ABC DE PROTECCIÓN DE DATOS PERSONALES

INE
Instituto Nacional Electoral

ABC DE PROTECCIÓN DE DATOS PERSONALES

ABC de protección de datos personales
Primera edición, 2023

ISBN impreso: 978-607-8870-86-8
ISBN electrónico: 978-607-8870-85-1

Impreso en México/*Printed in Mexico*
Distribución gratuita. Prohibida su venta

ABC DE PROTECCIÓN DE DATOS PERSONALES

INE
Instituto Nacional Electoral

Índice

Presentación

Este ABC tiene un doble fin: por un lado, concientizar a las personas servidoras públicas sobre la importancia de proteger los datos personales que las instituciones tienen bajo su resguardo y, por el otro, dotar a la ciudadanía de una herramienta útil y didáctica que le permita ejercer su derecho a plenitud.

Hoy sabemos que es imposible concebir un sistema democrático sin transparencia en su actuar, y sin rendir cuentas a la ciudadanía sobre la toma de decisiones. Es innegable que la democracia y la transparencia van de la mano.

La transparencia, el acceso a la información y la rendición de cuentas son un trinomio imprescindible que permite a la ciudadanía acceder a toda aquella información que le sea necesaria y útil para conocer el funcionamiento orgánico, presupuestal y funcional de todo órgano del Estado.

En el Instituto Nacional Electoral tenemos muy clara nuestra visión: "Ser el organismo electoral nacional autónomo que contribuya a la consolidación de la cultura y convivencia democrática en México, distinguiéndose por ser una institución moderna, transparente y eficiente, en la que la sociedad confíe plenamente para la organización de elecciones equitativas e imparciales".[1]

Los principios que rigen nuestra actuación institucional y que se encuentran plasmados en el plan estratégico institucional 2016-2026 son: certeza, legalidad, independencia, imparcialidad, objetividad y máxima publicidad.

1 https://www.ine.mx/sobre-el-ine/cultura-institucional/

Quiero enfocarme en este último, derivado de que todas las acciones y la información que generamos son, por regla general, públicas. Esto nos obliga a transparentarlas de manera clara, sencilla y accesible para la ciudadanía.

La transparencia es un valor transversal en cualquier institución de carácter público, pues:

- Nos ayuda a dar claridad a la ciudadanía sobre la información que generamos en el día a día.

- Nos permite rendir cuentas sobre el uso de los recursos públicos que se nos asignan anualmente.

- Nos permite brindar información sobre la composición del Instituto, con sus distintas áreas y atribuciones, así como de las acciones que llevamos a cabo.

- Nos da la oportunidad de informar sobre las decisiones que tomamos y el impacto que éstas tienen en la ciudadanía.

La importancia de continuar e incluso mejorar los trabajos que venimos realizando para fortalecer la transparencia, el acceso a la información y la rendición de cuentas garantiza a la ciudadanía el pleno ejercicio de sus derechos políticos y electorales, fortalece la confianza y la participación ciudadana en la vida democrática y política de nuestro país.

Considerando que, a la fecha, contamos con un padrón electoral de poco más de 98 millones y medio de personas, es indispensable que se garantice el tratamiento adecuado de los datos personales que nos han confiado.

Por lo anterior, la presente obra está orientada a explicar de manera muy didáctica, esquemática y sencilla lo que son los datos personales, quién es su titular, la persona responsable del tratamiento que se les debe dar y la importancia de protegerlos.

Como se podrá deducir, a lo largo de esta obra se detallan las leyes y procedimientos para coordinar, supervisar y realizar las acciones necesarias que garanticen la protección de los datos personales que obran en poder del Instituto Nacional Electoral (INE).

Es importante señalar que la normativa en materia de acceso a la información pública y de protección de datos personales contempla la obligación de contar con comités de transparencia que adopten resoluciones respecto de la clasificación o desclasificación de la información, de la inexistencia de la información, de las disposiciones en materia de protección de datos personales, entre otras.

De la lectura integral del *ABC de la protección de datos personales* podemos advertir que la transparencia es una obligación de todas las personas servidoras públicas de cualquier órgano del Estado mexicano. Se trata de un ejercicio transversal de protección de datos personales y rendición de cuentas, basado en un esquema institucional de buenas prácticas conformado por procedimientos, acciones y tareas en las que participa todo el personal.

Toda solicitud de acceso, rectificación, cancelación, oposición y portabilidad de datos personales (derechos ARCOP) requiere plazos y procedimientos para generar una respuesta acorde con lo planteado. En este libro se desarrolla a detalle la atención que el INE da a las solicitudes de derechos ARCOP y se describe detalladamente

el medio de impugnación que se puede interponer ante una respuesta insatisfactoria.

En el INE hemos trabajado para que la protección de datos personales sea tan eficaz y transparente como la organización de los procesos electorales que han dado confianza a la ciudadanía de que su voto cuenta y se cuenta.

Norma Irene De La Cruz Magaña
Consejera Electoral del Instituto Nacional Electoral

Introducción

Una de las características medulares de un sistema democrático es el establecimiento de normas que:

- Coadyuven a garantizar la privacidad individual y colectiva.

- Enmarquen límites a la divulgación de la información personal, así como a los sistemas de monitoreo y vigilancia.

María Solange Maqueo Ramírez y Alessandra Barzizza Vignau, en su obra *Democracia, privacidad y protección de datos personales*,[1] advierten que la capacidad del ser humano para desarrollar juicios, forjar criterios, tomar decisiones autónomas, establecer relaciones o conformar asociaciones encuentra sustento en la privacidad, pues esta propicia el desenvolvimiento de las personas con una identidad propia, exclusiva, que las diferencia de otras. Gracias a estos atributos es posible que el ser humano ejerza de manera efectiva sus derechos civiles y políticos.

En este orden de ideas, la privacidad y la protección de datos personales se erigen como elementos indispensables en la adopción de un sistema electoral democrático, dado que a través de estos se garantiza el anonimato de las deliberaciones electorales. Así, estos elementos se colocan como básicos para que las personas puedan participar de manera activa en la vida política de un país.

1 M. S. Maqueo Ramírez y A. Barzizza Vignau (2020). *Democracia, privacidad y protección de datos personales*. México: INE (Cuadernos de Divulgación de la Cultura Democrática, núm. 41). Disponible en https://www.ine.mx/wp-content/uploads/2021/02/CDCD-41.pdf (fecha de consulta: 4 de julio de 2023).

El reconocimiento constitucional de la protección de los datos personales como un derecho humano ha generado diversos retos normativos y organizacionales para el Instituto Nacional Electoral (en adelante, INE o Instituto); esto implica la necesidad de armonizar de manera efectiva disciplinas como el derecho a la privacidad, la seguridad de la información y la materia político-electoral.

El INE, como la máxima autoridad electoral del Estado mexicano, es responsable de salvaguardar los datos personales que recaba –los cuales son necesarios para realizar actividades lícitas y legítimas en el ejercicio de sus funciones y atribuciones–, así como de velar por su adecuado tratamiento, conforme a los principios y deberes establecidos en la normativa en materia de protección de datos personales. Para las entidades públicas como el INE, las obligaciones están contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante, Ley General de Datos).

La Ley General de Datos ha sido un valioso incentivo para que el INE fortalezca su política de protección de datos personales, al establecer la articulación necesaria para su cumplimiento; con su entrada en vigor, el Instituto ha diseñado e implementado mecanismos adicionales a los que ya operaba, con el objetivo de afrontar los retos que la normativa en la materia ha impuesto, los cuales se describen a lo largo de este documento.

El objetivo principal del *ABC de protección de datos personales* editado en el INE es brindar una herramienta de apoyo y acompañamiento al personal del Instituto y público interesado, para facilitar la operación de la Ley General de Datos y mostrar el cumplimiento de las obligaciones que de esta derivan. Además, busca promover

la concientización sobre la importancia de proteger los datos personales y fomentar buenas prácticas en su tratamiento y, con ello, contribuir al fortalecimiento de la cultura de protección de dicha información tanto al interior como al exterior del Instituto.

Los capítulos que componen esta publicación reflejan el recorrido que el Instituto ha seguido desde un enfoque proactivo en la protección de datos personales; su contenido responde a las preguntas: ¿Qué es?, ¿para qué sirve? y ¿cómo la lleva a cabo el Instituto?

En primer lugar, se aborda la pregunta "¿qué es?" con el fin de exponer algunos conceptos clave, de forma clara y concisa, en materia de protección de datos personales para cualquier organización. A continuación, se responde a la pregunta "¿para qué sirve?", detallando los objetivos y beneficios que conlleva la aplicación del concepto de la protección de datos personales. Por último, se plantea la pregunta "¿cómo la lleva a cabo el Instituto?", en la descripción de las acciones y mecanismos implementados por el INE para observar los principios, cumplir con los deberes, garantizar los derechos y atender las obligaciones que la Ley General de Datos establece.

En función de lo anterior, esta publicación se compone de cinco capítulos:

El capítulo I realiza un recorrido por las actividades que el Instituto ya llevaba a cabo en materia de datos personales, previo a la entrada en vigor de la Ley General de Datos. De manera adicional, desarrolla brevemente los conceptos clave vinculados con la materia y la importancia de la protección de los datos en dos vertientes: para las personas y para el INE.

El capítulo II hace referencia a las acciones para conocer la situación actual en materia de protección de datos personales de una organización; además, presenta el panorama del INE posterior a la aplicación de tales acciones. Finalmente, detalla la estructura organizacional implementada por el Instituto para el cumplimiento de sus obligaciones.

El capítulo III puntualiza el Modelo de operación diseñado por el INE para el cumplimiento de la protección de datos personales, el cual provee al Instituto la ruta a seguir para cumplir de manera sistemática y atemporal sus obligaciones respecto de los principios y deberes en la materia, establecer un sistema de gestión e implementar la Plataforma de Medición, Evaluación y Monitoreo del Cumplimiento en Protección de Datos Personales. Cierra señalando acciones de capacitación y actualización disponibles para el personal del Instituto, que son replicables entre organismos de la misma naturaleza, o bien con la adecuación pertinente, por cualquier institución.

El capítulo IV describe, a grandes rasgos, cómo se atienden las solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales (en adelante, derechos ARCOP) en el Instituto, así como el recurso de revisión previsto en la Ley General de Datos y los que derivan de los trámites o procedimientos específicos con los que cuenta el INE.

Finalmente, el capítulo V señala las afectaciones que derivan del incumplimiento a las obligaciones en materia de protección de datos personales; por un lado, aquellas que tienen un impacto directo sobre la privacidad de las

personas; por otro, las que resultan en medidas de apremio y la imposición de sanciones para las organizaciones. Asimismo, se expone el impacto reputacional que ambos casos representan.

CAPÍTULO I

Consideraciones previas

Reconocimiento por parte del Instituto de actividades previas a la entrada en vigor de la Ley General de Datos

Para el INE, desde su constitución como Instituto Federal Electoral (IFE) hasta ahora, proteger los datos personales y prevenir su vulneración ha sido una tarea constante. Aun sin la existencia de una legislación específica en la materia, el Instituto ha trabajado diligentemente a través de diversas acciones, para garantizar a la ciudadanía la protección de sus datos y, con ello, su privacidad. A continuación, se describen estas acciones:

1990-2013

Se realizó un diagnóstico preliminar que consistió en diseñar, regular y ejecutar acciones para el tratamiento de los datos personales en posesión del INE, para conocer el estatus que prevalecía entonces en el Instituto.

2014

Entre 2014 y 2015 el INE revisó y actualizó su Listado de sistemas de datos personales, en el marco del Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública entonces vigente. Si bien en dicho periodo no se contaba con una norma especializada en protección de datos personales, el Instituto empezaba a preparar el terreno ante la emisión de la Ley General de Datos, como lo anunciaba la reforma constitucional en materia de transparencia de 2014 (artículo 6°).

2015

La Unidad Técnica de Transparencia y Protección de Datos Personales del INE (en adelante, Unidad de Transparencia)

reforzó su estructura para contar con un área especializada en protección de datos personales.

2016

La Unidad de Transparencia elaboró un primer diagnóstico sobre las bases de datos que se encontraban registradas en el Listado de sistemas de datos personales. En ese mismo año, el Consejo General del INE aprobó el Acuerdo INE/CG312/2016, por el cual se establecían los principios, criterios, plazos y procedimientos para garantizar la protección de datos personales en posesión del Instituto Nacional Electoral y los partidos políticos.

Conviene destacar que este documento es el primero especializado en la materia, aunado a la particularidad de que consideraba a otros sujetos obligados, ahora responsables directos, como los partidos políticos.

Con la entrada en vigor de la Ley General de Datos, este instrumento quedó sin efectos.

2017

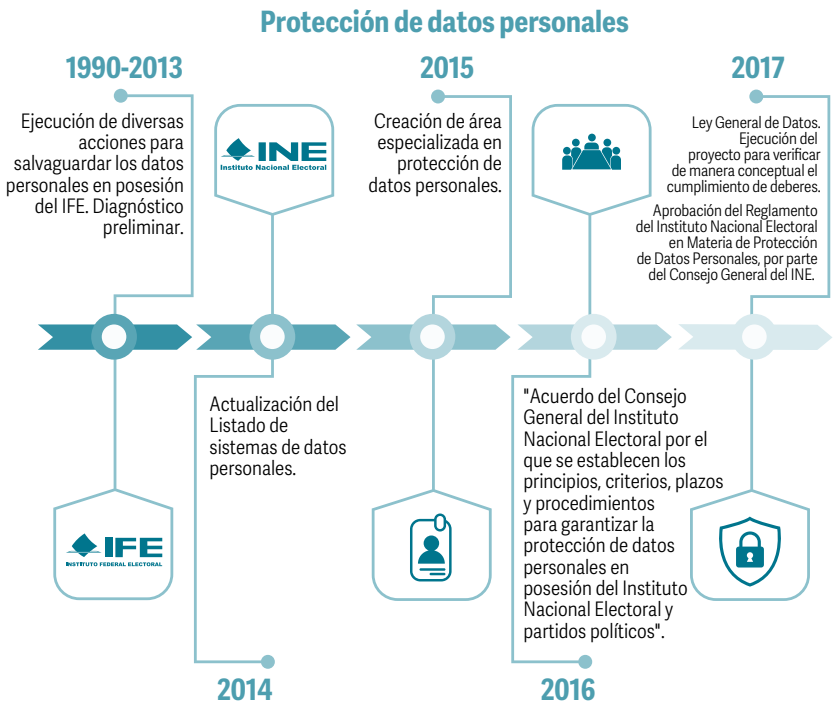
La Unidad de Transparencia verificó el cumplimiento de los deberes de manera conceptual, es decir, a través de un análisis de la información recabada mediante un cuestionario dirigido a las unidades administrativas del Instituto, seleccionadas de acuerdo con el alcance establecido, para poder contar con un dictamen que especificara las acciones y las recomendaciones que les permitieran alinearse a las nuevas disposiciones que prevé la Ley General de Datos.

Adicionalmente, se realizó un análisis del impacto normativo que la Ley General de Datos ha tenido en las

disposiciones internas vigentes del INE que, hasta ese momento, preveían los principios, deberes y procedimientos en materia de protección de datos personales. Esta acción derivó en la aprobación, por parte del Consejo General, del Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales, mediante el Acuerdo INE/CG557/2017.[1]

Figura 1

Acciones por parte del INE previas a la entrada en vigor de la Ley General de Datos



Fuente: Elaboración propia.

1 El Acuerdo INE/CG557/2017 se puede consultar en la página CGor201711-22-ap-8.pdf (ine.mx)

Privacidad y protección de datos personales. Conceptos clave

El derecho a la privacidad se define como el derecho de las personas para separar aspectos de su vida privada del escrutinio público, es decir, el derecho para desarrollar en un espacio reservado ciertos aspectos de la vida personal. Tiene dos componentes esenciales: el derecho de aislarse y el derecho de controlar la información de carácter personal.[2]

Por otro lado, el derecho a la protección de datos personales es el derecho humano que protege a la persona física identificada o identificable (titular) frente al tratamiento ilícito de sus datos personales, otorgándole, en la medida de lo posible dado el actual estado de la técnica, la facultad de decidir y controlar de manera libre e informada las condiciones y características del tratamiento de sus datos personales (autodeterminación informativa), y permitiéndole, además, el ejercicio de determinados derechos y medios de tutela jurídicos para garantía y eficacia práctica de estos últimos.[3] Busca proteger la privacidad, dignidad y autonomía de las personas.

Como todos los derechos, el de protección de datos personales no es absoluto. Admite aquellas restricciones prescritas en la ley que resulten razonables en una sociedad democrática: la seguridad nacional, disposiciones de

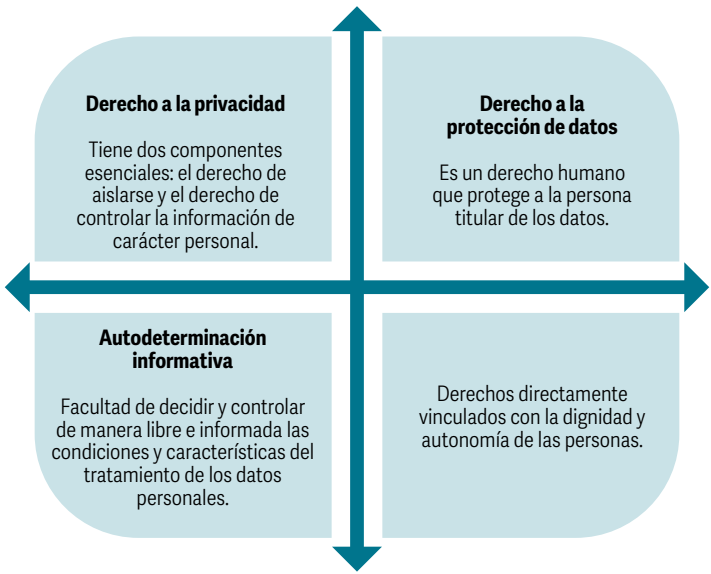
2 INAI (2019). *Diccionario de Protección de Datos Personales, conceptos fundamentales*. México: INAI, p. 672. Disponible en https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf (fecha de consulta: 4 de julio de 2023).

3 *Ibid*., p. 688.

orden público, seguridad y salud pública o la protección de los derechos de terceras personas.[4]

Figura 2

¿Qué es la protección de datos personales?



Fuente: Elaboración propia.

En 1980 la protección de datos personales adquirió una dimensión internacional que se ha consolidado en leyes y regulaciones en todo el mundo, entre las que destacan:

- Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE)[5]

4 Constitución Política de los Estados Unidos Mexicanos, artículo 16, segundo párrafo.

5 OCDE (23 de septiembre de 1980). Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales. Disponible en http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf (fecha de consulta: 4 de julio de 2023).

- Convenio 108 del Consejo de Europa (Consejo de Europa, 1981)[6]

- Resolución 45/95 de la Asamblea General de la ONU[7]

- Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana[8]

- Estándares internacionales sobre protección de datos personales y privacidad: Resolución de Madrid[9]

- Estándares de protección de datos personales para los Estados iberoamericanos[10]

6 Consejo de Europa (28 de enero de 1981). Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Disponible en https://inicio.inai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf (fecha de consulta: 4 de julio de 2023).

7 ONU (14 de diciembre de 1990). Directrices para la regulación de los archivos de datos personales informatizados. Disponible en https://archivos.juridicas.unam.mx/www/bjv/libros/12/5669/17.pdf (fecha de consulta: 4 de julio de 2023).

8 Red Iberoamericana de Protección de Datos (2007). Directrices para la armonización de la protección de datos en la Comunidad Iberoamericana. Disponible en https://archivos.juridicas.unam.mx/www/bjv/libros/12/5669/22.pdf (fecha de consulta: 4 de julio de 2023).

9 Agencia Española de Protección de Datos (2009). Estándares internacionales sobre protección de datos personales y privacidad: Resolución de Madrid. Disponible en https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf (fecha de consulta: 4 de julio de 2023).

10 Red Iberoamericana de Protección de Datos (20 de junio de 2017). Estándares de protección de datos personales para los Estados iberoamericanos. Disponible en https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf (fecha de consulta: 4 de julio de 2023).

En cuanto a su contenido esencial, las normativas que rigen tanto al sector público (Ley General de Datos) como al privado (Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en adelante, Ley Federal de Datos) establecen ocho principios: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad; y dos deberes: seguridad y confidencialidad, para quien trata los datos, así como una serie de derechos para las personas titulares: acceso a sus datos, rectificación, cancelación y oposición al tratamiento, añadiéndose en la normativa del sector público el derecho a la portabilidad (derechos ARCOP) y garantías de protección en caso de que esos derechos se vean infringidos o de que, a través del tratamiento de los datos personales, se haya incurrido en algún otro tipo de violación.

Esta función de tutela corresponde al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante, INAI u órgano garante) y los organismos garantes locales.[11]

¿Qué son los datos personales?

Tanto la Ley General de Datos como la Ley Federal de Datos definen al dato personal como "cualquier información concerniente a una persona física identificada (que sabemos quién es) o identificable (que fácilmente podemos determinar quién es)".

En síntesis, los datos personales son toda información que nos identifica o nos hace identificables y nos distingue de las demás personas (tabla 1):

11 INAI, *op. cit.*, p. 690.

Tabla 1
Datos personales, tipos y ejemplos

Tipo de dato	Ejemplos
Identificación	Nombre, apellidos, fotografía, firma autógrafa, lugar y fecha de nacimiento, número de pasaporte, clave de elector, clave única de registro de población (CURP), entre otros.
Contacto	Domicilio, correo electrónico, número telefónico (fijo o móvil), entre otros.
Laborales	Cargo, correo electrónico y teléfono institucionales, salario, entre otros.
Características físicas	Color de piel, del iris o del cabello, señas particulares o cicatrices, estatura, peso, complexión, tipo de sangre, entre otros.
Académicos	Trayectoria académica, certificados, reconocimientos, título y cédula profesionales, entre otros.
Patrimoniales	Propiedades (bienes muebles e inmuebles), ingresos y egresos, historial crediticio, seguros, números de cuenta y de tarjetas bancarias, entre otros.
Biométricos	Forma de iris, huella dactilar, forma de la palma de la mano, patrones de voz u otras características únicas.

Por regla general, los datos personales son considerados información confidencial; sin embargo, determinados datos que corresponden a personas servidoras públicas, prestadoras de servicios, funcionarias o militantes de partidos políticos, candidatos o candidatas y precandidatos o precandidatas podrían ser públicos dependiendo del caso.

¿Qué es un dato personal sensible?

De acuerdo con la Ley General de Datos, un dato personal sensible es aquel que refiere y puede afectar la esfera más íntima de la persona titular, o cuyo uso indebido puede ocasionarle discriminación o algún riesgo grave. De manera enunciativa, esta ley considera como datos personales sensibles aquellos que puedan revelar aspectos de la persona como: origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual (tabla 2).

Tabla 2

Datos personales sensibles, tipos y ejemplos

Tipo de dato	Ejemplos
Ideológicos	Posturas ideológicas, religiosas, filosóficas o morales; opiniones políticas y afiliación partidista o sindical, entre otros.
De salud	Estado de salud físico o mental (valoración, preservación, cuidado, mejoramiento y recuperación) e información genética, entre otros.
Vida sexual	Comportamiento, preferencias, prácticas o hábitos sexuales, entre otros.
Origen étnico	Pertenencia a una etnia o pueblo indígena, costumbres, tradiciones o creencias, entre otros.

¿Quién es titular de los datos personales?

La persona física identificada o identificable a quien pertenecen los datos personales es titular de estos. Se considera que una persona física es identificable cuando es

posible determinar su identidad directa o indirectamente, es decir, cuando su identidad se puede reconocer a través de algún tipo de información.

¿Quién es el responsable del tratamiento de los datos personales?

Son los sujetos obligados a que se refiere el artículo 1 de la Ley General de Datos.

El INE es responsable del tratamiento de los datos personales que trata en el ejercicio de sus funciones y atribuciones, conforme a las finalidades establecidas, las cuales deben ser informadas previamente en los avisos de privacidad a las personas titulares.[12]

Al interior del INE, son los órganos y personas servidoras públicas, así como toda persona o institución ajena al Instituto que esté vinculada con el tratamiento de datos personales que realice este, de acuerdo con el artículo 2 del Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales (en adelante, Reglamento de Datos Personales).

¿Qué es el tratamiento de datos personales?

Tratamiento es cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados, en este caso, a los datos personales, relacionados con:

12 El artículo 7 del Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales conceptúa como sujetos obligados a los órganos y personas servidoras públicas que decidan sobre el tratamiento de los datos personales.

Figura 3
Tratamiento de datos personales

Fuente: Elaboración propia.

Como se observa, estas operaciones –en esencia– hacen referencia a las actividades que involucran la ejecución de determinados procedimientos o acciones tendientes a la utilización de datos personales por parte del responsable, el encargado o un tercero.[13]

Algunos ejemplos de tratamiento de datos en el INE son:

- Los datos proporcionados por la ciudadanía para tramitar la credencial para votar o para participar como persona observadora electoral.

- Los datos proporcionados por las personas que prestan sus servicios en el INE para integrar el expediente de personal o el censo institucional.

13 INAI, *op. cit.*, p. 860.

- Los datos proporcionados por las personas proveedoras del INE para integrar el Registro Único de Proveedores y Contratistas o el Registro Nacional de Proveedores.

- Los datos para la organización del Parlamento Infantil y Juvenil.

Los principios rectores de la protección de los datos personales

El INE, como responsable del tratamiento de los datos personales, observa los principios previamente listados que se traducen en obligaciones concretas (tabla 3).

Tabla 3

Principios que rigen el tratamiento de datos personales

Principio	El responsable debe:
Licitud	Realizar el tratamiento conforme a las facultades y atribuciones establecidas en la normativa aplicable.
Finalidad	Tener un propósito concreto, lícito, explícito y legítimo, que motive el tratamiento de los datos de acuerdo con las disposiciones que resulten aplicables.
Lealtad	Priorizar la protección de los intereses y la expectativa razonable de privacidad de la persona titular, evitando el uso de medios engañosos o fraudulentos.

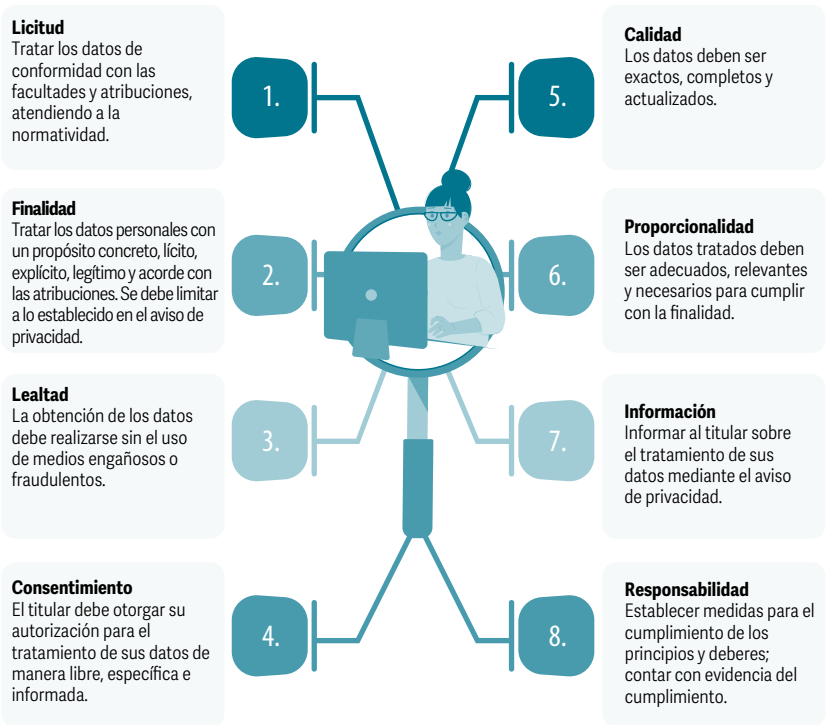
Continúa...

Principio	El responsable debe:
Consentimiento	Obtener el consentimiento de la persona titular de manera libre, específica e informada previo al tratamiento de los datos. Este puede ser **expreso** o **tácito**: • **Expreso:** cuando la voluntad de la persona titular se manifiesta verbalmente y por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología. • **Tácito:** cuando habiéndose puesto a disposición de la persona titular el aviso de privacidad, esta no manifieste su voluntad en sentido contrario. Por regla general será válido el consentimiento tácito, salvo que la Ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente; para el tratamiento de datos personales sensibles el consentimiento debe ser expreso y por escrito.[14]
Calidad*	Adoptar medidas para mantener los datos personales exactos, completos, correctos y actualizados.
Proporcionalidad	Tratar únicamente los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que motiva su tratamiento.
Información	Informar a la persona titular, a través de un aviso de privacidad,** la existencia y las características principales del tratamiento de sus datos personales, para que pueda tomar decisiones informadas al respecto.
Responsabilidad***	Implementar mecanismos para demostrar el cumplimiento de los principios, deberes y obligaciones establecidos en la Ley General de Datos.

