos personales sea el de las telecomunicaciones, debido a que tiene el mayor número de titulares, la vulnerabilidad no tiene mecanismos efectivos para identificar y hacer frente al riesgo, así como por la relevancia económica que se presenta en segundo lugar de los sectores analizados y finalmente porque la efectividad de la estrategia es potencialmente alta a un costo relativamente bajo. Además no existe información precisa sobre la exposición al riesgo que se pueda presentar, razón por la cual una estrategia de protección de datos personales puede apoyar la denuncia de este tipo de problemas. Es decir, se requiere la construcción de información que permita ubicar el riesgo potencial.

En segundo lugar se propone al sector salud porque tiene el mayor número de titulares y a pesar de que existen controles para manejar la vulnerabilidad a través de las instituciones de salud, su relevancia económica también es importante. En términos relativos, se observa que este sector es más importante que el financiero. Al igual que en el sector de las telecomunicaciones, en el sector de salud es muy importante recabar información que permita conocer el riesgo y la estrategia puede difundir esta necesidad.

En tercer lugar se propone el sector de niños y jóvenes porque este sector tiene el tercer mayor número de titulares, potencialmente pueden tener una capacidad alta para diseminar y posicionar la estrategia si utilizan

medios masivos de información y porque este grupo se debe ver como una inversión a futuro en la estrategia. Además, también se comenta que dentro de los sectores de telecomunicaciones, el de salud y el financiero se puede ubicar una estrategia focalizada para este rango de edades, que puede ser fortalecida por otras campañas más tradicionales.

Finalmente se propone como cuarta estrategia al sector financiero porque es la última posición en el número de titulares y porque en este sector existen mecanismos para que los usuarios puedan limitar los efectos de los daños causados. Sobre este último punto se puede señalar que las instituciones bancarias tienen seguros que cubren uno de los daños más frecuentes que se refiere al robo de identidad y la clonación de tarjetas de crédito o débito.

IX. ESTRATEGIA DE ALIANZAS EN UN MARCO AMPLIO PARA DIFUNDIR EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Como hemos mencionado, la necesidad de posicionar el derecho a la protección de datos personales en la ciudadanía en general, se hace patente ante el incremento del uso de la tecnología, mediante redes sociales y aparatos inteligentes que permiten almacenar patrones de comportamiento de los usuarios y datos de su personalidad una vez que son almacenados, pero también para garantizar la privacidad de los datos personales en manos de empresas privadas y de instancias del sector público.

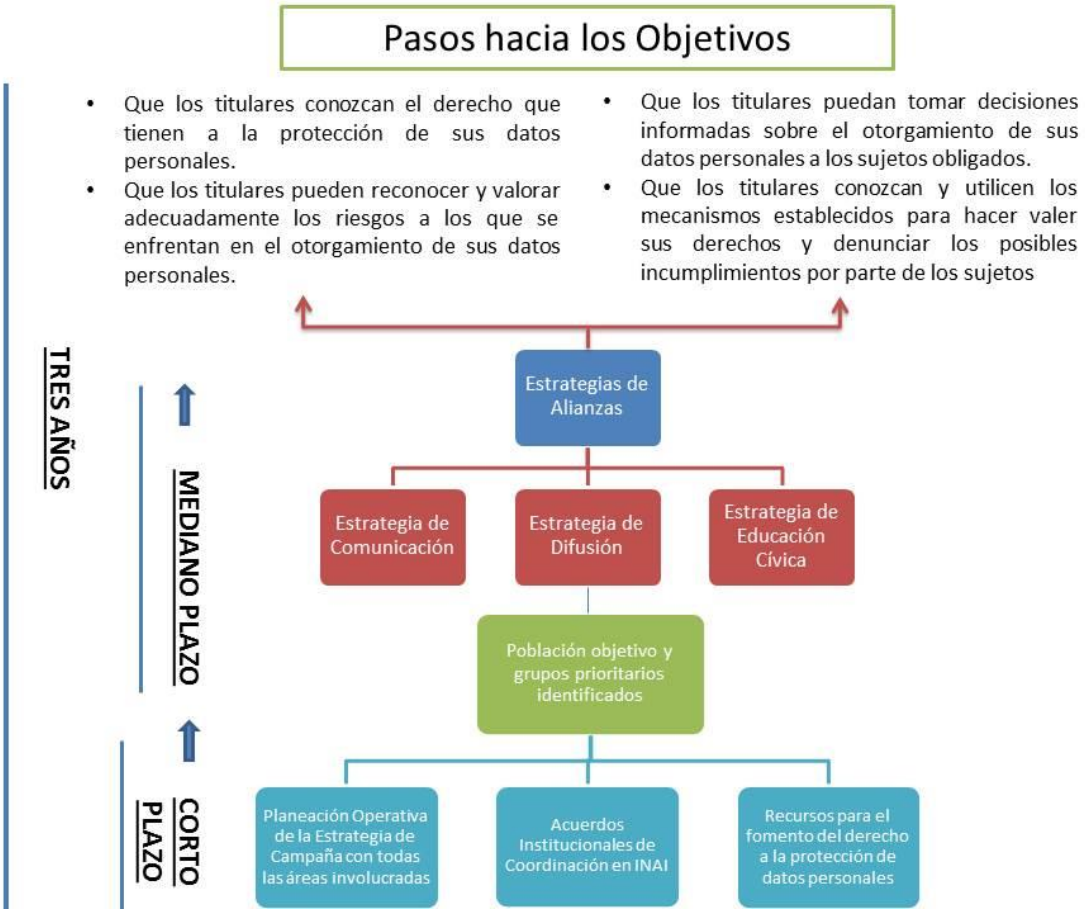
Esta propuesta no deja de lado la importancia de dirigir los esfuerzos de promoción del derecho hacia la población en general, en el entendido de que todos los individuos, de cualquier estatus socioeconómico, poseen datos personales y que éstos se encuentran almacenados en alguna instancia física o virtual, pública o privada. Sin embargo como hemos enfatizado en el capítulo anterior, la propuesta se enfoca en los segmentos de población que tienen un alto riesgo vinculado a que sus datos personales reciban un mal trato o un mal uso, y además, que sea una población que pueda contribuir a posicionar el derecho en otros segmentos de población y que pueda replicar el aprendizaje, por su grado de vulnerabilidad, por el costo-efectividad, por el nivel de importancia en la economía y por el número de los titulares de la población.

Se propone desde esta consultoría utilizar la "teoría del cambio" que utilizan muchos organismos internacionales para construir campañas de opinión pública y que permite incluir las estrategias de educación, difusión y comunicación, tomando en cuenta insumos de corto y mediano plazo para ver resultados a mediano y largo plazo. Los insumos son las actividades y espacios que el INAI ha construido, así como los que las instancias aliadas tienen y algunas actividades y estrategias retomadas de otros organismos nacionales que promueven derechos y los que de otros países promueven el derecho a la protección de datos.

La teoría de cambio puede ser una herramienta útil para el desarrollo de soluciones a problemas sociales complejos, como se ha detectado, en este caso es un problema el desconocimiento del derecho a la protección de datos personales por parte de los titulares. En su forma más básica, una teoría de cambio se explica como un grupo de acciones tempranas e intermedias que genera escenarios con resultados de largo alcance. La teoría de cambio articula los supuestos sobre el proceso a través del cual se producirá el cambio, y especifica la forma en que todos los resultados requeridos relacionados con la consecución del cambio a largo plazo se producen.

Ahora, no es sólo una estrategia de educación cívica y cultura, sino que se plantea una estrategia de campaña

que permite integrar las tres líneas y que busca en primer lugar generar la conciencia del riesgo entre los y las titulares del derecho y de esa forma fortalecer su exigibilidad.



En el flujograma anterior, se muestran tres etapas para llegar a los objetivos: En el centro se encuentra la población objetivo y los grupos prioritarios. En la primera etapa se encuentran las actividades a corto plazo: destino de recursos, coordinación y planeación dentro del INAI. En la segunda etapa, a mediano plazo, se encuentran las estrategias de comunicación y difusión del INAI y en el tercer momento, que se encuentra al mismo nivel (es decir, se planea de manera paralela) está la estrategia de alianzas, un componente clave de la estrategia para que ésta sea integral —alianzas tanto con actores públicos como privados. Las alianzas deben concebir un mismo objetivo: que se comprometan no solamente a dar un buen trato a los datos personales de los titulares, sino también a educar a éstos en el derecho a la protección de sus datos como parte de su compromiso con la construcción de un Estado democrático. Para lograr alcanzar al mayor número de titulares en una

población de alrededor de 121 millones de habitantes[145] es necesario recurrir a la construcción de alianzas con el mayor número de instancias públicas y privadas que entiendan la importancia de contribuir a educar en este derecho.

No se plantean en esta estrategia acciones de difusión ni de comunicación nuevas, pues éste no fue el objetivo ni se encuentra establecido este compromiso en los Términos de Referencia, sin embargo, se plantea aquí la articulación de las estrategias existentes desde el INAI y desde las instancias públicas y privadas con las que se establecerán alianzas, así como algunas propuestas derivadas de las estrategias que se han echado a andar en otros países para la educación en materia del derecho a la protección de datos personales.

En tal sentido, la oferta de espacios físicos y virtuales de educación cívica en el derecho a la protección de datos en alianza con instancias públicas y privadas, se deberían establecer a partir del Sistema Nacional de Transparencia, Acceso a la Información y Protección de datos Personales ya que esta instancia, según su mandato, tiene facultades en todo el territorio nacional[146]. Para la operación de la estrategia, se sugiere realizar análisis de contexto y coyuntura por cada estado de la República con las instancias con las que se realicen las alianzas institucionales, tomando en cuenta cada una de las poblaciones objetivo y prioritarias.

Desde esta consultoría se propone que las actividades que ya se realizan actualmente por el INAI se revisen y se coordinen en el marco de una estrategia integral y ordenada de tal forma que apunten a los objetivos señalados en la estrategia y de esta forma logren el impacto buscado.

a. Desarrollo de la Estrategia de Alianzas Institucionales

La necesidad de tener un mayor alcance en la población objetivo, lleva a buscar colocar en los objetivos de instancias públicas y privadas posibles aliadas del INAI, el objetivo de contribuir con el INAI a educar en el

[145] Encuesta Nacional de la Dinámica Demográfica 2014 INEGI (en línea) disponible en : http://www.inegi.org.mx/est/contenidos/proyectos/encuestas/hogares/especiales/enadid/enadid2014/doc/resultados_enadid14.pdf

[146] Por estar constituido por los órganos garantes estatales, por el INAI, por el Archivo General de la Nación, por el INEGI y por la Auditoría Superior de la Nación, y bajo los considerandos del la declaratoria de Instalación del Consejo del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales del 16 de junio del 2004, se establece que: "el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales debe ser el espacio para construir una política pública integral, ordenada y articulada con una visión nacional, con objeto de garantizar el efectivo ejercicio y respeto de los derechos de acceso a la información y de protección de datos personales promoviendo y fomentando una educación y cultura cívica de estos dos derechos en el territorio nacional".

derecho a la protección de datos personales, esto es lo que mueve a construir una política de alianzas. El nivel de colaboración entre el INAI y otros organismos del sector público, social y privado para enriquecer, definir e implementar los modelos educativos propuestos por el INAI para la promoción del derecho a la protección de datos personales ha sido insuficiente a la fecha. A pesar de que el Instituto realiza tareas en materia de educación cívica dirigidas a la promoción de este derecho, su alcance está limitado por la ausencia de una política estratégica que guíe la formación de alianzas orientadas a objetivos y metas específicas. Esta situación ha dificultado el aprovechamiento pleno del conjunto de convenios que el INAI ha firmado con distintas organizaciones públicas, sociales y privadas. La propuesta de esta consultoría en tal sentido, se dirige entonces a aliados clave vinculados a la población objetivo y grupos prioritarios a los que proponemos que se dirija esta estrategia.

