

Seminario, “El impacto de las transferencias internacionales de datos en América Latina

Otros Instrumentos preventivos en la aplicación de la normativa de protección de datos

Lina Ornelas Núñez

Directora General de Autorregulación
IFAI



Plan de Exposición

- IFAI; experiencia adquirida
- Verificaciones
- Capacitación
- Manifestaciones de Impacto a la Privacidad (PIA's)
- Nuevos Retos

IFAI... experiencia adquirida

- Previo a la Ley de Protección de Datos, el IFAI contaba ya con experiencia en materia de protección de datos, en virtud de las disposiciones contenidas en la Ley Federal de Transparencia y Acceso a la Información, (2002).
- Su ámbito de aplicación se limitó a las bases de datos del sector público a nivel federal.
- En un sólo capítulo (IV) establece un marco muy general que reguló la obtención, almacenamiento, transmisión, uso y manejo de los datos personales en posesión de dependencias y entidades federales.

IFAI... experiencia adquirida

- Emitió los “Lineamientos de Protección de Datos Personales”, a fin de establecer las condiciones y requisitos mínimos para el manejo y custodia de los sistemas de datos personales.
- De 2007 a la fecha, llevó a cabo 182 verificaciones a sistemas de datos personales de 13 dependencias y organismos de la administración pública federal.
- De entre éstas destacan: el Sistema de Información Anticipada sobre Pasajeros, APIS, el Registro Nacional de Víctimas u Ofendidos del Delito y el Registro de Beneficiarios de Programas Sociales.

Verificaciones

- El IFAI examina lo siguiente:
 - Principios
 - Licitud
 - Finalidad
 - Calidad
 - Proporcionalidad
 - Información
 - Custodia y cuidado
 - Seguridad

Verificaciones

- El IFAI examina lo siguiente:
 - Ejercicio de Derechos: Acceso y Corrección – Rectificación-.
 - Transmisiones de datos personales.
 - Contratación con terceros para el tratamiento de datos.
 - Registro en el Sistema “Persona”.

Capacitaciones

- El IFAI cuenta con una herramienta de capacitación (e-learning) que cuenta con un módulo de protección de datos y ha impartido numerosas capacitaciones in situ, entre las que destacan:
 - Registro Federal de Electores del Instituto Federal Electoral (IFE).
 - Curso sobre “La aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en materia de protección de datos”, a personal del INEGI.
 - “La protección de los datos personales en México, logros y retos”, impartida a personal de SEMARNAT.

Manifestación de Impacto a la Privacidad

- Valoración acerca de los riesgos reales o posibles que comprometan o vulneren la debida protección de los datos personales, derivados de la implementación de nuevas tecnologías o sistemas electrónicos.

Manifestación de Impacto a la Privacidad

- Derivado de experiencias internacionales, el momento adecuado para la elaboración de una PIA debe ser “ex ante” del lanzamiento de la política pública o proyecto de que se trate.
- Permite la construcción y consolidación de proyectos “seguros” en los que se vea involucrado, el tratamiento de información de carácter personal a través de nuevas tecnologías.

Ámbito Internacional

- Las legislaciones de Reino Unido, Canadá y Australia obligan a realizar Manifestaciones de Impacto a la Privacidad, antes de pretender implementar nuevas tecnologías de información que involucre el tratamiento o manejo de datos personales.

Alcances

- Determinar el grado de cumplimiento del proyecto evaluado con relación a la normatividad aplicable en materia de protección de datos personales.
- Identificar y detectar los posibles riesgos en el tratamiento de información personal con la implementación de la nueva tecnología.
- Aportar visiones innovadoras que contribuyan a robustecer el proyecto.
- Evaluar que las medidas de seguridad implementadas correspondan a la criticidad o sensibilidad de la información tratada, garantizando la confidencialidad, integridad y disponibilidad de la misma.