14 Salvo en las excepciones previstas en el artículo 22 de la Ley General de Datos.

*Cuando los datos personales dejen de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, deben ser suprimidos, previo bloqueo en su caso, conforme a los plazos de conservación establecidos. Se presume que se cumple con la calidad cuando la persona titular proporciona directamente los datos, y hasta que esta no manifiesta y acredita lo contrario.
** Un aviso de privacidad eficiente debe estar redactado y estructurado de manera clara y sencilla.
*** Se debe rendir cuentas sobre el tratamiento a la persona titular, al INAI o a los organismos garantes correspondientes.

Figura 4
Los principios que rigen el tratamiento de los datos personales



Fuente: Elaboración propia.

Deberes en la protección de datos personales

Para garantizar la protección de los datos personales, la normativa en esta materia establece el cumplimiento de dos deberes: **seguridad** y **confidencialidad**, los cuales se materializan a través de la implementación de medidas de seguridad. A continuación, revisaremos a qué se refiere cada uno:

- **Seguridad**. El responsable del tratamiento debe establecer y mantener acciones, actividades, controles o mecanismos que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizados, así como garantizar su confidencialidad, integridad y disponibilidad.

  Al conjunto de esas acciones se le conoce como **medidas de seguridad**, y estas pueden ser **administrativas**, **técnicas** o **físicas**.

Del deber de seguridad emanan las siguientes obligaciones para los responsables del tratamiento de datos personales:

- Crear políticas internas para la gestión y tratamiento de los datos personales.
- Definir las funciones y obligaciones del personal involucrado en el tratamiento.
- Elaborar un inventario de datos personales y de los sistemas de tratamiento.
- Realizar un análisis de riesgo de los datos personales.

- Realizar un análisis de brecha de las medidas de seguridad.
- Elaborar un plan de trabajo para implementar las medidas faltantes o mejorar las actuales.
- Monitoreo y revisión periódica de las medidas de seguridad.
- Capacitar al personal, atendiendo a los roles y responsabilidades respecto del tratamiento de los datos personales.
- Establecer un sistema de gestión.
- Elaborar un documento de seguridad.
- Gestionar las vulneraciones y llevar una bitácora de estas.

- **Confidencialidad**. El responsable debe establecer controles o mecanismos para que las personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de estos, subsistiendo aún después de finalizar las relaciones que lo motivaron.

Figura 5

Tipos de medidas de seguridad para salvaguardar los datos personales

Fuente: Elaboración propia.

Para el ejercicio de los principios y deberes, el INE diseñó un Modelo de operación, el cual se desarrolla en el capítulo III de esta publicación.

Derechos ARCOP

Los derechos ARCOP[15] son un conjunto de prerrogativas conferidas en la Ley General de Datos a las personas titulares (tabla 4).

Tabla 4

Descripción de los derechos ARCOP

El derecho de		Permite a las personas titulares solicitar
A	**A**cceso	El acceso a sus datos personales que están en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacena o utiliza, así como conocer la información relacionada con el uso que se da a sus datos.
R	**R**ectificación	La rectificación o corrección de sus datos personales cuando estos sean inexactos o incompletos, o no se encuentren actualizados. En otras palabras, pueden solicitar a quien posea o utilice sus datos personales que los corrija cuando sean incorrectos, desactualizados o inexactos.
C	**C**ancelación	Que se eliminen sus datos de los archivos, registros, expedientes, sistemas y/o bases de datos del responsable que los posee, almacena o utiliza.

Continúa...

15 INAI (s.f.). *Guía para titulares de los datos personales* (vol. 3). México: INAI. Disponible en https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/Guia%20Titulares-03_PDF.pdf (fecha de consulta: 4 de julio de 2023).

El derecho de		Permite a las personas titulares solicitar
O	**O**posición	Que sus datos no se utilicen para ciertos fines o, de requerirlo, que se concluya el uso de estos a fin de evitar un daño a su persona. La persona titular podrá oponerse al tratamiento de sus datos personales cuando: • Aun siendo lícito, el tratamiento debe cesar para evitar que su persistencia le cause un daño o perjuicio. • Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar –sin intervención humana– determinados aspectos personales, o bien a analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.
P	**P**ortabilidad	Cuando sus datos personales sean tratados por vía electrónica en un formato estructurado y comúnmente utilizado, la o el titular tiene el derecho a obtener del responsable una copia de estos, también en un formato electrónico estructurado y comúnmente utilizado, que le permita seguir usándolos.

Figura 6
Componentes de la protección de datos personales

Fuente: Elaboración propia.

La importancia del aviso de privacidad y el documento de seguridad

Los avisos de privacidad y documentos de seguridad son elementos fundamentales en el ámbito de la protección de datos personales y la privacidad. Ambos desempeñan roles importantes y complementarios en la gestión adecuada de los datos personales.

Aviso de privacidad

Un aviso de privacidad es una comunicación o documento a través del cual una organización informa a las personas sobre cómo se recopilan, utilizan, almacenan y protegen sus datos personales.

El responsable de cualquier tratamiento de datos personales tiene la obligación de poner a disposición de la o el titular el aviso de privacidad, previo a que recaben sus

datos personales, con el objeto de informarle los propósitos y las características principales del tratamiento.

Estos avisos son esenciales para garantizar la transparencia y la confianza entre las organizaciones y las personas cuyos datos están siendo procesados.

Algunas de las razones de importancia de los avisos de privacidad son:

a. **Información:** Permiten a las personas titulares conocer qué tipo de información se recopila, cómo se utiliza, con quién se comparte y con qué fines, para que puedan tomar decisiones informadas sobre el tratamiento de sus datos personales y entender los riesgos asociados.

b. **Consentimiento:** Aunque no es el único medio donde se obtiene el consentimiento, con frecuencia se utilizan formularios con casillas de verificación para que la o el titular manifieste su consentimiento respecto del tratamiento de los datos personales que se requieran.

   Los avisos de privacidad suelen incluir una sección donde las personas otorgan su consentimiento informado para el procesamiento de sus datos, elemento fundamental en la protección de su privacidad y su autodeterminación.

c. **Cumplimiento normativo:** Proporcionar avisos de privacidad integrales y simplificados, que sean claros y completos es parte de las obligaciones establecidas en la Ley General de Datos; por tanto, su cumplimiento es esencial para evitar sanciones y mantener la confianza de las personas titulares.

Como se observa en la figura 7, el principio de información se materializa directamente en el aviso de privacidad.

Figura 7
Materialización del principio de información

Fuente: Elaboración propia.

Documento de seguridad

El documento de seguridad establece las medidas, procedimientos y controles que una organización debe implementar para proteger los datos personales y garantizar su confidencialidad, integridad y disponibilidad.

Algunas de las razones por las cuales el documento de seguridad es importante son:

a. **Protección de la información:** Define las políticas y prácticas necesarias para proteger la información confidencial de una organización. Esto puede incluir aspectos como la gestión de contraseñas, el acceso restringido a ciertos datos, el cifrado de la información y otras medidas de seguridad físicas, técnicas y administrativas.

b. **Cumplimiento normativo:** La Ley General de Datos exige que las organizaciones implementen medidas de seguridad adecuadas para proteger los datos personales. El documento de seguridad ayuda a demostrar el cumplimiento de estas obligaciones.

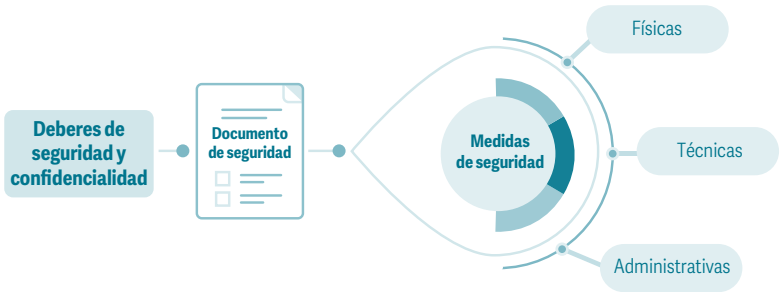
c. **Identificación de funciones y obligaciones:** En el documento de seguridad no sólo se identifican los roles que participan en el tratamiento de los datos personales, sino también cuáles son las responsabilidades derivadas de su tratamiento, lo que permite determinar de forma clara la rendición de cuentas.

d. **Identificación de los datos personales:** Como cualquier activo de una organización, la identificación de los datos personales, dónde residen y a través de qué sistemas están siendo tratados durante todo su ciclo de vida permite determinar el riesgo al que están expuestos, e implementar las medidas necesarias para su mitigación.

Los deberes de seguridad y confidencialidad se materializan, de manera general, en el documento de seguridad, como se observa en la figura 8.

Figura 8

Materialización del deber de seguridad y confidencialidad



Fuente: Elaboración propia.

En resumen, los avisos de privacidad son herramientas de transparencia y consentimiento que informan a las personas sobre el uso de sus datos personales, mientras que el documento de seguridad establece las políticas y controles necesarios para salvaguardarlos.

En esta era digital ambos son cruciales para proteger la privacidad, mantener la confianza y garantizar el cumplimiento normativo.

Por otro lado, para cumplir con las obligaciones en materia de protección de datos personales, el INE, en su carácter de responsable, desarrolla y divulga diversos materiales (guías, procedimientos e infografías, por mencionar algunos) a través de la Unidad de Transparencia, a los cuales se puede acceder desde el Apartado virtual "Protección de datos personales".[16]

La rendición de cuentas con enfoque en la protección de datos personales

Uno de los conceptos novedosos de la Ley General de Datos es la inclusión del **principio de responsabilidad** (artículos 29 y 30),[17] el cual señala que el responsable (en nuestro caso el INE) debe implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidas en la ley, así como **rendir cuentas a las personas titulares** y al INAI sobre el tratamiento de los datos personales en su posesión.

A este principio se le conoce también como **principio de rendición de cuentas,** ya que establece la obligación de los responsables de velar por el cumplimiento del resto

16 INE (26 de junio de 2022). *Apartado virtual "Protección de datos personales"*. Disponible en https://www.ine.mx/transparencia/proteccion dp/ (fecha de consulta: 17 de agosto de 2023).

17 El artículo 29 de la Ley General de Datos señala que el responsable deberá implementar los mecanismos previstos en el artículo 30 de esa misma ley para acreditar el cumplimiento de los principios, deberes y obligaciones que establece. El artículo 30 detalla los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad.

de los principios, adoptar las medidas necesarias para su aplicación y demostrar ante las personas titulares y la autoridad que cumple con sus obligaciones con respecto a la protección de los datos personales.[18]

En palabras de Nelson Remolina, el **principio de responsabilidad** demanda menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones en materia de tratamiento de datos personales. El éxito de este dependerá del compromiso real de los cargos directivos de los sujetos obligados, ya que sin su apoyo franco y decidido todo esfuerzo será insuficiente para diseñar, implementar, revisar, actualizar y evaluar los programas de gestión de datos.

Es necesario destinar recursos humanos y económicos para esta labor y con ello propiciar un ambiente armónico de trabajo en varias dependencias de la organización, ya que no se trata sólo de un tema jurídico; ante todo es una cuestión de gestión gerencial y estratégica de gobierno corporativo. El reto de los sujetos obligados frente al principio de responsabilidad va mucho más allá de la mera expedición de documentos, pues también exige que se demuestre el cumplimiento real y efectivo de estos en la práctica cuando realizan sus funciones.[19]

La **rendición de cuentas** es una oportunidad real para demostrar que las organizaciones establecen altos

18 INAI (s.f.). *Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. Disponible en https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/_GuiaPrincipiosDeberes.pdf (fecha de consulta: 27 de julio de 2023).

19 M. S. Maqueo Ramírez (coord.) (2018). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, comentada*. México: INAI. p. 86.

estándares de privacidad y predican con el ejemplo para promover una actitud positiva hacia la protección de datos en toda la organización.[20] Permite minimizar los riesgos derivados del tratamiento de los datos personales al implementar políticas, procedimientos y medidas adecuadas y efectivas, los cuales deben ser proporcionales a los riesgos, que pueden variar según la cantidad de datos que se manejen o transfieran, su sensibilidad y la tecnología utilizada.

A través de esta publicación, el INE muestra la forma en que rinde cuentas como responsable del tratamiento de todos los datos personales que posee, esto para cumplir con la legislación y garantizar el ejercicio de otros derechos y libertades de las personas, como son los derechos político-electorales.

La importancia de proteger los datos personales

La protección de los datos personales es de suma importancia en el entorno actual, ya que su recopilación, uso y procesamiento se ha vuelto omnipresente en nuestra sociedad. Algunas de las razones que destacan su relevancia se enumeran a continuación:

1. **Privacidad.** La protección de los datos personales es fundamental para preservar la privacidad de todas y todos. Cada persona tiene el derecho de mantener el control sobre su información y decidir cómo se recopila, utiliza y comparte. La protección de datos personales asegura que no sean utilizados de manera indebida o invasiva.

20 Information Commissioner's Office (s.f.). *Accountability Framework*. Disponible en https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/ (fecha de consulta: 5 de julio de 2023).

2. **Seguridad.** Los datos personales pueden incluir información sensible, como números de identificación, datos financieros, historial médico, preferencias políticas o creencias religiosas. La protección de estos datos es esencial para evitar el riesgo de robo de identidad, fraude, abuso o discriminación.

3. **Confianza.** La protección de datos fomenta la confianza entre las personas y las organizaciones que manejan su información. Cuando las personas confían en que sus datos serán tratados de manera segura y respetuosa, están más dispuestas a compartir información relevante y participar en interacciones, en particular, en el espacio digital.

4. **Derechos humanos.** La protección de los datos personales se reconoce como un derecho humano fundamental, consagrado en diversas legislaciones nacionales e internacionales. Está intrínsecamente vinculada con la dignidad, la privacidad y la autonomía de las personas.

5. **Innovación responsable.** La protección de datos no implica una prohibición en su uso, sino que busca garantizar que se utilicen de manera responsable y ética. Al establecer controles y regulaciones adecuadas, se fomenta una cultura de innovación responsable que beneficia tanto a las personas titulares como a las organizaciones.

6. **Cumplimiento normativo.** Las legislaciones y regulaciones exigen cada vez más el cumplimiento de requisitos específicos en materia de protección de datos. Las organizaciones que no cumplen con estas regulaciones pueden enfrentar sanciones legales, multas y daños a su reputación.

7. **Protección infantil.** Los datos personales de las infancias requieren una protección especial debido a su situación de vulnerabilidad. La protección de sus datos garantiza que no sean objeto de prácticas invasivas o manipuladoras y que se respeten sus derechos, en particular, en línea.

De acuerdo con María Maqueo y Alessandra Barzizza en *Democracia, privacidad y protección de datos personales,* proteger los datos personales permite al INE:[21]

1. Garantizar elecciones libres.

2. Proveer las condiciones necesarias para la adopción de prácticas democráticas mediante la secrecía del voto.

3. Evitar la intimidación y la coacción como medios para influir en la toma de decisiones, así como la captura de votantes por parte de grupos de interés.

4. Establecer la línea divisoria entre, por un lado, el tratamiento de datos personales necesario para garantizar la confianza del electorado, la integridad de las elecciones y el cumplimiento de los objetivos legítimos de los actores políticos, y, por el otro, el tratamiento abusivo e injustificado de los datos personales en las campañas (o precampañas) electorales.

5. Fortalecer la democracia.

Transversalidad y apropiación de la materia

La transversalidad se refiere a la forma de plantear un tema de manera holística, en lugar de tratarlo de manera

21 M. S. Maqueo Ramírez y A. Barzizza Vignau, *op. cit*.

aislada, sectorial o en silos. Al ser un activo de información, el dato personal debe ser reconocido desde la "alta dirección", para lo cual requiere:[22]

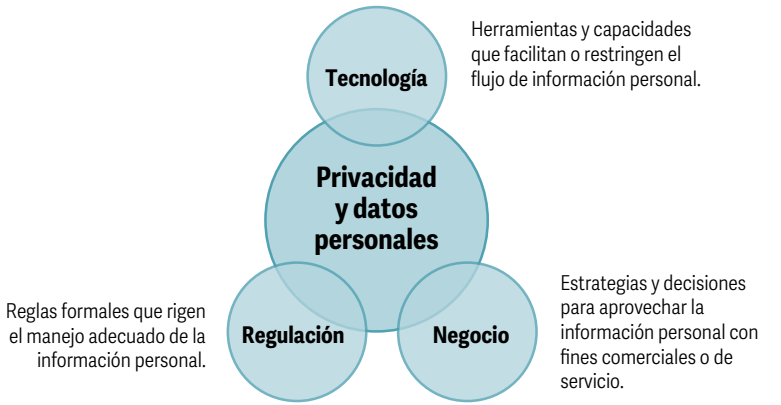
- Alejarse del **pensamiento en silos**, por ejemplo, dejar de tratar los datos como una preocupación exclusiva de las áreas encargadas de las tecnologías de la información o del área legal o normativa.

- Asegurarse de que la gestión de datos personales se considere un **tema estratégico** crítico para la organización (el negocio).

- Fomentar una **cultura organizacional consciente de los datos personales y la privacidad** que sustente todas las consideraciones estratégicas y operativas.

Figura 9

Privacidad y datos personales: donde la tecnología, los negocios y la regulación se unen



Fuente: Elaboración propia con base en M. Crompton y M. Trovato. *The New Governance of Data and Privacy: Moving from Compliance to Performance.* Australian Institute of Company Directors. Edición de Kindle, posición en Kindle: 151.

22 M. Crompton y M. Trovato (2018). *The New Governance of Data and Privacy: Moving beyond Compliance to Performance.* Australian Institute of Company Directors. Edición de Kindle.

En palabras de Crompton y Trovato: "La privacidad ya no puede ser sólo un problema de cumplimiento. El manejo de información personal tiene implicaciones financieras, legales, estratégicas y de riesgo",[23] por lo que la protección de datos personales es reconocida como una materia transversal. Esto implica que la organización debe:

- Considerarla y aplicarla en todas las áreas y procesos internos, así como en las actividades diarias, sin importar su tamaño o sector.

- Integrarla en todos los aspectos de las operaciones, desde la cultura organizacional y las políticas hasta los procedimientos y la capacitación del personal.

La transversalidad de la protección de datos personales involucra una serie de aspectos clave a ser considerados, entre los que destacan:

1. **Concientización y capacitación.** Todo el personal de la organización debe estar consciente de la importancia de proteger los datos personales y procurar buenas prácticas en su manejo. Esto se logra a través de la concientización y la capacitación.

2. **Implementación de políticas y procedimientos.** Se deben establecer políticas y procedimientos claros en relación con la protección de datos personales. Estos instrumentos deben ser comunicados y entendidos por todas las personas que integran la organización, e implementados de manera consistente en todas las áreas.

23 *Ibid.*

3. **Evaluación de riesgos.** Se deben evaluar los riesgos en todos los procesos de negocio que traten datos personales, identificar medidas de mitigación y garantizar el cumplimiento de los principios de protección de datos, esto mediante la ejecución de evaluaciones de impacto en la materia para identificar y gestionar los riesgos y las vulnerabilidades potenciales.

La transversalidad de la protección de datos personales en una organización impulsa un cambio de paradigma que habilita las bases para atender dos obligaciones de suma importancia: **la protección de datos por diseño y por defecto** –conocida también como privacidad desde el diseño y por defecto–.

Aunque la tecnología y las herramientas desempeñan un papel importante, **las personas** son **quienes impulsan, planifican, implementan y ejecutan** las acciones para la protección de datos personales. El factor humano abarca a todas las personas involucradas en el proceso, desde quienes fungen los roles de liderazgo y dirección hasta quienes integran los equipos, así como usuarios y usuarias finales.

El factor humano es esencial para la transversalización y el éxito de los objetivos de protección de datos personales establecidos en cualquier organización, ya que el compromiso, la comunicación efectiva, la creatividad, la adaptabilidad y la capacidad de aprender y mejorar, entre otros factores, son fundamentales, como se muestra a continuación:[24]

24 IBS americas (1° de junio de 2023). "Factor humano en los proyectos: Ventajas y desafíos". Disponible en https://blogibsamericas.com/es/2023/06/01/factor-humano-en-los-proyectos-ventajas-y-desafios-es/ (fecha de consulta: 24 de julio de 2023).

1. **Compromiso y motivación:** Cuando las personas se sienten involucradas y tienen un sentido de pertenencia están más motivadas para contribuir y trabajar en pro del éxito. El compromiso del personal es fundamental para enfrentar los desafíos y superar los obstáculos.

2. **Comunicación efectiva:** Una comunicación clara y efectiva facilita la coordinación y asegura que todos estén alineados en los objetivos y las tareas.

3. **Flexibilidad y adaptabilidad:** Las organizaciones suelen enfrentar cambios y desafíos inesperados, por lo que un equipo humano bien involucrado puede ser más flexible y adaptable para ajustarse a esos cambios y encontrar soluciones efectivas.

4. **Creatividad e innovación:** El factor humano puede aportar ideas innovadoras y creativas para resolver problemas y mejorar los procesos de protección de datos personales. En ese sentido, fomentar un ambiente donde se promueva la colaboración y el intercambio de ideas contribuye a la innovación.

5. **Aprendizaje y mejora continua:** El factor humano es esencial para aprender de las experiencias y aplicar ese conocimiento en el futuro. La mejora continua es clave para el crecimiento y el éxito a largo plazo.

6. **Identificación de necesidades y expectativas:** Tanto quienes fungen el rol de usuarios finales como las partes interesadas tienen necesidades y expectativas específicas. Al involucrar el factor humano, es más probable que se identifiquen estas necesidades y se cumplan de manera efectiva.

7. **Alineación con la visión en la materia:** Cuando las personas están involucradas desde las etapas iniciales, es más probable que comprendan y se alineen con la visión y los objetivos de esta.

CAPÍTULO II

La protección de datos personales en el INE

De la evolución de un esquema político-electoral a la adopción del lenguaje técnico en la materia

En un esquema político-electoral, como el del INE, la adopción del lenguaje técnico en materia de protección de datos implica comprender y aplicar los principios y requisitos establecidos por las leyes y regulaciones de protección de datos personales; asimismo, incluye la implementación de medidas de seguridad adecuadas y el respetar los derechos de las y los titulares.

Previo a la entrada en vigor de la Ley General de Datos, el INE ya realizaba diversas acciones para el adecuado tratamiento de los datos personales en su posesión, como se ha mencionado anteriormente; si bien aún no se contaba con un instrumento normativo específico en la materia que fuera aplicable al Instituto, en su momento se encontró soporte en las leyes, tanto la federal como la general, de Transparencia y Acceso a la Información Pública, en la Ley Federal de Datos y en la adopción de diversos estándares internacionales de seguridad de la información.

El Instituto ha elaborado diversos instrumentos y procedimientos que han sido traducidos al lenguaje técnico en materia de protección de datos (tabla 1).

Tabla 1
Relación de los instrumentos en materia electoral con los conceptos de protección de datos personales

Instrumentos en materia electoral	Conceptos de protección de datos personales relacionados
"Lineamientos para el acceso, verificación y entrega de los datos personales en posesión del Registro Federal de Electores por los integrantes de los consejos General, locales y distritales, las comisiones de vigilancia del Registro Federal de Electores y los Organismos Públicos Locales"	• Principio de calidad y finalidad • Deberes de seguridad y confidencialidad • Vulneraciones a la seguridad de los datos personales • Principio de minimización
"Lineamientos del Instituto Nacional Electoral para el acceso, rectificación, cancelación y oposición de datos personales que forman parte del Padrón Electoral"	• Derechos ARCO
"Lineamientos para la incorporación, actualización, exclusión y reincorporación de los registros de las ciudadanas y los ciudadanos en el Padrón Electoral y la Lista Nominal de Electores"	• Principio de calidad
Reglamento para la Destrucción de Formatos de Credencial y Credenciales para Votar	• Principio de calidad • Deberes de seguridad y confidencialidad
"Anexo 19.3. Procedimiento y Protocolo de seguridad para la generación, impresión, entrega, devolución y destrucción de las Listas Nominales de Electores para su uso en las Jornadas Electorales", del Reglamento de Elecciones	• Principio de finalidad • Principio de calidad • Deberes de seguridad y confidencialidad

Continúa...

Instrumentos en materia electoral	Conceptos de protección de datos personales relacionados
"Lineamientos que establecen los plazos y términos para el uso del Padrón Electoral y las listas nominales de electores para los procesos electorales locales 2022-2023"	• Principio de finalidad
"Lineamientos del Instituto Nacional Electoral para la atención de requerimientos de información y documentación formulados en términos de lo dispuesto en el artículo 126, párrafo 3 de la Ley General de Instituciones y Procedimientos Electorales"	• Principio de finalidad • Principio de información
Procedimiento para la Destrucción de la Documentación Electoral establecido y aprobado por la Comisión Nacional de Vigilancia	• Principio de calidad • Deberes de seguridad y confidencialidad

Acciones de reconocimiento de la situación actual a través de un proceso de evaluación

La evaluación es un proceso mediante el cual se examina detalladamente el estado actual de una organización; su objetivo principal es obtener una comprensión clara y completa de la situación presente, incluyendo fortalezas, debilidades, oportunidades y amenazas en una materia o tema específico.

El análisis de la situación actual a través de la evaluación implica recopilar y analizar información relevante

proveniente de diversas fuentes: datos internos, estadísticas, informes y opiniones de las partes interesadas. Este proceso debe realizarse cada vez que se produzca un cambio significativo que pueda afectar a la organización, o en periodos establecidos para iniciar un ciclo de mejora continua.

En este capítulo se desarrollan las acciones para conocer la situación actual en materia de protección de datos personales de una organización; además, se muestra el panorama del INE luego de la aplicación de dichas acciones. Finalmente, se detalla la estructura organizacional implementada por el Instituto para el cumplimiento de sus obligaciones en materia de protección de datos personales.

Iniciaremos con las cinco acciones a realizar para el reconocimiento de la situación actual:

1. Análisis del contexto organizacional.

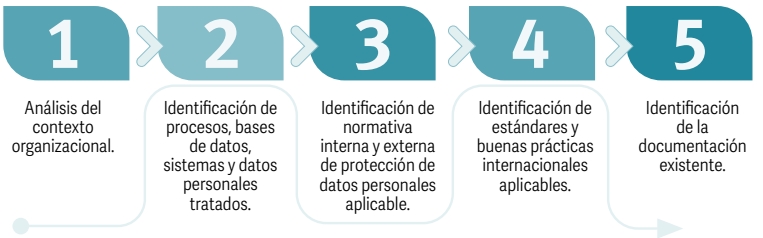
2. Identificación de procesos, sistemas, bases de datos, y datos personales tratados.

3. Identificación de normativa interna y externa de protección de datos personales aplicable.

4. Identificación de estándares y buenas prácticas internacionales aplicables.

5. Identificación de la documentación existente.

Figura 1
Acciones para evaluar la situación actual



Fuente: Elaboración propia.

En los siguientes apartados se describen de forma detallada estas acciones.

Acción 1. Análisis del contexto organizacional

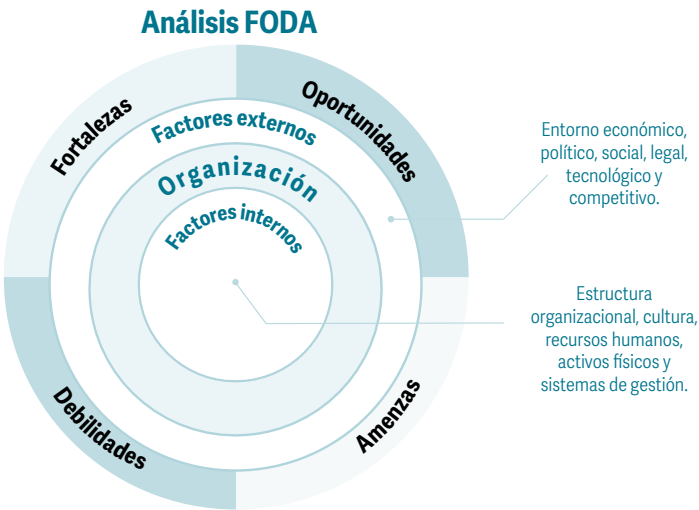
El contexto organizacional se refiere al entorno interno y externo en el que opera una organización; es una parte fundamental del enfoque basado en el riesgo.

La finalidad de esta acción es analizar el contexto a través de la identificación de los factores y las circunstancias que pueden afectar la capacidad de la organización para lograr sus objetivos de protección de datos personales y cumplir con la normativa en la materia, así como las expectativas de las personas titulares y otras partes interesadas.

1. **Análisis FODA**

Un **análisis FODA** resume los hallazgos del estudio de factores internos y externos de una organización, destacando sus **f**ortalezas, **o**portunidades, **d**ebilidades y **a**menazas, de ahí las siglas FODA.

Figura 2
Análisis FODA para identificar el contexto institucional



Fuente: Elaboración propia.

Esto ayuda a identificar las áreas clave en las que la organización destaca y las áreas de oportunidad que requieren mejoras; además, proporciona información para determinar las necesidades y los desafíos que deben considerarse para lograr los objetivos deseados para la protección de los datos personales que posee la organización.

