Aspectos relevantes sobre la gestión de confidencialidad y protección de datos personales en el INEGI y el SNIEG

Documento de análisis

Marzo de 2019

Versión 0.2

Resumen Ejecutivo

En este documento se analiza la instrumentación de los mecanismos para la gestión de confidencialidad y protección de datos personales, adoptados en los ámbitos nacional e internacional. El propósito es revisar si existen condiciones para promover y garantizar el derecho de protección de los datos personales que son proporcionados a las Unidades del Estado (entre las que se encuentra el INEGI), por parte de los informantes del Sistema Nacional de Estadística y Geografía (SNIEG). Lo anterior para, en su caso, proponer la aplicación de los mecanismos por parte de las áreas productoras de información, al ejecutar el proceso de producción de información en el marco del Modelo del Proceso Estadístico y Geográfico (MPEG).

Se realiza una revisión de la evolución que ha tenido el marco jurídico mexicano en materia de protección de los datos personales, particularmente de aquellos que se encuentran en posesión de entes del sector público, identificando y explicando los principales mecanismos, pautas y obligaciones; así también, se analizan prácticas y mecanismos en el contexto internacional, tanto los contenidos en instrumentos que son vinculantes para el Estado mexicano y otros que, sin serlo, representan un referente importante en la materia.

Los mecanismos, pautas y obligaciones identificados como buenas prácticas son expuestos bajo un enfoque de procesos, de tal manera que se propone su establecimiento e instrumentación en consistencia con cada una de las fases que comprenden el Modelo del Proceso Estadístico y Geográfico (MPEG). Lo anterior, con el fin de garantizar el cumplimiento de obligaciones en materia de protección de datos personales, a través de la adopción de un modelo de confidencialidad y protección de datos estandarizado y consistente con las actividades estadísticas y geográficas.

Dentro de la propuesta destacan las prácticas y regulaciones en la Unión Europea para la disociación de los datos personales. Mediante la adopción de estos mecanismos se posibilita y materializa el cumplimiento de la obligación de que los datos de los informantes deben ser agregados, para su divulgación, de tal manera que no se pueda identificar a los Informantes del Sistema. En suma, se debe analizar la conveniencia de que en el contexto del SNIEG se expida normatividad en materia de confidencialidad y protección de datos personales.

Contenido

1. Introducción

La expresión “confidencial”, de acuerdo con el Diccionario de la Real Academia de la Lengua Española se conceptualiza como *“que se hace o se dice en la confianza de que se mantendrá la reserva de lo hecho o lo dicho”*; por excelencia, tienen estos carácter aquellos datos que se refieren a la esfera íntima o privada de las personas; por su parte, la Ley Federal de Transparencia y Acceso a la Información Pública, en su artículo 113 fracción I, considera información confidencial a la que contiene datos personales concernientes a una persona física identificada o identificable.

Tanto el Estado como los particulares en ocasiones, derivado de las relaciones que sostienen con las personas titulares de dichos datos, han adquirido la obligación de guardar secrecía o reserva de los mismos y su utilización queda condicionada al marco normativo que les aplica.

La evolución de las Tecnologías de la Información y Comunicaciones (TICs) ha provocado la generación de interacciones entre prestadores de servicios, organismos públicos y ciudadanos cada vez más dinámicas, así como la necesidad de que se establezcan medidas de protección y seguridad específicas, ya que a través del tiempo ha aumentado la cantidad de datos que son obtenidos, resguardados y en ocasiones publicados a través de las TICs.

La confidencialidad y protección de datos personales constituyen un aspecto fundamental que debe ser garantizado por parte de cualquier organismo del estado que los obtiene, resguarda y maneja, con el propósito de salvaguardar los derechos y libertades de los titulares de dichos datos y en algunas ocasiones su seguridad e integridad corporal y patrimonial.

Con el propósito de hacer un uso uniforme de terminología, se utiliza la establecida en los ámbitos de la confidencialidad y la protección de datos. En el Anexo VI se incorpora la definición de las principales expresiones que son empleadas, indicando en cada caso la fuente respectiva.

Para ilustrar la problemática, a continuación se exponen ejemplos de robo de datos personales que se han presentado en los últimos años[1]:

- El ciberataque más importante de la historia afectó a Yahoo! en 2013 y alcanzó las cuentas de sus 3.000 millones de usuarios. Revelado en diciembre de 2016, el alcance del pirateo, que en un principio se estimó en 1.000 millones de cuentas, fue revisado al alza en 2017. No se vieron afectados ni las contraseñas ni las coordenadas bancarias, aseguró el grupo.
- En septiembre 2017, la agencia de crédito Equifax, que se encarga de recabar datos personales de los consumidores que solicitan un crédito, reveló el pirateo de datos sensibles de más de 147 millones de clientes estadounidenses, canadienses y británicos.
- La cadena de distribución estadounidense Target fue víctima de un ataque informático a gran escala en diciembre de 2013 que afectó a 110 millones de clientes, a 70 millones de los cuales les robaron datos personales (nombre, dirección postal, número de teléfono y dirección de correo electrónico) y 40 millones de datos bancarios.

[1] Liga electrónica que constituye la fuente correspondiente a los primeros casos de robo de datos personales: https://www.elespectador.com/tecnologia/los-principales-casos-de-robo-de-datos-personales-articulo-755788

- En agosto de 2015, el grupo de piratas informáticos The Impact Team publicó 30 gigabytes de datos de clientes de la página de contactos adúlteros Ashley Madison, con nombres, correos e incluso preferencias sexuales de los usuarios.

A continuación se señalan algunos ejemplos relativos a los riesgos sobre la anonimización de información, la cuál es abordada con detalle más adelante:

- Netflix liberó los datos de 500.000 usuarios para una consulta pública que consistía en intentar mejorar su sistema de sugerencias y recomendaciones, tomando como principal medida de privacidad la eliminación de datos (nombres de usuario, etc). Se hizo un estudio sobre cómo utilizando los datos públicos de *"Internet Movie Database (IMDb)"*, permitió reidentificar a usuarios que aparecieron en las muestras que publicó Netflix.
- Durante un tiempo, instituciones como U.S. National Institute of Health (NIH) permitían el acceso público a datos como las frecuencias agregadas de SNPs (single-nucleotide polymorphisms, mutaciones de ADN en localizaciones específicas). Eran estudios que comparaban las secuencias de ADN de dos grupos de participantes, unos con la mutación que se estudia y un grupo de control. Se propusieron ataques que podían localizar con una alta probabilidad en qué grupo se encontraba alguna persona, suponiendo que se dispone de la información de su ADN. Tras esto, se restringió el acceso público a estos datos.

Los casos anteriores reiteran la necesidad de que las organizaciones públicas y privadas que resguardan datos personales adopten mecanismos para su protección.

En lo que respecta a la información estadística y geográfica en México, la Ley del Sistema Nacional de Estadística y Geografía (LSNIEG), emitida en junio de 2008, prevé una excepción de aplicación de la entonces Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), emitida en el 2002, con relación a la Información de Interés Nacional (IIN); así también, dota a la Junta de Gobierno del INEGI (JG) de facultades para regular la confidencialidad de los datos que proporcionen los informantes del Sistema.

Conforme al artículo 47 de la LSNIEG, los datos que proporcionen los Informantes del Sistema, serán confidenciales en términos de esta Ley y de las Reglas Generales que conforme a ella dicte el Instituto; se considera que las referidas Reglas deben establecer los mecanismos y medios a través de los cuáles se asegurará la confidencialidad de los mencionados datos. Al día de hoy, las mencionadas Reglas Generales no han sido emitidas.

En contraste, México cuenta con un marco jurídico en materia de transparencia, acceso a la información, confidencialidad y protección de datos personales que ha evolucionado en forma considerable de manera posterior a la emisión de la LSNIEG. En los últimos años, posteriores a la emisión de la LSNIEG, se han emitido dos leyes generales, una ley federal y múltiples disposiciones administrativas y documentos no normativos de apoyo; es de destacar el reconocimiento de la protección de datos personales como derecho en nuestra Constitución Política, así como la adopción por parte de nuestro país del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal; este marco normativo es abordado de manera general en el presente análisis.

La LSNIEG regula la confidencialidad de manera abstracta y general, en comparación con el marco jurídico de la materia, pues dicha Ley se limita a establecer los principios de confidencialidad y reserva, así como las condiciones esenciales inherentes a los mismos, siendo el caso de la no

identificación de informantes, así como de la exclusividad de uso para fines meramente estadísticos; estos aspectos son importantes y esenciales, pero no suficientes para garantizar la protección de los datos personales y su confidencialidad, toda vez que se requiere de mecanismos para que las áreas productoras de información cumpan con las referidas condiciones.

En el Sistema Nacional de Información Estadística y Geografía (SNIEG) no se cuenta con instrumentos que detallen los aspectos particulares que deben ser observados para garantizar el cumplimiento del derecho que tienen todos los ciudadanos a la protección de sus datos personales, en lo que respecta a la información estadística y geográfica; dentro de estos aspectos se encuentra la conceptualización propia de información confidencial ¿que es la información confidencial para efectos del SNIEG? se trata de los datos personales, ¿cuáles son estos? ¿cuál es el catálogo de esos datos? y más aún ¿qué datos tienen mayor nivel de sensibilidad? y, consecuentemente, requieren un tratamiento con controles más robustos.