Beneficios

- Mitigar la exposición y vulnerabilidad de los datos personales con la implementación de innovadoras tecnologías.
- Minimizar y evitar los posibles riesgos desde la creación de la infraestructura funcional del proyecto o política pública.
- Construir proyectos “seguros” relativos al tratamiento de información personal.
- Generar confianza en los titulares de la información, al garantizar una debida protección de sus datos personales y del tratamiento que se les da a los mismos.

Beneficios

- Mitigar la exposición y vulnerabilidad de los datos personales con la implementación de innovadoras tecnologías.
- Minimizar y evitar los posibles riesgos desde la creación de la infraestructura funcional del proyecto o política pública.
- Construir proyectos “seguros” relativos al tratamiento de información personal.
- Generar confianza en los titulares de la información, al garantizar una debida protección de sus datos personales y del tratamiento que se les da a los mismos.

Casos de Éxito... NOM-024-SSA3-2007

- La NOM tiene como objeto establecer los objetivos funcionales y funcionalidades que deberán observar los productos de sistemas de expediente clínico electrónico para garantizar la interoperabilidad, procesamiento, interpretación, confidencialidad, seguridad y uso de estándares y catálogos de la información de los registros electrónicos en salud.
- Por la complejidad del diseño de la estructura funcional de la NOM, la Secretaría de Salud y el IFAI, como órgano garante, sometieron el proyecto a una Evaluación de Impacto a la Privacidad.
- Garantizar que antes de la puesta en operación dicha política pública cumpliera con los estándares internacionales en materia de protección, teniendo especial cuidado en los controles de seguridad que se requieren en un proyecto de tal envergadura.

Casos de Éxito... NOM-024-SSA3-2007

- Esta política pública fue la primera en todo México en someterse a una PIA.
- El consultor que realizó la PIA fue ex director de la Agencia Española de Protección de Datos.
- Durante la elaboración de la PIA se tuvieron reuniones con los actores involucrados:
 - Área médica y legal que participó en la elaboración de la NOM.
 - Principales instituciones de salud en México.
 - Expertos en tecnologías de la información.
 - Representantes de las principales empresas tecnológicas.
- Se tiene un reporte final de resultados.

Casos de Éxito.... CEDULA DE IDENTIDAD

- En julio de 2009, el Gobierno Federal dio a conocer de manera oficial la implementación de una política pública con la finalidad de acreditar fehacientemente la identidad de todas las personas que integran la población del país y de los nacionales residentes en el extranjero.
- A cargo de la Secretaría de Gobernación, se conformaría la plataforma tecnológica del Servicio Nacional de Identificación Personal -SNIP- y la expedición de la Cédula de Identidad Ciudadana (para mayores de edad) y de la Cédula de Identidad Personal (para menores de 18 años).

Casos de Éxito.... CEDULA DE IDENTIDAD

- El IFAI advirtió la necesidad de someter el proyecto al escrutinio de un experto externo, a través de la elaboración de una PIA.
- En atención a la recomendación, SEGOB contrató los servicios de asesoría de un consultor para la elaboración de la PIA. (parte conceptual).
- Del análisis de los hallazgos, el Pleno del IFAI emitió las Recomendaciones dirigidas al Registro, y de manera general a la fase de la eventual expedición de la Cédula de Identidad, en los siguientes términos:

Casos de Éxito... CEDULA DE IDENTIDAD

- Principio de licitud. De justificar la SEGOB la necesidad de recabar el dato biométrico relativo al iris de ambos ojos, se recomendó realizar las modificaciones conducentes al Reglamento de la Ley General de Población, a efecto de que se incluya en dicha disposición la captura del biométrico.
- Principio de proporcionalidad Aportar mayores elementos técnicos que justifiquen la necesidad de recabar las 10 huellas dactilares y la imagen del iris de ambos ojos, y reducir los datos a los mínimos necesarios, estableciendo un procedimiento a través del cual de forma gradual la SEGOB disminuya la recolecta de datos biométricos. De tal manera, que la información que se solicite a las personas sea la menor posible.