Para reiterar lo que es la protección de datos en este documento retomamos lo que el Dr. D. Miguel Ángel Davara Rodríguez desarrolló como concepto de protección de datos "el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad"[147]. Este concepto remite a la protección de la intimidad y por tanto al de la privacidad, remite también no sólo al derecho a que el titular de los datos, decida si se pueden tratar sus datos o no, sino cómo se deben tratar éstos. **Entonces el derecho y los procedimientos se restringen a los principios del uso y tratamiento de los mismos.**

A pesar de que la LFPDPPP no regula al sector público, la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP)[148] sí lo hace y a partir de ésta, todas las instancias públicas en México deben cumplir con los Lineamientos de Protección de Datos Personales[149]; Lineamientos para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal, publicados en el Diario Oficial de la Federación de 18 de agosto de 2003; Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal para notificar al Instituto el listado de sus sistemas de datos personales, publicados en el Diario Oficial de la Federación de 30 de septiembre del 2005; Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos, publicados en el Diario Oficial de la Federación de 25 de agosto de 2003, y Lineamientos que deberán observar las dependencias y

[147] Instituto Federal de Acceso a la Información Pública Gubernamental "Estudio sobre Protección de Datos", IFAI, México, 2004.
[148] LGTAIP en el Diario Oficial de la Federación del 04 de mayo del 2015 (en línea) disponible en : http://www.dof.gob.mx/nota_detalle.php?codigo=5391143&fecha=04/05/2015
[149] Lineamientos de Protección de Datos Personales, publicados en el Diario Oficial de la Federación (en línea) disponible en : http://dof.gob.mx/nota_detalle.php?codigo=2093669&fecha=30/09/2005

entidades de la Administración Pública Federal, en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares, publicados en Diario Oficial de la Federación de 6 de abril de 2004.

Habiendo sentado el marco sobre el que se basa la estrategia y en el entendido de que en la primera etapa y la más temprana, que es la que se refiere a la coordinación y acuerdos institucionales, esta consultoría no fue solicitada, comenzamos revisando los elementos transversales para las estrategias de educación, comunicación y difusión.

Elementos Transversales : Materiales y Espacios de difusión: Contenido y guión de los mensajes: Dirección General de Prevención y Autorregulación y Dirección General de Normatividad y Consulta Formas y mecanismos de los mensajes: Dirección General de Promoción y Vinculación con la Sociedad y Dirección General de Comunicación Social y Difusión				
Materiales		**Espacios de distribución**		**Denuncia**
Impresos: Folletos, carteles, trípticos, juegos de mesa dirigidos a la niñez. **Museo Itinerante dirigido a la niñez**	Escuelas primarias, secundarias y preparatorias, casas de la cultura delegacionales y municipales.		El uso de los espacios que cada instancia pública tiene para el acercamiento a la población, tanto con ciudadanía organizada como con población en general, puede ser una línea de acción de bajo costo y alto impacto con respecto al costo.	Facilitar el acceso a la denuncia mediante mecanismos que además de una llamada, estén disponibles y sean de fácil acceso electrónico en aparatos electrónicos: celulares (con compañías telefónicas), virtuales (con las empresas comerciales líderes en internet), tablets. Con mensajes y colores aptos para las diferentes edades de la población objetivo.
Narración de casos	Revistas impresas y virtuales del INAI y de las instancias aliadas			
Blogs, aplicaciones y vínculos a espacios de educación con mensajes diferenciados por edad que informen sobre el derecho, los	Página web del INAI y de actores aliados	El uso de plataformas virtuales de las principales marcas comerciales de internet que alerten sobre la importancia de la protección de datos personales, que vayan dirigidos a los titulares por medio de acciones adecuadas a los públicos señalados por edad e interés y con mensajes que		Botones que lleven a los pasos a seguir para la denuncia llenado de datos que ayuden a dar seguimiento a la denuncia.El uso de instrumentos accesibles en lenguaje será de ayuda.

riesgos y brinden mecanismos de denuncia expeditos.		permitan valorar el tiempo invertido en conocer el riesgo, el derecho y mecanismos de denuncia en contraste con la ganancia de su seguridad que no tiene precio.
Aplicaciones en teléfonos celulares: androids, iphone y tabletas que informen sobre el derecho, que avisen de los riesgos y que brinden vínculos directos para denunciar.	Con compañías de telefónicas celulares.	

Con base en los materiales mencionados anteriormente, así como con la población objetivo definida y priorizada, se proponen las siguientes alianzas estratégicas:

- **Para la industria de las telecomunicaciones planteada como prioridad 1, se proponen las alianzas con Instituto Federal de Telecomunicaciones, TELCEL, TELMEX, MOVISTAR, AT&T, DISH, CABLEVISIÓN, SKY, Netflix, Google, Yahoo, Hotmail y Facebook.**

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario					
Población Objetivo Prioridad 1	**Empresas privadas**	**Acciones**	**Instancias Públicas**	**Acciones**	**Zona geográfica prioritaria**
Usuarios de Telecomunicaciones (Convergen Comercio electrónico) **103 millones de usuarios, titulares del derecho.**	TELCEL, TELMEX, MOVISTAR, AT&T, DISH, CABLEVISIÓN, SKY, Netflix Alianzas con Telcel, AT&T y Movistar y Apple	Generación de una app (aplicación) para bajar al aparato celular con la información de qué es el derecho a la protección de datos, riesgos, links a la normatividad y un link para denunciar.	Instituto Federal de Telecomunicaciones (IFT) Alianza específica con la Subdirección de Regulación en Materia de Usuarios.	Espacios físicos y virtuales de acercamiento a los usuarios de servicios de telecomunicaciones (incluidos teléfono fijo, teléfono móvil servicios de internet de banda ancha y servicios de televisión de paga): **Espacios virtuales** • Gaceta Bimestral • Redes sociales • Página web oficial **Espacios físicos** Talleres, seminarios y conferencias con organizaciones de sociedad civil que se encargan de la protección de los usuarios de servicios de	Por el número de titulares a los que potencialmente puede llegar, se proponen la Ciudad de México; Monterrey, Nuevo León y Guadalajara, Jalisco. Estas tres ciudades serían la zona prioritaria en una primera fase. Se sugiere alcanzar en los tres años de la propuesta a las tres principales ciudades de la República mexicana en alcance por población.

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario					
Población Objetivo Prioridad 1	**Empresas privadas**	**Acciones**	**Instancias Públicas**	**Acciones**	**Zona geográfica prioritaria**
				telecomunicaciones	
	Sky, Cablevisión, Dish y Netflix y principales Radiodifusoras nacionales: Grupo Radio Centro, Grupo ABC Radio, Grupo Fórmula, Grupo Imagen, MVS Radio, IMER (Instituto Mexicano de la Radio) y el Sistema de Radiodifusoras Culturales Indigenistas	Alianza para espacios de publicidad gratuitos (probono) Se propone utilizar las historias narradas por algún actor (niña o niño, joven y adulto) con experiencias de compra en internet o de usuario de red social.			
	Telmex, Google, Yahoo, Hotmail y Facebook	Alianza para generar espacios de información en todos las formas de publicidad y aparatos que estas empresas tienen dirigidas a grupos por edades y/o intereses Se propone utilizar las historias narradas por algún actor (niña o niño, joven y adulto) con experiencias de compra en internet o de usuario de red social			

- **Justificación Institucional para el trabajo con el IFT**: Los objetivos Institucionales del Instituto Federal de Telecomunicaciones como órgano autónomo son: promover y regular la competencia y el desarrollo eficiente de las telecomunicaciones y la radiodifusión en México, con apego a lo establecido en la Constitución y en la Ley Federal de Telecomunicaciones y Radiodifusión. Según la información en su página web150, para lograrlo, deberá regular, promover y supervisar el uso, aprovechamiento y explotación de:

- El espectro radioeléctrico
- Los recursos orbitales
- Los servicios satelitales
- Las redes públicas de telecomunicaciones
- La prestación de los servicios de radiodifusión y telecomunicaciones, así como
- El acceso a la infraestructura pasiva y activa.

Asimismo, es la autoridad en materia de competencia económica en los sectores de radiodifusión y telecomunicaciones. La integración del IFT se dió el 10 de septiembre de 2013 derivada de la Reforma Constitucional al artículo sexto en materia de telecomunicaciones.

"Los objetivos son los elementos que identifican la finalidad hacia la cual deben dirigirse los recursos y esfuerzos del IFT, para dar cumplimiento a su misión y realizar su visión, sujeta a los principios y valores institucionales. A su vez, todos estos elementos de planeación recuperan los principios establecidos en el Decreto de Reforma Constitucional, asociados a la promoción de la libertad de expresión, el derecho a la información, la universalización del acceso, la diversificación de los servicios, la pluralidad y diversidad de los contenidos y la competencia en los mercados de las TyR. En este marco, el IFT se ha planteado seis objetivos principales

1. Contribuir a la libertad de expresión y el acceso universal a la información, impulsando la pluralidad y diversidad en los servicios de las telecomunicaciones y la radiodifusión.

2. Garantizar la competencia y la libre concurrencia, así como eliminar las restricciones a la convergencia e innovación de los servicios de las telecomunicaciones y la radiodifusión.

3. Promover el acceso universal a los servicios de las telecomunicaciones y la radiodifusión en condiciones de calidad, precios competitivos y seguridad.

[150] Página web del IFT, objetivos institucionales (en línea) disponible en: http://www.ift.org.mx/conocenos/objetivosinstitucionales

4. Regular y supervisar en forma eficaz y oportuna el uso y aprovechamiento del espectro radioeléctrico, las redes y los servicios de las telecomunicaciones y la radiodifusión.

5. Proteger los derechos de los usuarios y las audiencias en lo referente a los servicios de las telecomunicaciones y la radiodifusión.

6. Ser un regulador eficaz, imparcial, transparente y con mejores prácticas de gestión."[151]

Esta instancia tiene espacios tanto físicos como virtuales de acercamiento a los usuarios de servicios de telecomunicaciones (incluidos teléfono fijo, teléfono móvil servicios de internet de banda ancha y servicios de televisión de paga):

1. Sus espacios virtuales: Espacios para entrevistas, gaceta bimestral. En entrevista señalaron que en el 2016 comenzarán a usar medios masivos para la difusión y educación de los usuarios (televisión y radio y revistas de circulación nacional) Actualmente lo hacen en redes sociales y en su página web oficial.

2. Espacios físicos: El IFT cuenta con espacios de interlocución con organizaciones de sociedad civil que se encargan de la protección de los usuarios de servicios de telecomunicaciones. La propuesta de esta consultoría es aprovechar estos espacios para alcanzar a este grupo de organizaciones de sociedad civil con trabajo en este tema en particular.