Existen aspectos cuya aplicación debe ser definida para garantizar la protección de los datos personales de los ciudadanos, destacándose las medidas de seguridad que deben adoptar los entes públicos, el ejercicio de los derechos acceso, rectificación, cancelación y oposición a los referidos datos, la generación de versiones públicas, documentos en que consten medidas de protección, el análisis de vulnerabilidades e identificación de los riesgos relacionados con la protección de los datos personales y, de manera especial, algo que es muy importante para cualquier oficina de producción de información estadística, la disociación de los datos.

Consideramos necesario que cada Unidad del Estado tenga la certeza jurídica y operativa necesaria, con relación a las disposiciones que deben ser observadas en el tratamiento de los datos personales que tienen bajo su responsabilidad y han sido proporcionados por los informantes del SNIEG, pues ello permitirá:

- Definir controles de seguridad de los datos desde el momento de su captación;
- Aplicar criterios de conservación y clasificación homogéneos;
- Desarrollar reglas de reserva de información, así como de protección uniformes y consistentes con el nivel de sensibilidad de los datos personales;
- Emitir con claridad las hipótesis y razones por las cuáles la información es negada o, en su caso, proporcionada mediante la generación de versiones públicas;
- Establecer controles que permitan evitar la fuga de información y en los casos que resulte procedente la destrucción segura de la misma, y
- Establecer reglas para la disociación de datos personales.

Bajo un enfoque de procesos, y con el objetivo de proteger los datos personales a nuestro cargo y de disociar la información estadística y geográfica, en el presente análisis se expondrán mecanismos que deberían aplicarse de manera sistemática en la ejecución del proceso de producción de información estadística y geográfica, considerando las siguientes fases:

- Documentación de necesidades.
- Diseño.
- Construcción.
- Captación.
- Procesamiento.
- Análisis de la producción.

- Difusión.
- Evaluación del Proceso.

Esto en razón de que el proceso aludido, debe ser instrumentado por las Unidades del Estado[2].

Actualmente cada Unidad del Estado o Unidad Administrativa Productora de información genera y aplica sus propios mecanismos de seguridad para el tratamiento de datos personales; no obstante, en los ámbitos nacional e internacional existe un marco jurídico-administrativo que establece en forma detallada y precisa las medidas, obligaciones, pautas y criterios para garantizar la protección de dichos datos.

Así también, se estima necesario que el INEGI en su calidad de coordinador del SNIEG, defina las Reglas Generales para que se establezca y aplique un mecanismo de disociación para que los datos personales no puedan asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación la identificación del mismo; este mecanismo deberá establecerse para cada Programa de Información y atendiendo a sus propias características, a fin de que sea irreversible y garantizar con ello la salvaguarda de los datos personales.

Algunas características del derecho a la protección de datos personales.

De manera introductoria a este documento de análisis, se exponen algunas características generales del derecho humano a la protección de los datos personales, con independencia de que más adelante se abordará con mayor profundidad la forma en que este es regulado en los ámbitos nacional e internacional.

Como se detalla más adelante en el presente documento de análisis, el 1o. de junio de 2009 se incorporó a la Constitución Política de los Estados Unidos Mexicanos el derecho fundamental a la protección de datos personales. En la exposición de motivos del dictamen por el que se reformó el artículo 16 de la carta magna se destacó que el derecho a la protección de datos atribuye a la persona un poder de disposición y control sobre los datos que le conciernen, partiendo del reconocimiento de que tales datos van a ser objeto de tratamiento por responsables públicos y privados.

La justificación del constituyente permanente de concebir a la protección de datos personales como un derecho fundamental radica en su evolución y en la necesidad de generar un punto de equilibrio entre este derecho y el de acceso a la información pública.

De acuerdo con el Artículo “Derecho a la protección de datos personales; su diseño constitucional”, escrito por Víctor Hugo Hiram Magallanes Martínez y publicado por el Instituto de Investigaciones Jurídicas de la UNAM, dentro de los semblantes que corresponden al derecho fundamental a la protección de datos personales, se tiene:

- Se relaciona con los demás derechos fundamentales, y en especial con el de acceso a la información, originando que exista una mayor eficacia para su debida observancia y respeto.

[2] De acuerdo con lo previsto en el artículo 2, fracción XV de la Ley del Sistema Nacional de Información Estadística y Geográfica, por Unidades del Estado se considera a las áreas administrativas que cuenten con atribuciones para desarrollar Actividades Estadísticas y Geográficas o que cuenten con registros administrativos que permitan obtener Información de Interés Nacional; por su parte, las Actividades Estadísticas y Geográficas, de acuerdo con la fracción I del mismo numeral se definen como las relativas al diseño, captación, producción, actualización, organización, procesamiento, integración, compilación, publicación, divulgación y conservación de la Información de Interés Nacional.

- Es concebido como un principio constitucional indeterminado y como un mandato constitucional de optimización; es decir, como una norma de valor en la sociedad que se presume justa y sirve de directriz para la actuación estatal.
- Crea una especie de frontera infranqueable que los poderes públicos y particulares no pueden invadir.

En este mismo sentido, la Comisión Interamericana de Derechos Humanos, en el documento titulado "El derecho de acceso a la información en el marco jurídico interamericano" (http://www.oas.org/es/cidh/expresion/docs/publicaciones/ACCESO%20A%20LA%20INFORMACION%20FINAL%20CON%20PORTADA.pdf), señala que uno de los límites del derecho de acceso a la información es la protección de los datos personales que sólo pertenecen a su titular y cuya divulgación podría afectar un derecho legítimo de este último como el derecho a la intimidad. En consecuencia, cuando se está ante un dato personal sensible, en principio, sólo su titular podrá tener acceso.2 La confidencialidad y protección de datos personales en el SNIEG.

En el Anexo I, "Marco normativo relativo a la confidencialidad y protección de datos en el SNIEG" se señalan de manera precisa las disposiciones, tanto legales como administrativas que regulan dicha temática en el ámbito del SNIEG.

La LSNIEG establece de manera general y abstracta, entre otros aspectos:

- La obligación de las Unidades de Estado de observar los principios de confidencialidad y reserva de la información y no identificación de las personas objeto de información e informantes.
- El uso exclusivo de los datos para fines estadísticos.

No obstante, resulta imprescindible el establecimiento y aplicación de mecanismos específicos y estandarizados que posibiliten el cumplimiento del enunciado legislativo; es decir, la LSNIEG no contiene las obligaciones, condiciones, pautas y mecanismos necesarios para tal efecto y más aún, para garantizar la observancia del derecho que tienen todas las personas para la protección de sus datos personales y que es explicado con mayor detalle en el numeral 5 "Marco Jurídico Mexicano", en el que se aborda el marco jurídico mexicano en esta materia.

El criterio al interior del INEGI ha consistido en que no es aplicable el marco normativo existente en materia de protección de datos personales, derivado de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y que las acciones a realizarse en esa materia deben ser las previstas en la LSNIEG; no obstante, dicha Ley -en concordancia con su nivel de abstracción normativo- no establece las condiciones necesarias y por otro lado, tampoco se ha regulado esa materia por parte del INEGI en su carácter de instancia normativa, mediante la emisión de las Reglas Generales que se prevén en el artículo 47 de la LSNIEG y demás normatividad necesaria para tales efectos.

Conforme al último párrafo del artículo mencionado, la información correspondiente a la gestión administrativa del INEGI sí se encontraba sujeta a la abrogada LFTAIPG; de tal manera que el criterio interno ha consistido en que a esa información sí le es aplicable el marco normativo derivado de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados; lo cual se ha reiterado con la publicación de los *Lineamientos de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Instituto Nacional de Estadística y Geografía* (DOF 19-IV-2018).

Paradójicamente, la información correspondiente a la gestión administrativa del Instituto cuenta con mecanismos y condiciones definidas respecto a la protección de datos personales, los cuáles se describen en el Anexo II de este documento de análisis; lo que no sucede con la Información del SNIEG, que es la que se utiliza para la toma de decisiones de política pública, a fin de coadyuvar al desarrollo nacional; ya que esta no cuenta con mecanismos estandarizados para la protección de los datos personales.

Lo anterior implica que normativamente, en el ámbito del SNIEG no se han establecido las obligaciones, condiciones, pautas y mecanismos necesarios para garantizar la protección y confidencialidad de los datos personales de los informantes del Sistema, así como de las personas objeto de información.

Se considera indispensable dar certidumbre a las áreas y unidades productoras de información del SNIEG, respecto de las condiciones mínimas que deben observar para estar en aptitud de garantizar la confidencialidad y protección de los datos personales proporcionados por los informantes del Sistema, sin perjuicio de que estas puedan instrumentar otros mecanismos que consideren pertinentes o que les resulten aplicables.

El artículo 104, fracción I de la LSNIEG prevé como infracción imputable a los servidores públicos del Instituto o a los servidores públicos de las Unidades la revelación de datos confidenciales; aspecto que suma relevancia a la necesidad de establecer reglas claras y homogéneas que definan la forma y términos en que los servidores públicos mencionados cumplirán con los principios de confidencialidad y reserva de los datos e información que tienen bajo su posesión.