Análisis de factores externos e internos

El análisis de los factores externos se refiere al estudio de estos fuera de la organización que pudieran influir en la toma de decisiones internas en materia de protección de datos personales, como el entorno económico, político, social, legal, tecnológico y competitivo. Esto implica el análisis de las regulaciones aplicables, las expectativas de las personas titulares y las necesidades de las partes interesadas.

Por su parte, en el análisis de los factores internos son evaluados los recursos, las capacidades y los procesos internos de la organización referentes a la protección de datos personales. Esto incluye la estructura organizacional, su cultura, los recursos humanos, los activos físicos y los sistemas de gestión. Con este análisis son identificadas las fortalezas y debilidades organizacionales en esta materia.

A partir del resultado obtenido, la organización puede diseñar y aplicar diversas estrategias para el fortalecimiento y mejora de los procesos para proteger los datos personales que posee.

2. **Partes interesadas**

Su análisis considera a las personas, grupos u organizaciones que pueden afectar o verse afectados por las actividades y el desempeño de la organización. Esto puede incluir proveedores, personal, partidos políticos y otros actores relevantes. Identificar y comprender las necesidades, las expectativas y los requisitos de las partes interesadas referentes a la protección de datos personales es esencial para su gestión eficaz en la organización.

Los recursos humanos y legales, las tecnologías de la información, el desarrollo de *software* y la gestión de cambios juegan un papel clave en el apoyo a los esfuerzos primarios en la protección de datos personales para sus propias áreas.

Quienes son responsables del tratamiento de los datos personales de cada área deben comprender e identificar tanto la información personal como los requisitos legales para su protección aplicables a su alcance de responsabilidad.

A través de la definición de las partes interesadas, la organización establece:

a. A qué tipo de información tendrán acceso.

b. Cuáles son sus responsabilidades respecto de esta.

Figura 3

Identificación de las partes interesadas en el contexto institucional

Fuente: Elaboración propia.

De manera enunciativa, y considerando las buenas prácticas internacionales, se identifican las siguientes partes interesadas internas y externas:[1]

- **Partes interesadas internas**
    - **Alta dirección**. Se refiere a la persona o grupo de personas que dirige y controla la organización al

1 ISACA (2018). *ISACA Privacy Principles and Program Management Guide.*

más alto nivel. Son las áreas que toman las decisiones al interior de esta.

- **Oficial o delegado [persona delegada] de protección de datos personales**. Es la persona profesional designada por el responsable y/o encargado del tratamiento de los datos personales para ocuparse de la aplicación y cumplimiento de la normativa de protección de datos personales y privacidad en el interior de la organización.

- **Órganos en materia de protección de datos personales (PDP) u otros órganos colegiados relacionados con la materia.** Comités, comisiones o equivalentes relacionados con la toma de decisiones en protección de datos personales.

- **Otros órganos colegiados.** Comités, comisiones o equivalentes que, por sus funciones y atribuciones, pueden considerar las políticas de protección de datos personales en la toma de decisiones.

- **Auditoras y auditores internos.** Son las personas responsables de llevar a cabo las auditorías internas en materia de protección de datos personales.

- **Áreas responsables del cumplimiento.** Se refiere a las unidades administrativas o instancias de la organización previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes que cuentan o pueden contar, dar tratamiento y ser responsables o encargadas de los datos personales.

- **Áreas de tecnologías de la información.** Se refiere a las unidades administrativas o instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes que proveen la infraestructura tecnológica para el tratamiento de datos personales para un servicio o producto.

- **Usuarias y usuarios internos**. Se refiere a las personas o unidades administrativas en la organización que utilizan la información o que rigen el tratamiento de datos personales (políticas, procesos, procedimientos, manuales, lineamientos, informes, por mencionar algunos).

- **Partes interesadas externas**

  - **Autoridades de protección de datos personales.** Para entidades nacionales corresponde a los organismos garantes, y para los internacionales, a las autoridades de control o equivalentes.

  - **Encargados.** Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o en conjunto con otras trate datos personales a nombre y por cuenta del responsable.

  - **Otros sujetos obligados.** Los señalados en la Ley General de Datos.

  - **Titulares.** Persona física a la que corresponden los datos personales.

Acción 2. Identificación de procesos, sistemas, bases de datos y datos personales tratados

Los procesos de negocio y los datos personales están estrechamente relacionados en el entorno organizacional. Estos datos son un componente clave debido a que se utilizan para llevar a cabo diversas actividades y funciones dentro de la institución (tabla 2).

Tabla 2

Relación entre los procesos de negocio y la protección de datos personales

Procesos de negocio	Relación con la protección de datos personales
Recopilación/ obtención y almacenamiento	Los procesos de negocio suelen implicar la recopilación y el almacenamiento de datos personales. Esto puede ocurrir cuando las y los titulares u otras partes interesadas proporcionan este tipo de datos para acceder a los servicios del Instituto, solicitar empleo o participar en actividades similares.
Procesamiento y uso	Los datos personales recopilados en los procesos de negocio se utilizan para diversos fines, lo que implica su procesamiento, ya sea mediante su análisis, segmentación, transferencia a terceros o cualquier otra operación necesaria para cumplir con los objetivos institucionales.
Seguridad y protección	Los procesos de negocio deben garantizar la seguridad y protección de los datos personales que manejan. Esto implica establecer medidas físicas, técnicas y administrativas adecuadas para prevenir el acceso no autorizado, el uso indebido, la divulgación o la pérdida de datos. Los procesos de seguridad, como el cifrado, la autenticación de usuarios y usuarias y el monitoreo de actividades, son esenciales para proteger los datos personales durante su procesamiento y almacenamiento.

Continúa...

Procesos de negocio	Relación con la protección de datos personales
Cumplimiento normativo	Los procesos de negocio deben cumplir con las leyes y regulaciones de protección de datos aplicables. Esto incluye el cumplimiento de los principios, la obtención del consentimiento adecuado, el respeto de los derechos de las personas sobre sus datos y la notificación de cualquier violación de estos que ocurra durante los procesos de negocio.
Gestión del ciclo de vida	Los procesos de negocio también están vinculados al ciclo de vida de los datos personales. Esto implica la gestión adecuada de los datos desde su recopilación hasta su eliminación. Los procesos deben garantizar la actualización y corrección de los datos, así como su eliminación segura cuando ya no sean necesarios o cuando se solicite por parte de la o el titular de los datos.

En resumen, los procesos de negocio dependen de los datos personales para su funcionamiento, los cuales son cruciales para el logro de los objetivos organizacionales. La forma en que los datos personales se recopilan, almacenan, procesan y protegen dentro de los procesos de negocio es fundamental para garantizar la privacidad de las personas y cumplir con las regulaciones en la materia.

Acción 3. Identificación de normativa interna y externa de protección de datos personales aplicable

La organización tiene la responsabilidad de identificar toda la normativa aplicable a sus procesos de negocio, asegurándose de satisfacer los requisitos específicos de cada jurisdicción en la que estos operan para garantizar el cumplimiento de las leyes y regulaciones aplicables.

La normativa en materia de datos personales está en constante evolución para adaptarse a los avances tecnológicos y los nuevos desafíos en la protección de la privacidad; por ello, es imprescindible identificar sus cambios tanto a nivel interno como externo y aplicar actualizaciones a la documentación que rige los procesos de negocio, cuyas actividades tratan datos personales, para asegurar el cumplimiento continuo y evitar posibles inconvenientes legales.

Acción 4. Identificación de estándares y buenas prácticas internacionales aplicables

Además de atender la normativa interna y externa, es elemental que las organizaciones identifiquen e implementen de manera permanente normas comunes y mejores prácticas establecidas en estándares, tanto en cuestión de privacidad y protección de datos personales como de seguridad de la información, para incorporarlas en la documentación que rige sus procesos de negocio y garantizar con ello la privacidad de las personas, así como el cumplimiento normativo en la materia.

Esta acción prevé a la organización de los elementos que se describen a continuación:

- Armonización y consistencia
    - Proporcionan una base común para las regulaciones y prácticas en diferentes jurisdicciones. Esto facilita la armonización y la consistencia en la forma en que se protegen los datos personales y se gestionan los riesgos asociados en todo el mundo.

- Ayudan a evitar la fragmentación normativa y facilitan un marco común desde una perspectiva internacional.

- Protección de los derechos individuales

  - Se centran en salvaguardar los derechos individuales en relación con los datos personales.

  - Suelen estar basados en los principios de privacidad y transparencia y promueven el consentimiento informado, el acceso a la información y los mecanismos de corrección y eliminación de datos.

  - Ayudan a asegurar que las personas tengan un mayor control sobre sus datos y que se respeten sus derechos fundamentales.

- Mejores prácticas de seguridad

  - Integran la seguridad de la información y establecen pautas para la protección de los datos contra amenazas y riesgos.

  - Definen medidas técnicas, físicas y administrativas que pueden implementarse para proteger la confidencialidad, integridad y disponibilidad de los datos personales.

  - Ayudan a prevenir brechas de seguridad, pérdidas de datos y otros incidentes relacionados.

- Confianza y transparencia

    - Contribuyen a generar confianza entre la organización y las partes interesadas. Seguir estos estándares demuestra el compromiso de la organización con la protección de los datos personales y la seguridad de la información. Esto ayuda a establecer relaciones de confianza y a mejorar su reputación.

    - Requieren que las organizaciones informen detalles sobre el tratamiento de los datos personales, fomentando prácticas transparentes y éticas.

- Cumplimiento legal y regulatorio

    - Su adopción coadyuva al cumplimiento de obligaciones legales y regulatorias en materia de privacidad y seguridad, dado que a menudo estos estándares internacionales se reflejan en las leyes y regulaciones de protección de datos en diferentes países.

    - Reducen el riesgo de sanciones legales, multas y daños a la reputación debido a infracciones o incumplimientos.

- Transferencias internacionales

    - Consideran la transferencia de datos personales entre países.

    - Establecen requisitos y mecanismos para garantizar que los datos se transfieran de manera segura y legal, incluso hacia países que no brinden un nivel adecuado de protección de datos.

- Promueven la aplicación de salvaguardias y acuerdos apropiados para proteger la privacidad de los datos en las transferencias transfronterizas.

Acción 5. Identificación de la documentación existente

Como acción final y tomando como insumos las cuatro acciones anteriores, es necesario identificar la documentación mínima para operar la protección de los datos personales.

El proceso para identificar la documentación existente relacionada con la protección de datos personales puede variar según el tamaño y la estructura de cada organización, así como el estado actual de su programa de protección de datos personales (tabla 3).

Tabla 3

Pasos generales para identificar la documentación referente a datos personales

Pasos	Actividades
Revisión de políticas y procedimientos existentes	• Examinar las políticas y procedimientos internos relacionados con la protección de datos personales, políticas de privacidad, políticas de seguridad de la información, políticas de retención de datos, acuerdos de confidencialidad y otros documentos relevantes. • Identificar los documentos clave que establecen los principios y las prácticas de protección de datos de la organización.
Análisis de contratos y acuerdos	• Identificar y revisar los contratos y acuerdos celebrados con terceros, como proveedores de servicio u otras organizaciones, en busca de cláusulas relacionadas con la protección de datos, responsabilidades de las partes en su tratamiento y medidas de seguridad aplicables.

Continúa...

Pasos	Actividades
Revisión de informes y auditorías previas	• Revisar los informes y resultados obtenidos en auditorías o evaluaciones de protección de datos realizadas en el pasado, en caso de existir. • Identificar información valiosa sobre las fortalezas y debilidades existentes en el programa de protección de datos, así como las áreas en las que se requiere mejorar la documentación.
Realizar entrevistas y consultas	• Hablar con las personas responsables y colaboradoras clave en la organización, involucradas en la gestión de datos personales. • Realizar entrevistas o consultas para identificar cualquier documentación adicional que se haya desarrollado o utilizado en relación con la protección de datos personales, así como políticas, directrices, manuales u otros documentos específicos utilizados en la práctica diaria.
Organizar y catalogar la documentación	• Organizar y catalogar de manera estructurada la documentación relevante en la materia, asegurando su accesibilidad y correcto etiquetado.

Esto es sólo el primer paso. A medida que se avanza en el proceso de protección de datos, es posible que se deba revisar, actualizar y desarrollar nueva documentación para garantizar un programa de protección de datos efectivo y que cumpla con las leyes y regulaciones aplicables.

Panorama del INE tras aplicar las acciones de reconocimiento de la situación actual

El resultado de las acciones anteriores, después de ser aplicadas en el INE, ha permitido:

1. Identificar los riesgos y las oportunidades que podrían afectar el desempeño y los resultados previstos.

2. Tomar decisiones informadas.

3. Desarrollar estrategias para tratar los desafíos de manera adecuada y aprovechar las oportunidades de mejora en torno a la protección de los datos personales.

La importancia que el INE confiere al derecho humano a la protección de los datos personales se ve reflejada en uno de sus proyectos estratégicos, como se observa en la figura 4.

Figura 4

Mapa del Plan Estratégico del Instituto Nacional Electoral 2016-2026

Fuente: Elaboración propia.

Por lo que respecta al análisis FODA del Instituto, de un primer ejercicio podrían obtenerse resultados, con criterios positivos y negativos como los que se presentan a continuación.

Factores externos positivos

Contar con:

- Normativa internacional de privacidad y protección de datos personales, así como de estándares y buenas prácticas de seguridad y privacidad.

- Herramientas tecnológicas para la gestión automatizada de los resultados de protección de datos personales en el ámbito europeo, como marco de referencia.

- Un órgano garante nacional en materia de protección de datos personales proactivo y capacitador.

- Un instrumento que define las bases de la política pública de protección de datos personales en el país para el sector público (Programa Nacional de Protección de Datos Personales, en adelante PRONADATOS).

Factores externos negativos

Existencia de:

- Ambiente político y social inestable que volatiliza la estructura organizacional establecida.

- Movimientos de interés político que buscan desprestigiar a la organización.

- Interés por parte de diversos entes públicos y privados por obtener las bases de datos de la organización.

- Reducción de recursos económicos.

- Hechos de caso fortuito o fuerza mayor.

Factores internos positivos

Contar con:

- Planes estratégicos que contemplen el fortalecimiento a la protección de datos personales como proyecto estratégico.

- Una unidad administrativa especializada en materia de protección de datos personales dentro de la estructura organizacional establecida.

- Normativa interna en materia de protección de datos personales que impulsa acciones en la materia.

- Políticas institucionales para la transversalización del enfoque de protección de datos personales.

- Programas y estrategias establecidas para el cumplimiento del marco normativo en materia de protección de datos personales.

- Sistemas de gestión de seguridad de la información o similares que coadyuven a garantizar la integridad, disponibilidad y confidencialidad de los datos personales.

- Un grupo de Gobierno de Seguridad de la Información.

- Políticas, estándares, procedimientos y protocolos de seguridad que incluyen la protección de datos personales.

- Herramientas tecnológicas seguras para trabajo a distancia.

Factores internos negativos

Existencia de:

- Esfuerzos de protección de datos personales y seguridad de la información por silos.

- Falta de personal especializado que atienda los temas de protección de datos personales, o constante rotación de este.

- Poca concientización del personal respecto al ejercicio de este derecho.

- Poca capacitación especializada a los responsables del tratamiento de datos personales en seguridad de la información y protección de datos personales.

- Falta de identificación de procesos de negocio que tratan datos personales desde su concepción.

- Mecanismos de medición de efectividad para la protección de datos personales no homologados.

Las partes interesadas identificadas son:

Partes interesadas internas

- **Alta dirección.**
    - En materia electoral: Consejo General, Secretaría Ejecutiva, titulares de direcciones ejecutivas y unidades técnicas.
    - En materia de protección de datos personales: Comité de Transparencia (a partir de 2017).
- **Oficial o delegado [persona delegada] de Protección de Datos Personales.** En el INE las funciones de esta figura corresponden a la Unidad Técnica de Transparencia y Protección de Datos Personales.
- **Órganos en materia de PDP u otros órganos colegiados relacionados con la materia.** Grupo de trabajo en materia de transparencia.
- **Otros órganos colegiados.**
    - **Grupos de gobierno:** Grupo de Gobierno de Tecnologías de la Información, Grupo de Gobierno de Seguridad de la Información.
    - **Comisiones permanentes:** Comisión de Organización Electoral, Comisión de Capacitación Electoral y Educación Cívica, Comisión de Prerrogativas y Partidos Políticos, Comisión del Registro Federal de Electores, Comisión del Servicio Profesional Electoral Nacional, Comisión de Quejas y Denuncias, Comisión de Vinculación con Organismos Públicos Locales, Comisión de Fiscalización, Comité de Radio y Televisión, Comisión de Igualdad de Género y No Discriminación.

  - **Comisiones temporales:** Presupuesto.

  - **Comités permanentes:** Comité Editorial, Grupo de Trabajo de Igualdad y No Discriminación, Comité de Gestión y Publicación Electrónica, Comité en Materia de Tecnologías de Información y Comunicaciones (TIC), Comité de Ética, Comisión Nacional de Vigilancia.

- **Auditores internos en protección de datos personales.** Sus funciones corresponden a la Dirección de Acceso a la Información y Protección de Datos Personales, adscrita a la Unidad Técnica de Transparencia y Protección de Datos Personales.

- **Áreas responsables del cumplimiento.** Todos los órganos centrales y delegacionales del INE.

- **Áreas de tecnologías de la información.** La Unidad Técnica de Servicios de Informática; la Coordinación de Tecnologías de Información Administrativa, adscrita a la Dirección Ejecutiva de Administración; la Coordinación de Procesos Tecnológicos, adscrita a la Dirección Ejecutiva del Registro Federal de Electores, y la Dirección de Procesos Tecnológicos, adscrita a la Dirección Ejecutiva de Prerrogativas y Partidos Políticos.

- **Usuarios internos.** Todos los órganos centrales y delegacionales del INE.

Partes interesadas externas

- **Autoridades de protección de datos personales.** INAI.

- **Encargados.** Todos los proveedores de bienes y servicios que son contratados para tratar datos personales en alguna parte de su ciclo de vida.

- **Otros sujetos obligados.**

    - **Secretarías de Estado:** Relaciones Exteriores, de Hacienda y Crédito Público.

    - **Autoridades judiciales:** aquellas pertenecientes al Poder Judicial de la Federación.

    - **Autoridades electorales:** Tribunal Electoral del Poder Judicial de la Federación, Fiscalía Especializada en materia de Delitos Electorales, Organismos Públicos Locales.

    - **Organismos desconcentrados:** instituciones de seguridad social, Servicio de Administración Tributaria, Registro Civil, Comisión Nacional de Búsqueda de Personas.

    - **Entidades de interés público:** los diversos partidos políticos.

    - **Fideicomisos:** Fondo para atender el pasivo laboral del Instituto Nacional Electoral.

- **Titulares de los datos personales.** Ciudadanía; contratistas, proveedores y personal del INE en cualquier esquema de contratación; personas prestadoras de servicio social en el Instituto; niñas, niños y adolescentes; precandidatos, precandidatas, candidatos y candidatas; observadoras y observadores electorales; familiares de hasta tercer grado por consanguinidad

y afinidad de las personas servidoras públicas que realizan declaraciones de situación patrimonial, entre otros.

Para la **identificación de los datos personales,** las áreas responsables de cumplir esa función en el Instituto ejecutan los siguientes pasos:

1. **Analizan los procesos de negocio** con el fin de identificar aquellos que, debido a su operación, tratan datos personales, ya sea como un insumo o como parte de un resultado. El análisis se realiza en apego al Modelo de Gestión por Procesos del propio INE,[2] cuyo objetivo es establecer la metodología para la implementación de la gestión por procesos en el Instituto, con el propósito de que estos tengan un enfoque transversal y orientado a la persona usuaria, considerando el control interno en el diseño de estos e identificando posibles mejoras que contribuyan al desempeño institucional.

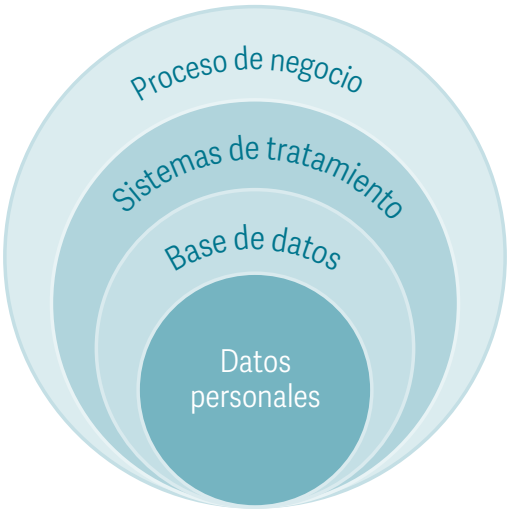
2. **Reconocen los sistemas de tratamiento,** aplicaciones informáticas o plataformas mediante los cuales son tratados los datos personales en el proceso de negocio.

3. **Examinan las bases de datos** asociadas al proceso de negocio donde son almacenados los datos personales.

4. **Identifican los datos personales,** discerniendo de aquellos que no son considerados como tales.

2 Disponible en https://sidj.ine.mx/restWSsidj-nc/app/doc/998/20/1

Figura 5
Identificación de datos personales en un proceso de negocio institucional



Fuente: Elaboración propia.

Respecto del **análisis de la normativa interna y su adecuación** a los requerimientos establecidos en la Ley General de Datos, el Consejo General del INE emitió el Reglamento de Datos Personales el 22 de noviembre de 2017. Esta acción se llevó a cabo dentro del plazo transitorio previsto en la Ley General de Datos para tramitar, expedir o modificar su normatividad interna. En los meses posteriores se extendió la adecuación a otras normas, principalmente las vinculadas con el Padrón Electoral.

En la elaboración del anteproyecto del Reglamento de Datos Personales participaron diversos actores del INE (tabla 4).

Tabla 4
Elaboración del anteproyecto del Reglamento de Datos Personales

Actores	Participación en el anteproyecto
Unidad de Transparencia	Análisis y diseño
Dirección Jurídica	Revisión
Comité de Transparencia	Coordinación
Comité de Protección de Datos Personales (ya extinto)	Aprobación
Consejo General del INE	Aprobación

Con ello se da cuenta del grado de involucramiento del personal de distintos niveles, así como de la convivencia entre órganos colegiados en materia electoral (Consejo General, integrado por Consejeras y Consejeros Electorales y representaciones de los partidos políticos) y en materia de protección de datos personales (Comité de Protección de Datos Personales –ya extinto– y Comité de Transparencia).

El anteproyecto fue remitido al INAI para obtener su opinión especializada y sus recomendaciones fueron retomadas en el Reglamento de Datos Personales. Esto fortaleció los instrumentos emitidos por el INE para garantizar la protección de datos personales y refleja el acompañamiento brindado por el órgano garante nacional.

Esta acción también se estima replicable por parte de otros sujetos, ya sea para verificar si sus normas se encuentran adecuadas a la ley aplicable en la materia o para llevarla a cabo. De igual forma, para identificar, controlar o asumir los riesgos de la aplicación de la Ley General de Datos y lograr la cohesión de los distintos órganos que conforman su estructura.

La implementación de cualquier ley implica riesgos. Por ello, tras el diagnóstico de la situación normativa realizado en 2017, la Unidad de Transparencia detectó distintos **espacios de riesgo legal,** clasificados con prioridades **alta, media** y **baja.**

Entre los riesgos clasificados con **prioridad alta** se encuentran los derivados del cumplimiento de los principios y deberes de la protección de datos, que resultaron en acciones inmediatas en términos de la Ley General de Datos, incluyendo las obligaciones que requerían una actuación del Instituto en el corto plazo.

Referente al **marco normativo**, la Unidad de Transparencia desarrolló y mantiene actualizada la **Matriz de normativa aplicable en materia de protección de datos personales** (en adelante, la Matriz), la cual contempla tanto la legislación en materia de protección de datos personales o privacidad, como la regulación y las decisiones judiciales y administrativas aplicables, de acuerdo con lo siguiente:

- **Norma fundamental del Estado mexicano:** Constitución Política de los Estados Unidos Mexicanos, Convenio 108.

- **Regulación de alcance federal:** Lineamientos de Protección de Datos Personales para el Sector Público.

- **Decisiones administrativas:** Parámetros de Mejores Prácticas en Materia de Protección de Datos Personales del Sector Público.

- **Regulación propia del Instituto:** Reglamento de Datos Personales.

- **Legislación:** Ley General de Datos.

La identificación de los elementos que integran la Matriz comprendió la realización de ejercicios entre la Unidad de Transparencia y los órganos del Instituto.

Por lo que respecta a las normas específicas, están contenidas en los documentos de seguridad y avisos de privacidad de cada proceso de negocio institucional relacionado con el tratamiento de datos personales.[3]

Sobre los **estándares internacionales de privacidad y seguridad de la información** adoptados por el INE, estos han desempeñado un papel fundamental en la protección de datos y la seguridad de la información. Son los siguientes:

- **Para el documento de seguridad**

    - *ISO/IEC 27002. Information technology — Security techniques — Code of practice for information security controls*. Es una guía de buenas prácticas para la gestión de seguridad de la información; se utiliza para ejecutar el análisis de brecha debido a que proporciona recomendaciones detalladas sobre controles de seguridad y medidas de salvaguardia aplicables a la protección de datos personales.

    - *ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management.*[4] Su objetivo es proporcionar un

3 Para más información, consultar https://ine.mx/transparencia/listado-bases-datos-personales/

4 ISO (2018). *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management.* Disponible en https://www.iso.org/standard/75281.html (fecha de consulta: 5 de julio de 2023).

enfoque sistemático y estructurado para la gestión de riesgos de seguridad de la información. Se utiliza para ejecutar los análisis de riesgos al establecer las pautas y los procesos para identificar, evaluar y tratar los riesgos de seguridad de la información de manera eficaz, así como tomar decisiones informadas para proteger los activos de información, entre los que se encuentran los datos personales.

- *ISO/IEC 27018. Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.*[5] Es un estándar que establece pautas para el procesamiento de datos personales en la nube, centrándose en los aspectos de privacidad y seguridad específicos para los proveedores que ofrecen este servicio. Se utiliza para evaluar a los proveedores que le ofrecen este servicio al Instituto en su rol de encargados.

- *ISO/IEC 27701:2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 2700 for privacy information management — Requirements and guidelines.*[6] Es una extensión de la norma ISO/IEC 27001 y proporciona pautas para

5 ISO (2019). ISO/IEC 27018:2019 Information technology — *Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.* Disponible en https://www.iso.org/standard/76559.html (fecha de consulta: 5 de julio de 2023).

6 ISO (2019). *ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.* Disponible en https://www.iso.org/standard/71670.html (fecha de consulta: 5 de julio de 2023).

establecer, implementar, mantener y mejorar un sistema de gestión de privacidad de la información. Es utilizada en el INE para ejecutar el análisis de brecha.

- *ISO/IEC 29100. Information technology — Security techniques — Privacy framework.*[7] Establece los principios y marcos para la privacidad en la tecnología. Proporciona directrices sobre la protección de la privacidad en el diseño de productos y servicios. En el INE se utiliza para ejecutar el análisis de brecha.

- *ISO/IEC 29151. Information technology — Security techniques — Code of practice for personally identifiable information protection.*[8] Establece objetivos de control, controles y lineamientos para implementar dichos controles según los requisitos identificados por una evaluación de riesgos e impactos relacionados con datos personales. El INE la utiliza para ejecutar el análisis de riesgos.

- **Para el Sistema de Gestión para la Protección de Datos Personales**

  - *ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements.*[9] Esta norma

7 ISO (2011). *ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework*. Disponible en https://www.iso.org/standard/45123.html (fecha de consulta: 5 de julio de 2023).

8 ISO (2017). *ISO/IEC 29151:2017 Information technology — Security techniques — Code of practice for personally identifiable information protection.* Disponible en https://www.iso.org/standard/62726.html (fecha de consulta: 5 de julio de 2023).

9 ISO (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.*

establece los requisitos para un sistema de gestión de seguridad de la información. Aunque no se centra exclusivamente en la privacidad, es fundamental para garantizar la seguridad de los datos personales y se ocupa en conjunto con otros estándares y marcos de privacidad. En el INE se utilizó como referencia para el diseño del Sistema de Gestión para la Protección de Datos Personales.

- *ISO/IEC 27701:2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.*[10] También fue utilizada en el INE como referencia para el diseño del Sistema de Gestión para la Protección de Datos Personales.

- *ISO/IEC 27004:2016. Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation.*[11] Establece un enfoque sistemático para la medición de la seguridad de la información y proporciona directrices sobre los indicadores clave de desempeño y las métricas que se pueden utilizar para evaluar y controlar la seguridad de la información. Al implementar las recomendaciones de la norma, el INE puede evaluar y demostrar el impacto de su sistema de gestión en la protección de la información y en el cumplimiento de los objetivos de seguridad.

10 ISO (2019), *op. cit*.

11 ISO (2016). *ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation.* Disponible en https://www.iso.org/standard/64120.html (fecha de consulta: 5 de julio de 2023).