➢ **¿Por qué y para qué alianzas con TELMEX, TELCEL, MOVISTAR, AT&T?:**

Telcel y Telmex (América Móvil) cuentan con alrededor de 70 millones de usuarios en toda la República mexicana según el Instituto Federal de Telecomunicaciones[152] lo que representa el 69.6% del mercado. El uso de los aparatos celulares para emitir información a través de apps para la protección de datos personales en los que se especifiquen los riesgos y lo que es un mal uso de datos personales, así como los lineamientos que deben seguir instancias tanto públicas como privadas para la protección de datos personales, así como mecanismos de fácil acceso a la denuncia en caso de mal uso de los datos personales. En el caso de Movistar al primer trimestre del 2015 contaba con cerca de 22 millones de usuarios que representa el 21.7% del mercado y AT&T (Nextel) cuenta con el 2.9% del mercado .[153]

[151] Página web del IFT, objetivos institucionales (en línea) disponible en: http://www.ift.org.mx/conocenos/objetivosinstitucionales
[152] Informe de Investigación de Mercados en The Competitive Intelligence Unit. Disponible en http://the-ciu.net/ciu_0k/xsearch/investigacion_mercados.htm
[153] Reportede Telconomía citado en el diario El Financiero del 20 de mayo del 2015. http://telconomia.com/category/reportes

- **¿Por qué y para qué alianzas con DISH, CABLEVISIÓN, SKY, Netflix, Google, Yahoo, Hotmail y Facebook y las principales Radiodifusoras nacionales: Grupo Radio Centro, Grupo ABC Radio, Grupo Fórmula, Grupo Imagen, MVS Radio, IMER (Instituto Mexicano de la Radio) y el Sistema de Radiodifusoras Culturales Indigenistas?**

Debido al incremento en el uso de las redes sociales y del incremento de la televisión de paga y el histórico uso de la radio, la televisión de paga así como las principales Radiodifusoras y las principales plataformas de internet son estratégicas en el alcance a un amplio número de titulares, a partir del uso de espacios de difusión sin paga (o probono). Según el IFT al 2015 hay alrededor de 17 millones de usuarios de Cable[154], Facebook cuenta al 2015 con alrededor de mil cuatroscientos millones de usuarios[155], gmail cuenta con alrededor de 280 millones de usuarios[156], alrededor de 20 millones de personas escuchan la radio en el Valle de México, 33% de los radioescuchas tienen menos de 25 años[157], p.ej.. En estos espacios, la difusión del derecho, del riesgo, de la normatividad y de los mecanismos de denuncia, son estratégicos. Actualmente el INAI ya cuenta con difusión del teléfono al que se denuncia, éste debe ser el mismo para no generar confusiones en los titulares del derecho. Sin embargo, el contenido de los mensajes no debe ser generados desde la Dirección General de Promoción y Vinculación con la Sociedad, sino desde el área sustantiva y en coordinación con la Dirección General de Comunicación Social y Difusión.

Formas de alianza: Estos proveedores de servicios tienen cierto porcentaje de donaciones, para evitar los costos, se propone construir una estrategia en la que los espacios sean donados mediante los llamados "probono" como parte del servicio al desarrollo del país.

[154] Fuente: Segundo Informe trimestral 2015 del IFT
[155] Consultado en http://www.trecebits.com/2015/07/30/facebook-ya-tiene-1-490-millones-de-usuarios-activos/ el 1 de enero del 2016
[156] Consultado en : https://www.fayerwayer.com/2012/10/ahora-si-gmail-supera-en-cantidad-de-usuarios-a-hotmail/ el 1 de enero del 2016
[157] Asociación de radios del Valle de México. Consultado el 3 de enero en línea: http://arvm.mx/description/use-la-radio/

➢ **Secretaría de Educación Pública (SEP):**

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario			
Población Objetivo Prioridad 3	**SEP** **Escuelas públicas y privadas de educación básica**	**Acciones**	**Zona geográfica prioritaria**
Niñez entre 6 y 12 años: 13.4 millones de niñas y niños	Para escuelas públicas y privadas, la alianza se debe realizar, para la Ciudad de México mediante la Dirección de Vinculación y Planeación de la Administración Federal de Servicios Educativos en el D.F., quien tiene como función la vinculación y la inclusión temática en las actividades de las escuelas primarias. La alianza en este caso sería estratégica, de corto, mediano y largo plazo.	Talleres, seminarios y conferencias en el marco de las actividades del Consejo Nacional de Participación Social en la Educación. Se propone que los talleres, seminarios y/o conferencias sean tanto presenciales como virtuales. Museo Itinerante sobre el derecho a la protección de datos personales con materiales y mensajes aptos para estas edades (el INAI ya tiene un modelo en el área de Promoción y Vinculación) Para acciones dirigidas a población en esta edad en redes sociales, tabletas, celulares, televisión y radio, revisar telecomunicaciones o la Matriz resumen.	Por número de titulares (en este caso indirectos (padres) directos (niñas y niños de 6 a 12 años) se propone comenzar por la Ciudad de México.
Jóvenes entre 12 y 17 años: 13.4 millones de jóvenes **NOTA: Esta población cuando se cruza con los usuarios de**	En este caso se sugiere generar la alianza con los encargados del Programa "Escuela para padres" que opera en el nivel de	Talleres, seminarios y conferencias en el marco de las actividades del Consejo Nacional de Participación Social en la Educación. Se propone que los talleres, seminarios y/o conferencias sean tanto	Se propone comenzar la primera etapa (1 año) por la Ciudad de México y por el estado de México- Igual que en los otros casos, se

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario			
Población Objetivo Prioridad 3	**SEP** **Escuelas públicas y privadas de educación básica**	**Acciones**	**Zona geográfica prioritaria**
telecomunicaciones y comercio electrónico incrementa su grado de riesgo por exposición.	secundaria. Alianza con el área de la UNAM encargada de la educación contiua en las preparatorias de la UNAM, CCH y Bachilleres. Subsecretaría de Educación Media Superior de la SEP CONACULTA y SEP: casa de la cultura en cada delegación en el caso de la Ciudad de México y en el caso de estado de México por municipio.	presenciales como virtuales. Museo Itinerante sobre el derecho a la protección de datos personales con materiales y mensajes aptos para estas edades (el INAI ya tiene un modelo en el área de Promoción y Vinculación) Para acciones dirigidas a población en esta edad en redes sociales, tabletas, celulares, televisión y radio, revisar telecomunicaciones o la Matriz resumen. Utilización de las casas de la cultura para la impartición de talleres, conferencias y seminarios presenciales y virtuales, así como la posibilidad de hacer concursos de performance y pintura o cortometrajes.	propone que el alcance sea gradual en los estados restantes durante los siguientes dos años, tomando como criterio el número de población.

La alianza con SEP se propone con base en dos factores clave, el primero: Que es una enorme oportunidad la apuesta de la administración actual en el Programa Sectorial de Educación la cual concibe al proyecto educativo de la siguiente forma: "La educación integral es un derecho humano y un mandato del artículo 3o constitucional. La tarea propuesta está orientada a la formación de personas responsables consigo mismas y con su entorno, conocedoras de sus derechos y respetuosas de los de los demás, capaces de dialogar, respetar las diferencias y aprender de ellas. El quehacer educativo habrá de nutrirse de las bases filosóficas, humanistas y sociales que han sustentado a la educación pública. Las actividades físicas y deportivas, el arte y la cultura, la ciencia y la tecnología tienen un lugar en la formación integral que el Gobierno Federal apoyará.

La tarea educativa es responsabilidad de todos. Autoridades, maestros, alumnos, padres de familia, investigadores, organizaciones de la sociedad civil, grupos filantrópicos y la sociedad en su conjunto habremos de trabajar armónica y constructivamente para el mejoramiento educativo que el país requiere. El Programa Sectorial de Educación 2013-2018 está concebido para dar un lugar a todos quienes participan o se sumen a la tarea educativa. Sólo con concurso de todos lograremos el avance en la educación que el país requiere. La educación en todos sus tipos, niveles y modalidades constituye un compromiso prioritario del Gobierno de la República."[158]

La población infantil, particularmente aquella entre los 6 y los 17 años que cursan la educación básica, son por las definiciones de población seleccionadas quienes cumplen con los criterios de ser una población con alto riesgo, con la capacidad de aprender y posicionar el tema y también de replicarlo. Este riesgo se incrementa con la vulnerabilidad que presenta esta población por ser menores de edad y ser presas fáciles en las redes sociales. En este grupo se incrementa la prioridad de promoción del derecho.

Formas de Alianza: La alianza se debe realizar, para la Ciudad de México mediante la Dirección de Vinculación y Planeación de la Administración Federal de Servicios Educativos en el D.F., quien tiene como función la vinculación y la inclusión temática en las actividades de las escuelas primarias tanto públicas como privadas. La alianza en este caso sería estratégica, de corto, mediano y largo plazo, incluyendo :

1. Campañas escolares en el marco de los derechos humanos básicos sobre "Derecho Humano a la Protección de Datos Personales".

[158]Secretaría de Educación Pública, "Programa Sectorial de Educación 2013-2018", 2013, (en línea), disponible en: http://www.sep.gob.mx/work/models/sep1/Resource/4479/4/images/PROGRAMA_SECTORIAL_DE_EDUCACION_2013_2018_WEB.pdf (Consultada el 15 de noviembre de 2015)

2. La inclusión del tema en la currícula escolar, en el marco de derechos humanos, se considera una estrategia a mediano y largo plazo

3. Inclusión de talleres seminarios y/o conferencias con los padres y/o tutores y con la población objetivo directamente. Los talleres, seminarios y/o conferencias podrán ser presenciales y/o virtuales. En el caso de estudiantes de secundaria, se propone hacerlo en el marco del programa "Escuela para Padres" de la SEP establecido en las escuelas secundarias. En este sentido, para la niñez entre 6 y 11 años se proponen campañas dirigidas a la educación y supervisión de los padres y/o tutores como primera prioridad y en segundo lugar, las campañas educativas dirigidas a la población directamente en espacios lúdicos escolares: ferias, quermeses. El material a desarrollar será impreso para su distribución en los talleres y/o seminarios específicos para esta edad. Se propone que los materiales sean desarrollados por pedagogos que den continuidad a la primera etapa de acercamiento con los símbolos y significados de este derecho, mediante los instrumentos de seguimiento y reforzamiento del conocimiento en redes sociales, televisión y radio.

4. El museo itinerante se propone circularlo entre las escuelas públicas y privadas de la Ciudad de México y del estado de México en una primera etapa y en los dos años siguientes en el resto del país, aplicando criterios de número de población en estas edades y revisando con la SEP en cada estado las posibilidades y los criterios para definir qué escuelas públicas y qué escuelas privadas.

En el caso de los jóvenes entre 12 y 17 años, que son también población con alto riesgo por exposición en redes sociales, se proponen campañas de educación dirigidas a esta población de manera presencial, virtual y en las redes sociales y la utilización de plataformas de internet. En una segunda prioridad a los padres y/o tutores, en espacios lúdicos de ferias y quermeses o ferias del libro y casa de la cultura. (CONACULTA depende de la SEP) y la alianza con la SEP puede incluir los espacios en los que el CONACULTA imparte talleres y conferencias, como son las casas de cultura delegacionales y en los estados de la República en las casas de la cultura de los municipios.

Es relevante hacer alianza con la Subsecretaría de Educación Media Superior de la SEP y con la UNAM para las preparatorias vinculadas a la UNAM. **Asimismo, se recomienda el uso de espacios de educación informal que puedan complementar el uso de materiales impresos y en línea. Las actividades dirigidas a esta población en otros espacios como son ferias y concursos que ya realiza en este momento el INAI, deberían ser revisados con un enfoque de alcance en los espacios ya señalados en este apartado y el contenido debe ser revisado por la Dirección General de Prevención y Autorregulación así como por la Dirección General de Normatividad y Consulta**

- **Secretaría de Salud**

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario			
Población Objetivo Prioridad 2	**Secretaría de Salud Hospitales públicos y Privados de la República Mexicana.**	**Acciones**	**Zona geográfica prioritaria**
Usuarios de Servicios Médicos: **552 mil personas que utilizan servicios privados.** **Alrededor de 91 millones de usuarios de servicios médicos públicos.**	La Secretaría de Salud atiende a un alto número de población que se encuentra en un alto riesgo vinculado al uso y trato de datos personales sensibles tanto en hospitales públicos como privados, por lo que la alianza con esta Secretaría resulta estratégica tanto por su alcance en número como por el impacto que puede tener en la prevención.	I. Generar espacios de análisis de conexto y de coyuntura con las delegaciones de la Secretaría de Salud en cada estado. II. Utilización de espacios de acercamiento de la Secretaría de Salud con usuarios de servicios en las clínicas y hospitales públicos y privados para brindar talleres, seminarios y conferencias. III. Elaboración de materiales físicos específicamente destinados a titulares del derecho en la temática de servicios médicos: folletos, trípticos, audiovisuales. IV. Espacio en la página web del INAI con mecanismos visuales dirigidos a esta población. Acceso fácil a mecanismos de denuncia mediante la página, teléfono fijo y celular, incluido un 01800.	Por el número de titulares a los que potencialmente se puede llegar, se proponen la Ciudad de México, Monterrey, Nuevo León y Guadalajara, Jalisco. Estas tres ciudades serían la zona prioritaria en una primera fase. Se sugiere alcanzar en los tres años de la propuesta al mayor número de estados de la República mexicana en alcance por número de población.