Por otra parte, las Políticas para la Seguridad de la Información del INEGI establecen que para la protección de la Información estadística y geográfica corresponderá a cada Unidad Administrativa, en su ámbito de competencia, establecer mecanismos que garanticen de manera particular la confidencialidad de los datos personales de los informantes.

Lo anterior ha generado aplicación de criterios y métodos heterogéneos de clasificación, agrupación, conservación y tratamiento de la información confidencial por parte de las unidades productoras; es decir, no existe un estándar mínimo que deban cumplir las unidades productoras de información para dar cumplimiento a la obligación de protección de los datos personales.

La normatividad que el INEGI, en su carácter de instancia normativa en materia estadística emita, deberá dotar de certidumbre a las Unidades del Estado y consecuentemente garantizar la observancia del derecho consistente en la protección de datos personales, con lo cuál se evita y mitigan los riesgos que se advierten en el numeral 3 de este documento de análisis; al efecto, en el numeral 6 se realizan las propuestas respectivas.

A continuación se mencionan algunos Programas de Información Estadística en virtud de los cuáles se realiza el tratamiento de datos personales:

A) Datos de personas morales:

A.1) Directorio Estadístico Nacional de Unidades Económicas (2018).

- Nombre.
- Razón social.
- Actividad.

- Domicilio.

A.2) Censos económicos (2014).

- Información contable.
  - Valor de la producción.
  - Existencias e inventarios.
  - Activos fijos.
  - Cuentas bancarias.
  - Personal.
  - Remuneraciones.
  - Gastos.
  - Ingresos.

B) Datos de personas físicas.

B.1) Encuesta Nacional de Ocupación y Empleo (2018)

- Ingreso.
- Parentesco.

B.2) Encuesta Nacional de los Hogares.

- Estado de salud emocional.

B.3) Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (2018).

- Victimización por tipo de delito, precisando circunstancias de modo, tiempo y lugar de los hechos.

B.4) Censo de Población y Vivienda (2010).

- Discapacidad.

Por lo que hace a los programas de información en los que se tratan datos de personas morales, estimamos que deben de establecerse los mismos mecanismos de protección de datos que los que se prevean para las personas físicas; esto en razón de los criterios judiciales sentados por la Suprema Corte de Justicia de la Nación, mediante las tesis que a continuación se mencionan:

- Tesis jurisprudencial P./J. 1/2015 (10a.), de título: "PRINCIPIO DE INTERPRETACIÓN MÁS FAVORABLE A LA PERSONA. ES APLICABLE RESPECTO DE LAS NORMAS RELATIVAS A LOS DERECHOS HUMANOS DE LOS QUE SEAN TITULARES LAS PERSONAS MORALES", en la que se indica que *"El artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos, al disponer que en los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en dicha Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, no prevé distinción alguna, por lo que debe interpretarse en el sentido de que comprende tanto a las personas físicas, como a las morales, las que gozarán de aquellos derechos en la medida en que resulten conformes con su naturaleza y fines"*.

- Tesis aislada II/2014 (10a.) de título: "PERSONAS MORALES. TIENEN DERECHO A LA PROTECCIÓN DE LOS DATOS QUE PUEDAN EQUIPARARSE A LOS PERSONALES, AUN CUANDO DICHA INFORMACIÓN HAYA SIDO ENTREGADA A UNA AUTORIDAD", en la que se indica que "*el derecho a la protección de datos personales podría entenderse, en primera instancia, como una prerrogativa de las personas físicas, ante la imposibilidad de afirmar que las morales son titulares del derecho a la intimidad y/o a la vida privada; sin embargo, el contenido de este derecho puede extenderse a cierta información de las personas jurídicas colectivas, en tanto que también cuentan con determinados espacios de protección ante cualquier intromisión arbitraria por parte de terceros respecto de cierta información económica, comercial o relativa a su identidad que, de revelarse, pudiera anular o menoscabar su libre y buen desarrollo*".

3. Riesgos generados con motivo de la falta mecanismos estandarizados y homologados en materia de protección de datos personales de los informantes del SNIEG

La falta de obligaciones, condiciones, pautas y mecanismos de carácter estandarizado para la protección de los datos personales de los informantes representa diversos riesgos tanto para los titulares de los datos mencionados, como para los servidores públicos adscritos a las Unidades del Estado que participan en el tratamiento de dichos datos.

De manera enunciativa, más no limitativa, a continuación se enlistan algunos de los riesgos que podrían verificarse y materializarse con motivo de la falta de mecanismos estandarizados y homologados en esta materia:

3.1 Riesgos para las Unidades del Estado

- Incumplimiento de la obligación constitucional, consistente en promover, respetar, proteger y garantizar los derechos humanos; particularmente, el derecho a la protección de los datos personales[3].
- Verificación de la infracción[4] establecida en la LSNIEG, consistente en la revelación de datos confidenciales.
- Inclumplimiento de la obligación establecida para todo servidor público en la Ley General de responsabilidades Administrativas, consistente en custodiar y cuidar la documentación e información que por razón de su empleo, cargo o comisión, tenga bajo su responsabilidad, e impedir o evitar su uso, divulgación, sustracción, destrucción, ocultamiento o inutilización indebidos[5].
- Determinación de hallazgos u observaciones, así como instrumentación de procedimientos administrativos de carácter disciplinario, por parte de instancias fiscalizadoras e

[3] El artículo 1 de la Constitución Política establece la obligación de promover, respetar, proteger y garantizar los derechos humanos; el derecho humano a la protección de los datos personales está previsto en el artículo 6, apartado A, fracción VIII de la norma primaria; *Ver Anexo II; Marco jurídico mexicano relativo a la Protección de los datos personales y confidencialidad en el SNIEG.*

[4] Infracción establecida en el artículo 104, fracción I de la LSNIEG.

[5] Obligación prevista en el artículo 49 fracción V de la Ley General de Responsabilidades Administrativas.

investigadoras, con motivo de la falta del establecimiento e instrumentación mecanismos idóneos para la protección y confidencialidad de los datos personales del SNIEG.

- Posibles acciones de carácter legal (judiciales y administrativas) por parte de los titulares de los datos personales que consideran fueron objeto de un tratamiento o manejo indebido; con motivo de los daños o perjuicios que, en su caso, pudieran generarse en su contra.
- Afectación importante del prestigio institucional, así como pérdida de la confianza y credibilidad por parte de los sectores público, social y privado.
- Determinación de sanciones por faltas administrativas[6] determinadas con motivo del incumplimiento de las obligaciones que tienen los servidores públicos con relación a la confidencialidad y protección de datos personales, las cuales pueden consistir en:
    - Amonestación pública o privada.
    - Suspensión del empleo, cargo o comisión.
    - Destitución de su empleo, cargo o comisión.
    - Inhabilitación temporal para desempeñar empleos, cargos o comisiones en el servicio público y para participar en adquisiciones, arrendamientos, servicios u obras públicas.

3.2 Riesgos para los titulares de los datos personales

- Sustracción y/o revelación indebida de datos que se refieran a la esfera más íntima de su titular; por ejemplo, de datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.
- Utilización de los datos personales para fines ilícitos, como fraude, secuestro y/o extorsión.
- Afectación y daños a su seguridad e integridad física y/o patrimonial.
- Actos de discriminación.

4 Contexto internacional

Para estar en condiciones de generar alternativas y propuestas para la protección y confidencialidad de los datos personales proporcionados por los informantes y por las personas objeto de información en el SNIEG, en principio se consideró importante realizar una revisión y análisis de los principales instrumentos de carácter internacional en la materia; esto en forma previa a abordar el marco jurídico mexicano.

En el ámbito internacional, se han adoptado los instrumentos de cooperación para la protección de los datos en sus instancias de procesamiento que se indican en este numeral; cabe destacar que los primeros dos instrumentos, es decir, los incluidos en los numerales 4.1 y 4.2 han sido adoptados por el Estado Mexicano[7]; no se omite incluir las demás referencias por considerar que constituyen un

[6] El artículo 75 de la Ley General de Responsabilidades Administrativas establece los tipos de sanciones administrativa a que pueden ser sujetos los servidores públicos.

[7] Conforme al artículo 133 de nuestra Constitución Política, los Tratados Internacionales que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión.

antecedente de contexto internacional relevante para la materia de confidencialidad y protección de datos personales.

4.1 Convención Internacional de Derechos Civiles y Políticos (1966)

Este pacto tiene carácter vinculante; fue adoptado por la Asamblea General de las Naciones Unidas el 16 de diciembre de 1966 y entró en vigor el 23 de marzo de 1976. La Convención ha sido ratificada por 167 estados; México se adhirió a esta Convención el 23 de marzo de 1981.

El pacto desarrolla los derechos civiles y políticos y las libertades recogidas en la Declaración Universal de los Derechos Humanos.

Entre derechos individuales garantizados por el pacto, en su artículo 17 se encuentra *el derecho a la privacidad y a su protección por la Ley.*

La Convención puede ser consultada en la siguiente liga electrónica: https://aplicaciones.sre.gob.mx/tratados/ARCHIVOS/DERECHOS%20CIVILES%20Y%20POLITICOS.pdf

4.2 Convenio Nº 108 del Consejo de Europa para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal

Primer instrumento europeo en ser abierto a países no miembros de la Unión Europea; suscrito el 28 de Enero de 1981, es adoptado por los estados miembros del Consejo de Europa, considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados.