- *ISO/IEC 27007. Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing.*[12] Establece los principios, procesos y actividades relacionados con la auditoría de un sistema de gestión de seguridad de la información, centrándose en su auditoría interna. Tiene como objetivo ayudar a evaluar la efectividad de este y mejorar continuamente su desempeño en materia de seguridad de la información. Esta guía es utilizada como referencia para diseñar las auditorías internas en materia de protección de datos personales del Instituto.

- *ISO/IEC 19011:2018. Guidelines for auditing management systems.*[13] Es una norma internacional que proporciona directrices para la auditoría de sistemas de gestión. Establece los principios y las prácticas fundamentales de la auditoría, así como los requisitos para la competencia y la evaluación de los auditores. En el INE es utilizada como referencia para diseñar las auditorías internas en materia de protección de datos personales del Instituto.

- **Para las evaluaciones de impacto**

  - *ISO/IEC 29134. Information technology — Security techniques — Guidelines for privacy impact*

12 ISO (2020). *ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing.* Disponible en https://www.iso.org/standard/77802.html (fecha de consulta: 5 de julio de 2023).

13 ISO (2018). *ISO/IEC 19011:2018 Guidelines for auditing management systems*. Disponible en https://www.iso.org/standard/70017.html (fecha de consulta: 15 de septiembre de 2023).

assessment.[14] Provee directrices sobre cómo realizar una evaluación de impacto en privacidad. Se utiliza en el INE como referencia en el diseño de materiales guía para la ejecución de las evaluaciones de impacto.

- **De apoyo general**

    - *NIST SP 800-53*. Es un conjunto de controles y pautas de seguridad de la información desarrollado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (National Institute of Standards and Technology [NIST]). Incluye controles específicos para la protección de los datos personales y la privacidad.

    - *NIST Privacy Framework.*[15] El Marco de Privacidad del NIST proporciona orientación para que las organizaciones gestionen los riesgos de privacidad y desarrollen programas de privacidad efectivos. Se centra en la gestión de riesgos y en el fomento de la confianza y la transparencia en el tratamiento de datos personales.

    - *NIST 800-30. Revision 1. Guide for Conducting Risk Assessments.*[16] Es un documento de referencia

14 ISO (2017). *ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment.* Disponible en https://www.iso.org/standard/62289.html (fecha de consulta: 5 de julio de 2023).

15 NIST (s.f.). *NIST Privacy Framework.* Disponible en https://www.nist.gov/privacy-framework (fecha de consulta: 6 de julio de 2023).

16 NIST (18 de septiembre de 2012). *NIST 800-30 Revision 1. Guide for Conducting Risk Assessments.* Disponible en https://csrc.nist.gov/news/2012/nist-special-publication-800-30-revision-1 (fecha de consulta: 6 de julio de 2023).

que proporciona directrices y recomendaciones para llevar a cabo evaluaciones de riesgos en seguridad de la información.

- *NISTIR 8062. An Introduction to Privacy Engineering and Risk Management in Federal System.*[17] Proporciona una introducción al concepto de ingeniería de privacidad y gestión de riesgos en sistemas de información, destacando la importancia de afrontar la privacidad de manera proactiva desde su diseño, desarrollo y operación.

- *ISO 31000:2018 Risk management — Guidelines.*[18] Establece un enfoque sistemático y estructurado para la gestión de riesgos en cualquier tipo de organización, pública o privada, grande o pequeña, y en cualquier sector o industria. Su objetivo es ayudar a identificar, evaluar y gestionar los riesgos de manera eficaz, con el fin de mejorar la toma de decisiones y alcanzar los objetivos establecidos.

Finalmente, respecto de los resultados obtenidos en la **identificación de la documentación existente,**[19] se obtuvieron hallazgos referentes a:

a. Gestión del Programa para la Protección de Datos Personales

17 NIST (enero de 2017). *NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal System.* Disponible en https://csrc.nist.gov/publications/detail/nistir/8062/final (fecha de consulta: 6 de julio de 2023).

18 ISO (2018). *ISO 31000:2018 Risk management — Guidelines.* Disponible en https://www.iso.org/standard/65694.html (fecha de consulta: 5 de julio de 2023).

19 ISACA (2017). *Implementing a Privacy Protection Program: Using COBIT 5 Enablers with the ISACA Privacy Principles.* ISACA.

b. Presupuesto para la protección de datos personales
c. Gestión de proyectos de datos personales
d. Políticas, estándares y procedimientos de datos personales
e. Requerimientos para la protección de los datos personales (técnicos y normativos)
f. Materiales de capacitación y concientización
g. Reportes de cumplimiento en la protección de datos personales
h. Gestión de riesgos de los datos personales
i. Tablero del Sistema de Gestión para la Protección de Datos Personales

La información obtenida se plasmó en una matriz que relaciona la participación de las partes interesadas con respecto a la información identificada (ver tabla 5).

Tabla 5

Nomenclatura utilizada en la matriz de participación de las partes interesadas

Nomenclatura	Participación	Descripción
A	Aprobador/a	Área que verifica que la actividad se cumpla sin tener que ejecutarla.
C	Creador/a	Área que genera o desarrolla la actividad.
I	Informado/a	Área a quien debe informarse de la actividad.
U	Usuario/a de la información	Área que utilizará la información.
NP	No participa	Área que NO participa.

Figura 6
Participación de las partes interesadas, internas y externas

Partes interesadas	Gestión del Programa para la Protección de Datos Personales	Presupuesto para la protección de datos personales	Gestión de proyectos de datos personales	Políticas, estándares y procedimientos de datos personales	Requerimientos para la protección de los datos personales
Internas					
Alta dirección (Comité de Transparencia en el sector público)	**I/U**	**A**	**A**	**I**	**NP**
Órganos en materia de transparencia	**C/A**	**C**	**C**	**C**	**C**
Otros órganos colegiados	**U**	**NP**	**NP**	**A**	**A**
Áreas responsables	**U**	**NP**	**NP**	**U**	**U**
Áreas de seguridad de la información	**NP**	**NP**	**NP**	**U**	**U**
Áreas de TIC	**NP**	**NP**	**NP**	**U**	**U**
Externas					
Autoridades de protección de datos	**NP**	**NP**	**NP**	**NP**	**NP**
Encargados	**NP**	**NP**	**NP**	**U**	**U**
Titulares	**NP**	**NP**	**NP**	**I**	**NP**
Otros sujetos obligados	**NP**	**NP**	**NP**	**U**	**U**

Continúa...

Partes interesadas	Materiales de capacitación y concientización	Reportes de cumplimiento en la protección de datos personales	Gestión de riesgos de los datos personales	Tablero (*dashboard*) del Sistema de Gestión para la Protección de Datos Personales
Internas				
Alta dirección (Comité de Transparencia en el sector público)	**NP**	**NP**	**A**	**I**
Órganos en materia de transparencia	**C/A**	**C**	**C**	**C**
Otros órganos colegiados	**NP**	**A**	**I**	**A**
Áreas responsables	**U**		**C**	**I**
Áreas de seguridad de la información	**U**	**U**	**U**	**U**
Áreas de TIC	**NP**	**U**	**U**	**NP**
Externas				
Autoridades de protección de datos	**NP**	**NP**	**NP**	**I**
Encargados	**NP**	**NP**	**NP**	**NP**
Titulares	**NP**	**NP**	**NP**	**NP**
Otros sujetos obligados	**NP**	**NP**	**NP**	**NP**

Fuente: Elaboración propia.

La organización del INE para atender sus obligaciones en materia de protección de datos personales

El Comité de Transparencia

La alta dirección[20] se refiere al nivel más alto de liderazgo y toma de decisiones en una organización. Está compuesta por los altos cargos directivos, gerentes o ejecutivos que tienen la responsabilidad de establecer la dirección estratégica y supervisar el funcionamiento general de la organización.

Su liderazgo, experiencia y toma de decisiones informadas son fundamentales para alcanzar los objetivos estratégicos y garantizar el buen funcionamiento de la organización en su conjunto. Su capacidad para adaptarse a los cambios y liderar la transformación es esencial en un entorno dinámico y competitivo.

En materia de datos personales para el sector público, la alta dirección está representada por un comité de transparencia. En el sector privado, puede ser conocida como un comité directivo de privacidad (*privacy steering committee*).

El artículo 83 de la Ley General de Datos dispone el deber de todo responsable de contar con un comité de transparencia, concediéndole la atribución de máxima autoridad en la materia[21] y dotándolo de autonomía (característica fundamental para su funcionamiento y la emisión de resoluciones referentes a datos personales).[22] Su papel en el interior de las organizaciones es fundamental,

20 También conocida como dirección ejecutiva o dirección *senior*.
21 Ley General de Datos, artículo 83.
22 M. S. Maqueo Ramírez, *op. cit.*, p. 266.

dado que el logro de los objetivos establecidos requiere de su apoyo y compromiso para liderar y respaldar activamente la implementación y el cumplimiento de las políticas de protección de datos en toda la organización.

En este contexto, además de las atribuciones establecidas en el artículo 84 de la Ley General de Datos, el **Comité de Transparencia** del INE:

- **Define la visión estratégica.** Establece una visión clara sobre la importancia de la protección de datos personales y su integración en la cultura y los valores del Instituto, fomenta una mentalidad de privacidad y garantiza que todo el personal comprenda la importancia y las implicaciones de la protección de datos personales.

- **Establece políticas y estándares.** Promueve el desarrollo de políticas y estándares internos que regulen la obtención, el almacenamiento, el uso y la divulgación de los datos personales en cumplimiento de las leyes y regulaciones de protección de datos, verificando que las políticas sean claras, completas y coherentes con los principios y requisitos de la normativa aplicable.

- **Fomenta la cultura de cumplimiento.** Esto implica comunicar y capacitar al personal sobre las políticas y procedimientos de protección de datos personales, establecer mecanismos de supervisión y vigilancia y promover una actitud proactiva hacia la protección de datos.

- **Supervisa y evalúa el cumplimiento.** Supervisa y evalúa regularmente el cumplimiento de las obligaciones de protección de datos, lo que requiere establecer

procesos de auditoría interna, revisar informes periódicos sobre la gestión de datos personales y tomar medidas correctivas cuando sea necesario.

- **Promueve la transparencia y la responsabilidad.** Garantiza que el INE sea transparente en relación con sus prácticas de obtención y uso de datos personales. Establece mecanismos para responder a las solicitudes de las personas titulares sobre sus datos y asegura la rendición de cuentas en caso de incidentes de seguridad que afecten los datos personales.

Fortalecimiento de la estructura de protección de datos personales

La Unidad de Transparencia del Instituto cuenta desde 2015 con un área especializada en protección de datos personales, entre cuyas funciones destacan:

- Atender solicitudes de derechos ARCOP y consultas en la materia.

- Alinear los tratamientos con los principios de protección de datos personales, revisiones de avisos de privacidad[23] y cédulas de sistemas.[24]

En 2017 la aprobación de la Ley General de Datos impuso nuevos desafíos en la materia. Para hacerles frente, la

23 Antes de la entrada en vigor de la Ley General de Datos, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (abrogada el 9 de mayo de 2016 con la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública) se refería a los avisos de privacidad en su artículo 20, fracción III, como "manifestación de datos personales".

24 Documento que describe el sistema mediante el cual son tratados los datos personales.

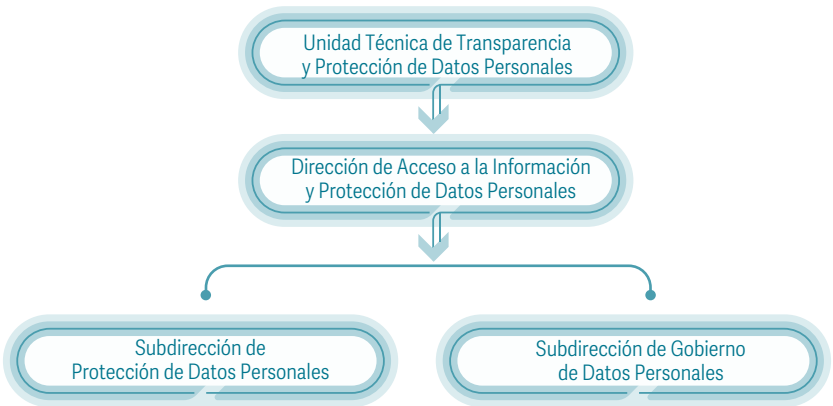
Unidad de Transparencia decidió robustecer su estructura, incorporando un área con funciones para atender:

- Los deberes de seguridad y confidencialidad
- Los esquemas de buenas prácticas
- Los mecanismos para atender el principio de responsabilidad

De esta forma, el INE cuenta con una estructura que atiende las obligaciones establecidas en la Ley General de Datos, abarcando tanto el enfoque normativo como el tecnológico y de seguridad de la información.

Figura 7

Estructura organizacional para la protección de datos personales en el INE



Fuente: Elaboración propia.

Con esta estructura multidisciplinaria, el INE suple la figura del Oficial de Protección de Datos Personales propuesta en el artículo 85 de la Ley General de Datos, aplicable –sin obligatoriedad– para aquellos responsables

que lleven a cabo tratamientos de datos personales relevantes o intensivos en el ejercicio de sus funciones.

Para la selección de las personas encargadas de estas áreas, el Instituto considera:

- Experiencia
- Conocimientos técnicos y de las leyes y regulaciones aplicables
- Habilidades en gestión de riesgos
- Capacidad para trabajar en colaboración con diferentes áreas del INE y comunicarse efectivamente con las partes interesadas

Con tal acción el INE consolida:

1. **El cumplimiento normativo** que asegura que el Instituto desempeñe sus obligaciones legales en materia de protección de datos y evite posibles sanciones o multas por incumplimiento.

2. **La *expertise*,** al robustecer los conocimientos especializados en materia de protección de datos y privacidad, y permitir al Instituto tratar de manera efectiva los desafíos y riesgos relacionados con la protección de datos.

3. **El asesoramiento y consultoría,** ya que aporta asesoramiento y consultoría interna sobre cuestiones relacionadas con la protección de datos, además de orientar a la alta dirección, al personal y a las áreas responsables del Instituto en cuanto a políticas, prácticas y procesos concernientes al tema.

4. **La supervisión y monitoreo,** pues se vigila el cumplimiento de las políticas y procedimientos de protección de datos dentro del Instituto y se monitorean las actividades de su procesamiento a través de auditorías internas, evaluación de riesgos e implementación de medidas para garantizar que se mantenga un alto nivel de protección.

5. **La gestión de incidentes,** ya que para atender casos de violaciones de seguridad o incidentes relacionados con la protección de datos se ofrece acompañamiento a las áreas responsables para responder de manera oportuna y adecuada, minimizando los riesgos y protegiendo los derechos de las personas cuyos datos se pudieran ver comprometidos.

La conformación de una estructura multidisciplinaria con experiencia en protección de datos personales ha sido fundamental en el INE para:

- Garantizar el cumplimiento normativo y el asesoramiento especializado.

- Monitorear y supervisar de manera efectiva las actividades de protección de datos.

- Gestionar de forma adecuada los riesgos de privacidad.

- Fortalecer la confianza de las personas titulares en el tratamiento de sus datos.

CAPÍTULO III

Modelo de operación para el cumplimiento de la protección de datos personales

El INE, a través de la Unidad de Transparencia, diseñó en 2019 un Modelo de operación para el cumplimiento de la protección de datos personales (en adelante, el Modelo de operación), con el objetivo de implementar el principio de responsabilidad desde un enfoque proactivo.

El Modelo de operación es un concepto innovador en cuanto al tratamiento de datos personales, pues indica al Instituto la ruta a seguir para cumplir de manera sistemática y atemporal sus obligaciones respecto de los principios y deberes, no sólo en atención a las disposiciones normativas vigentes, sino también tomando en consideración otros elementos y documentos rectores que complementan su correcta aplicación. Su diseño tomó como insumos:

a. La **evaluación de la situación actual,** que desencadenó el reforzamiento de la estructura de protección de datos personales en el Instituto, como se describe en el capítulo anterior de esta publicación.

b. El PRONADATOS, construido por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT). Se analizaron las acciones del PRONADATOS correspondiente al periodo 2018-2022 para garantizar el cumplimiento del Instituto como sujeto obligado de la política pública de protección de datos personales en el país, así como los objetivos propios del INE en la materia.

El PRONADATOS cuenta con una actualización (2019 y 2020), denominada primer PRONADATOS, y una segunda versión correspondiente al periodo 2022-2026, denominada segundo PRONADATOS, que recupera los

objetivos de la primera edición y refuerza las acciones que dan solución a las causas de los principales problemas diagnosticados.

Figura 1

Acciones tomadas para diseñar el Modelo de operación del INE

Fuente: Elaboración propia.

El **primer PRONADATOS** incluyó una proyección a 20 años con una línea del tiempo dividida en cuatro etapas:

1. ¿Dónde estamos? (2018-2020)
2. ¿Dónde estaremos? (2020-2022)
3. ¿Hacia dónde vamos? (2022-2026)
4. ¿A qué aspiramos? (2037)

Esta línea resultó de suma importancia para el Instituto y fue considerada para poder determinar su avance en el cumplimiento de la protección de datos a nivel nacional.[1]

El **segundo PRONADATOS** establece una temporalidad a cinco años y plantea la intención de elaborar un tercer PRONADATOS.

La figura 2 detalla una comparativa entre las acciones señaladas en las cuatro etapas del segundo PRONADATOS:

1. ¿Dónde estamos? (2021-2022)

2. ¿Dónde estaremos? (2022-2026)

3. Hacia el tercer PRONADATOS

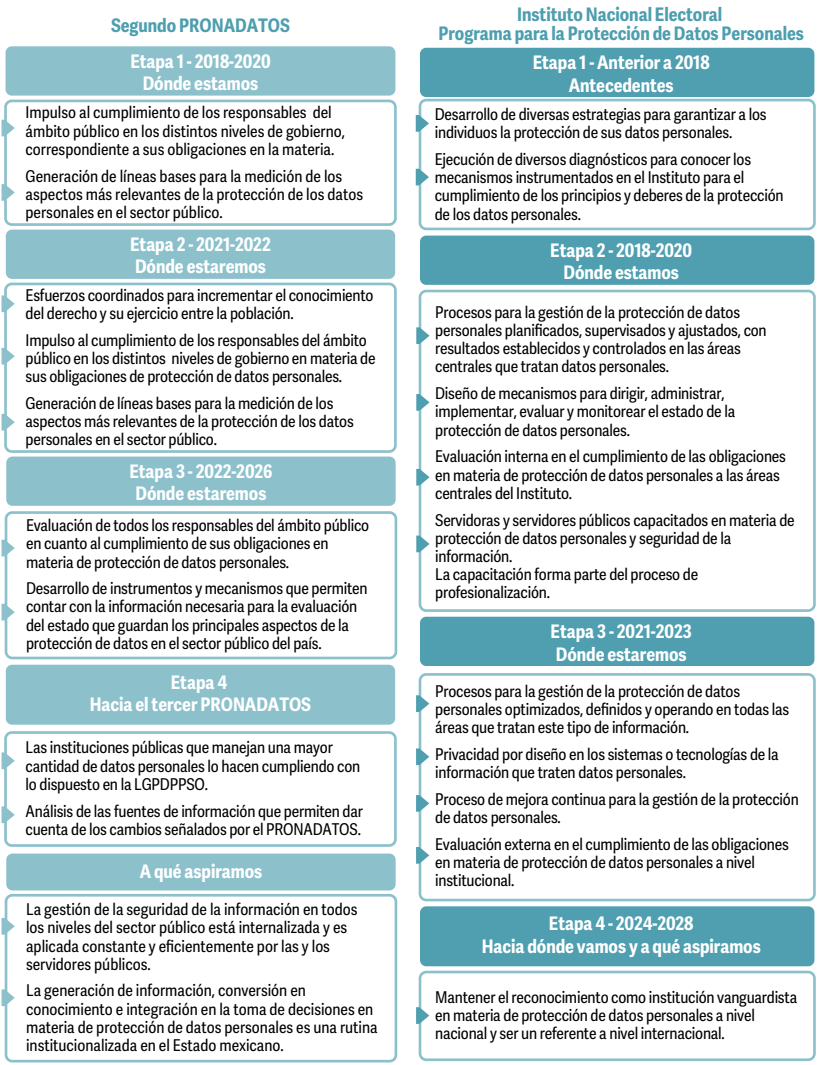
4. ¿A qué aspiramos?

Cabe señalar que el segundo PRONADATOS no afectó las acciones proyectadas por el Instituto en el Modelo.

Las acciones del Modelo que el Instituto ha implementado, así como las que está por implementar, permiten visualizar en dónde se ubica en relación con el PRONADATOS.

1 Para más información, consultar el sitio oficial disponible en https://proyectos.inai.org.mx/pronadatos/

Figura 2
Etapas para el cumplimiento del Programa para la Protección de Datos Personales del INE vs. PRONADATOS



Fuente: Elaboración propia.

El Modelo de operación consta de cuatro grandes apartados enfocados en la protección de datos personales:

1. Un **Programa**, integrado a su vez por dos estrategias enfocadas en el cumplimiento de los deberes de seguridad y confidencialidad, y en los principios.[2]

2. El **Sistema de Gestión para la Protección de Datos Personales** (en adelante, SiPRODAP), integrado por una base regulatoria, un catálogo de controles y un Modelo de implementación.[3]

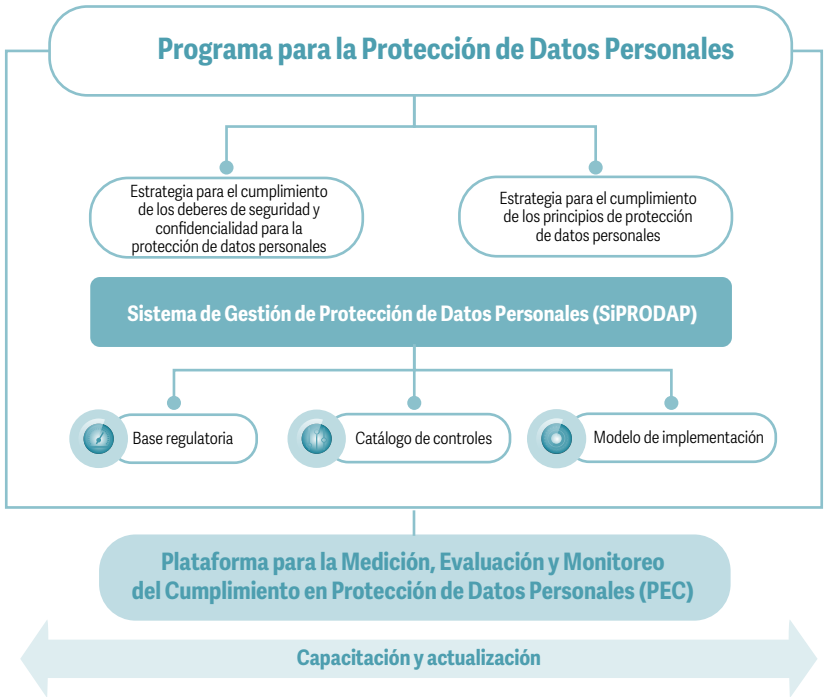
3. La **Plataforma para la Medición, Evaluación y Monitoreo del Cumplimiento en Protección de Datos Personales** (en adelante, PEC) como la herramienta informática para la operación del SiPRODAP.

4. **Capacitación y actualización** del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.[4]

La figura 3 esquematiza estos componentes:

2 Ley General de Datos, artículo 30, fracción II.
3 Ley General de Datos, artículo 30, fracción V.
4 Ley General de Datos, artículo 30, fracción III.

Figura 3
Modelo de Protección de Datos Personales



Fuente: Elaboración propia.

El uso de este modelo permite al INE consolidarse como una institución confiable en cuanto al tratamiento de datos personales. En los siguientes apartados, se describen a profundidad sus componentes.

Programa para la Protección de Datos Personales

Un programa de protección de datos personales consiste en un conjunto de medidas y prácticas implementadas por una organización para garantizar la seguridad, privacidad e integridad de la información personal que recopila, almacena y procesa.

El objetivo principal de un programa de protección de datos personales es garantizar que su tratamiento se realice atendiendo los principios y deberes de la normativa aplicable en la materia.

Algunos elementos clave que suelen formar parte de un programa de protección de datos personales son los que se muestran en la figura 4:

Figura 4

Elementos clave de un programa de protección de datos personales

Fuente: Elaboración propia.

- **Políticas y procedimientos**: Se establecen directrices claras sobre cómo se deben manejar y proteger los datos personales, incluyendo la forma en que se recopilan, almacenan, procesan y comparten.

- **Evaluación de riesgos**: Se lleva a cabo una evaluación de riesgos para identificar posibles vulnerabilidades y amenazas que puedan afectar la seguridad de los datos personales.

- **Medidas de seguridad**: Se implementan medidas técnicas y organizativas para proteger los datos, como el uso de *firewalls*, cifrado de datos, controles de acceso, capacitación del personal, entre otros.

- **Consentimiento informado**: Se obtiene el consentimiento de las personas antes de recopilar y procesar sus datos personales, asegurándose de que comprendan claramente cómo se utilizará su información.

- **Gestión de incidentes de seguridad**: Se establecen procedimientos para manejar y responder ante incidentes de seguridad, como fugas de datos o accesos no autorizados.

- **Cumplimiento normativo**: Se asegura el cumplimiento de las leyes y regulaciones de protección de datos aplicables.

- **Educación y capacitación**: Se confiere formación y concienciación al personal sobre las mejores prácticas de protección de datos personales para fomentar una cultura de privacidad dentro de la organización.

Los programas de protección de datos personales varían según la organización y su contexto, pues deben adaptarse a las necesidades específicas y a las regulaciones vigentes que norman sus procesos de negocio.

La implementación del Programa para la Protección de Datos Personales del INE (en adelante, el Programa)[5] se sustenta en el desarrollo de dos grandes estrategias; la primera para cumplir con los deberes de seguridad

5 Aprobado mediante el Acuerdo INE-CT-ACG-PDP-004-2018 el 8 de noviembre de 2018.

y confidencialidad y la segunda para cumplir con los principios rectores de protección de datos personales.

Garantizar la protección de los datos de millones de personas es de suma importancia para el Instituto, pues ello multiplica la confianza de la ciudadanía en los comicios, cimienta la certeza entre los actores políticos de que existen condiciones de equidad en la contienda electoral y fortalece el orden democrático que hemos elegido como vía para la transmisión pacífica del poder.

El trabajo realizado por el INE en el diseño e implementación de este Programa no sólo pretende el cumplimiento llano de la norma establecida por el Legislativo; además, busca constituir una gestión institucional mediante el establecimiento de elementos y actividades de dirección, operación y control de todos sus procesos que impliquen un tratamiento de datos personales a efecto de proteger estos de manera sistemática y continua, para acreditar el cumplimiento de los principios, deberes y obligaciones.

Asimismo, busca que las personas se apropien del derecho a la protección de los datos personales, sea como titulares o como responsables de su tratamiento.

El Programa del INE integra todos los esfuerzos de la institución a lo largo de su historia por aplicar un adecuado tratamiento a los datos personales que posee. Tanto este como las estrategias que lo conforman y sus planes de implementación tienen las siguientes características:

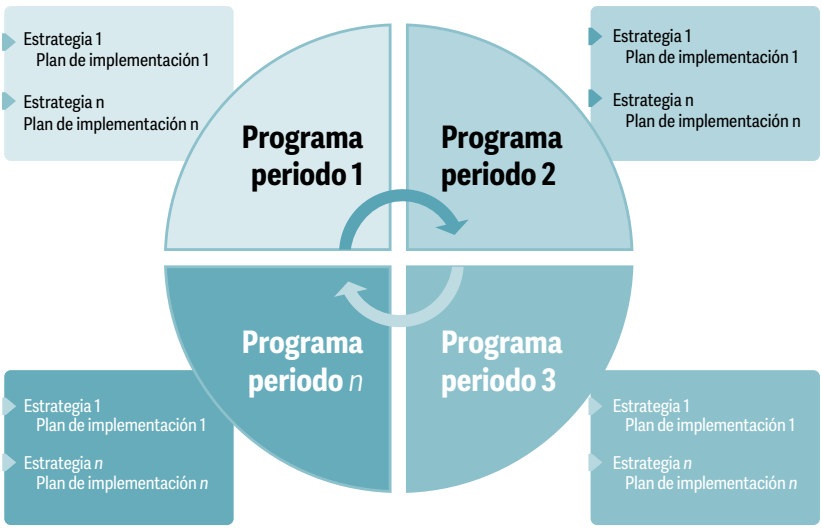
1. **El Programa es estático y atemporal,** con periodos cíclicos determinados, sugiriendo que cada ciclo tenga una **vigencia de, al menos, cuatro años,** con la finalidad de permitir el logro de los objetivos proyectados.

2. **Las estrategias son elementos semidinámicos** que tienen la finalidad de afrontar los cambios, lo que incluye identificar, reconocer, regularizar, innovar e implementar, con base en la experiencia adquirida con el paso del tiempo y en las normas que emite el Sistema Nacional de Transparencia durante el periodo que comprenda el Programa. Se sugiere que cada estrategia tenga un periodo de **vigencia de, al menos, dos años,** lo que dará como mínimo dos ciclos por estrategia.