De acuerdo a la Constitución Política de los Estados Unidos Mexicanos en su artículo 26 apartado A, establece que el "Estado organizará un sistema de planeación democrática del desarrollo nacional que imprima solidez, dinamismo, competitividad, permanencia y equidad al crecimiento de la economía para la independencia y la democratización. La Constitución establece asimismo específicamente que habrá un Plan Nacional de Desarrollo, al que se sujetarán, obligatoriamente los programas de la Administración Pública Federal. El Plan Nacional de Desarrollo 2013-2018 aprobado por Decreto publicado el 20 de mayo de 2013 en el Diario Oficial de la Federación - es el principal instrumento de planeación de esta administración; define las prioridades nacionales que busca alcanzar el gobierno mediante objetivos, estrategias y líneas de acción. A su vez, la Ley de Planeación señala en su artículo 16 fracción IV que las dependencias de la Administración Pública Federal deberán asegurar la congruencia de los programas sectoriales con el Plan Nacional de Desarrollo y programas especiales que determina el Presidente de la República. Para la elaboración de los programas sectoriales, en términos de elementos y características, se publicó el 10 de junio de 2013 el Acuerdo 01/2013 por el que se emiten los Lineamientos para dictaminar y dar seguimiento a los programas derivados del Plan Nacional de Desarrollo 2013 2018. En este sentido, el Programa Sectorial de Salud 2013 2018 define los objetivos, estrategias y líneas de acción en materia de salud en un marco guiado por el ordenamiento jurídico aplicable en materia de salud y por el Plan Nacional de Desarrollo 2013 - 2018".

Con base en sus atribuciones, en el alcance y cercanía con la población, la Secretaría de Salud atiende a un alto número de población que se encuentra en un alto riesgo vinculado al uso y trato de datos personales sensibles tanto en hospitales públicos como privados y en atención en consultorios médicos. La promoción del derecho entre esta población, resulta estratégica tanto por su alcance en número como por el impacto que puede tener en la prevención.

Al 2010, de cerca de 109.3 millones de usuarios de servicios médicos públicos y privados, la Secretaría de Salud atendía a cerca de 34.2 millones de éstos, el IMSS a 29.6 millones, el ISSSTE a 5.9 millones y el resto entre PEMEX y los hospitales privados. [159] Por tipo de institución se aprecia que seis de cada diez usuarios y usuarias recurren a los servicios que proporciona la Secretaría de Salud, por lo que se considera esta institución la que debería ser la aliada. Además, en este universo tan amplio, esta consultoría sugiere priorizar a los usuarios cuyos datos sean sensibles por el alto riesgo que implican en situaciones laborales o incluso de extorsión: usuarios con VIH SIDA y/o con cualquier enferemedad de transmisión sexual, enfermedades terminales así como mujeres embarazadas.

[159] Fuente, informe de Estadísticas del Inmujeres, disponible en : http://estadistica.inmujeres.gob.mx/myhpdf/93.pdf

Formas de Alianza: El uso de los espacios que cada instancia pública tiene para el acercamiento a la población, tanto con ciudadanía organizada como con población en general, como hemos señalado, los consideramos espacios con bajo costo y alto impacto con respecto al costo.

1. Los espacios de atención a los usuarios en los hospitales públicos de la Secretaría de Salud Pública de todos estados de la República, comenzando en la Ciudad de México; Monterrey, Nuevo León y Guadalajara, Jalisco e incrementando por estados con el criterio de número de población.

2. El acercamiento institucional a los hospitales y consultorios médicos privados para la impartición de talleres, seminarios y conferencias en los que se difunda material impreso y el material virtual de la página web del INAI.

3. La distribución del material impreso en consultorios, clínicas y hospitales públicos y privados.

- **Instituto Mexicano de la Juventud (IMJUVE)**

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario				
Población Objetivo 3	**Instituto Mexicano de la Juventud**		**Acciones**	**Zona geográfica prioritaria**
Jóvenes de 12 a 17 años **13.4 millones de jóvenes** **Nota: esta población se atiende también con SEP, con la UNAM y a partir de la población objetivo de Telecomunicaciones**	La importancia del IMJUVE radica en que tiene un alcance de importante con la población, ya que llega a jóvenes de todas las condiciones socioeconómicas y no necesariamente escolarizados, mediante los diferentes espacios y tiene alianzas a su vez con otras instituciones públicas y privadas que se deben aprovechar. Para la acción II se sugiere establecer una alianza entre el INAI y el IMJUVE para aprovechar el potencial de ambas instituciones que ya tienen trabajo conjunto enfocado a población juvenil. El IMJUVE en diferentes temas ha hecho alianza con empresas privadas para generar incentivos a los y las jóvenes.	I. II. III. IV. V. VI.	Planeación, Diseño y Construcción de las acciones con el IMJUVE. Realización de concursos y festivales con el apoyo de empresas aliadas del IMJUVE Materiales impresos dirigidos a esta población con mensajes de riesgo, derecho y formas de denuncia. Página web del INAI con espacios destinados a esta población, diseñados por especialistas tomando en cuenta lenguaje, mensaje, colores y formas. Cursos breves virtuales sobre el derecho a la protección de datos. E- learning. Difusión en los diferentes espacios de educación: escuelas, casa de cultura, ferias del libro, museos itinerantes. Uso de redes sociales para la educación en el derecho a la protección de datos.	Por el número de titulares jóvenes a los que potencialmente se puede llegar, se proponen la Ciudad de México y Estado de México. Estas dos ciudades serían la zona prioritaria en una primera fase. Se sugiere alcanzar en los tres años de la propuesta al mayor número de estados de la República mexicana en alcance por número de población, dependiendo de los acuerdos institucionales y de las capacidades financieras del INAI.

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario			
Población Objetivo 3	**Instituto Mexicano de la Juventud**	**Acciones**	**Zona geográfica prioritaria**
		Segunda Etapa	
Jóvenes de 12 a 17 años **13.4 millones de jóvenes**	IFT y Compañías de telefonía celular, telecomunicaciones y comercio electrónico: Telefonía celular: Telcel, Movistar y AT&T. Telecomunicaciones: Dish, Sky y Cablevisión. Empresas líderes en internet: Yahoo, Google, Hotmail y Facebook.	I. Acciones de incidencia con las compañías para interesarlas en la implementación de las acciones. II. Elaboración, Diseño y Construcción de las acciones con las empresas interesadas. III. Elaboración de imágenes y estrategias de mercadotecnia dirigida a esta población para ser difundida en los teléfonos celulares, tablets y aparatos electrónicos. IV. Vínculos electrónicos al material de educación de la página web del INAI V. Espacios con mensajes breves dirigidos específicamente a esta población en las compañías de televisión de paga y en los canales abiertos y en radio. VI. Utilización de los instrumentos que tiene el IFT como son su "Carta de los derechos del usuario" y "Las 10 del IFT". Así como los espacios físicos de cercanía con los usuarios organizados.	Por el número de titulares jóvenes a los que potencialmente se puede llegar, se proponen la Ciudad de México y Estado de México. Estas dos ciudades serían la zona prioritaria en una primera fase. Se sugiere alcanzar en los tres años de la propuesta la mayor población objetivo, en las tres principales ciudades de la República mexicana en alcance por población.

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario			
Población Objetivo 3	**Instituto Mexicano de la Juventud**	**Acciones**	**Zona geográfica prioritaria**
		Tercera Etapa	
Jóvenes de 12 a 17 años **13.4 millones de jóvenes**	IMJUVE, SEP, IFT y Compañías de telefonía celular, telecomunicaciones y comercio electrónico: Telefonía celular: Telcel, Movistar y AT&T Telecomunicaciones: Dish, Sky y Cablevisión y radio difusoras. Empresas líderes en internet: Yahoo, Google, Hotmail y Facebook.	**I.** Concursos de Música, fotografía, ensayo y oratoria en escuelas, espacios del IMJUVE y las compañías privadas de telecomunicaciones. **II.** Historias narradas por los protagonistas en espacios donados por las televisoras. **III.** Acceso fácil a la denuncia por diferentes vías: telefónica, internet, página web del INAI, del IMJUVE.	Por el número de titulares jóvenes a los que potencialmente se puede llegar, se proponen la Ciudad de México y Estado de México. Estas dos ciudades serían la zona prioritaria en una primera fase. Se sugiere alcanzar en los tres años de la propuesta al mayor número de estadosde la República mexicana en alcance por número de población, de acuerdo a las alianzas institucionales y la capacidad financiera del INAI.

Como en los dos casos anteriores, el criterio del número de población entre los 12 y los 17 años de edad así como por el perfil de la población a la que atiende y su cercanía con esta población, se considera a esta instancia como una aliada estratégica.

Según el informe 2014 del IMJUVE, éste tiene como una línea estratégica contribuir al Objetivo 4 del Programa Sectorial de Desarrollo Social, "Construir una sociedad igualitaria donde exista acceso irrestricto al bienestar social mediante acciones que protejan el ejercicio de los derechos de todas las personas"[160]

Garantizar el adecuado desarrollo de las personas jóvenes en el contexto actual, es un reto para los gobiernos. El conocimiento de sus derechos básicos permiten a los y las jóvenes ser individuos con plena consciencia de su ser social. El conocimiento de un derecho fundamental en un contexto de incremento del uso de la tecnología y manejo de datos por diferentes agentes implica un conocimiento clave para la sobrevivencia digna y cuidada.

- **Formas de alianza:**

1. El uso de los espacios que el IMJUVE tiene con esta población mediante sus institutos estatales y municipales, se considera de un alto impacto con respecto a los costos.

2. La estrategia incluye la generación de materiales impresos que sustenten una campaña con espacios de educación físicos y virtuales dirigida a esta población con mensajes que les alerten sobre el riesgo que implica el otorgamiento de sus datos personales en redes sociales y en el uso de aparatos de telecomunicación, colocando el aprendizaje y la inversión de muy poco tiempo en el conocimiento del derecho, contra una ganancia en protección que no tiene precio.

3. El IMJUVE llega a jóvenes de todas las condiciones socioeconómicas en sus diferentes espacios y tiene alianzas a su vez con otras instituciones públicas y privadas en las que se pueden eventualmente construir talleres, seminarios, conferencias, ferias, etc.

[160] Gobierno de la República, "Plan Nacional de Desarrollo 2013-2018", 2013, (en línea), disponible en: http://www.imjuventud.gob.mx/imgs/uploads/Informe_Projuventud_2014.pdf (Consultada el 15 de noviembre de 2015)

➢ **Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF)**

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario			
Población Objetivo Prioridad 4	**CONDUSEF**	**Acciones**	**Zona geográfica prioritaria**
Usuarios de Servicios Financieros: 29.4 millones de usuarios	Entre los derechos que la CONDUSEF promueve, se encuentra el derecho a la protección de datos personales, por lo que resulta un aliado fundamental en la Estrategia.	I. Utilización de espacios de acercamiento de la Condusef con usuarios de servicios financieros para brindar talleres, seminarios y conferencias. II. Difusión en su revista mensual de historias narradas por usuarios. III. Elaboración de materiales físicos específicamente destinados a titulares del derecho en la temática de servicios financieros: folletos, trípticos, audiovisuales. IV. Espacio en la página web del INAI, de Condusef y de los bancos privados y cámaras empresariales con mecanismos visuales dirigidos a esta población y con acceso fácil a mecanismos de denuncia.	Por el número de titulares a los que potencialmente se puede llegar, se proponen la Ciudad de México, el Estado de México, Guadalajara, Jalisco y Monterrey, Nuevo León, por considerarse las ciudades con alta población urbana, con base al número de usuarios en zonas urbanas. Se sugiere alcanzar en los tres años de la propuesta al mayor número deestados de la República mexicana enalcance por número de población urbana.