De acuerdo a publicación en el Diario Oficial de la Federación del 12 de junio de 2018, este convenio fue aprobado por la H. Cámara de Senadores del Congreso de la Unión.

Tiene por objeto garantizar, en el territorio de cada parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.

En este Convenio se establecen parámetros para la protección de datos personales, reglas en torno a la transferencia de datos personales entre Estados miembros, así como disposiciones que facilitan la cooperación internacional.

El Convenio puede ser consultado en la siguiente liga electrónica: http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf.

4.3 Directiva 95/46/CE del Parlamento Europeo y del Consejo

Adoptada el 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; en este instrumento se reitera la obligación de los Estados Miembros del Parlamento Europeo para garantizar la protección del derecho a la intimidad, en lo que respecta a la protección de los datos personales.

Adicionalmente, se indica que los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre ellos, por motivos relacionados por la protección garantizada.

El contenido de esta directiva puede ser consultado en la siguiente liga electrónica: http://www.wipo.int/wipolex/es/text.jsp?file_id=313009.

4.4 Directiva 2002/58/CE del Parlamento Europeo y del Consejo

Adoptada el 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas; este instrumento armoniza las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad Europea.

El contenido de esta directiva puede ser consultado en la siguiente liga electrónica: https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_es.pdf.

4.5 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

Adoptado el 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

Dentro de los aspectos que se regulan en este Reglamento se destaca:

- Condiciones de licitud para el tratamiento de datos personales.
- Condiciones para el otorgamiento del consentimiento del interesado, o titular de los datos personales.
- Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.
- Tratamiento de categorías especiales de datos personales .
- Tratamiento que no requiere identificación.
- Derechos del interesado.
    - Acceso.
    - Rectificación.
    - Supresión.
    - Limitación del tratamiento.
    - Oposición.
- Información que deberá facilitarse cuando los datos personales se obtengan del interesado.
- Responsable del tratamiento y encargado del tratamiento.
- Evaluación de impacto relativa a la protección de datos y consulta previa.

Este Reglamento puede ser consultado en la siguiente liga electrónica: https://www.boe.es/doue/2016/119/L00001-00088.pdf.

4.6 Código de buenas prácticas estadísticas europeas para los servicios estadísticos nacionales y comunitarios

Este Código fue adoptado por el Comité del Sistema Estadístico Europeo el 28 de septiembre de 2011 y establece como principio 5 la confidencialidad estadística, en el que se indica que la privacidad de

los informantes (hogares, empresas, administraciones y otros encuestados), la confidencialidad de la información que proporcionan y su uso exclusivo con fines estadísticos están totalmente garantizados.

En el Código en cuestión se consideran los siguientes aspectos:

- La confidencialidad estadística está garantizada por ley.
- El personal estadístico firma un compromiso jurídico de confidencialidad cuando es contratado.
- Se han establecido sanciones por cualquier incumplimiento deliberado de la confidencialidad estadística.
- Se proporcionan al personal estadístico instrucciones y orientaciones sobre la protección de la confidencialidad estadística en los procesos de producción y difusión. La política de confidencialidad está a disposición del público.
- Existen disposiciones físicas, tecnológicas y organizativas para proteger la seguridad y la integridad de las bases de datos estadísticas.
- Se aplican protocolos estrictos a los usuarios externos que acceden a microdatos estadísticos con fines de investigación.

4.7 Dictamen 05/2014 sobre técnicas de anonimización

El Grupo de Trabajo sobre protección de las personas[8], en lo que respecta al tratamiento de datos personales, creado por el Parlamento Europeo emitió el Dictamen 05/2014 sobre técnicas de anonimización.

En este dictamen, el Grupo de Trabajo analiza la eficacia y las limitaciones de las técnicas de anonimización existentes, atendiendo al marco legal de la Unión Europea sobre protección de datos, y formula recomendaciones para la gestión de estas técnicas teniendo en cuenta el riesgo residual de identificación inherente a cada una de ellas.

4.8 Recomendación del Consejo de la OCDE sobre Buenas Prácticas Estadísticas, relacionada con la materia de confidencialidad

La Comisión de Estadística y Política Estadística de la OCDE, ha realizado recomendaciones sobre Buenas Prácticas Estadísticas, en las que ha hecho patente la importancia y la necesidad de proteger la confidencialidad de los informantes, indicando en su recomendación número 4 “Confidencialidad”, contenida en el documento titulado “*Aplicación por México de la Recomendación del Consejo de la OCDE sobre buenas prácticas estadísticas: informe de revisión entre pares*”:

> ***“Proteger la privacidad de los informantes*** *(incluyendo individuos, hogares, empresas, y administraciones en todos los niveles de gobierno), y garantizar por ley la confidencialidad de la información individual provista y su uso exclusivo con fines estadísticos.”*

En este aspecto, el equipo revisor llegó a los siguientes hallazgos:

> *“La base legal e institucional del INEGI para proteger la confidencialidad es extensa y en general sólida, pero destaca que* ***debe mantenerse bajo revisión***

[8] Este Grupo de Trabajo fue creado en el artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo europeo independiente que aborda cuestiones relativas a la protección de datos y la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y el artículo 15 de la Directiva 2002/58/CE.

periódica *dada la velocidad con la que avanzan las fronteras tecnológicas y cada vez más datos personales y confidenciales se están volviendo accesibles, incluso a partir de datos administrativos emergentes y nuevas fuentes de datos. Por lo tanto, se apoya el plan de INEGI de* ***desarrollar documentación para (i) garantizar la aplicación consistente de la anonimización de datos y las normas y procedimientos para proteger la confidencialidad de los datos****, (ii) especificar completamente los* ***estándares y procedimientos para que las UE aseguren la privacidad de los informantes****, y (iii) establecer esquemas de flujos de datos para facilitar las actividades de control y auditoría relacionadas con la protección de datos."*

5. Marco jurídico mexicano

5.1 Consideraciones generales

Como puede observarse del contexto internacional plasmado en el punto que antecede, en las últimas décadas, tanto los Estados como las instituciones han otorgado mayor protección a los datos personales de los ciudadanos en posesión tanto de otros particulares, como de sujetos obligados de los estados, bajo la premisa de que la protección de los datos personales es un derecho fundamental de todo ciudadano y tomando en consideración las dinámicas de intercambio y tratamiento de la información personal, en razón de las nuevas formas y medios derivados de las TICs, siendo el caso del comercio electrónico, redes sociales y otros servicios de comunicaciones.

Las nuevas dinámicas de TICs traen consigo mayor efectividad, rapidez y capacidad de respuesta en el procesamiento de la información, pero también representan una serie de riesgos en cuanto a la indebida sustracción y utilización de los datos personales, pudiéndose afectar inclusive, la vida y la integridad emocional, corporal y patrimonial de los individuos, hecho que ha motivado el que este tema sea abordado inclusive de manera global; en el numeral 3 del presente análisis se exponen los riesgos que se consideran de probable verificación de no existir los mecanismos idóneos tendientes a garantizar la confidencialidad y protección de los datos personales.

Las oficinas encargadas de la producción estadística no escapan de la necesidad de establecer mecanismos que doten de seguridad y certidumbre tanto a los ciudadanos titulares de los datos personales como a las áreas encargadas de la producción de información estadística, con relación a la confidencialidad y protección de los referidos datos; de ello depende en gran medida la confianza y legitimación de las referidas oficinas con respecto a la población, siendo de especial relevancia acreditar de manera explícita y fehaciente la existencia de los referidos mecanismos, cuyo sustento debe estar plasmado en la normatividad que emita el propio órgano generador de la información.

Sobre este aspecto es de destacar que el INEGI tiene facultades normativas suficientes para emitir reglas generales relacionadas con la confidencialidad de los datos que proporcionen los informantes del Sistema.

Para el debido ejercicio de las facultades normativas del INEGI es preciso conocer las diversas regulaciones que forman parte del marco jurídico mexicano en materia de protección de los datos personales y confidencialidad; es por ello, que en el presente apartado se plasma la evolución que ha tenido dicho marco, en congruencia y consistencia con las nuevas dinámicas que han representado las TICs; fenómeno al cual también ha respondido la comunidad internacional.

5.2 Evolución del marco jurídico mexicano y excepción de aplicación prevista en la LSNIEG.

En el Anexo II de la presente nota “Marco jurídico mexicano relativo a la Protección de los datos personales y confidencialidad en el SNIEG”, pueden apreciarse con mayor detalle los diversos dispositivos constitucionales y legales que dan sustento a la protección de los datos personales en posesión de los sujetos obligados del Estado, así como algunas interpretaciones que tienen injerencia en la materia por parte del Poder Judicial de la Federación.

Es de destacar la salvaguarda que realiza nuestra Constitución Política con relación al derecho a la protección de datos personales, así como para el acceso, rectificación y cancelación de los mismos; todas las autoridades -incluyendo desde luego al INEGI- están obligadas a respetar proteger y garantizar el derecho que nos ocupa, así como los demás derechos humanos reconocidos por la Constitución.