3. **Los planes de implementación son elementos dinámicos** con **temporalidad anual**, lo que permite programar los recursos humanos, materiales, tecnológicos y financieros.

Figura 5

Ejemplo de planeación atemporal de un programa de protección de datos personales



Fuente: Elaboración propia.

Las acciones que el INE realizó conforme a los diagnósticos de principios y deberes descritos en el capítulo anterior de esta publicación se describen en la tabla 1.

Tabla 1

Resumen de las acciones realizadas por el INE

2014	2015	2016	2017
Se realizó la identificación y actualización de las bases de datos personales a nivel central publicadas en el portal INE.	Inició con la regularización y actualización del Listado de sistemas de datos personales del INE.	Se llevó a cabo el diagnóstico de las bases de datos registradas en el Listado de sistemas de datos personales.	Se ejecutó una verificación conceptual de medidas de seguridad.

En relación con estas acciones, la Unidad de Transparencia etiqueta –según su estado– los procesos de negocio del Instituto cuyas actividades tratan datos personales de la siguiente manera:

Figura 6

Estado de los procesos de negocio institucionales

Fuente: Elaboración propia.

1. **Identificado.** Proceso de negocio creado para atender una obligación institucional; puede o no tratar datos personales.

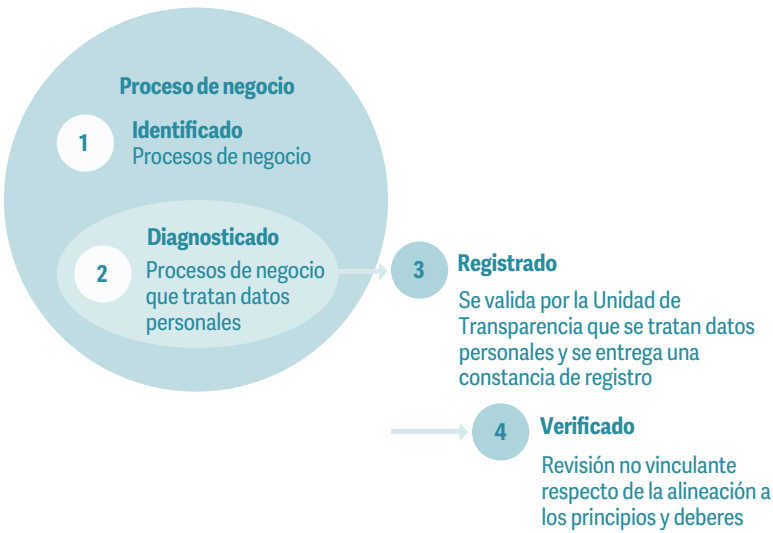
2. **Diagnosticado.** Proceso de negocio sometido a una revisión documental para determinar y validar si sus actividades tratan datos personales.

3. **Registrado.** Proceso de negocio –incluyendo sus bases de datos y sistemas de tratamiento– que, tras ser sometido a revisión documental, es validado por la Unidad de Transparencia como proceso que trata datos personales, asignándole una constancia de registro.[6]

4. **Verificado.** Proceso de negocio –incluyendo sus bases de datos y sistemas de tratamiento– sometido a una **revisión no vinculante ejecutada a través de las estrategias de principios y deberes para determinar su alineación al cumplimiento normativo**.

Figura 7

Estados que recorre un proceso de negocio que trata datos personales



Fuente: Elaboración propia.

6 Para más información del procedimiento interno para el registro de sistemas de tratamiento de datos personales en posesión del INE, consultar la URL https://sidj.ine.mx/restWSsidj-nc/app/doc/1715/20/1

Para tener una visión clara del estado en que se encuentra cada uno de los procesos de negocio del Instituto, se ordenan en ejes; todos los estados parten del eje 1 y recorren un camino hasta llegar al eje 4, como se observa en la tabla 2.

Tabla 2

Orden de los procesos de negocio

Estado				
Eje	**Identificado**	**Diagnosticado**	**Registrado**	**Verificado**
1	X			
2	X	X		
3	X	X	x	
4	X	X	x	X

El siguiente apartado detalla las estrategias que integran el Programa, a través de las cuales se brindan las bases para verificar, es decir, alinear, los procesos de negocio que tratan datos personales al cumplimiento de los principios y deberes de protección de ese tipo de datos.

Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad para la Protección de Datos Personales

El objetivo de esta estrategia es determinar las acciones concretas a seguir por parte del Instituto[7] en relación con el tratamiento de los datos personales y proveer a los órganos del INE las bases para el cumplimiento de los

7 Referentes al Título Segundo, Capítulo II De los Deberes, de la Ley General de Datos.

deberes de seguridad y confidencialidad. Sus objetivos específicos son:

- Generar el documento de seguridad para demostrar el cumplimiento respecto de la protección de los datos personales.

- Coadyuvar en la implementación del Sistema de Gestión para la Protección de Datos Personales.

Las bases de esta estrategia se cimientan en el análisis de normas y buenas prácticas, así como en las guías nacionales e internacionales en materia de privacidad, protección de datos personales y seguridad de la información descritas más adelante.

La Estrategia de Deberes se compone de cinco etapas, como se observa en la figura 8.

Figura 8

Etapas que conforman la Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad para la Protección de Datos Personales

Fuente: Elaboración propia.

- **Etapa Preliminar. Identificación del propietario de las bases de datos y necesidades del área**

Para iniciar la implementación, adecuación o mejora de las medidas de seguridad aplicadas a los datos personales, en esta etapa las unidades administrativas del Instituto identifican:

a. El proceso/subproceso

b. La base o las bases de datos personales

c. La persona o personas responsables de dicho tratamiento

Con esta información se genera y mantiene actualizado un directorio de responsables y bases de datos.

- **Etapa 1. Identificación del flujo de los datos personales**

Esta etapa tiene la finalidad de identificar y documentar:

- Los datos personales que componen cada base, su clasificación y tipo.

- El personal que tiene acceso, los permisos otorgados, funciones y obligaciones.

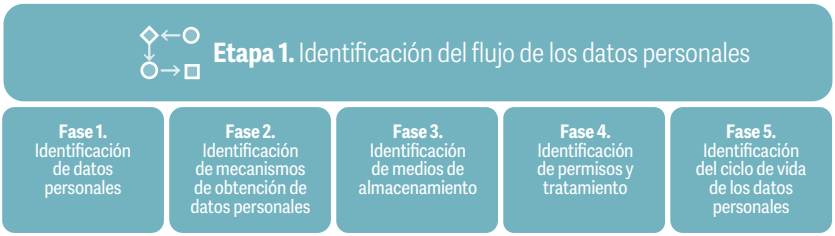
- El ciclo de vida de los datos personales.[8]

Lo anterior se logra a lo largo de las siguientes fases:

8 Conforme al artículo 59 de los "Lineamientos Generales de Protección de Datos Personales para el Sector Público".

Figura 9

Fases de la etapa 1 de la Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad para la Protección de Datos Personales



Fuente: Elaboración propia.

- *Fase 1. Identificación de datos personales*

  Las unidades administrativas, con apoyo de las áreas involucradas y de la Unidad de Transparencia, identifican los datos personales tratados, así como su tipo y categorización (estándar, sensible o especial) en relación con el proceso de negocio que corresponda.

- *Fase 2. Identificación de mecanismos de obtención de datos personales*

  Las unidades administrativas identifican la forma en que recaban los datos personales, proporcionando elementos para verificar si se obtienen de una manera libre, específica e informada.

- *Fase 3. Identificación de medios de almacenamiento*

  Tomando en consideración, de ser el caso, la existencia de encargados, destinatarios o terceros receptores de las transferencias que se efectúen, las unidades administrativas identifican:

- Los sitios, medios, soportes documentales y formatos utilizados para almacenar los datos personales.

- Si se resguardan en un sitio específico o en un área común.

- Si son resguardados en medios de almacenamiento físicos o digitales.

- *Fase 4. Identificación de permisos y tratamiento*

  Considerando, de ser preciso, la existencia de encargados, destinatarios o terceros receptores, las unidades administrativas identifican:

  - Al personal y, en su caso, prestadores y prestadoras de servicios que intervienen en el tratamiento de los datos personales, así como el puesto, rol y permisos les son asignados y las responsabilidades que ostentan en relación con el tratamiento de este tipo de información.

  En cuanto al sistema de tratamiento:

  - El nombre, objetivo, fecha de creación y última actualización.

  - El área dueña del sistema.

  - El área responsable de su desarrollo y mantenimiento.

  - Si el sistema de tratamiento es manual, automatizado o mixto.

- *Fase 5. Identificación del ciclo de vida de los datos personales*

  Las unidades administrativas detallan mediante un diagrama de flujo, con base en la información resultante de las fases anteriores, qué datos son tratados en cada fase del ciclo de vida de este tipo de datos, considerando los activos secundarios utilizados y los roles involucrados en su tratamiento. Además, se genera un inventario de datos personales y sistemas de tratamiento.

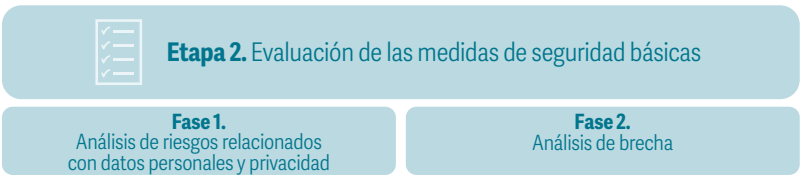
- **Etapa 2. Evaluación de las medidas de seguridad básicas**

Esta etapa tiene como finalidad la gestión del riesgo. Si bien no es posible eliminar los riesgos, es necesario identificar e implementar medidas de seguridad adecuadas a la categoría del dato personal, con la finalidad de proteger estos datos ante una vulneración.[9]

Esta etapa se compone de dos fases:

Figura 10

Fases de la etapa 2 de la Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad para la Protección de Datos Personales



Fuente: Elaboración propia.

9 La obligación de establecer medidas de seguridad se encuentra contemplada en los artículos 31, 32 y 33, fracciones VI y VII, de la Ley General de Datos y en el artículo 60 de los "Lineamientos Generales de Protección de Datos Personales para el Sector Público".

- *Fase 1. Análisis de riesgos relacionados con datos personales y privacidad*

El área responsable identifica los riesgos derivados del tratamiento de datos personales, es decir, aquellos a los que se exponen en cada etapa de su ciclo de vida, así como los posibles impactos de eventos temidos o no deseados en la privacidad de las personas, los grupos o la sociedad, para la posterior implementación o adecuación de las medidas de protección o controles correspondientes.

Para este análisis se sugiere la adopción de algún estándar en la materia, por lo que el INE generó una metodología propia basada en los estándares ISO/IEC 27005,[10] ISO 31000,[11] NIST 800-30[12] y NISTIR 8062.[13]

Mediante cuestionarios y formatos, las unidades administrativas:

a. Identifican los escenarios de riesgo existentes en cada una de las fases del ciclo de vida de los datos personales, de acuerdo con el tipo de dato.

b. Analizan los eventos temidos, las amenazas y sus fuentes por cada uno de los escenarios de riesgos previamente identificados.

c. Determinan los riesgos y su posibilidad de ocurrencia.

10 *ISO/IEC 27005..., op. cit.*
11 ISO (2018), *op. cit.*
12 NIST (18 de septiembre de 2012), *op. cit.*
13 NIST (enero de 2017), *op. cit.*

- *Fase 2. Análisis de brecha*

  El área responsable identifica las medidas de seguridad físicas, técnicas y administrativas existentes, así como las faltantes o la necesidad de reforzar las actuales.[14]

  Para tal efecto se sugiere adoptar un estándar de seguridad de la información; el INE utiliza el ISO/IEC 27002[15] e ISO/IEC 27701.[16]

  Las unidades administrativas mediante cuestionarios y formatos:

  a. Identifican los controles de seguridad implementados en el proceso de negocio, los controles faltantes o el necesario reforzamiento de los existentes.

  b. Clasifican las medidas de seguridad por cada control identificado en físicas, técnicas o administrativas.

En la ejecución de estos análisis debe participar el conjunto de personas involucradas en el tratamiento de los datos personales durante todo su ciclo de vida. En el INE esto se realiza con el apoyo de la Unidad de Transparencia

14 De acuerdo con el artículo 33, fracción V, de la Ley General de Datos y el artículo 61 de los "Lineamientos Generales de Protección de Datos Personales para el Sector Público".

15 ISO (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.* Disponible en https://www.iso.org/standard/75652.html (fecha de consulta: 15 de septiembre de 2023).

16 ISO (2019), *op. cit.*

y, en su caso, de los órganos vinculados con seguridad de la información y/o seguridad física.

Esta etapa genera como entregables los riesgos de privacidad y datos personales y las brechas de las medidas de seguridad en los procesos de negocio que tratan datos personales.

- **Etapa 3. Plan de trabajo**

Para elaborar el plan de trabajo[17] el área responsable identifica al menos los siguientes elementos:

a. El orden de prioridad de las acciones a realizar para la implementación de las medidas de seguridad faltantes y de las que serán sustituidas o reforzadas, como resultado del análisis de brecha y el análisis de riesgos.

b. El tiempo de ejecución.

c. La persona responsable de ejecutar las actividades.

d. Los recursos requeridos.

Con el resultado de la identificación, el área responsable:

a. Elabora el plan de trabajo para la implementación o adecuación de las medidas de seguridad.

b. Determina los recursos necesarios para cumplir con las acciones en el periodo establecido.

El entregable de la etapa es el plan de trabajo.

17 En atención al artículo 33, fracción VI, de la Ley General de Datos.

- **Etapa 4. Mejora continua**

La mejora continua se logra a través del monitoreo y revisión periódica de las medidas de seguridad implementadas, así como de las amenazas y vulneraciones a las que están sujetos los datos personales, considerando:

- Nuevos activos que se incluyan en la gestión de riesgos.

- Modificaciones necesarias a los activos –cambio o migración tecnológica, entre otras–.

- Nuevas amenazas que podrían estar activas dentro y fuera de la organización y que no han sido valoradas.

- Posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.

- Vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.

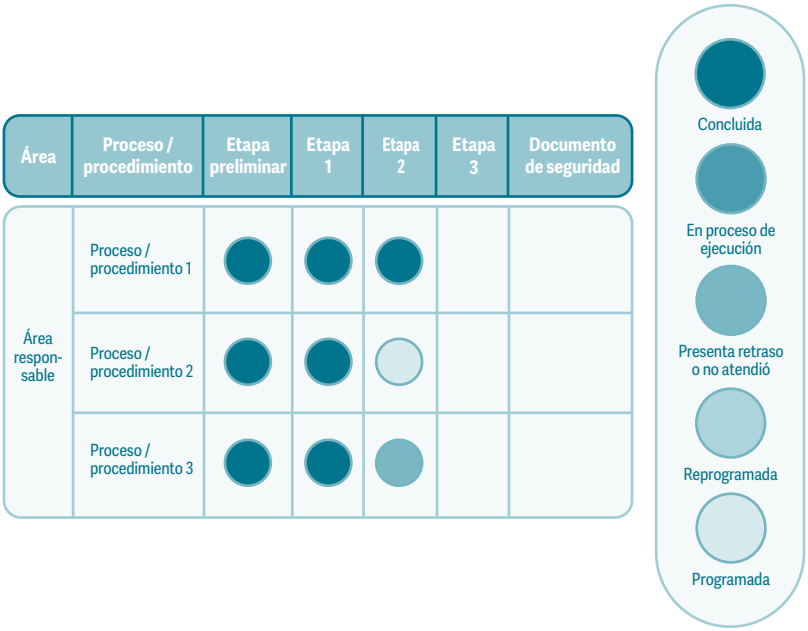
- Cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto que resulten en un nivel inaceptable de riesgo.

- Incidentes y vulneraciones de seguridad ocurridas.

Para tal efecto, la Unidad de Transparencia propone la elaboración de un programa de seguridad enfocado en la información que contiene datos personales, y que considere los puntos antes mencionados.

La Unidad de Transparencia genera un plan de implementación anual en donde determina tiempos, áreas y responsables para ejecutar las acciones anteriores; además, elabora diversos materiales de apoyo que pueden ser consultados en el Apartado virtual "Protección de datos personales", [18] que se encuentra en la página web del Instituto.

Figura 11
Ejemplo de semáforo de seguimiento



Fuente: Elaboración propia.

Disponer de un plan de implementación es de suma importancia porque permite dar seguimiento e identificar retrasos en las actividades programadas, así como establecer un semáforo de cumplimiento.

18 INE (26 de junio de 2022), *op. cit.*

Finalmente, quienes fungen como responsables del tratamiento de datos personales en las unidades administrativas generan un documento de seguridad por cada proceso de negocio que utiliza este tipo de información. Para ello, la Unidad de Transparencia desarrolló el documento "Procedimiento para elaborar el Documento de Seguridad".[19]

Con los entregables generados en cada etapa por área responsable, se conforma el documento de seguridad institucional,[20] el cual es integrado por la Unidad de Transparencia.

Estrategia para el cumplimiento de los principios de protección de datos personales

El objetivo de esta estrategia es determinar las acciones a seguir por parte de la Unidad de Transparencia y de las áreas responsables respecto al tratamiento de los datos personales en lo referente al Título Segundo, Capítulo I De los Principios, de la Ley General de Datos.

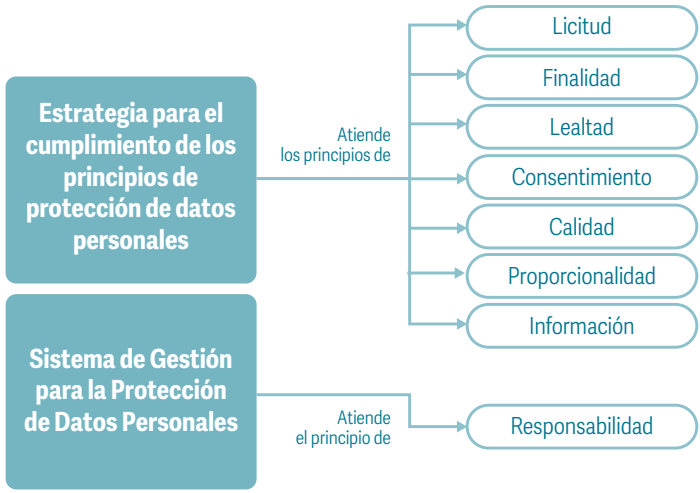
Esta estrategia prevé dotar a los órganos del INE de los elementos que les permitan cumplir con las obligaciones de la normativa aplicable, para atender los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad e información, quedando excluido el de responsabilidad, debido a que su cumplimiento se lleva a cabo de manera general mediante el SiPRODAP.

19 INE (s.f.). *Procedimiento para elaborar el Documento de Seguridad.* Disponible en https://ine.mx/wp-content/uploads/2021/05/SSPPDP-Proce-elaborar-DocSeg.pdf (fecha de consulta: 6 de julio de 2023).

20 En cumplimiento al artículo 35 de la Ley General de Datos.

Figura 12

Elementos para cumplir con las obligaciones normativas aplicables a los principios



Fuente: Elaboración propia.

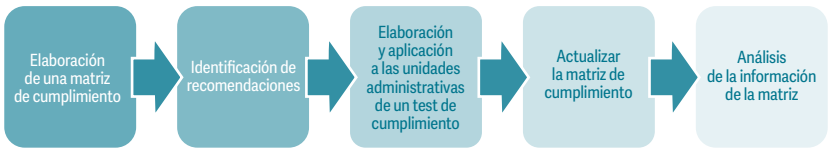
En un primer momento la Estrategia de principios trabajó sobre los ejes 1, 2 y 3 con acciones a corto y mediano plazo, con la finalidad de alinear los tratamientos existentes con lo establecido en la Ley General de Datos.

Las acciones se describen a continuación:

- Corto plazo (diagnóstico)

Figura 13

Acciones a corto plazo con la finalidad de regularizar los tratamientos existentes



Fuente: Elaboración propia.

- **Elaboración de una matriz de cumplimiento** con cada uno de los principios previstos en la Ley General de Datos.

- **Identificación de recomendaciones** formuladas en el Diagnóstico sobre las Bases de Datos registradas en el Listado de Sistemas de Datos Personales (en adelante, Diagnóstico).[21]

- **Elaboración y aplicación a las unidades administrativas de un test de cumplimiento** para identificar las acciones que han realizado para observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad e información, conforme a las nuevas disposiciones que prevé la Ley General de Datos.

- **Actualización de la matriz de cumplimiento** con base en las recomendaciones formuladas en el Diagnóstico y en la información obtenida de las unidades administrativas, esto derivado de la aplicación del test de cumplimiento.

- **Análisis de la información de la matriz**, a la luz de las facultades que tienen conferidas las unidades administrativas y del marco normativo aplicable

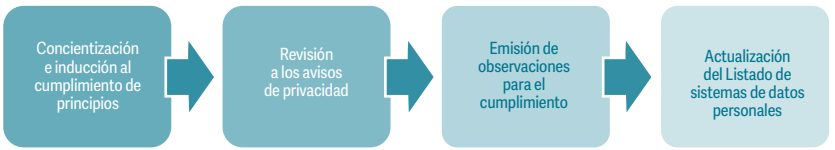
21 Durante el segundo semestre de 2016, la Unidad de Transparencia –con el apoyo de una consultora externa– realizó un Diagnóstico sobre las Bases de Datos registradas en el Listado de Sistemas de Datos Personales, a fin de identificar, por una parte, si las registradas efectivamente constituyen bases de datos personales y, por otra, el cumplimiento que los órganos del Instituto responsables de dichas bases dieron a los principios previstos en el Acuerdo INE/CG312/2016 (es decir, licitud, consentimiento, calidad, finalidad, proporcionalidad e información). Como resultado del Diagnóstico, se formularon una serie de recomendaciones generales y específicas, con la finalidad de alinear las bases al marco normativo vigente en ese momento.

en materia de protección de datos personales, a efecto de identificar las acciones que deberán llevar a cabo para cumplir con las obligaciones que derivan de cada principio y para trabajar en las áreas de oportunidad.

- Mediano plazo (regularización)

Figura 14

Acciones a mediano plazo con la finalidad de regularizar los tratamientos existentes



Fuente: Elaboración propia.

- **Concientización e inducción al cumplimiento de los principios** de protección de datos personales a las áreas responsables, para garantizar la adopción de buenas prácticas en la materia mediante la impartición de cursos y talleres en línea, así como la elaboración y distribución de materiales informativos y campañas de comunicación interna, con el objetivo de fomentar la cultura de protección de datos personales en el Instituto.

- **Revisión de los avisos de privacidad** y de las cédulas descriptivas de las áreas responsables publicadas en el portal INE, por base de datos, con el objeto de verificar que cuenten con los elementos establecidos en los artículos 27 y 28 de la Ley General de Datos y se encuentren alineados a los formatos institucionales elaborados por la Unidad de Transparencia.

- **Emisión de observaciones para el cumplimiento** por parte de las áreas responsables a través de compromisos establecidos para corregir las deficiencias encontradas en la revisión, e implementando las medidas necesarias para garantizar el cumplimiento normativo. El seguimiento de esos compromisos incluye la asignación de responsabilidades, plazos de ejecución y revisiones regulares para evaluar el progreso y tomar medidas correctivas cuando sea necesario.

- **Actualización del Listado de sistemas de datos personales** que poseen y tratan las diversas áreas responsables del Instituto, lo que implica identificar y catalogar todas las bases de datos personales por área responsable, especificando el proceso de negocio en el que son empleadas, así como las personas responsables de su manejo. Para ello se realizan revisiones periódicas del Listado, con el objetivo de verificar la exactitud de la información registrada y asegurar que refleje de manera precisa la realidad de las bases de datos en posesión del Instituto.

Una vez concluida la regularización y alcanzado un grado de madurez suficiente, se procede a verificar las bases de datos de nueva creación para que no sean objeto de regularización.

Para las acciones anteriores, la Unidad de Transparencia elabora materiales de apoyo que pueden ser consultados en el Apartado virtual "Protección de datos personales".[22]

22 INE (26 de junio de 2022), *op. cit.*

Sistema de Gestión para la Protección de Datos Personales

La adopción de un sistema de gestión representa el mecanismo para rendir cuentas a las personas titulares de los datos y al órgano garante nacional sobre su tratamiento, simboliza un esquema de buenas prácticas y, a su vez, materializa la implementación del principio de responsabilidad; además, engloba la acreditación del cumplimiento del resto de los principios, deberes y demás obligaciones establecidas en la Ley General de Datos.

De manera general, un sistema de gestión permite estructurar los elementos que conformarán la protección de los datos personales mediante un enfoque sistémico para lograr la mejora continua, esto con base en los objetivos de protección de datos personales en la organización y la normatividad aplicable.

Un sistema de gestión está conformado por una serie de procesos, acciones y tareas que se llevan a cabo sobre un conjunto de elementos (personas, procedimientos, estrategias, planes, recursos, productos, etcétera)[23] para que una organización logre sus objetivos,[24] en este caso, la protección de los datos personales.

El artículo 34 de la Ley General de Datos[25] dispone el deber de implementar un sistema de gestión. El INAI desarrolló

23 R. A. Giraldo Giraldo (2017). *Mejoramiento del proceso de compras de la Constructora SSINCO S.A.S.* Disponible en https://repositorio.ucm.edu.co/bitstream/10839/1885/1/Ricardo%20Alberto%20Giraldo.pdf (fecha de consulta: 28 de julio de 2023).

24 ISO (s.f.). *Management system standards*. Disponible en https://www.iso.org/management-system-standards.html (fecha de consulta: 6 de julio de 2023).

25 Artículo 34: "Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión".

la *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*, que, aunque se implementó para atender el cumplimiento de la Ley Federal de Datos,[26] también puede ser utilizada para el caso de los sujetos obligados; no obstante, dicho modelo está acotado a la implementación de la seguridad (deberes) de los datos personales, dejando fuera los principios, derechos y demás obligaciones.

Es importante mencionar que aun cuando las buenas prácticas de seguridad contribuyen a gestionar los riesgos tecnológicos –incidentes de seguridad– y los de cumplimiento legal –al proteger la información en general–, existen otros riesgos que pueden afectar los derechos y libertades de las personas cuyos datos son objeto de tratamiento. Estos riesgos derivan de la forma en que las organizaciones recopilan, almacenan, usan y comparten los datos personales para cumplir con su misión u objetivo de negocio.

Lo anterior permite dilucidar que la protección de los datos personales y la seguridad de la información son conceptos distintos pero interrelacionados. Considerando tal conjetura, la Unidad de Transparencia diseñó en 2019 el SiPRODAP, que provee al Instituto las bases para cumplir con los principios, deberes, derechos y demás obligaciones señaladas en la normativa aplicable, lo que permite:

- Verificar que las medidas implementadas para el cumplimiento de la normativa son eficaces, eficientes y apropiadas de acuerdo con el riesgo inherente del dato personal.

26 INAI (junio de 2015). *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales.* Disponible en https://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf (fecha de consulta: 15 de julio de 2023).

- Demostrar la conformidad de las actividades de tratamiento.

- Medir el aprovechamiento eficaz y permanente de los recursos destinados para el logro de los objetivos de protección de datos personales.

- Integrar a toda la organización en la protección de los datos personales.

Entre las características consideradas para el diseño del SiPRODAP, se encuentran las siguientes:

- Está integrado por las buenas prácticas nacionales e internacionales en materia de protección de datos, privacidad y seguridad de la información.

- Se sustenta en la Ley General de Datos.

- Considera la mejora continua.

- Es escalable en relación con el alcance del sistema de gestión, para que las medidas sean coherentes con los riesgos del procesamiento y la naturaleza del dato personal.

- Es compatible con otros sistemas de gestión y adaptable a diversos organismos públicos, y en su caso privados.

Disponer del Sistema de Gestión para la Protección de Datos Personales provee al Instituto los beneficios que muestra la tabla 3.

Tabla 3

Beneficios de un sistema de gestión para la protección de datos personales

Provee:	
A las personas titulares de los datos	• Transparencia en los mecanismos implementados para el debido tratamiento de sus datos personales. • Confianza en el debido tratamiento de sus datos personales.
Al Instituto y cualquier organización que lo implemente	**De manera general**
	• Las bases para homologar los procesos, acciones y actividades de protección de los datos personales. • Facilitar la transferencia segura entre sujetos obligados u organizaciones internacionales. • Un habilitador clave para lograr la protección de datos por diseño y por defecto. • Un esquema de mejores prácticas.[27] • Conocimiento de los mecanismos de protección de datos que son implementados. • Las bases para una mejor gestión de los riesgos en el tratamiento de los datos personales. • Medir el nivel de madurez en la protección de los datos personales.
	De manera particular
	• La gestión del programa de protección de datos personales de la organización. • Disponer de un sistema de gestión que incluya las medidas de seguridad implementadas para proteger los datos personales.[28]

27 Ley General de Datos, artículo 72.

28 Artículo 34 de la Ley General de Datos y artículo 32 del Reglamento del Instituto en Materia de Protección de Datos Personales.