La CONDUSEF tiene como su objetivo fundamental promover y difundir la educación y la transparencia financiera para que los usuarios tomen decisiones informadas sobre los beneficios, costos y riesgos de los productos y servicios ofertados en el sistema financiero mexicano también su misión se encuentra "proteger sus intereses mediante la supervisión y regulación a las instituciones financieras y proporcionarles servicios que los asesoren y apoyen en la defensa de sus derechos"[161].

Entre los derechos que la CONDUSEF promueve, se encuentra el derecho a la protección de datos personales. A decir del Director de Educación Financiera del organismo, el riesgo en el manejo de la información financiera se incrementa con los piratas en las redes. Con base en las cifras que se han citado y el nivel del riesgo que tiene esta población usuaria de servicios financieros, la CONDUSEF es un aliado natural y clave en el alcance.

- **Formas de alianza:** La CONDUSEF, al igual que las instancias señaladas anteriormente, tiene espacios de acercamiento con la ciudadanía en toda la república que resultan espacios estratégicos para el acercamiento por parte del INAI.

1. Semana de la Educación Financiera: en la que en todos los bancos privados y las instituciones con las que trabajan tienen talleres y espacios de difusión. Los materiales impresos y virtuales sobre el derecho a la protección de datos personales, así como personal del INAI participando en ellos es estratégico.

2. Su población objetivo, a decir del Director de Educación financiera son empresas (mediante las Cámaras empresariales) y los jóvenes. Los jóvenes son población objetivo con prioridad en esta estrategia y por otro lado, aunque los empresarios no lo son como titulares, es una oportunidad de llegar a esta población.

3. La revista de Condusef, a decir del Director de Educación Financiera tiene alrededor de 50 mil visitas al año. Éste se considera un espacio ideal para la educación en el derecho a la protección de datos.

4. Las Cámaras Empresariales si bien no promueven ni defienden derechos, son un espacio importante al ser considerados según la Ley de Cámaras Empresariales y sus Confederaciones, como órganos de consulta y de colaboración con el Estado. Asimismo, el alcance de éstas y su presencia en los estados es ideal para que el INAI establezca alianzas para la promoción del Derecho.

[161]Secretaría de Hacienda y Crédito Público, Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, "Misión y Visión", (en línea), disponible en: http://www.condusef.gob.mx/index.php/conoces-la-condusef/mision-y-vision (Consultada el 15 de noviembre de 2015)

- **Asociación de Bancos de México**

Justificación Institucional para el trabajo con el Asociación de Bancos de México (ABM): La Asociación no persigue un fin social y es un organismo altamente reconocido por su aporte al desarrollo integral de la Banca, que representa los intereses generales del gremio y contribuye a mejorar la comprensión de los servicios que el sistema bancario ofrece, con el fin de apoyar el desarrollo armónico y sustentable del país[162].

Los objetivos institucionales de la Asociación destacan:

- Representar y defender los intereses generales de sus asociados en cualquier gestión común ante la administración pública y ante organizaciones privadas.
- Facilitar la comunicación entre las instituciones asociadas para construir consensos en temas que requieren el establecimiento de estándares que eleven la eficiencia del sector.
- Fomentar el desarrollo de las actividades bancarias a través de foros en los que se compartan experiencias nacionales e internacionales que den como resultado mejores prácticas e innovación.
- Realizar estudios e investigaciones orientadas al desarrollo y buen funcionamiento del sistema bancario y financiero en general, así como los relativos al perfeccionamiento de sus métodos y prácticas de operación.

Desde su fundación, la ABM se ha desempeñado como el organismo cúpula de las instituciones de crédito, ha colaborado con sus asociados en el logro de sus objetivos generales, y ha jugado un papel fundamental en el marco de las relaciones de las instituciones de crédito entre sí, como en el de éstas con el gobierno mexicano, con intermediarios financieros no bancarios, con otros organismos de representación, y con instituciones internacionales.

Por otro lado, se destaca para fines de la alianza, que la Asociación actualmente cuenta con 26 bancos asociados que se rigen por una normatividad que los regula, entre ésta destaca la Ley de Protección y Defensa del Usuario de Servicios Financieros. También la ABM ha promovido entre sus agremiados el que las Instituciones de Crédito cuenten con Unidades Especializadas con el objetivo de atender las reclamaciones de los clientes por los servicios bancarios que reciben, también cuenta con un programa en su página web de educación financiera.

- **¿Por qué y para qué una alianza con la Asociación de Bancos de México.** En México hay más de 12, 233 sucursales bancarias operadas por 45 bancos comerciales, el número potencial de usuarios del servicio representa una oportunidad para que el INAI pueda establecer una alianza fuerte con este sector. La Asociación puede ser la ventana para un Convenio marco de trabajo

[162] Página web de la Asociación de Bancos de México, Misión y Visión, disponible en http://www.abm.org.mx/index.htm

general en cuanto a seminarios y conferencias sobre el Derecho a la Protección de Datos Personales, y a la vez le permitirá determinar al INAI cuáles son las instituciones bancarias estratégicas con las que puede establecer alianzas para comenzar con la promoción del Derecho mediante las ventanillas y espacios en sus sucursales.

- **Formas de alianza con la ABM**

- Utilización de espacios visibles en las sucursales bancarias para colocar posters con mensajes sobre el Derecho a la Protección de Datos Personales.
- Promoción de spots de 50 segundos sobre el Derecho a la Protección de Datos Personales para ser trasmitidos en las sucursales bancarias en las televisiones que se colocan frente a las filas de ventanillas. (Esto se está haciendo con el reglamento de tránsito de la CDMX)
- Convenio con la ABM para la distribución de la Carta de Derecho a la Protección de Datos Personales a los usuarios de la banca cuando realizan un trámite en ventanilla.
- Asesorar en contenidos a la ABM para que en su página web en la sección Recomendaciones de Seguridad se pueda ampliar la información sobre el robo de Información y establecer un vínculo al INAI.
- Convenio con la ABM para implementar una campaña de dos meses o más (dependiendo el costo y el alcance) con el objetivo de que la banca comercial mediante sus aplicaciones en dispositivos móviles incluyan un flash sobre el derecho a la protección de datos personales. Este convenio se propone como un convenio específico, en el marco de un convenio amplio que el INAI ya ha firmado con la ABM; firmado en el 2012 con el extinto IFAI y en el cual se establece como objeto del mismo establecer las bases y mecanismos entre ambas instituciones para la ejecución de diversas acciones y actividades dirigidas a difundir y ampliar el conocimiento del derecho a la protección de datos personales y promover el cumplimiento de la LFPDPPP[163].

[163] Convenio entre el IFAI y la Asociación de Bancos de México. En línea en http://inicio.ifai.org.mx/ConveniosProteccionDeDatos/1ConvenioAsociacindeBancosdeMxicoABMAC.pdf

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario			
Población Objetivo Prioridad 4	**Asociación de Bancos de México**	**Acciones**	**Zona geográfica prioritaria**
Usuarios de Servicios Financieros: 29.4 millones de usuarios	Según cifras de la Asociación de Bancos de México (ABM), en el país hay más de 12, 233 sucursales bancarias operadas por 45 bancos comerciales.	I. Utilización de espacios a través de posters temáticos colocados en lugares visibles en las sucursales bancarias. II. Promoción de spots de 50 segundos sobre el tema de protección de datos personales para ser trasmitidos en las sucursales bancarias. (Esto se está haciendo con el reglamento de tránsito de la CDMX) III. Convenio con la Asociación de Bancos de México para la distribución de la Carta de Derecho a la Protección de Datos Personales[164] a los usuarios de la banca cuando realizan un trámite en ventanilla. IV. Asesorar en contenidos a la Asociación de Bancos de México para que en su página web en la sección *Recomendaciones de Seguridad* se pueda ampliar la información sobre el *Robo de Información* y establecer un vínculo al INAI. V. Convenio con la Asociación de Bancos de México para	Por el número de titulares a los que potencialmente se puede llegar, se proponen la Ciudad de México, el Estado de México, Guadalajara, Jalisco y Monterrey, Nuevo León, por considerarse las ciudades con alta población urbana, con base al número de usuarios en zonas urbanas. Se sugiere alcanzar en los tres años de la propuesta al mayor número de estados de la República mexicana en alcance por número de población urbana.

[164] Se sugiere diseñar un tríptico descriptivo que enuncie el derecho.

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario			
Población Objetivo Prioridad 4	**Asociación de Bancos de México**	**Acciones**	**Zona geográfica prioritaria**
		implementar una campaña de dos meses con el objetivo de que la banca comercial a través de sus aplicaciones en dispositivos móviles incluyan un flash sobre el derecho a la protección de datos personales.	

- **Confederación Patronal de la República Mexicana**

Justificación Institucional para el trabajo con el Confederación Patronal de la República Mexicana (COPARMEX): La misión de este órgano empresarial es contribuir al establecimiento de condiciones para la prosperidad de todos los mexicanos que propicien una creciente cohesión social, para que las empresas se desarrollen, multipliquen y cumplan con su función creadora de empleo y de riqueza con responsabilidad social.[165]

La COPARMEX directamente se encamina a ser una institución independiente de referencia obligada para el empresariado y la sociedad en general por:

- Su contribución significativa al desarrollo integral basado en la competitividad y en la libre competencia en todos los ámbitos del país;
- Así como al establecimiento de las condiciones para la prosperidad de todos los mexicanos.

Los objetivos institucionales de la COPARMEX reflejan la finalidad de sus recursos e incidencia y marcan la guía con la que se dirige la Confederación en sus actividades y posicionamientos, siendo el "Bien Común" su principal máxima:

Entre sus objetivos estratégico destacan:

- Fortalecimiento de Coparmex
- **Educación de calidad para todos**
- **Cultura de libre competencia y emprendimiento**
- Competitividad y desarrollo económico Transparencia y rendición de cuentas
- Estado de derecho democrático, inclusión social y combate a la impunidad

En su Plan Estratégico destaca que desde 1929 la Confederación ha promovido el pleno y efectivo ejercicio de los derechos ciudadanos en todos los ámbitos, porque no existe la democracia sin ciudadanía. "La participación activa de la sociedad es la única forma que tenemos los ciudadanos de perfilar el México del futuro que todos queremos."[166]

En ese sentido, una alianza con la COPARMEX resulta ser estratégica para que el INAI pueda promover el Derecho a la Protección de Datos Personales, más aún aprovechar la presencia de ésta en el país y su grado de incidencia y alianza con los gobiernos federal y estatales.

[165] Página web de la COPARMEX, Misión y Visión, disponible en http://www.coparmex.org.mx/index.php?option=com_content&view=article&id=47&Itemid=107
[166] Página web de la COPARMEX, Plan Estratégico, disponible en http://www.coparmex.org.mx/images/stories/pdf/ser_coparmex_2015.pdf

¿Por qué y para qué una alianza con COPARMEX:

La COPARMEX está conformada por una red de 65 Centros Empresariales, 13 Federaciones, 2 Representaciones y 14 Delegaciones en todos los estados de la República. Sus más de 36 mil empresas socias en todo el país son responsables del 30% del PIB y de 4.8 millones de empleos formales. Además, 27 Comisiones de Trabajo nacionales se dedican al estudio y generación de propuestas en las temáticas más importantes de la economía y la sociedad, lo que puede ser una oportunidad para el INAI de promover entre sus empleados (as) el Derecho a la Protección de Datos Personales.