Para que el INEGI se encuentre en condiciones garantizar a la ciudadanía el derecho mencionado debe contar con reglas claras, suficientes y precisas sobre el tratamiento de datos personales, incluyendo su obtención, uso, almacenamiento, posesión, transferencia y supresión.

Como puede apreciarse en el Anexo II, la LSNIEG expedida en 2008 protege los datos y la información que proporcionen los informantes del Sistema, así como de las personas físicas y morales objeto de información de una manera general y abstracta.

En dicha Ley se reiteró la facultad normativa del INEGI para emitir -en este caso particular- Reglas Generales que regulen la confidencialidad de los datos que proporcionen los informantes del SNIEG (Art. 47); al día de hoy no se han emitido las referidas Reglas Generales.

Como se ha advertido, en el ámbito internacional se han presentado múltiples avances normativos en materia de confidencialidad y protección de datos personales; el marco jurídico mexicano no ha escapado de esta evolución, como puede apreciarse en la línea del tiempo de la Figura 1.

EVOLUCIÓN DEL MARCO JURÍDICO MEXICANO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

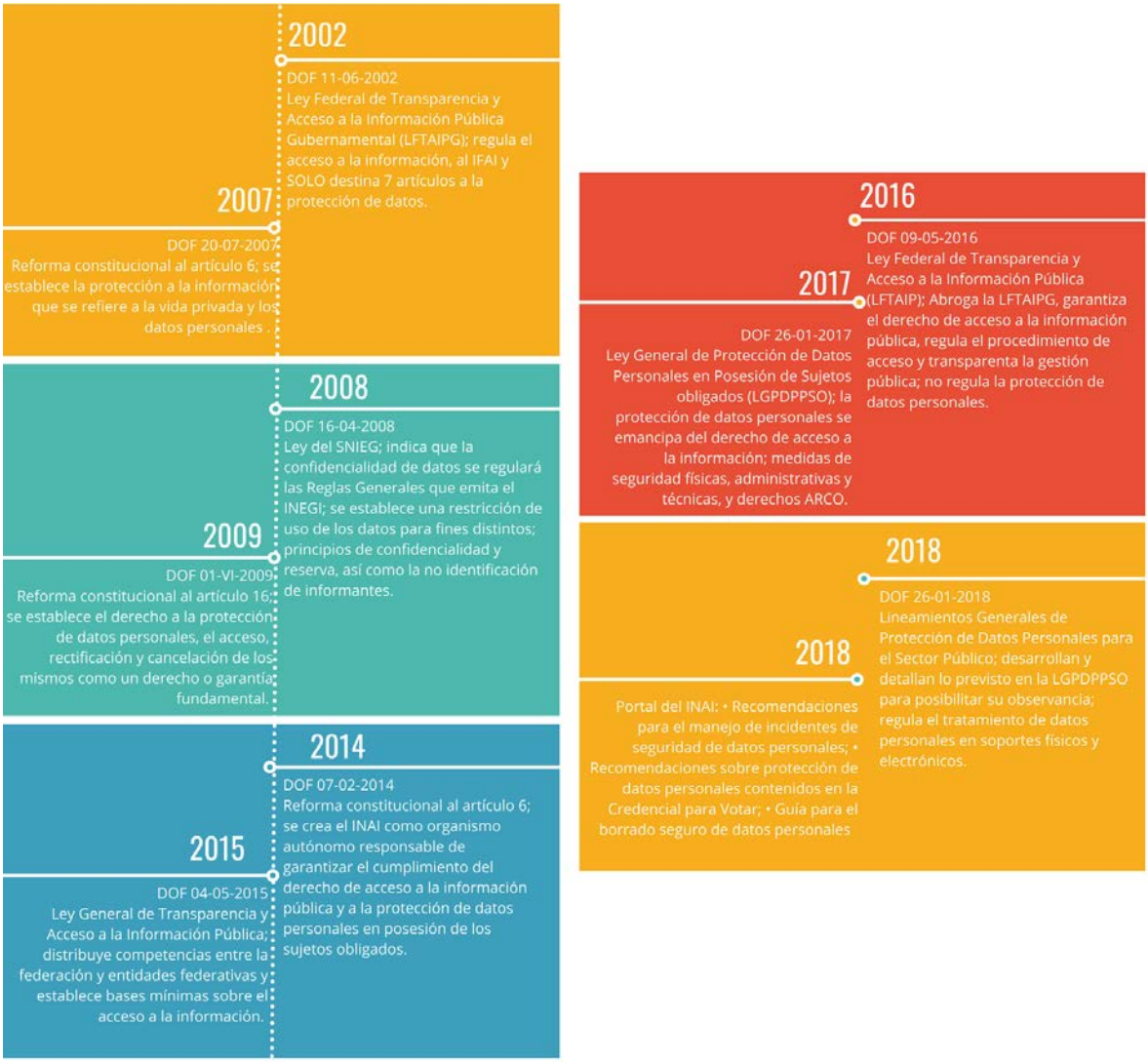

Figura 1, evolución de marco jurídico mexicano en materia de protección de datos personales.

Como puede observarse en la anterior línea del tiempo, la excepción de aplicación de la entonces Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) de 2002, con respecto a la información del SNIEG, se dio con la expedición de la LSNIEG (Art. 47) en 2008.

En ese momento, la LFTAIPG (2002) únicamente destinó 7 artículos para regular la protección de los datos personales; es decir, tenía un nivel de abstracción considerable ya que no reguló los mecanismos específicos para la protección de los datos referidos.

El marco jurídico mexicano en materia de protección de datos personales, de 2008 (fecha en que se estableció la excepción de aplicación de la LFTAIPG) al día de hoy ha evolucionado de manera muy considerable, ya que en la actualidad se cuenta con dispositivos jurídicos que establecen obligaciones, condiciones, pautas y mecanismos a nivel general para que todo organismo de cualquier ámbito de gobierno se encuentre en condiciones de garantizar la observancia del derecho consistente en la protección de datos personales.

Dentro de la referida evolución se destaca la emisión de dos leyes generales, una ley federal y un sin número de disposiciones administrativas y documentos no normativos de apoyo, así como el reconocimiento de la protección de datos constitucionales como derecho en nuestra Constitución Política; en el **Anexo II** del presente análisis se realiza con mayor detalle la descripción de los diversos dispositivos y reformas que han sido emitidos en esta materia.

Un aspecto medular, lo constituye el hecho de que el legislador, al expedir la Ley General de Protección de Datos Personales (2017) en posesión de los sujetos obligados, en la exposición de motivos indicó que la protección de datos personales queda emancipada del derecho de acceso a la información; lo que da lugar a un cuestionamiento que es abordado más adelante:

- *¿Pese a que la protección de datos personales ha sido emancipada del derecho de acceso a la información, la excepción prevista en el artículo 47 de la LSNIEG, continúa siendo aplicable, pese a que esta se refiere en forma exclusiva a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental?*

Cabe destacar que el criterio interno al interior del INEGI ha sido que la excepción mencionada continúa siendo aplicable; no obstante, se considera imprescindible tomar en consideración:

1) La evolución de marco jurídico en materia de protección de derechos personales, así como su emancipación del derecho de acceso a la información;
2) La abrogación de la LFTAIPG de 2002;
3) La falta de expedición de reglas generales o disposiciones por parte del INEGI que establezcan obligaciones, condiciones, pautas y mecanismos aplicables a la información del SNIEG en materia de confidencialidad y protección de datos personales, y
4) La obligación que tienen todos los organismos públicos de garantizar el respeto y observancia de los derechos humanos consagrados en la constitución, incluyendo desde luego, el correspondiente a la protección de los datos personales.

En suma, en concordancia con la evolución expuesta del marco normativo mexicano, así como con el contexto internacional, se considera que el INEGI debe ejercer sus facultades normativas a fin de dotar a los datos personales proporcionados por los informantes del SNIEG de los mecanismos tendientes a garantizar su protección.

En el Anexo III *"Consideraciones a partir de la controversia constitucional interpuesta por el INEGI"*, se realiza una descripción general de los argumentos jurídicos que se han hecho valer en la demanda de controversia constitucional interpuesta por el INEGI, en contra del Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI), con motivo de la invasión de competencias del INEGI por parte del INAI, en relación con la resolución de un recurso de revisión presentado por un particular, con motivo de una solicitud de acceso a la información.

Sobre ese particular, es preciso destacar que con independencia de la controversia constitucional promovida por el INEGI, la cuál se refiere al ejercicio de un derecho de acceso a la información, por lo que hace a la confidencialidad y protección de los datos personales de los informantes del SNIEG, resulta imperiosa la definición de criterios normativos respecto de la forma y términos en que se cumplirá con la confidencialidad de la información proporcionada por los informantes.

Por último, el Anexo IV incorpora algunos cuestionamientos identificados a partir del marco jurídico existente en materia de confidencialidad y protección de datos, los cuáles consideramos que tendrán respuesta a partir de la definición -en el ámbito normativo- de los diversos mecanismos que garanticen el cumplimiento de la obligación constitucional de garantizar la protección de los datos personales proporcionados por los informantes del SNIEG.