El SiPRODAP es un marco conceptual que provee al Instituto las bases para cumplir con los principios, deberes, derechos y demás obligaciones señaladas en la normativa aplicable.

Metodología empleada para el diseño del SiPRODAP

Un sistema de gestión con características de protección de datos personales para organismos públicos debe poseer elementos que a la postre permitan verificar y demostrar que las medidas utilizadas por los responsables son eficaces, eficientes y apropiadas de acuerdo con el riesgo inherente del dato personal, maximizando con ello la protección de los derechos y libertades de las personas titulares.

Es recomendable que el diseño de un sistema de gestión de este tipo, además de considerar la legislación nacional en la materia para el sector público, se sustente en marcos internacionales sobre privacidad, protección de datos personales y sistemas de gestión.

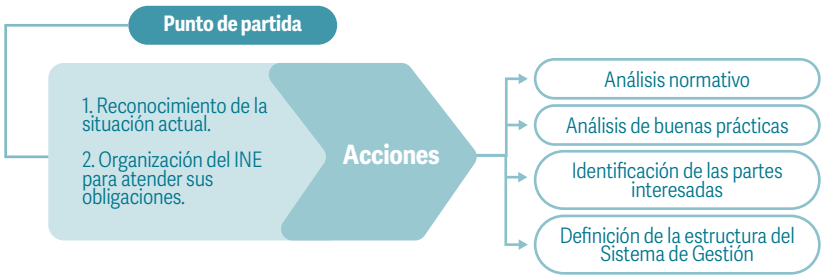
Existen marcos internacionales que homologan los principios, deberes, derechos y demás obligaciones; sin embargo, se ha de considerar que cada legislación en la materia incluye obligaciones específicas de acuerdo con el contexto económico, cultural, democrático y social.

Para demostrar el cumplimiento mediante un sistema de gestión, debido al alcance del INE, resultó imprescindible realizar un análisis que permitiera determinar la estructura, procesos, acciones y actividades de control de protección de datos personales considerando el ámbito nacional.

Para el diseño del SiPRODAP con las características mencionadas anteriormente, la Unidad de Transparencia toma como punto de partida las acciones de reconocimiento descritas en el capítulo II de esta publicación y suma cuatro acciones más, como se observa en la figura 15.

Figura 15

Acciones para diseñar el Sistema de Gestión para la Protección de Datos Personales



Fuente: Elaboración propia.

A continuación, se describe cada acción:

a. **Análisis normativo** nacional e internacional, con el fin de identificar las obligaciones de protección de datos personales que se tradujeron en controles. Este análisis consideró de manera holística los principios, deberes, derechos y demás obligaciones que los sujetos obligados deben atender conforme a la normativa y regulación nacional e internacional aplicable en la materia.

   El INE tomó para su análisis normativo el resultado de la acción 3 del reconocimiento de la situación actual, descrita en el capítulo anterior, que incluye:

   - Normativa nacional: Ley General de Datos y Lineamientos Generales de Protección de Datos Personales para el Sector Público.

- Normativa internacional: Reglamento General de Protección de Datos (RGPD) y Convenio 108.

b. **Análisis de buenas prácticas,** estándares y marcos internacionales de privacidad y protección de datos personales. Para este análisis el INE consideró el resultado de la acción 4 del reconocimiento de la situación actual (ver capítulo anterior), que incluye los estándares: ISO/IEC 27701:2019 e ISO/IEC 29100:2011. Esta acción consistió en identificar las partes interesadas en la protección de los datos personales con el objetivo de definir sus funciones y atribuciones; esto permite asignar roles y responsabilidades relacionados con la información clave de negocio en materia de protección de los datos personales. Para este análisis, el INE tomó el resultado de la acción 1 del reconocimiento de la situación actual (ver el capítulo anterior).

c. **Definición de la estructura del Sistema de Gestión** con base en lo establecido por la Organización de Estándares Internacionales (International Organization for Standardization, ISO por sus siglas en inglés), para lograr la compatibilidad con otros sistemas de gestión que se encuentren implementados en el Instituto.

   El Sistema de Gestión del Instituto está conformado por dos apartados (forjados con base en el Anexo SL[29] de las normas ISO/IEC), denominados base regulatoria y catálogo de controles:

29 La ISO, en 2012, publicó el ANEXO SL –en las Directivas ISO/IEC parte 1 (Suplemento consolidado ISO – Procedimientos específicos para ISO)–. Es una estructura de alto nivel para todos los sistemas de gestión de las normas ISO que sirve para definir estándares de sistemas de gestión.

- **Base regulatoria.** Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar el Sistema de Gestión para la Protección de Datos Personales de acuerdo con el ciclo de mejora continua o Ciclo de Deming[30] (que puede entenderse por las siglas en inglés PDCA: *plan, do, check, act* –planificar, hacer, verificar, actuar–). Es consistente con las mejores prácticas descritas en el **catálogo de controles,** descrito en los párrafos siguientes.

  La base regulatoria tiene como objetivo que el Sistema de Gestión esté **alineado y sea compatible** con las normas internacionales en la materia, simplificando posibles duplicidades con otros sistemas de gestión que se encuentren implementados; además, posee la cualidad de **poder agregar requisitos adicionales** específicos de la disciplina según sea necesario, que en este caso serían requisitos para la protección de datos personales.

  Sus características generales son:

  - **Apartado fijo:** periodos de revisión anuales o cuando exista un cambio en la normativa de protección de datos personales.

  - **Conformado por cláusulas** que sirven de guía para su implementación.

  - **Impersonal:** no hace referencia a una organización pública en particular.

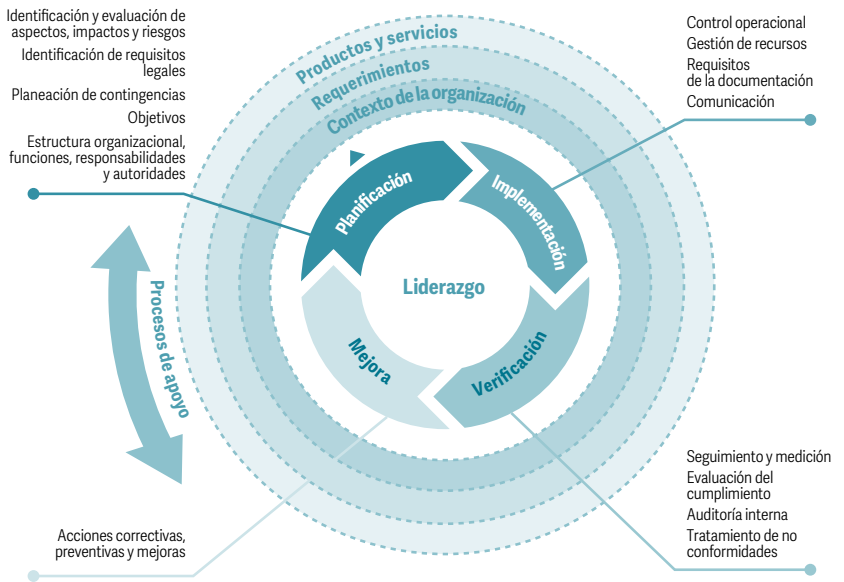
30 The Deming Institute (2023). *The PDSA Cycle.* Disponible en https://deming.org/explore/pdsa/ (fecha de consulta: 28 de julio de 2023).

- **Atemporal:** no señala plazos ni tiempos.
- **Holístico:** es aplicable a toda la organización del sujeto obligado.

El uso del Anexo SL provee a cualquier sistema de gestión un texto central idéntico, términos comunes y definiciones centrales.

Figura 16

Esquema para diseñar y operar un sistema de gestión basado en procesos



Fuente: Elaboración propia.

- **Catálogo de controles**

El objetivo del catálogo de controles es proveer a las áreas responsables, custodias y usuarias, las **actividades específicas para dar cumplimiento**

a un control, las cuales serán **posteriormente evaluadas** para medir cuantitativamente el nivel de cumplimiento.

Las actividades del control proveen las bases para que, además de **medir cuantitativamente** el nivel de cumplimiento, sea posible **conocer si el control es eficiente, efectivo y de acuerdo con el riesgo inherente al dato personal**, que son las características que permiten cumplir con el principio de responsabilidad.

Las 90 obligaciones o controles identificados en el análisis normativo se agruparon en 13 dominios, que corresponden a los procesos de protección de datos personales (tabla 4).

Tabla 4

Dominios correspondientes a los procesos de protección de datos personales

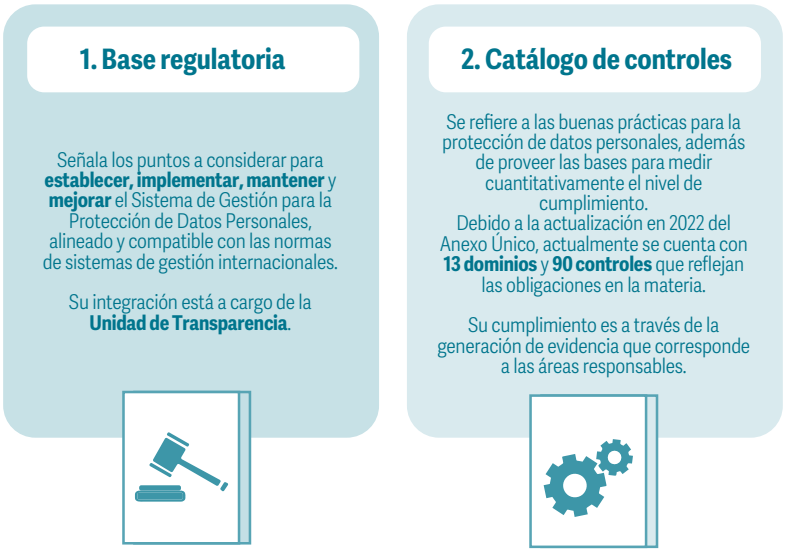
13 dominios
1. Política organizacional de protección de datos personales
2. Aspectos organizacionales de la protección de datos personales
3. Gestión de datos personales y mecanismos de transferencia y remisiones
4. Protección de datos personales en la operación
5. Protección de datos personales de los recursos humanos
6. Gestión de la seguridad en el tratamiento de los datos personales
7. Riesgos con encargados
8. Avisos de privacidad
9. Solicitudes ARCOP
10. Evaluaciones de impacto en la protección de datos personales
11. Gestión de vulneraciones
12. Monitoreo de la protección de los datos personales
13. Cumplimiento normativo

Cada dominio tiene un objetivo general y, a su vez, los controles cuentan con sus objetivos específicos. La declaración de objetivos tiene la finalidad de describir lo que se debe lograr como resultado de la implementación de controles.

Las características generales del catálogo de controles son las siguientes:

- **Apartado semifijo:** periodos de revisión semestrales o cuando exista un cambio en la normativa de protección de datos personales.
- **Conformado por controles** que podrán ser seleccionados por las unidades administrativas de la organización.
- **Impersonal:** los controles son aplicables a cualquier sujeto obligado.
- **Atemporal:** no señala plazos ni tiempos.
- **Holístico:** es aplicable a toda la organización del sujeto obligado.

Figura 17
Resumen de la estructura del SiPRODAP



Fuente: Elaboración propia.

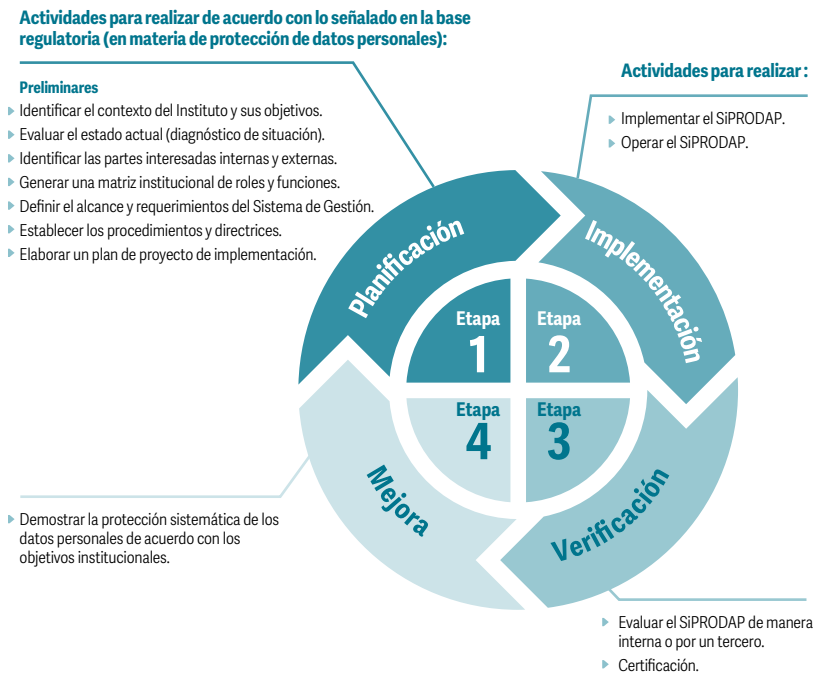
El principal diferenciador del SiPRODAP es el catálogo de controles, porque traduce los artículos de la Ley General de Datos y demás normativa aplicable en la materia que generan obligaciones al responsable en controles de protección de datos personales agrupados por procesos.

El catálogo de controles es operado mediante la PEC, que se describe más adelante. A través de esta herramienta, las áreas responsables del cumplimiento seleccionan los controles que les son aplicables y cargan la evidencia correspondiente; en caso de que el control no sea aplicable, integran la justificación apropiada.

Modelo de implementación del SiPRODAP

La implementación del SiPRODAP se lleva a cabo a través de cuatro etapas, mostradas en la figura 18.

Figura 18
Modelo de implementación del SiPRODAP



Fuente: Elaboración propia.

Cada etapa se describe a continuación de manera general:

Etapa 1. Planificación

Objetivo: Planear el proyecto de implementación del SiPRODAP mediante el análisis de la estructura organizacional, procesos, directrices, procedimientos, entre otros.

Actividades para realizar de acuerdo con lo señalado en la base regulatoria (en materia de protección de datos personales):

a. Preliminares

- Identificar el contexto del Instituto y sus objetivos.
- Evaluar el estado actual (diagnóstico de situación).
- Identificar las partes interesadas internas y externas.
- Generar una matriz institucional de roles y funciones.
- Definir el alcance y requerimientos del Sistema de Gestión.
- Establecer los procedimientos y directrices.

b. Elaborar un plan de proyecto de implementación.

Etapa 2. Implementación

Objetivo: Implementar el SiPRODAP con base en el alcance establecido en la etapa de planeación.

Actividades para realizar:

a. Implementar el Sistema de Gestión.

b. Operar el Sistema de Gestión.

Etapa 3. Verificación

Objetivo: Verificar el SiPRODAP mediante una evaluación interna o por parte de un tercero experto.

En materia de protección de datos personales, la validación se refiere a una auditoría voluntaria, según lo previsto en el artículo 151 de la Ley General de Datos, y es realizada por el INAI. Por su parte, la certificación tiene como objeto evaluar la conformidad de sistemas de gestión desarrollados e implementados por los responsables y encargados.

Etapa 4. Mejora

Objetivo: Mejorar el Sistema de Gestión para demostrar la protección sistemática de los datos personales de acuerdo con los objetivos institucionales, solicitando al órgano garante una nueva auditoría voluntaria.

Supervisión y vigilancia

El establecimiento de un sistema de supervisión y vigilancia[31] que incluya **auditorías para evaluar periódicamente la eficacia de los instrumentos de autorregulación establecidos** –como es el caso del SiPRODAP– es un mecanismo indispensable para **demostrar el cumplimiento** de las políticas de protección de datos personales.

En 2021 el INE diseñó un estándar para la ejecución de auditorías internas en materia de protección de datos personales, basado en la norma internacional ISO 19011:2018, que se erige como el instrumento para la supervisión y vigilancia del cumplimiento de los principios, deberes, derechos y obligaciones señalados en la Ley General de Datos, el cual:

- Tiene como objetivo detectar conformidades y no conformidades de cumplimiento, por medio de la

31 Ley General de Datos, artículo 30, fracción V.

revisión y comunicación de hallazgos o evidencias integrados en un documento que recogerá los resultados del proceso y servirá como referencia a auditores externos o al INAI.

- Es una actividad de revisión mediante la cual podrá verificarse el cumplimiento del SiPRODAP y su efectividad, y en caso contrario, evaluar la necesidad de una mejora o de una acción correctiva.

- Como requerimiento, propicia confianza en la sociedad satisfaciendo la necesidad de certeza requerida por las personas titulares de los datos personales en posesión del Instituto.

Su diferencia respecto de otros estándares de auditoría radica en que:

- Contempla referencias normativas nacionales específicas en materia de protección de datos personales.

- Su terminología está adaptada a la estructura institucional.

- Proporciona pautas generales y específicas para las personas servidoras públicas del INE involucradas en la planeación y ejecución de auditorías de cumplimiento de la normativa vigente en materia de protección de datos personales.

- Su contenido está orientado a la atención de la base regulatoria y el catálogo de controles del SiPRODAP, que a su vez se encuentran basados en los estándares internacionales ISO/IEC 27701:2019 e ISO/IEC 29100:2011.

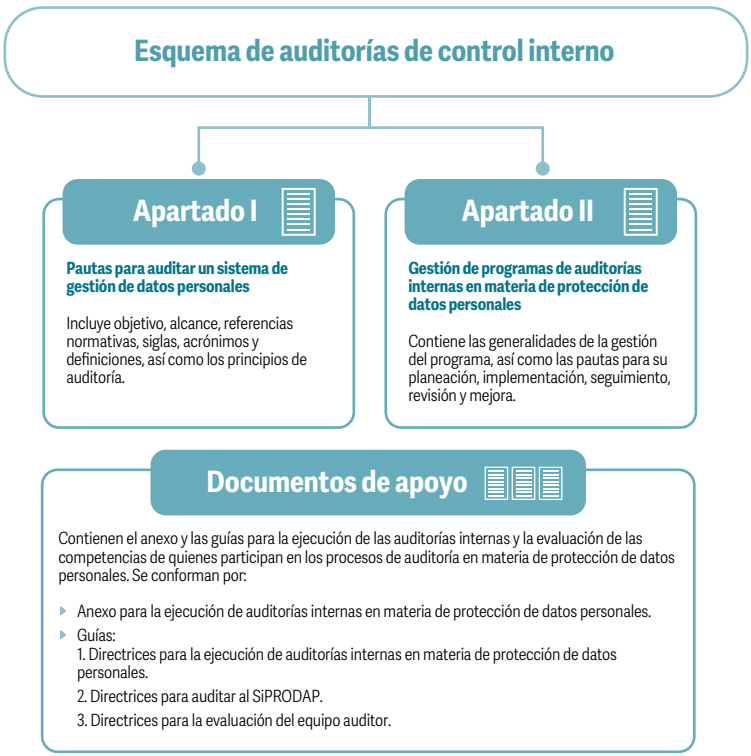
- Señala el procedimiento para la gestión de un programa de auditorías, así como la ejecución de las auditorías en sí mismas, con base en el Ciclo de Deming, PDCA o de mejora continua, el cual fue adoptado para el diseño y operación del SiPRODAP.

- Cuenta con un enfoque basado en riesgos alineado a la Metodología de Administración de Riesgos (procesos) institucional.

Disponer de un estándar provee orientación para la planeación y ejecución de las auditorías en materia de protección de datos personales del Instituto, y establece puntos de referencia conocidos por el ente auditor (rol desempeñado por la Unidad de Transparencia) y el ente auditado (rol desempeñado por las áreas responsables) para medir o valorar el nivel de cumplimiento.

Este instrumento está conformado por dos apartados y documentos de apoyo, como se observa en la figura 19.

Figura 19
Conformación del estándar de auditorías de control interno
en materia de protección de datos personales



Fuente: Elaboración propia.

Para la ejecución de estas auditorías es utilizada la PEC, que contiene un módulo específico para tal efecto.

Plataforma para la Medición, Evaluación y Monitoreo del Cumplimiento en Protección de Datos Personales

En 2019 el INE diseñó y desarrolló la PEC; se trata de una herramienta informática a través de la cual se da seguimiento a la implementación del catálogo de controles

del SiPRODAP de manera documentada, sistematizada, estructurada, repetible, eficiente y adaptada al entorno institucional. Tiene el triple propósito de ser:

1. Un repositorio de toda la evidencia de cumplimiento institucional.

2. Un registro y seguimiento de las auditorías internas en materia de protección de datos personales.

3. Un seguimiento de los riesgos de privacidad y datos personales, así como de las vulneraciones que pudieran presentarse.

Disponer de esta herramienta ofrece las siguientes ventajas:

- Gestionar la evidencia (documentos para demostrar el cumplimiento, es decir, responsabilidad demostrada).

- Establecer un proceso de verificación cuantitativo del cumplimiento de los principios, deberes, derechos y obligaciones en el tratamiento de datos personales.

- Apoyar en la identificación de las medidas de seguridad en las áreas que tratan datos personales.

- Proveer información para conocer el nivel de madurez.

- Apoyar en la supervisión y vigilancia del cumplimiento de las acciones establecidas en materia de protección de datos personales.

- Proveer información ante una auditoría de cumplimiento por parte del INAI.

- Disponer de un cuadro de mando integral que permita conocer en tiempo real el estado de cumplimiento.

La PEC ofrece información que permite conocer:

- Los procesos que tratan datos personales, sus sistemas y bases de datos.

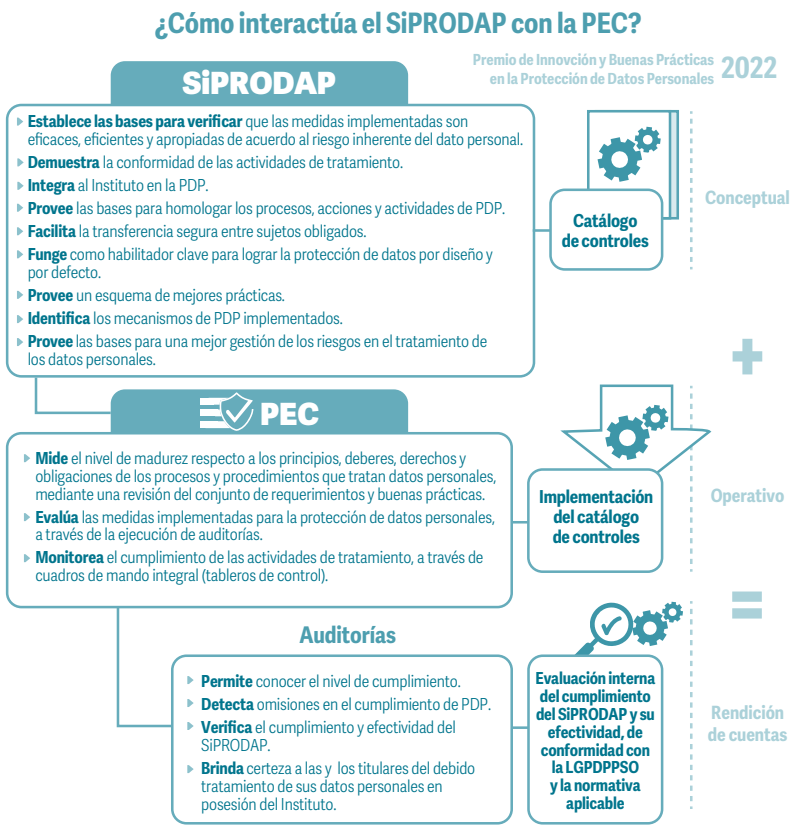
- Qué datos personales posee el Instituto y su categorización.

- Cuáles son los riesgos de privacidad derivados del tratamiento de los datos personales.

- Eventos temidos (posibles vulneraciones) y posibles impactos en la privacidad de las y los titulares.

La automatización del SiPRODAP a través de la PEC permite a cualquier organización operar la Ley General de Datos y demás normativa aplicable, así como demostrar el cumplimiento organizacional en materia de protección de datos personales –nacional e internacional– con una base conceptual sólida para lograr un nivel de madurez cuantificable con miras a la mejora continua.

Figura 20
Relación entre el SiPRODAP y la PEC



Fuente: Elaboración propia.

Capacitación y actualización

El factor y talento humanos son indispensables para que cualquier organización alcance sus objetivos. Por ello, contar con capacitación y actualización constantes en materia de protección de datos personales ofrece numerosas ventajas para una organización, entre las que destacan:

- **Apropiación del derecho a la protección de datos personales:** en un entorno en el que recopilar, procesar y almacenar datos personales es cada vez más común y crítico, es esencial que el capital humano reconozca la protección de datos personales como una materia imprescindible para las operaciones de la organización. La capacitación juega un papel fundamental debido a que proporciona al personal el conocimiento y las habilidades necesarias para comprender, adoptar, aplicar y cumplir con las políticas y prácticas relacionadas con la protección de datos de ciudadanos, ciudadanas, clientes, personal y otros individuos con quienes interactúan.

- **Cumplimiento normativo:** asegura que el personal esté al tanto de las leyes y regulaciones vigentes en cuanto a privacidad y protección de datos. Facilita el cumplimiento normativo y reduce el riesgo de multas, sanciones y daños a la reputación de la organización.

- **Conciencia de seguridad:** ayuda a crear conciencia sobre la importancia de la seguridad de los datos personales. El personal capacitado entenderá los riesgos asociados con su manejo incorrecto, como el robo de identidad, el fraude y las violaciones a la privacidad, lo que fomenta una cultura de seguridad y responsabilidad en toda la organización.

- **Mejora de las habilidades y competencias:** proporciona los conocimientos y habilidades necesarias para proteger adecuadamente los datos personales. El personal puede aprender mejores prácticas de seguridad, técnicas de cifrado, métodos de autenticación sólidos y cómo responder adecuadamente a incidentes de seguridad que afecten datos personales, lo que fortalece la capacidad para proteger este

tipo de información y minimizar el riesgo de brechas de seguridad.

- **Reducción de riesgos:** el personal capacitado es menos propenso a cometer errores que podrían comprometer la seguridad de los datos personales. La capacitación ayuda a identificar y evitar prácticas inseguras, como el uso de contraseñas débiles, el acceso no autorizado a los datos o la divulgación inadvertida de información sensible. Esto reduce los riesgos internos y externos para la organización.

- **Fortalecimiento de la confianza de las personas titulares:** la protección efectiva de los datos personales es fundamental para ganar la confianza de las personas titulares. Al demostrar un compromiso sólido con la seguridad y la privacidad de los datos, una organización puede diferenciarse de la competencia y construir una reputación positiva en términos de confidencialidad y protección de la información personal.

- **Adaptabilidad a cambios tecnológicos:** permite a la organización mantenerse al día con los cambios en los avances tecnológicos relevantes. Esto garantiza que el personal esté preparado para implementar las medidas necesarias y adaptarse a nuevas exigencias.

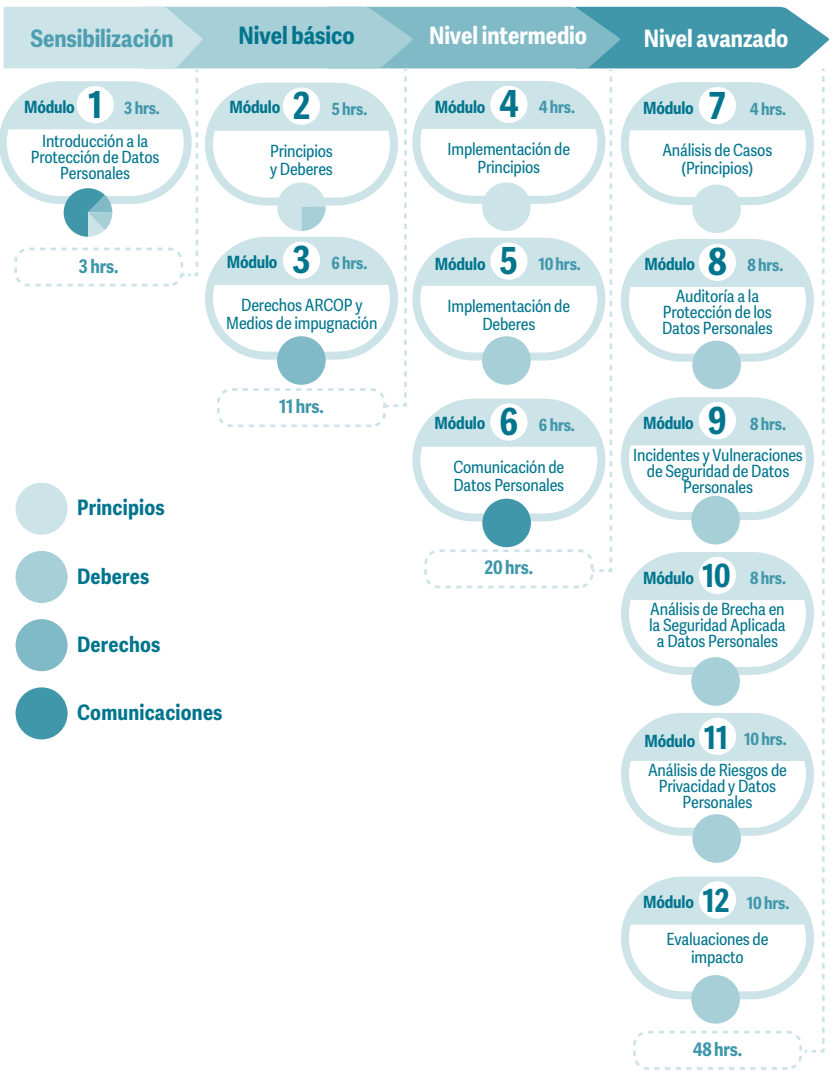
En resumen, la capacitación crea conciencia respecto de la importancia de cumplir con las regulaciones para fortalecer la confianza de las y los titulares; es una inversión valiosa para garantizar la privacidad y seguridad de los datos.