Formas de Alianza

- Organizar de manera conjunta espacios informativos para la defensa y promoción del Derecho a la Protección de Datos Personales.
- Establecer alianzas con las Cámaras locales para realizar jornadas de divulgación sobre la defensa y promoción del Derecho a la Protección de Datos Personales.
- Promover con sus afiliados en los estados la distribución de materiales informativos sobre la defensa y promoción del Derecho a la Protección de Datos Personales que puedan ser entregados a sus consumidores mediante el uso de espacios físicos y virtuales.

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario			
Población Objetivo Prioridad 4	**CONFEDERACIÓN PATRONAL DE LA REPÚBLICA MEXICANA**	**Acciones**	**Zona geográfica prioritaria**
Usuarios de Servicios Financieros: 29.4 millones de usuarios	La Confederación Patronal de la República Mexicana (COPARMEX) cuenta con más de 36,000 empresas afiliadas en todo el país y presencia en los 32 Estados de la República, organizados en 10 Federaciones, que cuentan en total con 65 Centros Empresariales, 14 Delegaciones y 3 Representaciones.	I. Alianza de colaboración para promover una cultura de derecho, a la promoción y defensa del Derecho a la Protección de Datos Personales y sus mecanismos de defensa. a) Organizar de manera conjunta espacios informativos para la defensa y promoción del Derecho a la Protección de Datos Personales. b) Establecer alianzas con las Cámaras locales para la realizar jornadas de divulgación sobre la defensa y promoción del Derecho a la Protección de Datos Personales. c) Promover con sus afiliados en los estados la distribución de materiales informativos sobre la defensa y promoción del Derecho a la Protección de Datos Personales que puedan ser entregados a sus consumidores.	Por el número de titulares a los que potencialmente se puede llegar, se proponen la Ciudad de México, el Estado de México, Guadalajara, Jalisco y Monterrey, Nuevo León, por considerarse las ciudades con alta población urbana, con base al número de usuarios en zonas urbanas. Asimismo, se sugiere aprovechar las alianzas con las Cámaras locales de los estados propuestos. Se sugiere alcanzar en los tres años de la propuesta al mayor número de estados de la República mexicana en alcance por número de población urbana.

- **Consejería en Seguros y Finanzas**

La CONSEFIN tiene una visión y misión enfocada únicamente a sus asociados y no va más allá que brindar asesoría y atención a sus clientes para la venta de sus productos. No obstante, se considera una ventana de oportunidad por las 18 alianzas que ésta tiene con las compañías del sector Asegurador, Afianzador, Salud, Bancario y de Afores, por ejemplo con:

- GNP Seguros
- INBURSA Grupo Financiero
- MAPFRE
- AXXA
- Seguros BANORTE
- AIG
- ASERTA Afianzadora
- ABA Seguros
- Médica VRIM
- Afianzadora SOFIMEX, S.A.
- GMX Seguros
- Quálitas
- Pr1mero Seguros
- RSA
- Insurgentes Afianzadora

¿Por qué y para qué una alianza con la Consejería en Seguros y Finanzas (CONSEFIN): Una alianza con ellos, permitiría incidir en una población amplia mediante sus sucursales y los titulares del derecho que cuenten con seguros o fianzas —según datos de la CONDUSEF, en México más de 15 millones de personas cuentan con algún seguro privado.[167]

[167] Página web de la CONDUSEF http://www.condusef.gob.mx/PDF-s/educacion_financiera/cuadernos/cuadernoSeguros.pdf

Formas de Alianza

- Utilización de espacios visibles en las compañías del sector asegurador para colocar posters con mensajes a los titulares del Derecho a la Protección de Datos Personales.
- Conferencias dirigidas a los titulares del derecho, que informen sobre los mecanismos y formas de denuncia, así como de la normatividad que hace valer sus derechos.
- Convenio con la CONSEFIN para la distribución de la Carta de Derecho a la Protección de Datos Personales a los usuarios del Sector.

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario			
Población Objetivo Prioridad 4	**CONSEJERÍA EN SEGUROS Y FIANZAS**	**Acciones**	**Zona geográfica prioritaria**
Usuarios de Servicios Financieros: 29.4 millones de usuarios	La Consejería en Seguros y Finanzas (CONSEFIN), tiene alianzas con 18 compañías de Sector Asegurador, Afianzador, Salud, Bancario y de Afores.	I. Utilización de espacios a través de posters temáticos colocados en lugares visibles en las compañías del sector asegurador. II. Conferencias dirigidas a los titulares del derecho, que informen sobre los mecanismos y formas de denuncia, así como de la normatividad que hace valer su derecho. III. Convenio con la CONSEFIN para la distribución de la Carta de Derecho a la Protección de Datos Personales a los usuarios del Sector.	Por el número de titulares a los que potencialmente se puede llegar a través de las alianzas que CONSEFIN tiene, se proponen la Ciudad de México, el Estado de México, Guadalajara, Jalisco y Monterrey, Nuevo León, por considerarse las ciudades con alta población urbana, con base al número de usuarios en zonas urbanas. Se sugiere alcanzar en los tres años de la propuesta al mayor número de estados de la República mexicana en alcance por número de población urbana.

- **Confederación de Cámaras Nacionales de Comercio, Servicios y Turismo**

Justificación Institucional para el trabajo con el Confederación de Cámaras Nacionales de Comercio, Servicios y Turismo (CONCANACO): La CONCANACO es una institución de interés público, autónoma y que representa, promueve y defiende a nivel nacional e internacional las actividades del Comercio, los Servicios y el Turismo.

Además colabora con el gobierno para lograr el crecimiento económico así como la generación de la riqueza. Es por Ley un órgano de consulta y colaboración de las autoridades federales, estatales y municipales en todos aquellos asuntos relacionados con el Comercio, los Servicios y el Turismo.[168]

Entre sus objetivos destacan:

- Coadyuvar a la unión y desarrollo de las Cámaras Confederadas.
- Fomentar la eficacia competitiva de los establecimientos de Comercio, Servicios y Turismo.
- **Fortalecer la imagen de los sectores Comercio, Servicios y Turismo.**
- **Promover el sano desarrollo de los negocios, procurando elevar la ética empresarial.**
- Establecer relaciones de colaboración con instituciones afines, nacionales y extranjeras.

La Concanaco ha participado en la promoción y ejercicio pleno de los derechos de los ciudadanos en distintos ámbitos, por ejemplo, actualmente mantiene convenios con el Instituto Nacional Electoral, la Procuraduría Federal del Consumidor, el Instituto Nacional de Educación para Adultos.[169] Por lo anterior, una alianza con la Concanaco puede resultar estratégica en la promoción del Derecho a la Protección de Datos Personales entre sus integrantes.

¿Por qué y para qué una alianza con CONCANACO: La CONCANACO es el Organismo Empresarial más grande y representativo de México, cuenta con 254 Cámaras y a su vez representa a más de 670,000 empresas. Además, la participación de los sectores representados por la Concanaco Servytur asciende a 52.5 por ciento del total de la economía, que se ha sostenido en los últimos 10 años. Asimismo, ha mantenido por arriba del 53 por ciento su participación en el empleo formal en México, lo que puede ser una oportunidad de incidencia para el INAI y aprovechar con ello llegar al mayor número de población posible.[170]

[168] Página web de la Concanaco, Misión y Visión, disponible en http://www.concanaco.com.mx/que-es-la-concanaco/
[169] [169] Página web de la Concanaco, Convenios, disponible en http://www.concanaco.com.mx/convenios-concanaco/
[170] Página web de la Concanaco, Misión y Visión, disponible en http://www.concanaco.com.mx/que-es-la-concanaco/

Formas de Alianza

- Organizar de manera conjunta espacios informativos para la defensa y promoción del Derecho a la Protección de Datos Personales.
- Establecer alianzas con las Cámaras locales para la realizar jornadas de divulgación sobre la defensa y promoción del Derecho a la Protección de Datos Personales.
- Promover con sus afiliados en los estados la distribución de materiales informativos sobre la defensa y promoción del Derecho a la Protección de Datos Personales que puedan ser entregados a sus consumidores.

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario			
Población Objetivo Prioridad 4	**CONFEDERACIÓN DE CÁMARAS NACIONALES DE COMERCIO**	**Acciones**	**Zona geográfica prioritaria**
Usuarios de Servicios Financieros: 29.4 millones de usuarios	La Confederación de Cámaras Nacionales de Comercio (CONCANACO) cuenta con 257 Cámaras en territorio nacional, 670 mil empresas afiliadas y presencia en 600 ciudades del País. Los giros que conforman esta Estructura están organizados por áreas, entre las que destacan: Automotriz, Construcción, Distribuidores de combustibles, Alimentación, Artículos para el Hogar, Servicios Financieros, Servicios Inmobiliarios, Área del vestido y el Calzado, Turismo, etc.	I. Alianza de colaboración para promover una cultura de derecho, a la promoción y defensa del Derecho a la Protección de Datos Personales y sus mecanismos de defensa. a) Organizar de manera conjunta espacios informativos para la defensa y promoción del Derecho a la Protección de Datos Personales. b) Establecer alianzas con las Cámaras locales para la realizar jornadas de divulgación sobre la defensa y promoción del	Por el número de titulares a los que potencialmente se puede llegar, se proponen la Ciudad de México, el Estado de México, Guadalajara, Jalisco y Monterrey, Nuevo León, por considerarse las ciudades con alta población urbana, con base al número de usuarios en zonas urbanas. Asimismo, se sugiere aprovechar las alianzas con las Cámaras locales de los estados propuestos. Se sugiere alcanzar en los tres años de la propuesta al mayor número de estados de la República mexicana en alcance por número de población

Alianzas y Acciones con Instancias Públicas y Privadas por población objetivo y grupo prioritario			
Población Objetivo Prioridad 4	**CONFEDERACIÓN DE CÁMARAS NACIONALES DE COMERCIO**	**Acciones**	**Zona geográfica prioritaria**
		Derecho a la Protección de Datos Personales. c) Promover con sus afiliados en los estados la distribución de materiales informativos sobre la defensa y promoción del Derecho a la Protección de Datos Personales que puedan ser entregados a sus consumidores. I.	urbana.

d. Etapas para la implementación

En la implementación de esta estrategia con base en la teoría de cambio, se debe tomar en cuenta que la formación de ciudadanía es un ejercicio que corresponde a diversos actores tanto públicos como privados y que tal propósito, que responde y contribuye a otro mayor, el objetivo de construir una democracia, en la que el poder se distribuya, se regule socialmente y las decisiones públicas sean incluyentes. La contribución del INAI en la comprensión de los valores y principios democráticos a través de la promoción del derecho a la protección de datos personales entre los titulares; la adquisición y ejercicio de las habilidades necesarias para una interacción eficaz y respetuosa entre ciudadanas y ciudadanos, y entre éstos y las organizaciones del poder público y de actores privados, es una contribución mayor para el funcionamiento y sentido de las instituciones que constituyen un régimen democrático. Cabe recordar que la asimilación de derechos, se encuentra ubicada en el espacio de la estructura cultural y que éste es un ámbito en el cual los procesos requieren de tiempo.

En la construcción de los valores antes mencionados, aún es necesario el fortalecimiento de la calidad de las y los habitantes del país como ciudadanos, así como su capacidad como agentes que ejercen responsablemente sus derechos para la configuración del espacio público. En una circunstancia tal, la promoción del derecho a la protección de datos personales, se convierte en una idea por madurar de manera urgente.

La presente estrategia se propone como un documento de planeación que define la orientación, propósitos y alcance de las acciones que realizará el INAI durante el periodo de 2016 a 2019, para dar cumplimiento al mandato constitucional, legal y reglamentario que tiene en materia de educación cívica en la promoción del derecho a la protección de datos personales.

La experiencia que tiene el Instituto en el desarrollo de sus actividades nos ha llevado a plantear un horizonte de mediano plazo (tres años) en la definición de sus aspiraciones, ya que el alcance y maduración de la ciudadanía en el ejercicio de este derecho debe ser revisado y evaluado de manera sistemática y tomando en cuenta la creciente y rápida evolución de los mecanismos informáticos.