6. Propuestas

Derivado del análisis a los diversos mecanismos, medidas, obligaciones, pautas y criterios establecidos en el ámbito nacional como aquellos derivados del contexto internacional expuesto en el presente documento para garantizar la protección y confidencialidad de los datos personales, en el presente apartado se exponen las diversas propuestas que a nuestro juicio son convenientes para posibilitar y materializar el cumplimiento y observancia de los principios de confidencialidad y reserva establecidos en la LSNIEG, así como del derecho de protección de datos personales que tiene cualquier sujeto en territorio nacional.

Las diversas propuestas y alternativas que se plantean en este apartado, eventualmente deberán encontrarse establecidas en las Reglas Generales a que hace referencia el artículo 47 de la LSNIEG, así como en la demás normatividad administrativa que estime pertinente emitir el INEGI, para posibilitar la observancia de los aludidos principios, así como del mencionado derecho.

Bajo un enfoque de procesos, en primer término, en el apartado 6.1 se exponen los diversos mecanismos que deberán aplicarse para las fases del proceso de producción de información estadística y geográfica, considerando las siguientes fases que comprende el referido proceso:

- Documentación de necesidades.
- Diseño.
- Construcción.
- Captación.
- Procesamiento.
- Análisis de la producción.
- Difusión.
- Evaluación del Proceso.

Para los efectos anteriores, se consideran las actividades contenidas en la Norma Técnica del Proceso de Producción de Información Estadística y Geográfica para el INEGI, aprobada por la Junta de

Gobierno de dicho instituto en su Octava Sesión de 2018, celebrada el 29 de agosto del mismo año, la cuál puede ser consultada en la siguiente liga electrónica: http://sc.inegi.org.mx/repositorioNormateca/O_05Sep18.pdf.

Una vez realizado lo anterior, en el apartado 6.2 se hace referencia a aquellos mecanismos de aplicación transversal o cuya observancia debe realizarse en cada una de las fases o con independencia de la instrumentación de proceso de producción de información estadística y geográfica.

Los mecanismos que se exponen en el presente apartado, son aquellos que -como mínimo- deberán estar regulados en la normatividad del SNIEG y que deberán ser observados por las unidades productoras de información para garantizar la confidencialidad y protección de los datos personales que proporcionan los informantes del aludido Sistema; esto con independencia de que las unidades del Estado implementen mecanismos o pautas adicionales a las descritas en el presente documentos con los mismos propósitos.

6.1 Confidencialidad y protección de datos personales en el proceso de producción de información estadística y geográfica.

Con motivo de la instrumentación del proceso de producción de información estadística y geográfica, en algunas de las fases que comprende dicho proceso es necesaria la aplicación de algunos de los mecanismos identificados con motivo del análisis tanto de las prácticas e instrumentos internacionales referidos en el Apartado 4 “Contexto Internacional”, así como de aquellos correspondientes a nuestro marco interno y que se indican en el Apartado 5 “Marco jurídico mexicano”.

En la figura 2 se realiza la representación gráfica del proceso de producción de información estadística y geográfica, con la referencia de los mecanismos que consideramos deben ser aplicados en las fases que se indican; en el apartado 6.2 se enlistan y explican los mecanismos o acciones de carácter transversal, que deben ser observados con independencia de la fase o ejecución del proceso de producción en cuestión, con el fin de garantizar la confidencialidad y protección de los datos personales en el SNIEG.

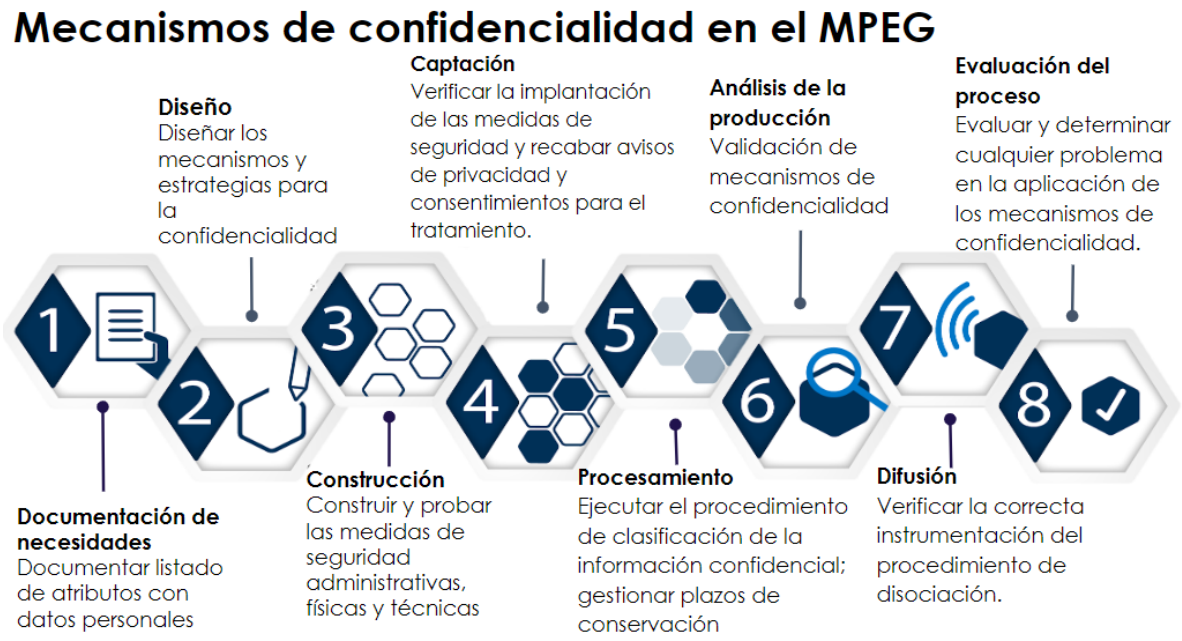

Figura 2, Aplicación de mecanismos de confidencialidad al proceso de producción de información estadística y geográfica.

6.1.1 Documentación de necesidades

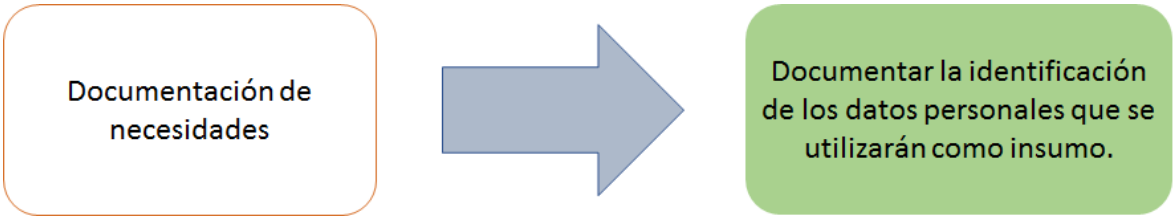

Figura 3.

6.1.1.1 Identificación de datos personales.

a) **Objeto.**

Contar desde el inicio del proceso de producción de información con la identificación de los datos personales que serán utilizados como insumo, con base en criterios y parámetros previamente definidos; esta acción se realizará dentro de las actividades del proceso de detección y gestión de necesidades.

b) Justificación y descripción.

De acuerdo con lo previsto en el numeral 1.4 del Modelo Genérico del Proceso Estadístico GSBPM[9], versión 5 (GSBPM), en el subproceso 1.5 "*Comprobación de la disponibilidad de datos*" se comprueba si fuentes de datos actuales podrían satisfacer los requerimientos de usuario y las condiciones bajo las cuales estarían disponibles; así también, de acuerdo con el artículo 12 fracción VI de la Norma Técnica del Proceso de Producción de Información Estadística y Geográfica del INEGI (Norma Técnica INEGI), el Actor del Rol Responsable de la Fase deberá recabar e integrar la evidencia que acredite la realización de las actividades a que hace referencia la normatividad relativa a la detección y aprobación de necesidades, dentro de la que se encuentra:

- *Listado de datos que se utilizarán como insumo para la generación de información, así como los instrumentos jurídicos que soportan su acceso.*

Conforme al artículo Quinto Transitorio de la Norma mencionada, la Junta de Gobierno expedirá, en un plazo no mayor a 180 días hábiles contados a partir de la entrada en vigor de la presente Norma, las disposiciones normativas asociadas a la detección y aprobación de necesidades; en ese sentido, en la fase de la Norma Técnica relativa a la documentación de necesidades solo se recaba el listado de los datos personales a que se hace referencia.

El área que instrumente el proceso de detección y aprobación de necesidades, al generar el listado de datos personales se encuentra en condiciones de identificar que tipo de datos personales serán considerados como insumo en el proceso de producción de información.

Al respecto, se deberá observar lo siguiente:

- Considerar únicamente los datos personales que resulten adecuados, relevantes y estrictamente necesarios para el proceso de producción de información.
- Se deben contemplar aquellos datos personales que tengan relación y sean consistentes con las facultades o atribuciones que la normatividad aplicable le confiere a la unidad que producirá la información.