En este tenor, para llevar a cabo la capacitación especializada del personal, el INE elaboró en 2019 el curso "Protección de datos personales", compuesto por 12

módulos, cada uno con una cantidad específica de horas, como se observa en el mapa curricular que se presenta a continuación:

Figura 21

Conformación del curso "Protección de datos personales"



Fuente: Elaboración propia.

El curso tiene la característica de ser modular y disponer de una alineación:

1. **Seriada (vertical por niveles).** Para este tipo de organización es prerrequisito cursar el nivel previo al que se desee cursar:

- **Sensibilización.** Conformado por el módulo Introducción a la Protección de Datos Personales.

- **Básico.** Conformado por los módulos Principios y Deberes, Derechos ARCOP y Medios de Impugnación.

- **Intermedio.** Conformado por los módulos Implementación de Principios (taller), Implementación de Deberes (taller) y Comunicaciones de Datos Personales.

- **Avanzado:** Conformado por los módulos Análisis de Casos (Principios), Auditoría a la Protección de los Datos Personales, Incidentes y Vulneraciones de Seguridad de Datos Personales, Análisis de Brecha en la Seguridad Aplicada a Datos Personales, Análisis de Riesgos de Privacidad y Datos Personales, Evaluaciones de Impacto.

2. **Flexible (módulos separados).** Se cursan módulos separados para la capacitación en temas específicos: áreas de tecnologías de la información o jurídicas, personas responsables del tratamiento o enlace de protección de datos personales.

3. **Áreas de conocimiento.** Se lleva a cabo por ejes de formación (horizontal), a través de un seguimiento seriado de los módulos; atendiendo a sus módulos predecesores, es posible obtener la especialización en las siguientes áreas de conocimiento:

- Principios. Conformada por los módulos Introducción a la Protección de Datos Personales, Principios y Deberes, Implementación de principios (taller), Análisis de casos (Principios).

- Deberes. Conformada por los módulos Introducción a la Protección de Datos Personales, Principios y Deberes, Implementación de Deberes (taller), Auditoría a la Protección de los Datos Personales, Incidentes y Vulneraciones de Seguridad de Datos Personales, Análisis de Brecha en la Seguridad Aplicada a Datos Personales, Análisis de Riesgos de Privacidad y Datos Personales, Evaluaciones de Impacto.

- Derechos. Conformada por los módulos: Introducción a la Protección de Datos Personales y Derechos ARCOP y Medios de Impugnación.

- Comunicaciones. Conformada por los módulos Introducción a la Protección de Datos Personales y Comunicación de los Datos Personales.

El diseño en el que es presentado el curso permite:

a. **Flexibilidad:** Para aquellas personas con requerimientos muy específicos y/o que cuenten con conocimientos previos en datos personales o seguridad de la información, es posible que cursen sólo los módulos que requieran para continuar su formación.

b. **Especialización:** Es posible especializarse en materia de datos personales por área de conocimiento cursando de manera horizontal o vertical los módulos.

CAPÍTULO IV

Atención de derechos ARCOP

En este capítulo se desarrolla en lo general la forma como se atienden las solicitudes de derechos ARCOP –conjunto de potestades conferidas en la Ley General de Datos a las personas titulares en el Instituto–, así como el **recurso de revisión** previsto en la Ley General de Datos y **los que derivan de los trámites o procedimientos específicos** con los que cuenta el INE.

Atención de las solicitudes de derechos ARCOP en el INE

Cuando se recibe una solicitud de derechos ARCOP, la Unidad de Transparencia la analiza e identifica el órgano u órganos del Instituto que son competentes para atenderla. Posteriormente la solicitud es asignada, dando pie a las actividades de atención por parte de quienes fungen como Enlaces de Transparencia y Protección de Datos Personales.

La figura de Enlace de Transparencia y Protección de Datos Personales (en adelante, Enlace de Datos Personales) recae en aquella persona servidora pública que recibe y da trámite a las solicitudes de acceso a la información y de datos personales en representación de su área o de algún órgano colegiado del INE.[1]

Las actividades realizadas por las personas Enlaces para la atención de una solicitud de derechos ARCOP se describen en la tabla 1.

1 Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública, artículo 2, fracción XXVI.

Tabla 1
Actividades de las personas Enlaces de Datos Personales para atender las solicitudes ARCOP

1	**Analizan** si la solicitud está dentro de sus competencias, facultades o funciones.
2	**Identifican el área interna competente** para atender la solicitud (puede ser más de una).
3	Piden al **área interna competente atender la solicitud** de datos personales y esperan su respuesta, de conformidad con los plazos establecidos.
4	**Revisan** si el área interna **atendió de forma integral la solicitud,** es decir, si atendió todos los rubros que la integran. De no ser el caso, piden completar la atención.
5	Verifican el **sentido** con el que atenderán la solicitud de datos personales, que puede ser: • Procedencia del derecho • Inexistencia • No procedencia del derecho
6	Elaboran la **respuesta final** y **la envían a la Unidad de Transparencia.**

La Unidad de Transparencia elaboró fichas técnicas que determinan los elementos formales indispensables para cumplir con la normativa en materia de protección de datos personales, las cuales pueden ser utilizadas por las personas que fungen como Enlaces de Datos Personales como guía para la elaboración de la respuesta final, en la cual habrá de usarse un lenguaje claro e incluyente.

La notificación con la respuesta a las personas titulares es realizada por la Unidad de Transparencia o, en su caso, por el personal de las juntas locales o distritales ejecutivas a petición de esta.

Tipos de respuesta

Es importante comprender los diferentes tipos de respuestas que pueden surgir para atender una solicitud de derechos ARCOP. En la figura 1 se describen los tipos de respuesta que se pueden otorgar ante una solicitud de datos personales:

Figura 1
Solicitudes ARCOP y tipos de respuesta

Fuente: Elaboración propia.

- **Procedencia del derecho.** La solicitud resulta procedente en los términos requeridos por la persona titular de los datos personales. El área del INE a la que le fue turnada la solicitud informa a la o el solicitante, por conducto de la Unidad de Transparencia, que su solicitud ha sido atendida satisfactoriamente.

  Tratándose de solicitudes de derechos ARCOP, será necesaria la acreditación de la identidad de la persona titular de los datos, o bien de su representante, de conformidad con la tabla 2.

Tabla 2
Solicitudes ARCOP, acreditación de la identidad

Derecho	Acreditación de la identidad
Acceso, portabilidad	Al momento de la **entrega de la información.**
Rectificación, cancelación y oposición	Cuando se **notifique la procedencia del derecho.**

- **Inexistencia.** La información solicitada no obra en los archivos, registros, sistemas o expedientes del Instituto. Luego de realizar una búsqueda exhaustiva de la información solicitada, el área del INE responsable de atender la solicitud declara la inexistencia de los datos personales a través de un informe fundado y motivado, considerando las circunstancias de modo, tiempo y lugar en las que realizó la búsqueda.

- **No procedencia del derecho.** Resulta improcedente atender la solicitud en los términos requeridos por la persona titular de los datos personales. En caso de que no proceda el ejercicio de los derechos ARCOP, el área que atienda la solicitud deberá incluir en su respuesta, de manera fundada y motivada, las razones por las cuales no procede el ejercicio del derecho.

Al igual que otros derechos humanos, el derecho de protección de datos personales puede tener límites en ciertas circunstancias, pues en ocasiones resulta necesario equilibrarlo con otros derechos, y considerar los intereses legítimos de terceros o las necesidades de la sociedad en general. Algunas limitantes en la normativa mexicana al ejercicio de los derechos ARCOP son: cuestiones

de seguridad nacional, orden, seguridad y salud públicos o salvaguarda de derechos de terceros.[2]

Las causas por las que puede negarse el ejercicio de los derechos ARCOP están previstas en los artículos 55 de la Ley General de Datos y 43, fracción III, párrafo 6, del Reglamento de Datos Personales, cuando:

- La persona titular de los datos personales o su representante no haya acreditado su identidad.
- Los datos personales no se encuentren en posesión del responsable.
- Exista un impedimento legal.
- Se lesionen derechos de un tercero, es decir, que se pueda afectar los derechos de otra persona.
- El ejercicio de los derechos ARCOP pueda obstaculizar procesos judiciales o tareas de una autoridad administrativa.
- Exista una resolución de autoridad competente que impida el acceso a los datos personales o no permita la rectificación, cancelación u oposición de estos.
- El titular haya solicitado previamente la cancelación u oposición de sus datos personales.
- El responsable al que se le solicite el ejercicio de los derechos ARCOP no sea competente para llevarlo a cabo.

2 Ley General de Datos, artículo 6, párrafo segundo.

- Los datos sean necesarios para proteger intereses jurídicamente tutelados de la persona titular o para dar cumplimiento a obligaciones legalmente adquiridas por esta.

- En función de sus atribuciones legales, el uso cotidiano, resguardo y manejo de los datos sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano.

Estas limitaciones deben ser interpretadas y aplicadas de manera restrictiva para garantizar la protección de los derechos fundamentales de las personas.

Toda declaración de no procedencia realizada por las áreas del INE deberá ser analizada por el Comité de Transparencia, órgano colegiado que tiene la facultad de confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCOP.

Plazos internos para atender solicitudes de derechos ARCOP

El INE ha desarrollado un procedimiento interno de atención de solicitudes de datos personales, el cual prevé los plazos reglamentarios para tal efecto. Conforme a ese procedimiento, las áreas responsables del Instituto tienen tiempos determinados en función del tipo de respuesta que han de otorgar (tabla 3).

Tabla 3

Plazos determinados en función del tipo de respuesta

Tipo de respuesta	Plazo (días hábiles)
Procedencia del derecho	**8 días**
Ampliación del plazo. El plazo se puede ampliar una sola vez cuando así lo justifiquen las circunstancias.	**+5 días**
Incompetencia	**2 días**
Prevención. En caso de que la solicitud no cuente con los elementos necesarios para dar atención.	**2 días**
No procedencia del derecho	**5 días**
Inexistencia	**5 días**

Figura 2

Plazos determinados en función del tipo de respuesta

Fuente: Elaboración propia.

Flujogramas del proceso de atención a solicitudes de derechos ARCOP

Para mejor comprensión, se adjuntan los flujogramas con el proceso de atención a solicitudes de derechos ARCOP (ver Anexo 1).

Recurso de revisión de solicitudes de derechos ARCOP

Presentación de un recurso de revisión

Cuando la persona titular o interesada no está conforme con la respuesta, atención, modalidad o cualquiera de las causas establecidas en la Ley General de Datos, puede presentar un recurso de revisión por sí misma o a través de su representante, contando para ello con 15 días hábiles posteriores a la notificación de la respuesta.

El recurso de revisión podrá presentarse ante:

- El INAI.
- La Unidad de Transparencia del INE.

En caso de que sea presentando ante la Unidad de Transparencia, esta deberá remitirlo al INAI para su trámite correspondiente.

La Ley General de Datos prevé dos procedimientos para el ejercicio de los derechos ARCOP:

1. El procedimiento general, regulado en la propia Ley General de Datos.
2. El trámite específico con el que cuenten los sujetos obligados.

En consecuencia, el medio de impugnación que corresponde al procedimiento general es el recurso de revisión ante el INAI y el relativo al trámite especifico será aquel que se establezca en los instrumentos jurídicos aprobados por el INE o adoptados por sus órganos responsables.

Respecto de los datos personales que forman parte del Padrón Electoral, la Dirección Ejecutiva del Registro Federal de Electores (DERFE) cuenta con un trámite específico para el ejercicio de los derechos ARCOP, establecido en los "Lineamientos del Instituto Nacional Electoral para el acceso, rectificación, cancelación y oposición de datos personales que forman parte del Padrón Electoral" (Lineamientos ARCO del Padrón Electoral), cuyo medio de impugnación es el juicio para la protección de los derechos político-electorales del ciudadano.

Autoridad competente para resolver

El pleno del INAI es la autoridad encargada de resolver los recursos de revisión interpuestos en contra de las respuestas proporcionadas por el INE a las solicitudes para el ejercicio de los derechos ARCOP, mientras que la Unidad de Transparencia es la encargada de la gestión interna del recurso de revisión, por lo que puede requerir informes a los diversos órganos del Instituto para ese propósito.

En el caso de los medios de impugnación presentados en contra de solicitudes atendidas de conformidad con los Lineamientos ARCO del Padrón Electoral, las instancias competentes para conocer son:

- La Sala Superior del Tribunal Electoral.

- La Sala Regional del Tribunal Electoral que ejerza jurisdicción en el ámbito territorial en que se haya cometido la violación reclamada, en única instancia.

Flujograma del recurso de revisión de solicitudes de derechos ARCOP

Se adjunta el flujograma con el proceso de gestión del recurso de revisión respecto de las solicitudes de derechos ARCOP (ver Anexo 2).

CAPÍTULO V

Consecuencias del incumplimiento

A través de los datos personales es posible conocer aspectos sobre la vida privada de las personas; por lo tanto, su protección va más allá del mero cumplimiento de requisitos legales. Es fundamental recordar que la protección de este tipo de información es un derecho humano que se centra en el individuo, no en las organizaciones.

En ese sentido, si bien el incumplimiento de la normativa aplicable en la materia deriva en consecuencias para las organizaciones (como sanciones legales, multas y daños a la reputación de una organización), el punto crucial a considerar es la afectación que tal incumplimiento podría generar de manera directa a las personas.

Este capítulo se enfocará en las consecuencias del incumplimiento para:

a. Las personas, que derivan en **impactos a su privacidad**.

b. Las organizaciones, que derivan en **medidas de apremio y sanciones**, entre otras.

Figura 1

Ejemplos de consecuencias del incumplimiento

Fuente: Elaboración propia con base en S. Joyee y D. Le Métayer (2016). *Privacy Risk Analysis*. Morgan & Claypool Publishers. Edición de Kindle.

Impactos a la privacidad

El impacto a la privacidad se refiere a la magnitud del daño que se puede esperar como resultado de la divulgación, modificación, alteración, destrucción o copia no autorizada de los datos personales, así como de su pérdida, robo, extravío o daño e, incluso, de la indisponibilidad de un sistema.[1]

1 M. A. Sánchez Barroso (2017). *Gestión Proactiva de la Protección de Datos: Cómo implementar Privacidad por Diseño y Evaluación de Impacto en la Privacidad en la empresa*. SSA-ASESORES.

Los daños a la privacidad se describen a continuación:[2]

- **Pérdida de autodeterminación.** La pérdida de la soberanía personal o la capacidad de una persona para tomar decisiones libremente. Se compone de:

    - **Pérdida de autonomía.** Incluye cambios innecesarios en el comportamiento, incluidas las restricciones autoimpuestas a la libertad de expresión o reunión.

    - **Exclusión.** Es la falta de conocimiento o acceso a los datos personales. Cuando las personas no saben qué información recopila o puede utilizar una organización, o cuando no tienen la oportunidad de participar en la toma de decisiones relacionadas con sus datos, disminuye la responsabilidad en cuanto a si la información es apropiada para que la organización la posea o si será utilizada de manera justa o equitativa.

    - **Pérdida de libertad.** Exposición indebida al arresto o detención. Incluso en sociedades democráticas, la información incompleta o inexacta puede conducir al arresto, y su exposición o uso inadecuado puede contribuir a situaciones de abuso del poder gubernamental. En sociedades no democráticas pueden surgir más situaciones que amenazan la vida.

    - **Daño físico real a una persona.** Si los datos de una persona se usan para ubicar y obtener

2 W. Stallings (2019). *Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices.* Pearson Education, p. 357.

acceso a los sistemas ciberfísicos[3] con los que interactúa, los daños pueden incluir, por ejemplo, la generación de lecturas imprecisas de un sensor de dispositivo médico o el mal funcionamiento de los controles críticos del automóvil inteligente, como el frenado y la aceleración.

- **Discriminación.** Trato injusto o desigual de las personas. Se compone por:

    - **Estigmatización.** Una situación en la que los datos personales están vinculados a una identidad real de tal manera que crea un estigma que puede causar vergüenza, angustia emocional o discriminación. Por ejemplo, la información confidencial –como datos de salud o antecedentes penales– o simplemente relacionada con ciertos servicios o programas –como acceder a cupones de alimentos o beneficios de desempleo– puede generar inferencias con respecto a las personas titulares.

    - **Desequilibrio de poder.** Poseer datos personales puede generar un desequilibrio, aprovechamiento o abuso de poder, por ejemplo, la recopilación de atributos, el análisis del comportamiento o las transacciones de las personas pueden dar lugar a diversas formas de discriminación.

3 "Un Sistema Ciber-Físico o CPS, siglas en inglés de Cyber-Physical System, es todo aquel dispositivo que integra capacidades de computación, almacenamiento y comunicación para controlar e interactuar con un proceso físico". Sistemas Ciber-Físicos para el control de procesos de producción. *Pódcast Industria 4.0.* Disponible en https://www.podcastindustria40.com/sistemas-ciber-fisicos/ (fecha de consulta: 28 de junio de 2023).

- **Pérdida de confianza.** El incumplimiento de expectativas o acuerdos implícitos o explícitos sobre el manejo de los datos personales, por ejemplo, la divulgación de datos personales o sensibles a una organización es un acto que va acompañado de una serie de expectativas sobre cómo se utilizan, protegen, transmiten y comparten esos datos, lo que puede generar que las personas se muestren renuentes a realizar más transacciones con esa organización.

- **Pérdida económica.** Pérdidas financieras directas para el o la titular como resultado del robo de identidad, así como el no recibir el valor justo en una transacción que involucre datos personales.

En resumen, el incumplimiento puede afectar a las personas titulares, a un grupo de titulares o a la sociedad en general, produciendo efectos negativos en las personas en ámbitos como el bienestar físico, mental o financiero, la reputación, dignidad, libertad, aceptación en la sociedad, autorrealización, vida doméstica, libertad de expresión o cualquier otro derecho fundamental.

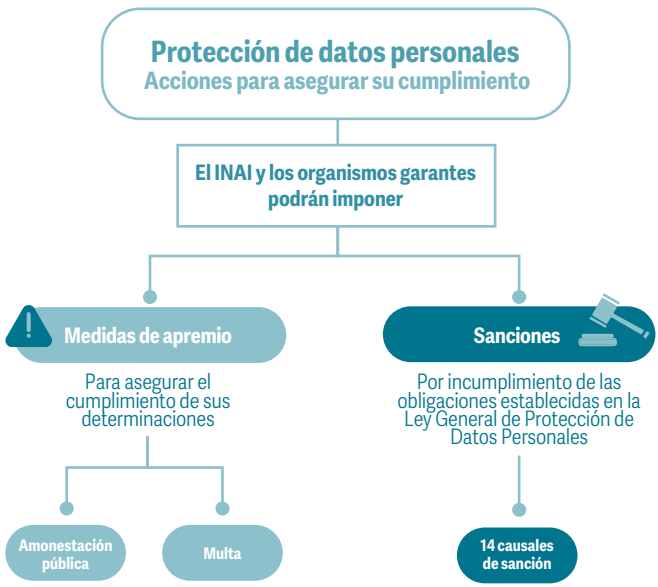
Medidas de apremio y sanciones

Un aspecto destacado de la Ley General de Datos es el conjunto de facultades y atribuciones otorgadas a distintas autoridades para establecer medidas de apremio y sanciones de carácter administrativo derivadas del incumplimiento de las obligaciones en materia de protección de datos personales.

Como lo señala Olivia A. Mendoza, esto resulta trascendental para la efectiva protección de la información personal, ya que el incumplimiento de las disposiciones en la

materia podría traer como consecuencia la imposición de sanciones económicas que deberán ser pagadas con los recursos propios del infractor.[4]

Figura 2
Acciones para asegurar el cumplimiento de las disposiciones en materia de protección de datos



Fuente: Elaboración propia.

Además de las medidas de apremio y las sanciones, destaca el daño reputacional entre las consecuencias del incumplimiento para las organizaciones, el cual se define, de acuerdo con Alejandro Riveros, como "la posibilidad de pérdida o merma en la reputación de una organización de forma que afecte negativamente a la percepción que el entorno social tiene sobre la misma. Este daño

4 M. S. Maqueo Ramírez, *op. cit.*, p. 425.

reputacional puede producir una pérdida directa o indirecta del valor de una compañía".[5]

Si bien es un riesgo difícil de medir, los efectos del daño reputacional son tangibles e impactan en toda la organización. La principal consecuencia de este tipo de daño radica en la reparación, debido a que en la gran mayoría de los casos suele estar asociada a una gran difusión social y mediática.[6]

Medidas de apremio

Las medidas de apremio son **facultades de carácter coercitivo** otorgadas por la ley a la autoridad competente con el propósito de garantizar el cumplimiento eficaz e inmediato de sus determinaciones, dentro o fuera de un procedimiento administrativo.[7]

En materia de protección de datos personales, el INAI y los órganos garantes locales serán los encargados de aplicar las medidas de apremio correspondientes para garantizar el cumplimiento de sus determinaciones, las cuales consisten en:

1. Amonestación pública ejecutada por el superior jerárquico inmediato del infractor con el que se relacione.[8]

5 A. Riveros (16 de junio de 2021). Cómo gestionar y mitigar el riesgo reputacional en las organizaciones. *Ealde Business School.* Disponible en https://www.ealde.es/gestion-de-riesgos-reputacional/ (fecha de consulta: 28 de julio de 2023).

6 Grupo ESG Innova (s.f.). La gestión de riesgos reputacionales en las organizaciones. *Grupo ESG Innova*. Disponible en https://www.isotools.us/2019/08/22/la-gestion-de-riesgos-reputacionales-en-las-organizaciones/ (fecha de consulta: 28 de julio de 2023).

7 INAI (2019), *op. cit.*, p. 549.

8 Ley General de Datos, artículo 153.

2. Multa[9] que se hará efectiva a través del Servicio de Administración Tributaria o las secretarías de finanzas de las entidades federativas, según corresponda.

Las medidas de apremio se califican de acuerdo con:[10]

1. La gravedad de la falta del responsable, determinada por elementos tales como el daño causado, los indicios de intencionalidad, la duración del incumplimiento de las determinaciones del INAI o los organismos garantes y la afectación al ejercicio de sus atribuciones.

2. La condición económica del infractor.

3. La reincidencia.

Sanciones

Según Émile Durkheim, una medida tiene el propósito de imponer una consecuencia negativa al infractor, con el fin de corregir su conducta, promover el cumplimiento de las normas y salvaguardar el orden, la seguridad o los derechos de las personas.

En materia de protección de datos personales, la imposición de sanciones es de carácter administrativo y **deriva del incumplimiento** de las siguientes obligaciones:

- **Actuar con negligencia, dolo o mala fe** durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCOP.

9 Equivalente a la cantidad de 150 hasta 1,500 veces el valor diario de la unidad de medida y actualización.
10 Ley General de Datos, artículo 157.

- **Incumplir los plazos de atención** previstos en la Ley General de Datos para responder las solicitudes para el ejercicio de los derechos ARCOP o para hacer efectivo el derecho de que se trate.

- **Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir** o **inutilizar, total o parcialmente y de manera indebida, datos personales** que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.

- **Dar tratamiento** a los datos personales **de manera intencional** en contravención de los principios y deberes establecidos en la Ley General de Datos.

- **No contar con el aviso de privacidad** u omitir alguno de sus elementos.[11]

- **Clasificar como confidenciales, con dolo o negligencia, datos personales,** sin que se cumplan las características señaladas en las leyes que resulten aplicables.[12]

- **Incumplir el deber de confidencialidad.**[13]

- **No establecer las medidas de seguridad.**[14]

11 Artículo 27 de la Ley General de Datos, según sea el caso, y demás disposiciones que resulten aplicables en la materia.

12 La sanción sólo procederá cuando exista una resolución previa que haya quedado firme, respecto del criterio de clasificación de los datos personales.

13 Establecido en el artículo 42 de la Ley General de Datos.

14 En los términos que establecen los artículos 31, 32 y 33 de la Ley General de Datos.

- **Vulnerar** los datos personales por la falta de implementación de medidas de seguridad.[15]

- **Llevar a cabo la transferencia de datos personales** en contravención a lo previsto en la Ley General de Datos.

- **Obstruir los actos de verificación** de la autoridad.

- **Crear bases de datos personales** en contravención a lo dispuesto por el artículo 5 de la Ley General de Datos.

- **No acatar las resoluciones** emitidas por el Instituto y los organismos garantes.

- **Omitir la entrega del informe anual** y demás informes, o entregarlos de manera extemporánea.[16]

15 Según los artículos 31, 32 y 33 de la Ley General de Datos.

16 Artículo 44, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública.

Glosario de términos

Activo:[1] cualquier cosa que tenga valor para una organización. En el contexto de la seguridad de la información, se pueden distinguir dos tipos de activos:

- Primarios: información, procesos de negocio y actividades.

- De apoyo o secundarios (de los que dependen los activos primarios): *hardware, software*, red, instalaciones, personal, entre otros.

Alta dirección: persona o grupo de personas que dirige y controla una organización al más alto nivel. Tiene el poder para delegar autoridad y proporcionar recursos dentro de la organización. Referente a los sistemas de gestión, si su alcance comprende sólo una parte de la organización, entonces la alta dirección se refiere a quienes dirigen y controlan esa parte.[2]

Áreas: instancias de los sujetos obligados, previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento y ser responsables o encargadas de los datos personales.

Base de datos: conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

1 *ISO/IEC 27002..., op. cit.*
2 ISO (2015). *ISO 9000:2015 Quality management systems — Fundamentals and vocabulary.* Disponible en https://www.iso.org/standard/45481.html (fecha de consulta: 28 de julio de 2023).

Ciclo Deming o de mejora continua: conocido también como el ciclo PDCA (*plan, do, check, act*). Metodología que describe las etapas para la implementación de un sistema de gestión, producto o servicio.[3]

Contexto de la organización: combinación de cuestiones internas y externas que puede tener un efecto en el enfoque de la organización para el desarrollo y logro de sus objetivos. Los objetivos de la organización pueden estar relacionados con sus productos y servicios, sus inversiones y su comportamiento hacia sus partes interesadas. El concepto de contexto de la organización aplica tanto para organizaciones sin fines de lucro o de servicio público como para aquellas que buscan beneficios con frecuencia.[4]

Control: acciones de protección de datos personales resultado de las obligaciones de la normativa en la materia. Es una medida que modifica el riesgo del dato personal.[5]

Custodio: área que implementa las medidas de seguridad de la información y asesora a los propietarios sobre los mecanismos de seguridad existentes.

DOF: *Diario Oficial de la Federación.*

Dominio: procesos que realiza una organización para la protección de datos personales.

3 The Deming Institute, *op. cit*.
4 ISO (2015), *op. cit*.
5 ISO (2018) *ISO/IEC 27000:2018 Information Technology — Security Techniques — Information security system — Overview and vocabulary.* Disponible en https://www.iso.org/standard/73906.html (fecha de consulta: 15 de septiembre de 2023).

Encargado: la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o con otras trate datos personales a nombre y por cuenta de esta. También tendrá el carácter de encargado quien preste el servicio de cómputo en la nube.

Ley Federal de Datos o LFPDPPP: Ley Federal de Protección de Datos Personales en Posesión de Particulares.

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

Marco de referencia o *framework*: conjunto estandarizado de conceptos, prácticas y criterios de un tipo de problemática particular que sirve como referencia para enfrentar y resolver nuevos problemas de índole similar.[6]

Organización: persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos. El concepto de organización incluye, entre otros, a un trabajador independiente, compañía, corporación, firma, empresa, autoridad, sociedad, asociación, organización benéfica o institución, o una parte o combinación de estas, ya sea que estén constituidas o no, sean públicas o privadas.[7]

Partes interesadas, grupos de interés o *stakeholders*: persona u organización que puede afectar, ser afectada

6 ICTEA (2023). ¿Qué es una Infraestructura Digital o 'Framework'? *Base de Conocimientos*. Disponible en https://www.ictea.com/cs/index.php?rp=%2Fknowledgebase%2F8991%2FQue-es-una-Infraestructura-Digital-o-andsharp039Frameworkandsharp039.html (fecha de consulta: 28 de julio de 2023).