En el entendido de que el ciclo básico lo establecen los periodos de gestión presupuestal, se proponen ciclos anuales de revisión de la estrategia que definan y redefinan programas operativos expresados tanto en las políticas y programas anuales del Instituto como en su calendario anual de actividades, revisando si las actividades y las metas han respondido a lo planeado y al mismo tiempo haciendo una revisión FODA (Fortalezas, Oportunidades, Debilidades y Amenazas), que permitan fortalecer las líneas de

acción que haya que fortalecer y continuar con aquellas que han sido exitosas para los alcances; sin embargo la estrategia debe contemplar el "mediano plazo" para fijar objetivos estratégicos considerando el alcance de las acciones en materia de educación cívica y las alianzas estratégicas a nivel nacional.

Adicional a lo anterior, otra de las razones por las que se optó por una decisión estratégica con una temporalidad de tres años está relacionada con el propósito fundamental de impulsar políticas públicas orientadas a la promoción del derecho a la protección de datos personales en alianza con diversos actores: autoridades e instituciones de los tres niveles de gobierno, organizaciones de la sociedad civil, instituciones académicas, entre otros. Este objetivo se puede alcanzar en dicho periodo, debido al tiempo y demás recursos que resultan necesarios para su implementación.

Del mismo modo la construcción de ciudadanía implica un cambio cultural que permita empoderar a los y las ciudadanos/as para ejercer sus derechos y que sean capaces de participar activamente en la responsabilidad de prever el riesgo que implica que sus datos estén en posesión de otros actores. Dicho cambio necesita un cierto tiempo de maduración, por lo que todos los proyectos en materia de educación cívica en este derecho deben tener continuidad y estar orientados al logro de este propósito.

Las etapas planteadas en la Matriz de la Estrategia son:

1ª etapa: Responde a la exposición de los individuos al lenguaje, a los símbolos y significados de este derecho. Es la primer parte del proceso de aprendizaje.

2ª etapa: Responde a la asimilación —mediante la familiarización y la repetición— del lenguaje, símbolos y significados del derecho a la protección de datos personales.

3ª etapa: Responde al último proceso del conocimiento que es la externalización de lo aprehendido[171].

Las etapas planteadas no deben ser necesariamente consecutivas. Algunas pueden ser permanentes y la mayor parte de las veces se deben instrumentar de manera paralela. La evaluación de la operación anual de la estrategia debe ayudar en esta definición.

[171] Berger, Peter y Luckmann Thomas. La construcción social de la realidad. Amorrortu editores. Argentina 1994. Pp 46 y 47

X. RESULTADOS ESPERADOS

Los resultados esperados que se plantean en esta estrategia, se plantean tanto por objetivos estratégicos, como se debe plantear de acuerdo a un Marco Lógico[172], tanto como por los grupos prioritarios propuestos.

Así, por objetivos planteados, los resultados esperados son :

Objetivo 1

Que los titulares conozcan el derecho que tienen a la protección de sus datos personales.

Actividades:

a) Talleres, seminarios y conferencias dirigidas a los titulares del derecho con información sobre lo que es el derecho a la protección de datos.

b) Generación de alianzas estratégicas con actores públicos y privados clave para alcanzar mediante diferentes estrategias de educación a las poblaciones objetivo prioritarias.

c) Utilización de redes sociales, plataformas y mecanismos virtuales para difundir el derecho a la protección de datos personales.

Resultados Esperados

Poblaciones objetivo titulares del derecho, prioritarias en esta estrategia, informadas sobre el mismo.

Objetivo 2

Que los titulares puedan reconocer y valorar adecuadamente los riesgos a los que se enfrentan en el otorgamiento de sus datos personales.

Actividades:

a) Talleres, seminarios y conferencias dirigidas a los titulares del derecho con información sobre los riesgos a los que se enfrentan al otorgar sus datos personales a sujetos públicos o privados.

[172] Es una herramienta analítica para planificación de la gestión y evaluación de programas y proyectos orientados a procesos, desarrollada en 1969. Es utilizado con frecuencia por organismos de cooperación internacional, por gobiernos y por organizaciones de sociedad civil. En el **Enfoque de Marco Lógico** se considera que la ejecución de un proyecto es consecuencia de un conjunto de acontecimientos con una relación causal interna. Estos se describen en: insumos, actividades, resultados, objetivo específico y objetivo global. Las incertidumbres del proceso se explican con los factores externos (o supuestos) en cada nivel. De modo general, se hace un resumen del proceso de desarrollo en una matriz que consiste en los elementos básicos arriba mencionados, dicha matriz es conocida como la **Matriz del Proyecto** (MP) a veces es conocida como Matriz de Planificación de Marco Lógico. Documento "Metodología de Marco Lógico para la planificación, evaluación y seguimiento de proyectos y programas" ILPES y CEPAL, Santiago de Chile, julio del 2005. Disponible en línea en: http://repositorio.cepal.org/bitstream/handle/11362/5607/S057518_es.pdf;jsessionid=B514CB74323CE225187235A8A522C4BE?sequence=1

b) Generación de alianzas estratégicas con actores públicos y privados clave para alcanzar mediante diferentes estrategias de educación a las poblaciones objetivo prioritarias.

c) Utilización de redes sociales, plataformas y mecanismos virtuales para difundir los riesgos a los que se enfrentan los titulares al otorgar sus datos personales.

Resultados Esperados:

Poblaciones objetivo titulares del derecho, prioritarias en esta estrategia, informadas sobre el riesgo que enfrentan al otorgar sus datos personales a instituciones tanto públicas como privadas.

Objetivo 3

Que los titulares puedan tomar decisiones informadas sobre el otorgamiento de sus datos personales a los sujetos obligados.

Actividades

a) Talleres, seminarios y conferencias dirigidas a los titulares del derecho, que brinden herramientas para que éstos puedan discernir sobre los mecansimos que los sujetos obligados deben tener para que los titulares del derecho otorguen sus datos personales de manera segura.

b) Generación de alianzas estratégicas con actores públicos y privados clave para alcanzar, mediante diferentes estrategias de educación, a las poblaciones objetivo prioritarias.

c) Utilización de redes sociales, plataformas y mecanismos virtuales para difundir las herramientas que los titulares deben conocer para discernir sobre los mecansimos que los sujetos obligados deben tener para que los titulares del derecho otorguen sus datos personales de manera segura.

Resultados Esperados

Poblaciones objetivo titulares del derecho, prioritarias en esta estrategia, conscientes de riesgos y de la normatividad para los sujetos obligados, al otorgar sus datos personales a instituciones tanto públicas como privadas.

Objetivo 4

Que los titulares conozcan y utilicen los mecanismos establecidos para hacer valer sus derechos y denunciar los posibles incumplimientos por parte de los sujetos obligados.

Actividades

a) Talleres, seminarios y conferencias dirigidas a los titulares del derecho, que informen sobre los mecanismos y formas de denuncia, así como de la normatividad que hace valer sus derechos.

b) Generación de alianzas estratégicas con actores públicos y privados clave para alcanzar, mediante diferentes estrategias de educación, a las poblaciones objetivo prioritarias.

c) Utilización de redes sociales, plataformas y mecanismos virtuales que informen y contengan los mecanismos y formas de denuncia, así como de la normatividad que permita ejercer el derecho a la protección de datos personales.

Resultados Esperados

Poblaciones objetivo titulares del derecho, prioritarias en esta estrategia, haciendo exigible su derecho a la protección de datos personales frente a los sujetos obligados.

Por grupos prioritarios:

2. **Prioridad 1. Usuarios de Telecomunicaciones (Convergen Comercio electrónico)**

   Número de Titulares: 103 millones de usuarios

Actividades: Planteadas en el capítulo anterior de estrategia de alianzas.

Resultados Esperados:

- Ciudadanos y ciudadanas usuarios de servicios de comercio electrónico y telecomunicaciones conscientes del derecho a la protección de sus datos personales conscientes del riesgo de otorgar sus datos personales.
- Ciudadanos y ciudadanas que conocen y hacen exigible su derecho a la protección de datos personales.

3. **Prioridad 2. Usuarios de Servicios Médicos**

   Número de Titulares: 552 mil personas que utilizan servicios privados y cerca de 91 millones de usuarios de servicios médicos públicos.

Actividades: Planteadas en el capítulo anterior de estrategia de alianzas.

Resultados Esperados:

- Ciudadanos y ciudadanas usuarios de servicios médicos conscientes del riesgo de proporcionar sus datos personales y de su posible uso por cualquier persona o institución que no garantice el uso de los datos conforme a la normatividad establecida
- Ciudadanos y ciudadanas usuarios de servicios médicos tanto públicos como privados que saben a qué instancia acudir y hacen exigible su derecho a la protección de datos personales frente a las instancias de salud públicas y privadas.

4. Prioridad 3. Niñez de 6 a 12 años y Jóvenes de 12 a 17 años

Número de Titulares: 26. 8 millones de titulares (13.4 millones de niñas y niños entre 6 y 12 años y 13.4 millones de jóvenes de 12 a 17)

Actividades: Planteadas en el capítulo anterior de estrategia de alianzas.

Resultados Esperados:

- Padres, madres y/o tutores concientizados en el derecho a la protección de datos personales y con conocimiento del riesgo de que los menores proporcionen datos personales.
- Niñas y niños conscientes del riesgo de proporcionar datos personales.
- Jóvenes conocedores de su derecho a la protección de datos personales y conscientes del riesgo que puede implicar otorgar sus datos personales sin precaución, así como jóvenes sujetos que hacen exigible su derecho a la protección de datos personales frente a los sujetos obligados.

5. Prioridad 4. Usuarios de Servicios Financieros

Número de Titulares: 29.4 millones de usuarios

Actividades: Planteadas en el capítulo anterior de estrategia de alianzas.

Resultados Esperados:

- Ciudadanos y ciudadanas usuarios de servicios financieros conscientes del riesgo de proporcionar sus datos personales y de su posible uso por cualquier persona o institución financiera que no garantice el uso de los datos conforme a la normatividad establecida.
- Ciudadanos y ciudadanas usuarios de servicios financieros conscientes de su derecho y ejerciéndolo denunciando toda anomalía en el uso y tratamiento de sus datos personales.

XI. ELEMENTOS ORGANIZACIONALES

Esta propuesta no es una evaluación organizacional dirigida a la estructura ni a los procesos y procedimientos de toma de decisión dentro del INAI, sin embargo es menester mencionar que, a partir de las entrevistas a funcionarios del INAI y de documentos revisados, se han evidenciado ausencias en procedimientos de coordinación así como un menor nivel de importancia institucional del tema de la promoción del Derecho a la Protección de Datos Personales, en comparación con el otorgado al de Transparencia y Acceso a la Información Pública Gubernamental, mismos que pueden impedir que la estrategia no tenga los alcances deseados ya que no se han institucionalizado algunos procedimientos y dependen aún de la voluntad de las personas en cargos de toma de decisión.

El nivel de importancia que el Estado mexicano ha dado a la protección de datos personales en la Constitución y en la normatividad derivada de ésta, no corresponde con el nivel de prioridad que el Instituto le ha concedido. A pesar de ser una de las líneas estratégicas de la Planeación Institucional, la forma en la que es asumido el tema del derecho a la Protección de Datos Personales en el Instituto, evidencia la necesidad de una estrategia coordinada entre las áreas a las que les compete la promoción del derecho e impulsada desde el máximo órgano de Dirección del Instituto. Esto se hace urgente para lograr el posicionamiento del derecho, no sólo entre los sujetos obligados, sino entre los titulares. Lo anterior se sostiene con la revisión del documento del INAI denominado Presupuesto Ciudadano 2015 en el que se informa a la ciudadanía sobre el presupuesto y el destino de los recursos del INAI: La Coordinación de Acceso a la Información manejó para el 2015 un presupuesto de $35, 674, 313.00 MN, mientras que la Coordinación de Protección de Datos manejó un presupuesto de $14, 070, 470.00 MN.[173] La responsabilidad del INAI en el posicionamiento de este derecho, como un derecho urgente de madurar en la ciudadanía debe ser asumida como tal.