6.1.2 Diseño

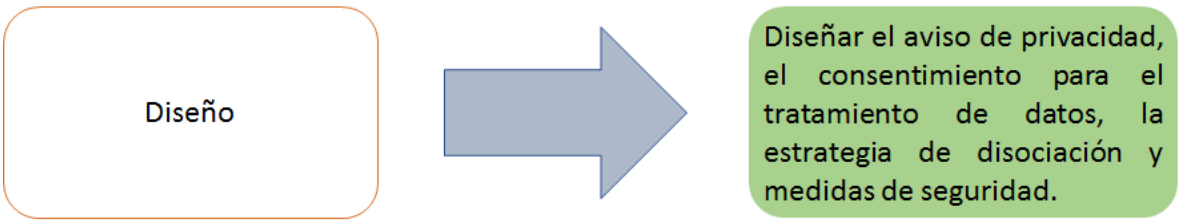

Figura 4

6.1.2.1 Diseño del aviso de privacidad.

a) Objetivo.

[9] Por las siglas en inglés Generic Statistical Business Process Model.

Diseñar el mecanismo para informar al titular de los datos personales los propósitos, características y finalidades del tratamiento de sus datos[10].

b) Justificación y descripción.

Es necesario contar con un documento que se ponga a disposición del titular de los datos personales de forma física, electrónica o en cualquier formato generado por la Unidad productora de información, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Conforme al numeral 2.3 del GSBPM, el subproceso "diseño de la recolección" determina el(los) método(s) de recolección e instrumento(s) más apropiado(s); por su parte, el artículo 14 fracción III de la Norma Técnica INEGI establece como actividad específica dentro de la fase de diseño el diseño y prueba de los instrumentos de captación.

Por lo anterior, dentro de las acciones de diseño de los instrumentos mencionados se debe considerar el diseño a su vez del aviso de privacidad, con el propósito de garantizar que los titulares tengan conocimiento -por escrito- del tratamiento que se le da a sus datos y realicen un ejercicio informado de sus derechos con relación a dichos datos.

Toda comunicación de datos personales que el responsable realice con encargados o terceros a quienes transfiera datos personales, siempre debe ir acompañada del aviso de privacidad, con la finalidad de que conozcan las condiciones a las que el titular sujetó el tratamiento de su información.

El aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que cuente la Unidad del Estado de que se trate; asimismo, consideramos que debe ser adaptable a las características peculiares de cada Programa de Información, ya que en cada uno de estos pueden realizarse diferentes tipos de tratamiento.

En la integración de este mecanismo puede ser utilizada como marco de referencia la "Guía para el Aviso de Privacidad" Publicada por el INAI en la siguiente liga electrónica: http://inicio.ifai.org.mx/SitePages/Guia-para-el-Aviso-de-Privacidad.aspx; en el **Anexo V** se incorpora un modelo tipo de un Aviso de Privacidad publicado por el mismo organismo, el cuál para su utilización en el contexto de la información estadística deberá ser ajustado.

6.1.2.2 Diseñar el consentimiento otorgado por el titular de los datos personales.

a) Objetivo.

Diseñar el esquema mediante el cual se sujetará el tratamiento de datos personales al consentimiento de su titular.

b) Justificación y descripción.

La Unidad productora de información deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

[10] La Ley General de Protección de Datos Personales en Posesión de Sujetos obligados define el tratamiento de los datos personales de la siguiente manera: *Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.*

- Libre: Sin que medie error, mala fe, violencia o dolo.
- Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas.
- Informada: Que el titular tenga conocimiento del aviso de privacidad.

Como se indicó en el párrafo que precede, en la fase de diseño se considera, entre otros aspectos, el diseño de los instrumentos de captación; tanto el aviso de privacidad, como el consentimiento de los titulares de los datos personales deben ser integrados en complemento a dicho instrumento, en el caso de que a través de este se recolecten datos personales, por lo que la Unidad o área productora de información deberá diseñar el texto en el cual se otorga el consentimiento para las acciones de tratamiento de los datos, precisando el tratamiento a que serán sujetos los datos en cuestión.

El responsable únicamente podrá tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones para tales efectos y medie el consentimiento del titular.

El Consentimiento otorgado por el titular de los datos personales puede hacerse constar en el cuerpo del Aviso de privacidad, cuyo formato ha sido incorporado en el **Anexo V.**

6.1.2.3 Diseño de las Medidas de Seguridad.

a) Objetivo.

Diseñar acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales

b) Justificación y descripción.

El subproceso 2.6 del GSBPM se refiere al "*Diseño de los sistemas de producción y de los flujos de trabajo"* y de manera precisa, el artículo 14, fracción V, inciso c) de la Norma Técnica INEGI considera como actividad específica la determinación de estrategias y mecanismos para la seguridad de la información, por lo que resulta indispensable, a fin de brindar protección a los datos personales, que en esta fase la Unidad o área productora de la información diseñe las medidas de seguridad cuya descripción se realiza en párrafos siguientes.

Las medidas de seguridad que deben definirse son de carácter tanto administrativo, como físico y técnico y deben constar en un documento de seguridad integrado por la Unidad o área productora de información; así también, resulta ideal que las mismas se encuentren documentadas y contenidas en un sistema de gestión[11].

A continuación se realiza una descripción de las medidas de seguridad según su tipo:

- **Medidas de seguridad administrativas**: Procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales; en el numeral 6.2 se realiza una descripción de los mecanismos existentes para la supresión segura de los datos.

[11] El artículo 34 de la Ley General de Protección de Datos Personales en Posesión de los sujetos obligados considera el sistema de gestión como el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

- **Medidas de seguridad físicas**: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
    - Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.
    - Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.
    - Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización.
    - Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.
- **Medidas de seguridad técnicas**: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
    - Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.
    - Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.
    - Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.
    - Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

En el diseño de estas medidas, la Unidad o área productora de información deberá coordinarse con la Coordinación General de Informática y con la Dirección General de Administración, según corresponda, en razón de que estas corresponden al ámbito de competencia de dichas Unidades Administrativas; en el caso de las Unidades del Estado deberán a su vez coordinarse con las áreas equivalentes respectivas para los efectos mencionados.

6.1.2.4 Diseño de la estrategia de disociación.

a) Objetivo.

Diseñar para cada programa, un mecanismo para que los datos personales no puedan asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación la identificación del mismo.

b) Justificación y descripción.

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

Conforme a la fracción VI del artículo 14 de la Norma Técnica INEGI, dentro de las actividades que deben ser realizadas en esta fase se encuentra el diseño del esquema de Difusión de los productos de información; un elemento esencial previo a la difusión de los productos debe ser la disociación de los datos personales para el efecto de que estos no posibiliten la identificación de sus titulares, por lo que el diseño de la estrategia de disociación resulta elemental.

Cabe apuntar que la Comunidad Europea ha advertido un riesgo implícito del proceso de anonimización, el cual ha de tenerse en cuenta al evaluar la validez del mismo; dispuso que han de tenerse en cuenta la identificabilidad, el contexto y las circunstancias particulares de cada caso, es decir, no basta con eliminar los elementos que pueden servir para identificar directamente a una persona sino que harán falta medidas adicionales para evitar dicha identificación.

En la regulación normativa de este mecanismo deberá obligarse a los responsables de los datos personales para que en la realización del procedimiento de disociación atiendan las particularidades de cada caso para que efectivamente, bajo ninguna circunstancia puedan identificarse a los titulares de los datos personales.

Es importante considerar que existen herramientas que posibilitan el que el procedimiento de disociación sea reversible, por lo que en el diseño de estos mecanismos habrá que establecer controles y procedimientos con un grado de robustez tal que posibilite la protección de los datos personales atendiendo a los aspectos peculiares de cada supuesto; esto considerando que algunas veces para la identificación de los titulares de los datos no es suficiente con la eliminación o supresión de ciertos datos, por lo que deben utilizarse otro tipo de técnicas que en efecto posibiliten la anonimización de la información, de tal manera que esta sea IRREVERSIBLE.

El riesgo de identificación de los titulares de los datos personales puede aumentar con el tiempo; ello depende del desarrollo de las tecnologías de la información y la comunicación; algunas teorías exponen diferencias entre anonimización, seudonimización y disociación, e indican que esta última es la que tiene un carácter irreversible y que las primeras tienen limitantes según los avances de la tecnología, ya que según algunas referencias únicamente implican la separación de algunos datos que permiten la no identificación de las personas, es decir, volviendolos a unir sería reversible la referida identificación.

En el derecho mexicano, la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados, en su artículo 3, fracción XVIII conceptualiza la expresión disociación como el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

El Dictamen 05/2014 sobre técnicas de anonimización, mencionado en el numeral 4.6, hace referencia a esta última expresión, sin distinción y dándole un carácter irreversible al resultado que se obtengan de las técnicas asociadas al mismo, por lo que independientemente de la denominación que se le de al procedimiento, la trascendencia radica en su carácter irreversible, es decir, que una vez ejecutado no sea posible asociar los datos a una persona.

En razón de lo expuesto, se considera pertinente que en el ámbito normativo del SNIEG y considerando lo establecido en nuestro marco jurídico se adopte la expresión disociación; de acuerdo a lo indicado en el Dictamen aludido, en el diseño del mecanismo de disociación, las Unidades o áreas productoras de información deberán observar lo siguiente:

- Pueden considerarse varias técnicas de disociación, sin que la normatividad aplicable sea prescriptiva o restrictiva respecto a una o varias técnicas.
- Hay que dar importancia a los elementos contextuales; debe considerarse el conjunto de los medios que puedan ser razonablemente utilizados para la identificación del titular de los datos.