Casos de Éxito.... CEDULA DE IDENTIDAD

- Principio de información. Se recomendó incorporar en los formatos de solicitud de inscripción al registro, la leyenda de privacidad.
- Principio de custodia y cuidado, medidas de seguridad. Se recomendó establecer un procedimiento de control de confianza e implementar estrictas medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos personales.

Casos de Éxito... CEDULA DE IDENTIDAD

- Recomendación adicional. Se estableció la necesidad de realizar una nueva verificación en cuanto iniciara la operación de la plataforma tecnológica, a efecto de evaluar el tratamiento que se realiza de los datos personales y la protección que se da a los mismos.
- En esta segunda etapa, la verificación se enfocará a las medidas de seguridad enfocadas sobre:
 - Auditoría y pruebas de penetración no intrusivas
 - Identificación y evaluación de riesgos del proceso de captura de información
 - Pruebas de acceso a los centros de datos e instalaciones
 - Determinar el nivel de seguridad del sistema de gestión de la base de datos

Caso RENAUT

- Se trata de un complejo diseño estructural y funcional, que entrañaba riesgos para la privacidad que debieron ser minimizados y evitados desde la creación de la infraestructura del modelo.
- De manera general, los beneficios y contribuciones que una PIA hubiese aportado a esta política pública se hubieran traducido en:
 - Proporcionar elementos para construir un “proyecto seguro” *ex ante* de su lanzamiento.
 - Identificar los posibles riesgos para la protección de los datos personales con la implementación de nuevas tecnologías.
 - Favorecer una visión integral de un proyecto que se adecue a los estándares internacionales en materia de protección de datos personales.

Caso RENAUT

- Asegurar la privacidad y confidencialidad de la información personal que es tratada a través de sistemas automatizados.
- Garantizar que el acceso, procesamiento y uso de información personal cumpla con la legislación nacional y principios de protección de datos personales, teniendo especial cuidado en los niveles de seguridad que se requieren.

Caso RENAUT

- De manera particular, con la elaboración de una PIA a esta política pública se hubiesen precisado los siguientes aspectos:
 - La definición de la autoridad responsable de administrar el RENAUT.
 - La definición de los datos de tráfico y localización que cada uno de los actores involucrados recabaría y conservaría.
 - El establecimiento de medidas de seguridad concretas que garantizaran la integridad, confidencialidad y disponibilidad durante todo el ciclo de vida de la información personal en manos de los diferentes actores, incluyendo las transferencias continuas de datos personales realizadas entre ellos.
 - El establecimiento de responsabilidades a cada uno de los actores involucrados (proveedores, comercializadoras y autoridades) con respecto a la información personal tratada, a efecto de identificar fehacientemente al responsable de algún acto contrario a la ley dentro de esta compleja política pública y sancionarlo según correspondiera

Reformas a la LFTAIPG

- El proyecto de reforma a la Ley Federal de Transparencia y Acceso a la Información (actualmente en análisis por las Comisiones de Justicia y Función Pública de la Cámara de Diputados), establece la obligatoriedad para los organismos y entidades de la Administración Pública Federal, la elaboración de PIAS, previo a la implementación de una política pública que involucre el tratamiento de datos personales.
- *Artículo 108. “Cuando las dependencias y los entidades elaboren anteproyectos de leyes, decretos o actos administrativos de carácter general relativos con el tratamiento de datos personales, los presentarán ante el Instituto, junto con una manifestación de impacto a la privacidad, cuando menos treinta días hábiles antes de la fecha en que se pretenda emitir el acto o someterlo a la consideración del Titular de Ejecutivo Federal, a efecto de que el Instituto emita el dictamen correspondiente por lo que respecta a la observancia de los principios y derechos en materia de datos personales”.*

Nuevos retos...

- Los mecanismos preventivos incluirán el uso de herramientas informáticas para :
- Capacitar e-learning,
- Generar avisos de privacidad,
- Registrar Códigos Tipo,
- Publicar cláusulas contractuales tipo para las transferencias
- Cuestionario de autoevaluación para medidas de seguridad, y
- Modelos de auditorías voluntarias.