[173] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Presupuesto Ciudadano 2015", 2015, (en línea), disponible en: http://inicio.ifai.org.mx/nuevo/PresupuestoCiudadano_INAI_Final_30Junio2015_VersionPleno.pdf (Consultada el 15 de noviembre de 2015)

XII. BIBLIOGRAFÍA

Arenas Ramiro, Mónica. Profesora Ayudante Doctor Universidad de Alcalá de Henares, **La protección de datos personales en los países de la Unión Europea**. (Versión PDF)

Berger, Peter y Luckmann Thomas. La construcción social de la realidad. Amorrortu editores. Argentina 1994. Pp 46 y 47

Gutwirth Serge, Poullet Yves, **Data protection in a profiled world**, De Hert Pal (editors), Bélgica, 2010.

Henry Mintzberg, **The rise and fall of strategic Planning: Reconceiving Roles for Planning, Plans, Planners**, The Free Press (editors), United States, 1994.

Instituto Federal de Acceso a la Información Pública Gubernamental, **Estudio sobre Protección de Datos**, IFAI, México, 2004.

Instituto Federal de Acceso a la Información y Protección de Datos Personales, **Metodología de Análisis de Riesgo BAA**, IFAI, México, 2013.

Jay Rosemary y Clarke Jane, **Data Protection Compliance in the UK. A pocket guide**, Second Edition, Pinsent Masons, IT Governance Publishing, United Kingdom, 2008.

IPSOS e IFAI, **Encuesta Nacional sobre Protección de Datos Personales a Sujetos Regulados por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y Población en General**, México, 2012.

Noriswadi Ismail, **Beyond data protection. Strategic case studies and practical guidance**, Lee Yong Cieh Edwing (editors), Germany, 2013.

Office of the Privacy Commissioner of Canada, **The OPC Privacy priorities 2015-2020. Mapping a course for greater protection**, Canada, 2015.

Torres Natalia, Caso de estudio: Argentina. En Torres Natalia (compiladora). **Acceso a la información y datos personales: una vieja tensión, nuevos desafío**. Universidad de Palermo, Centro de Estudios sobre la Libertad de Expresión, s/f.

XIII. FUENTES ELECTRÓNICAS

Agencia Española de Protección de Datos, disponible en: http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

Asociación Mexicana de Internet, "Día de Internet 2014. Estudio sobre los hábitos de los usuarios de internet en México 2014", 2014, disponible en: https://www.amipci.org.mx/estudios/habitos_de_internet/Estudio_Habitos_del_Internauta_Mexicano_2014_V_MD.pdf

Asociación Mexicana de Internet, "Estudio Comercio Electrónico en México 2015", 2015, disponible en: https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf

Australian Government, Office of the Australian Information Commissioner, disponible en: http://www.oaic.gov.au/about-us/our-regulatory-approach/all/

Campus Virtual de la Dirección Nacional de Protección de Datos Personales, Argentina, disponible en: https://capacitacion.jus.gov.ar/dnpdp

Carta de los derechos fundamentales de la Unión Europea, disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/B.1-cp--Carta-de-los-Derechos-Fundamentales.pdf

Código Civil Federal, México, 2013, disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/2_241213.pdf
Comisión Nacional de Informática y Libertades, Francia, disponible en: http://www.cnil.fr/

Comisión Nacional de los Derechos Humanos, México, disponible en: http://www.cndh.org.mx/

Conectar Igualdad, Argentina, disponible en: http://www.conectarigualdad.gob.ar/
Constitución Política de Brasil, 1988, disponible en:http://pdba.georgetown.edu/Constitutions/Brazil/esp88.html

Constitución Política de los Estados Unidos Mexicanos, 1917, disponible en: http://www.diputados.gob.mx/LeyesBiblio/htm/1.htm

Convenio nº 108 del consejo de Europa, "Para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", 1981, disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf

Declaración Universal de los Derechos Humanos, 1948, disponible en: http://www.un.org/es/documents/udhr/

Declaración de los Derechos del Hombre y del Ciudadano, 1789, disponible en: http://www.juridicas.unam.mx/publica/librev/rev/derhum/cont/30/pr/pr23.pdf

DLA PIPER, "Data protection laws of the world, World Map", 2015, disponible en: http://dlapiperdataprotection.com/#handbook/world-map-section

Dirección Nacional de Protección de Datos Personales, Argentina, disponible en: http://www.jus.gob.ar/datos-personales.aspx

Dirección Nacional de Protección de Datos Personales, Argentina, "Leyes y Decretos", disponible en: http://www.jus.gob.ar/datos-personales/documentacion-y-capacitacion/normativa/normativa-proteccion-de-datos-personales/leyes-y-decretos.aspx

Directrices de Armonización de la protección de datos en la Comunidad Iberoamericana, disponible en: http://inicio.ifai.org.mx/Estudios/Directrices_de_armonizacion.pdf

Educación Financiera y Condusef, "A, B, C De Educación Financiera", 2009, disponible en: http://www.condusef.gob.mx/PDF-s/mat_difusion/abc_09.pdf

European Parliament, disponible en: http://www.europarl.europa.eu/elections-2014/en/press-kit/civil-liberties-data-privacy-protecting-the-vulnerable

Encuesta Nacional de la Dinámica Demográfica 2014 INEGI disponible en: http://www.inegi.org.mx/est/contenidos/proyectos/encuestas/hogares/especiales/enadid/enadid2014/doc/resultados_enadid14.pdf

Fundación Protección de Datos Personales, Chile, disponible en: http://protecciondedatospersonales.cl/
García González Aristeo, "La protección de datos personales: derecho fundamental del siglo xxi. Un estudio comparado", 2011, disponible en: http://www.juridicas.unam.mx/publica/rev/boletin/cont/120/art/art3.htm

Gobierno de la República, "Plan Nacional de Desarrollo 2013-2018", México, 2013, disponible en: http://www.imjuventud.gob.mx/imgs/uploads/Informe_Projuventud_2014.pdf

Grupo de trabajo del artículo 29 sobre protección de datos, "Dictamen 11/2011 relativo al nivel de protección de datos personales en Nueva Zelanda", 2011, disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp182_es.pdf

Information Commissioner's Office, Inglaterra, 2015, disponible en: https://ico.org.uk/about-the-ico/news-and-events/events-and-webinars/

Instituto Federal de Telecomunicaciones, México, "Líneas de Telefonía Fija", 2015, disponible en: http://cgpe.ift.org.mx/2ite15/tel_fijas.html

Instituto Nacional Electoral, México, disponible en: http://www.ine.mx/portal/

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, México, disponible en: http://inicio.inai.org.mx/SitePages/ifai.aspx

Legal Corp, "El derecho a la protección de los datos personales", 2013, disponible en: http://legalcorp.com.sv/index.php?option=com_content&view=article&id=26:el-derecho-a-la-proteccion-de-datos-personales&catid=2:actualidad&Itemid=3

Ley de la Comisión Nacional de los Derechos Humanos, México, 1992, disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/47.pdf

Ley General de Instituciones y Procedimientos Electorales, México, 2014, disponible en: http://norma.ife.org.mx/documents/27912/310245/2014_LGIPE.pdf/5201e72c-0080-4acb-b933-5137ef1c0c86

Ley General de Transparencia y Acceso a la Información Pública, México, 2015, disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, México, 2002, disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/244_140714.pdf

Ley Federal de Protección al Consumidor, México, 1992, disponible en: http://www.profeco.gob.mx/juridico/pdf/l_lfpc_ultimo_CamDip.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, México, 2010, disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley de Protección de los Datos Personales, Argentina, 2000, disponible en: http://www.oas.org/juridico/PDFs/arg_ley25326.pdf

Ley de Protección de la Vida Privada, Chile, 1999, disponible: http://www.leychile.cl/Navegar?idNorma=141599

Ley de Protección y Defensa al Usuario de Servicios Financieros, México, 1999, disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/64.pdf

Listas Robinson de Exclusión Publicitaria, disponible en: www.listarobinson.es

National Agency for Personal Data Protection, Nueva Zelanda, "My Privacy" - Awareness Campaign with Schools Commenced", 2013, disponible en: http://www.amdp-rks.org/web/?page=2,10,128#.VilFyvkrLIU

Office of the Privacy Commissioner of Canada, disponible en: https://www.priv.gc.ca/index_e.asp

Personal Data Protection, Singapore, disponible en: https://www.pdpc.gov.sg/home

Principios de la Privacidad de la Información de la APEC, 2005, disponible en: http://biblio.juridicas.unam.mx/libros/7/3249/27.pdf

Privacy Commissioner Te Mana Matapono Matatapu, Nueva Zelanda, disponible en: https://privacy.org.nz

Procuraduría Federal del Consumidor, México, disponible en: http://www.profeco.gob.mx/

Proteja su dinero "Descubre los hábitos de los usuarios bancarizados en internet", 2014, disponible en: http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/servicios-financieros/462-a-un-solo-clic

Red Iberoamericana de Protección de Datos, "Cuadro Comparativo: Desarrollos Normativos Nacionales en Materia de Protección de Datos", 2004, disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/iberoamerica/common/pdfs/cuadro_comparativo_de_normativas_15-6-2004_22_07_05.pdf

Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, México, 2003, disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFTAIPG.pdf

Saltor Carlos, “La Protección de Datos Personales: Estudio Comparativo Europa-América con especial análisis de la situación de Argentina”, Universidad Complutense de Madrid, 2013, disponible en: http://eprints.ucm.es/22832/1/T34731.pdf

Secretaría de Educación Pública, “Programa Sectorial de Educación 2013-2018”, México, 2013, disponible en: http://www.sep.gob.mx/work/models/sep1/Resource/4479/4/images/PROGRAMA_SECTORIAL_DE_EDUCACION_2013_2018_WEB.pdf

Secretaría de Hacienda y Crédito Público, Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, México, disponible en: http://www.condusef.gob.mx/

Toledo Báez, María Cristina “Aproximación a la protección de datos personales en España, Inglaterra y Francia como ejercicio de derecho comparado previo a una traducción”, 2010, disponible en: http://www.eumed.net/rev/cccss/07/mctb.htm

University of Alicante Intellectual Property & Information Technology, “Ley 9507/1997, de 12 de Noviembre de 1997, Ley Reglamentaria de Habeas Data, Regula el Derecho de Acceso a Informaciones, Disciplinas, y el Procedimiento del Habeas Data”, Brasil, 1997, disponible en: http://www.uaipit.com/es/legislacion/2344/Ley-9507/1997--de-12-de-Noviembre-de-1997--Ley-Reglamentaria-de-Habeas-Data--Regula-el-Derecho-de-Acceso-a-Informaciones--Disciplinas--y-el-Procedimiento-del-Habeas-Data-

ANEXOS

ANEXO I. ENTREVISTAS A INSTANCIAS DE OTROS PAÍSES

A. Australia

B. Canadá

C. Nueva Zelanda

D. Reino Unido

ANEXO II. ENTREVISTAS CON INSTANCIAS NACIONALES

A. CONDUSEF

B. Instituto Nacional Electoral

C. PROFECO

D. Secretaría de Salud

ANEXO III. ENTREVISTA CON INSTITUTO NACIONAL DE ACCESO A LA INFORMACIÓN

A. Dirección de Normatividad y Consulta de la Coordinación de Protección de Datos

B. Subdirección General de Comunicación Social y Difusión del INAI

C. Dirección General de Promoción y Vinculación con la Sociedad

D. Minuta de Reunión con Directivos de INAI

ANEXO IV. GRUPOS FOCALES

A. Grupo Focal con la Secretaria de Salud

B. Grupo Focal con el Instituto Mexicano de la Juventud