7 ISO (2015), *op. cit*.

o se percibe a sí misma como afectada por una decisión o actividad.[8]

PEC: Plataforma para la Medición, Evaluación y Monitoreo del Cumplimiento en Protección de Datos Personales.

Proceso: conjunto de actividades mutuamente relacionadas o que interactúan, y que utilizan las entradas para proporcionar un resultado previsto.

Proceso de negocio: procesos que prescriben la forma en la que se utilizan los recursos –datos, capital, personas– de una organización para lograr sus objetivos de negocio.

PRONADATOS: Programa Nacional de Protección de Datos Personales.[9] Se trata de una política pública de protección de datos personales en el país para el sector público.

Propietario: el área que toma decisiones respecto del tratamiento de los datos personales; es el responsable final de la protección y el uso de los datos.

SiPRODAP: Sistema de Gestión para la Protección de Datos Personales.

Usuario: persona o área autorizada para acceder a los datos; son quienes utilizan la información.

8 Universidad Santiago de Cali (s.f.). *Términos y definiciones*. Disponible en https://www.usc.edu.co/index.php/gestion-de-calidad/terminos-y-definiciones (fecha de consulta: 28 de julio de 2023).

9 El cual puede consultarse en: https://dof.gob.mx/nota_detalle.php?codigo=5511542&fecha=26/01/2018#gsc.tab=0

Referencias

Agencia Española de Protección de Datos (2009). *Estándares internacionales sobre protección de datos personales y privacidad: Resolución de Madrid*. Disponible en https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf (fecha de consulta: 4 de julio de 2023).

Cámara de Diputados del H. Congreso de la Unión (26 de enero de 2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Disponible en https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf (fecha de consulta: 4 de julio de 2023).

Consejo de Europa (28 de enero de 1981). Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Disponible en https://inicio.inai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf (fecha de consulta: 4 de julio de 2023).

Crompton, M. y Trovato, M. (2018). *The New Governance of Data and Privacy: Moving beyond Compliance to Performance*. Australian Institute of Company Directors. Edición de Kindle.

Giraldo Giraldo, R. A. (2017). *Mejoramiento del proceso de compras de la Constructora SSINCO S.A.S*. Disponible en https://repositorio.ucm.edu.co/bitstream/10839/1885/1/Ricardo%20Alberto%20Giraldo.pdf (fecha de consulta: 28 de julio de 2023).

Grupo ESG Innova (s.f.). *La gestión de riesgos reputacionales en las organizaciones.* Grupo ESG Innova. Disponible en https://www.isotools.us/2019/08/22/la-gestion-de-riesgos-reputacionales-en-las-organizaciones/ (fecha de consulta: 28 de julio de 2023).

IBS americas (1° de junio de 2023). "Factor humano en los proyectos: Ventajas y desafíos". Disponible en https://blogibsamericas.com/es/2023/06/01/factor-humano-en-los-proyectos-ventajas-y-desafios-es/ (fecha de consulta: 24 de julio de 2023).

ICTEA (2023). ¿Qué es una Infraestructura Digital o 'Framework'? *Base de Conocimientos.* Disponible en https://www.ictea.com/cs/index.php?rp=%2Fknowledgebase%2F8991%2FQue-es-una-Infraestructura-Digital-o-andsharp039Framework andsharp039.html (fecha de consulta: 28 de julio de 2023).

INAI (s.f.). *Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.* Disponible en https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/_GuiaPrincipiosDeberes.pdf (fecha de consulta: 27 de julio de 2023).

INAI (s.f.). *Guía para titulares de los datos personales* (vol. 3). México: INAI. Disponible en https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/Guia%20Titulares-03_PDF.pdf (fecha de consulta: 4 de julio de 2023).

INAI (junio de 2015). *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales.* Disponible en https://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf (fecha de consulta: 17 de agosto de 2023).

INAI (26 de enero de 2018). "Acuerdo mediante el cual se aprueban, los lineamientos generales de protección de datos personales para el sector público". *Diario Oficial de la Federación.* Disponible en https://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf (fecha de consulta: 5 de julio de 2023).

INAI (2019). *Diccionario de Protección de Datos Personales, conceptos fundamentales.* México: INAI. Disponible en https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf (fecha de consulta: 4 de julio de 2023).

INE (s.f.). "Lineamientos del Instituto Nacional Electoral para el acceso, rectificación, cancelación y oposición de datos personales que forman parte del Padrón Electoral". Disponible en https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/97149/CGor201807-18-ap-9-a1.pdf (fecha de consulta: 6 de julio de 2023).

INE (s.f.). *Modelo de Gestión por Procesos del Instituto Nacional Electoral v.2.* Disponible en https://sidj.ine.mx/restWSsidj-nc/app/doc/998/20/1 (fecha de consulta: 5 de julio de 2023).

INE (s.f.). *Procedimiento para elaborar el Documento de Seguridad.* Disponible en https://ine.mx/wp-content/uploads/2021/05/SSPPDP-Proce-elaborar-DocSeg.pdf (fecha de consulta: 6 de julio de 2023).

INE (marzo de 2018). *Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales.* Disponible en https://sidj.ine.mx/restWSsidj-nc/app/doc/798/20/1/ (fecha de consulta: 6 de julio de 2023).

INE (8 de noviembre de 2018). *Programa para la Protección de Datos Personales del Instituto Nacional Electoral.* Disponible en https://sidj.ine.mx/restWSsidj-nc/app/doc/880/20/1 (fecha de consulta: 5 de julio de 2023).

INE (2020). *Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública.* Disponible en https://sidj.ine.mx/restWSsidj-nc/app/doc/30/20/1 (fecha de consulta: 13 de abril de 2023).

INE (26 de junio de 2022). *Apartado virtual "Protección de Datos Personales".* Disponible en https://www.ine.mx/transparencia/protecciondp/ (fecha de consulta: 17 de agosto de 2023).

Information Commissioner's Office (s.f.). *Accountability Framework.* Disponible en https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/ (fecha de consulta: 5 de julio de 2023).

ISACA (2017). *Implementing a Privacy Protection Program: Using COBIT 5 Enablers with the ISACA Privacy Principles.* ISACA.

ISACA (2018). *ISACA Privacy Principles and Program Management Guide.*

ISO (s.f.). *Management system standards.* Disponible en https://www.iso.org/management-system-standards.html (fecha de consulta: 6 de julio de 2023).

ISO (2011). *ISO/IEC 29100:2011. Information technology — Security techniques — Privacy framework.* Disponible en https://www.iso.org/standard/45123.html (fecha de consulta: 5 de julio de 2023).

ISO (2013). *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls.* Disponible en https://www.iso.org/standard/54533.html (fecha de consulta: 5 de julio de 2023).

ISO (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.*

ISO (2015). *ISO 9000:2015 Quality management systems* — Fundamentals and vocabulary. Disponible en https://www.iso.org/standard/45481.html (fecha de consulta: 28 de julio de 2023).

ISO (2016). *ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation.* Disponible en https://www.iso.org/

standard/64120.html (fecha de consulta: 5 de julio de 2023).

ISO (2017). *ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment.* Disponible en https://www.iso.org/standard/62289.html (fecha de consulta: 5 de julio de 2023).

ISO (2017). *ISO/IEC 29151:2017 Information technology — Security techniques — Code of practice for personally identifiable information protection.* Disponible en https://www.iso.org/standard/62726.html (fecha de consulta: 5 de julio de 2023).

ISO (2018). *ISO 31000:2018 Risk management — Guidelines.* Disponible en https://www.iso.org/standard/65694.html (fecha de consulta: 5 de julio de 2023).

ISO (2018). *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management.* Disponible en https://www.iso.org/standard/75281.html (fecha de consulta: 5 de julio de 2023).

ISO (2018) *ISO/IEC 27000:2018 Information Technology — Security Techniques — Information security system — Overview and vocabulary.* Disponible en https://www.iso.org/standard/73906.html (fecha de consulta: 15 de septiembre de 2023).

ISO (2018). *ISO/IEC 19011:2018 Guidelines for auditing management systems.* Disponible en https://www.iso.org/standard/70017.html (fecha de consulta: 15 de septiembre de 2023).

ISO (2019). *ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.* Disponible en https://www.iso.org/standard/76559.html (fecha de consulta: 5 de julio de 2023).

ISO (2019). *ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.* Disponible en https://www.iso.org/standard/71670.html (fecha de consulta: 5 de julio de 2023).

ISO (2020). *ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing.* Disponible en https://www.iso.org/standard/77802.html (fecha de consulta: 5 de julio de 2023).

ISO (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.* Disponible en https://www.iso.org/standard/75652.html (fecha de consulta: 15 de septiembre de 2023.

Joyee, S. y Le Métayer, D. (2016). *Privacy Risk Analysis.* Morgan & Claypool Publishers. Edición de Kindle.

Maqueo Ramírez, M. S. (coord.) (2018). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, comentada.* México: INAI.

Maqueo Ramírez, M. S. y Barzizza Vignau, A. (2020). *Democracia, privacidad y protección de datos personales.*

México: INE (Cuadernos de Divulgación de la Cultura Democrática, núm. 41). Disponible en https://www.ine.mx/wp-content/uploads/2021/02/CDCD-41.pdf (fecha de consulta: 4 de julio de 2023).

NIST (s.f.). *NIST Privacy Framework.* Disponible en https://www.nist.gov/privacy-framework (fecha de consulta: 6 de julio de 2023).

NIST (18 de septiembre de 2012). *NIST 800-30 Revision 1. Guide for Conducting.* Disponible en https://csrc.nist.gov/news/2012/nist-special-publication-800-30-revision-1 (fecha de consulta: 6 de julio de 2023).

NIST (enero de 2017). *NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal System.* Disponible en https://csrc.nist.gov/publications/detail/nistir/8062/final (fecha de consulta: 6 de julio de 2023).

NIST (septiembre de 2020). *NISTIR 8062 Security and Privacy Controls for Information Systems and Organizations.* Disponible en https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (fecha de consulta: 6 de julio de 2023).

OCDE (23 de septiembre de 1980). *Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales.* Disponible en http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf (fecha de consulta: 4 de julio de 2023).

ONU (14 de diciembre de 1990). Directrices para la regulación de los archivos de datos personales informatizados. Disponible en https://archivos.juridicas.

unam.mx/www/bjv/libros/12/5669/17.pdf (fecha de consulta: 4 de julio de 2023).

Red Iberoamericana de Protección de Datos (2007). Directrices para la armonización de la protección de datos en la Comunidad Iberoamericana. Disponible en https://archivos.juridicas.unam.mx/www/bjv/libros/12/5669/22.pdf (fecha de consulta: 4 de julio de 2023).

Red Iberoamericana de Protección de Datos (20 de junio de 2017). Estándares de protección de datos personales para los Estados iberoamericanos. Disponible en https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf (fecha de consulta: 4 de julio de 2023).

Riveros, A. (16 de junio de 2021). Cómo gestionar y mitigar el riesgo reputacional en las organizaciones. *Ealde Business School.* Disponible en https://www.ealde.es/gestion-de-riesgos-reputacional/ (fecha de consulta: 28 de julio de 2023).

Sánchez Barroso, M. A. (2017). *Gestión Proactiva de la Protección de Datos: Cómo implementar Privacidad por Diseño y Evaluación de Impacto en la Privacidad en la empresa.* SSA-ASESORES.

Sistemas Ciber-Físicos para el control de procesos de producción. *Pódcast Industria 4.0.* Disponible en https://www.podcastindustria40.com/sistemas-ciber-fisicos/ (fecha de consulta: 28 de junio de 2023).

Stallings, W. (2019). *Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats,*

Technology, and Regulations Based on Standards and Best Practices. Pearson Education.

The Deming Institute (2023). *The PDSA Cycle*. Disponible en https://deming.org/explore/pdsa/ (fecha de consulta: 28 de julio de 2023).

Universidad Santiago de Cali (s.f.). *Términos y definiciones*. Disponible en https://www.usc.edu.co/index.php/gestion-de-calidad/terminos-y-definiciones (fecha de consulta: 28 de julio de 2023).

Glosario de siglas

CT o Comité: Comité de Transparencia del INE.

ETyPDP: Enlace de Transparencia y Protección de Datos Personales.

INE o Instituto: Instituto Nacional Electoral.

JDE: Junta Distrital Ejecutiva.

JLE: Junta Local Ejecutiva.

PNT: Plataforma Nacional de Transparencia, a la cual hace referencia el artículo 49 de la Ley General de Datos.

RA: Requerimiento de Aclaración, medio utilizado por la Secretaría Técnica del CT para solicitar a las áreas del INE que subsanen aspectos de forma en las respuestas que han dado a solicitudes de derechos ARCOP.

RIA: Requerimiento Intermedio de Aclaración, medio utilizado por el INAI para solicitar mayores insumos respecto a informes presentados por el INE en la atención de recursos de revisión en materia de datos personales.

RII: Requerimiento Intermedio de Información, medio utilizado por la Secretaría Técnica del CT para solicitar a las áreas del INE que subsanen aspectos de fondo en las respuestas que han dado a solicitudes de derechos ARCOP.

RRD: Recurso de revisión en materia de datos personales.

Sistema INFOMEX-INE: Sistema electrónico autorizado por el INE para tramitar las solicitudes de acceso a la información y de datos personales al interior del propio Instituto.

Solicitudes de derechos ARCOP: Solicitudes de acceso, rectificación, cancelación, oposición y portabilidad de datos personales.

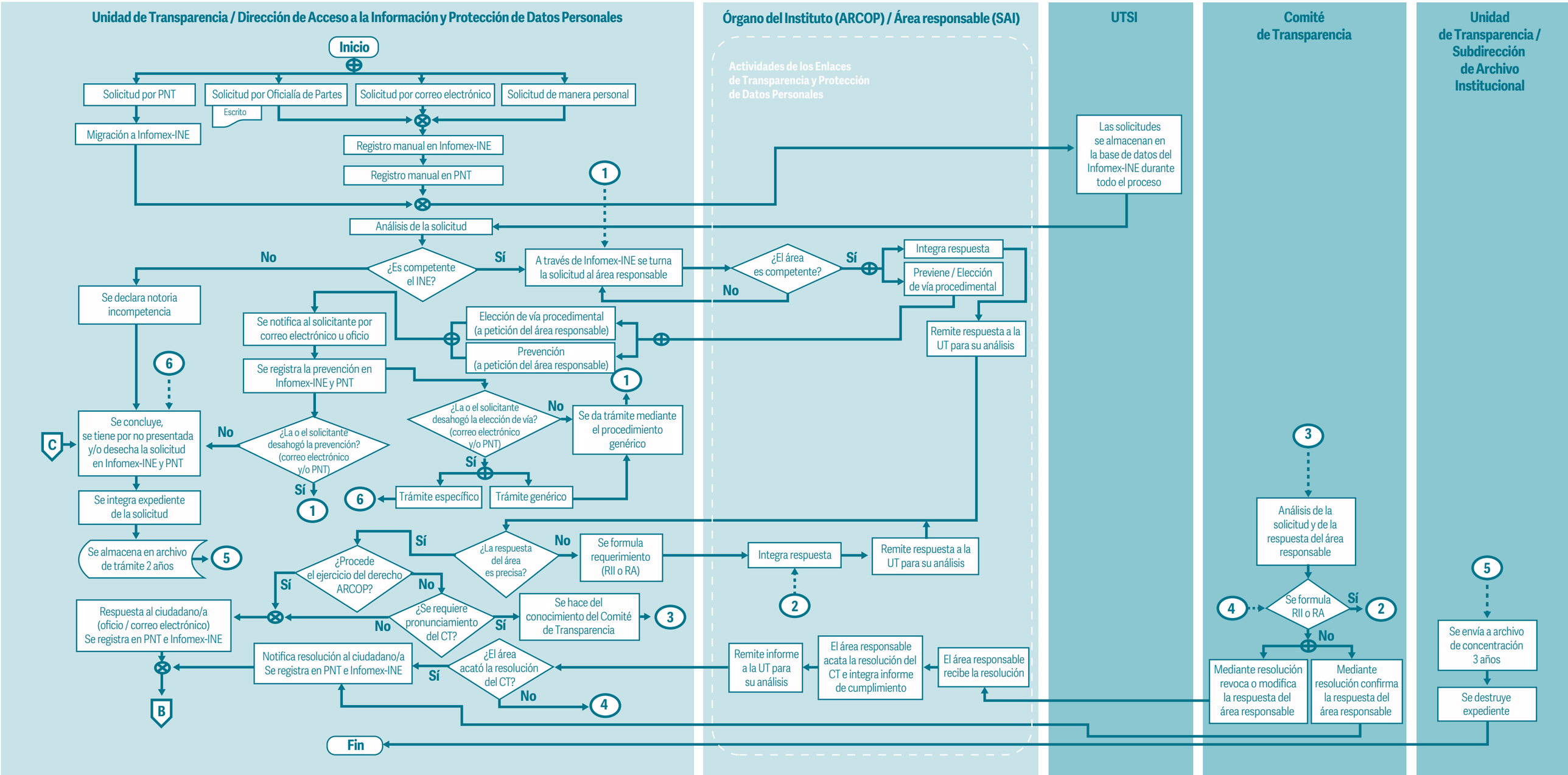
UT: Unidad de Transparencia del INE.

UTSI: Unidad Técnica de Servicios de Informática del INE.

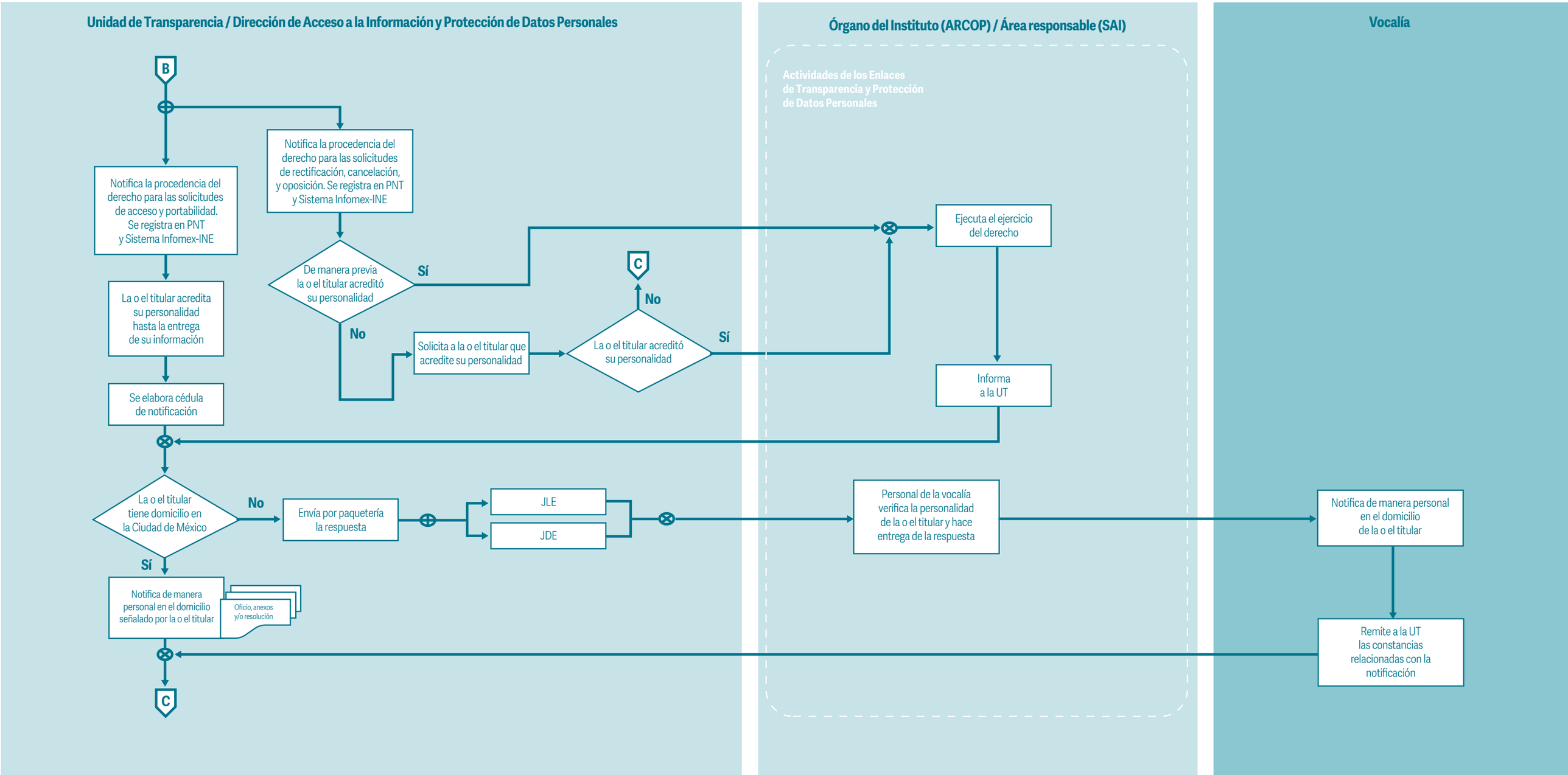
ABC de protección de datos personales

La edición estuvo al cuidado de la Dirección Ejecutiva
de Capacitación Electoral y Educación Cívica del
Instituto Nacional Electoral.

Anexo 1. Flujograma del proceso de atención a solicitudes de derechos ARCOP

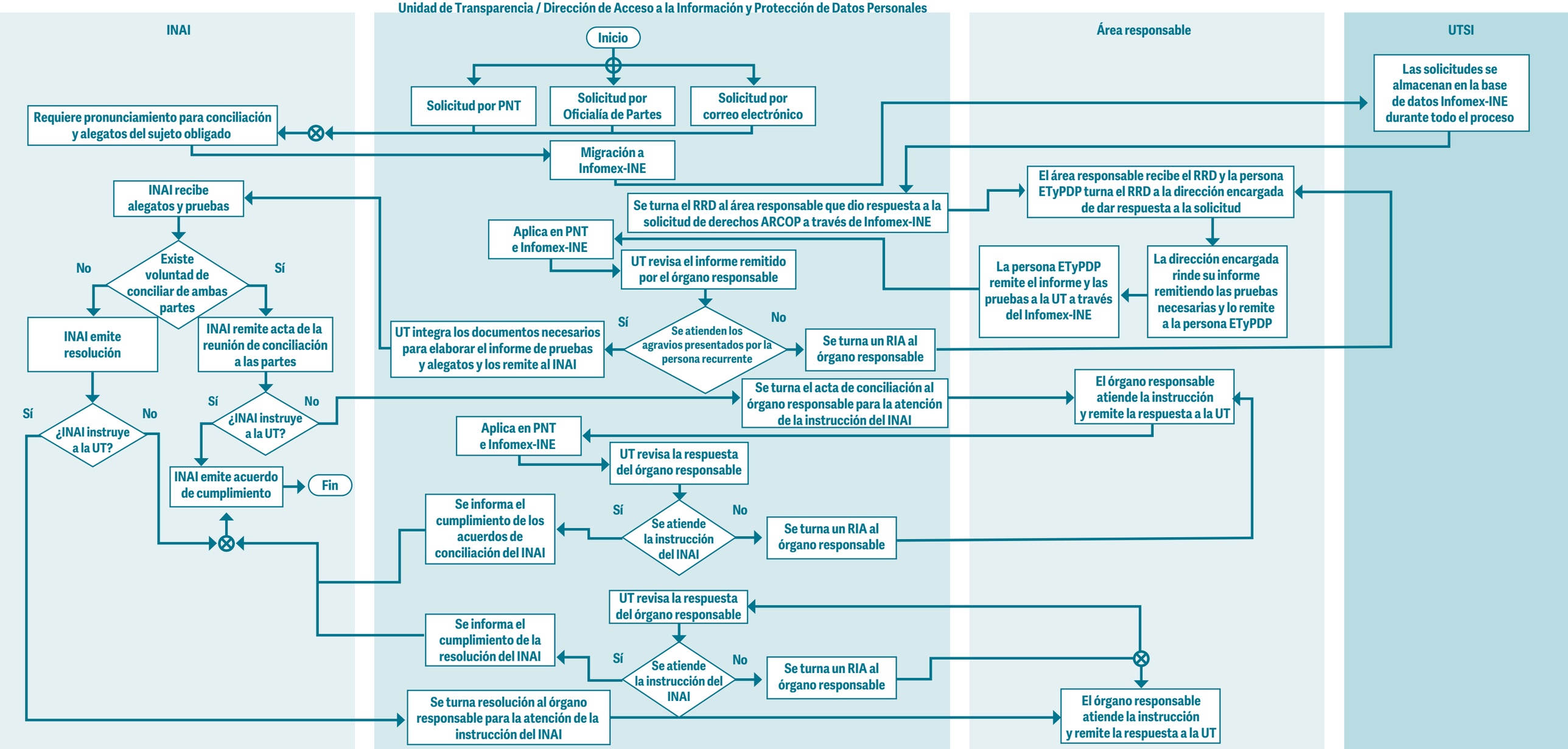


Anexo 1. Flujograma del proceso de atención a solicitudes de derechos ARCOP



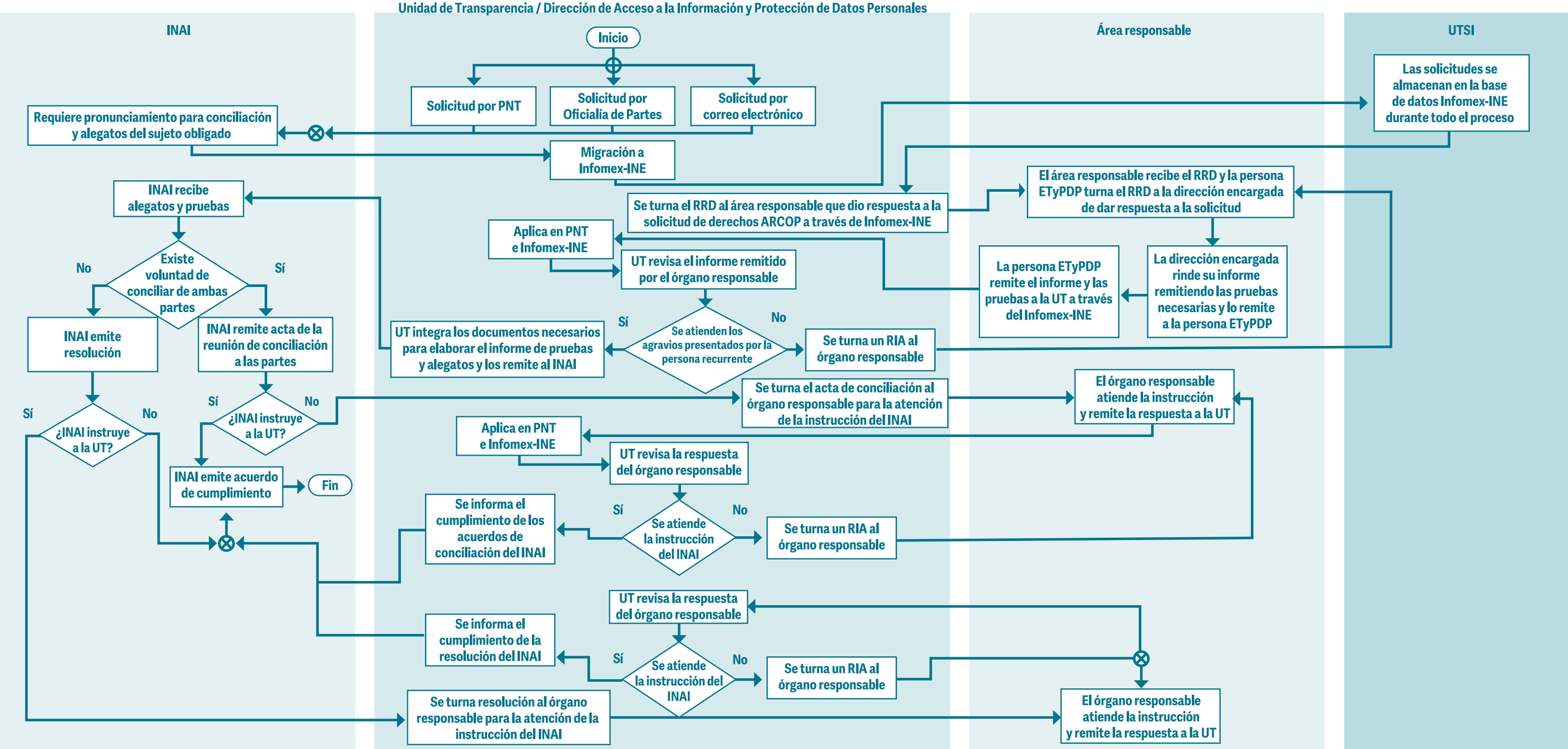
Anexo 2. Flujograma del proceso de gestión interna del recurso de revisión respecto de solicitudes de derchos ARCOP

Unidad de Transparencia / Dirección de Acceso a la Información y Protección de Datos Personales



Anexo 2. Flujograma del proceso de gestión interna del recurso de revisión respecto de solicitudes de derchos ARCOP

Unidad de Transparencia / Dirección de Acceso a la Información y Protección de Datos Personales




INE
Instituto Nacional Electoral