- No basta con eliminar los elementos que pueden servir para identificar directamente a una persona para garantizar que ya no se puede identificar al interesado.
- Una solución de anonimización eficaz impide a todos singularizar a una persona en un conjunto de datos, vincular dos registros en un conjunto de datos (o dos registros pertenecientes a conjuntos diferentes) e inferir cualquier tipo de información a partir de dicho conjunto.
- El concepto de identificación no conlleva únicamente la posibilidad de recuperar el nombre o la dirección de una persona, sino que incluye también la identificabilidad potencial por singularización, vinculabilidad o inferencia[12]. Una estrategia que prevenga estos tres riesgos tendrá la solidez necesaria para impedir la reidentificación de los datos mediante los medios más probables y razonables que puedan emplear el responsable del tratamiento y cualquier tercero.
- Las técnicas que pueden ser empleadas por la Unidad o área productora de información, en esencia consisten en lo siguiente:
    - Aleatorización.- Es una familia de técnicas que modifican la veracidad de los datos a fin de eliminar el estrecho vínculo existente entre los mismos y la persona. Si los datos se hacen lo suficientemente ambiguos, no podrán remitir a una persona concreta.
    - Generalización.- Es la segunda familia de técnicas de anonimización. Este enfoque generaliza o diluye los atributos de los interesados modificando las respectivas escalas u órdenes de magnitud (por ejemplo, sustituyendo una ciudad por una región, o una semana por un mes). Aunque la generalización pueda ser efectiva para descartar la singularización, no permite obtener una anonimización eficaz en todos los casos; en concreto, es necesario aplicar enfoques cuantitativos específicos y complejos para impedir la vinculabilidad y la inferencia.

  En el ámbito normativo podrían preverse las técnicas correspondientes a cada rubro de manera enunciativa no limitativa, con la indicación de que la Unidad o área productora de información deberá utilizar las que sean necesarias para garantizar la anonimización de la información de manera IRREVERSIBLE.

- Las Unidades o áreas productoras deben documentar la técnica o el conjunto de técnicas de anonimización que se utilizarán -preferentemente en un dictamen-, explicando las razones técnicas y prácticas por las que dichas técnicas mitigan los riesgos de la anonimización, sobre todo si tienen la intención de publicar el conjunto de datos anonimizado.

Para mostrar la importancia y necesidad de estos mecanismos, a continuación se transcribe un ejemplo ilustrado por el Grupo de Trabajo sobre protección de las personas del Parlamento Europeo:

[12] De acuerdo con el Dictamen 05/2014, estos son los 3 riesgos clave de la anonimización:
- Singularización: la posibilidad de extraer de un conjunto de datos algunos registros (o todos los registros) que identifican a una persona.
- Vinculabilidad: la capacidad de vincular como mínimo dos registros de un único interesado o de un grupo de interesados, ya sea en la misma base de datos o en dos bases de datos distintas. Si el atacante puede determinar (p. ej., mediante un análisis de correlación) que dos registros están asignados al mismo grupo de personas pero no puede singularizar a las personas en este grupo, entonces la técnica es resistente a la singularización, pero no a la vinculabilidad.
- Inferencia: la posibilidad de deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros atributos.

EJEMPLO:
Debido a su naturaleza única, los perfiles de datos genéticos constituyen un ejemplo de datos personales que están en riesgo de ser identificados si tan solo se utiliza la técnica de eliminación de la identidad del donante.
Diversos estudios científicos ya han demostrado que, al combinar los recursos genéticos disponibles para el público (p. ej., registros genealógicos, obituarios y resultados de consultas en motores de búsqueda) y los metadatos sobre donantes de ADN (fecha de donación, edad o lugar de residencia), se puede revelar la identidad de determinadas personas aunque el ADN se haya donado de forma «anónima».

Se recomienda tomar en consideración los aspectos técnicos y particulares previstos en el Manual de Técnicas de Anonimización, publicado en forma anexa al Dictamen 05/2014, mismo que puede ser consultado en la siguiente liga electrónica: http://studylib.es/doc/5271173/dictamen-05-2014-sobre-t%C3%A9cnicas-de-anonimizaci%C3%B3n.

por último, es importante mencionar que una vez que los datos personales han sido sometidos al procedimiento de disociación y por ende su titular no es susceptible de ser identificado o identificable, no es necesario el consentimiento por parte de los titulares de dichos datos para las acciones de tratamiento que se efectúen.

6.1.3 Construcción.

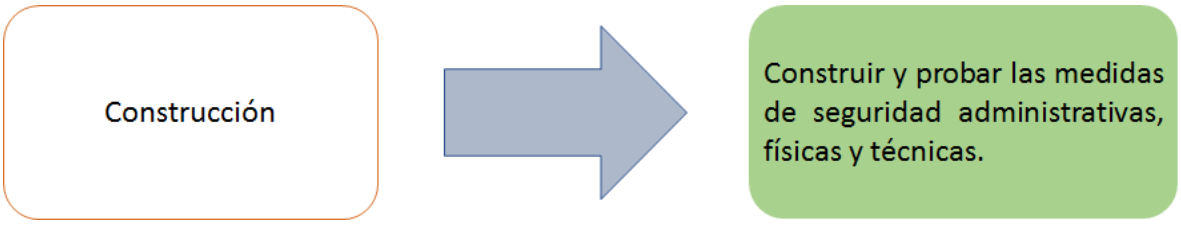

Figura 5

6.1.3.1 Construir y probar las medidas de seguridad administrativas, físicas y técnicas.

a) Objetivo.

Crear y realizar las pruebas necesarias de las medidas de seguridad administrativas, físicas y técnicas, a fin de garantizar que estas se encuentran en condiciones idóneas para la protección de los datos personales.

b) Justificación y descripción.

Conforme al GSBPM esta fase incluye pruebas al sistema de producción, al proceso estadístico y la finalización del sistema de producción; por su parte, la Norma Técnica INEGI, en su artículo 18 fracciones I y II considera dentro de las actividades de la fase la construcción, mejora y pruebas de los elementos de seguridad; es por ello que dentro de esta fase, las Unidades o áreas productoras de información deberán realizar la construcción y pruebas necesarias de las medidas de seguridad administrativas, físicas y técnicas que han sido descritas en el numeral 6.1.2.3 *"Diseño de las Medidas de Seguridad"* de este documento.

El objeto de esta actividad es contar con información objetiva y veraz con relación a la selección de las medidas de seguridad y sí es que estas cumplen con el propósito de salvaguardar la seguridad de los datos personales; en caso de ser necesario la Unidad o área productora podría realizar las adecuaciones que sean convenientes.

6.1.4 Captación.

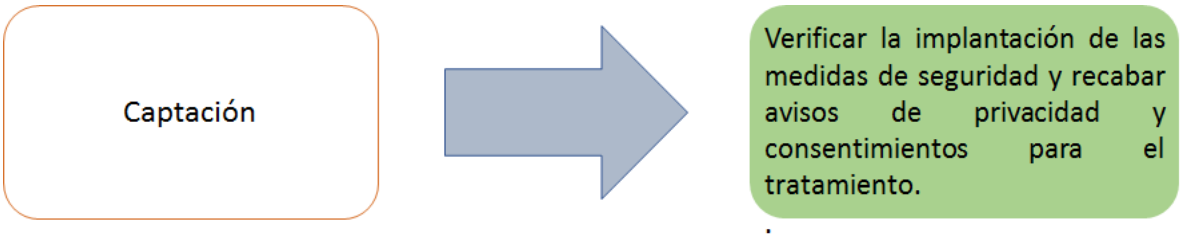

Figura 6

6.1.4.1 Verificar la implantación de las medidas de seguridad.

a) Objetivo.

Constatar que las medidas de seguridad administrativas, técnicas y físicas que han sido diseñadas, construidas y probadas efectivamente hayan sido aplicadas y se estén implementando.

b) Justificación y descripción.

Conforme al Subproceso 4.3 del GSBPM, en esta fase se ejecuta la recolección o captación de los datos con los diferentes instrumentos diseñados; por su parte, la Norma Técnica del INEGI, en su artículo 22 fracción IV considera dentro de las actividades de esta fase cargar o capturar los datos captados y sus metadatos a un ambiente adecuado para su posterior procesamiento; es decir, crear el Conjunto de Datos Captados, por lo que estos ya deben ser protegidos por las medidas de seguridad diseñadas para tal efecto y que se describen en el numeral 6.1.2.3, de tal manera que en esta fase la Unidad o área productora de información debe verificar la adecuada implantación de dichas medidas y si existiera alguna desviación, tomar las medidas pertinentes para mitigar los riesgos de incidentes o vulneraciones a los datos personales.

6.1.4.2 Recabar los avisos de privacidad y consentimientos otorgados por los titulares para el tratamiento de sus datos personales.

a) Objetivo.

Ejecutar el mecanismo diseñado para informar al titular de los datos personales los propósitos, características y finalidades del tratamiento de sus datos, así como recabar el consentimiento del titular de los datos personales.

b) Justificación y descripción.

Considerando que en esta fase se lleva a cabo la captación de los datos personales proporcionados por los informantes del SNIEG, este es el momento en que las Unidades o áreas productoras de información deben recabar los avisos de privacidad y consentimientos que fueron definidos en la fase

de diseño conforme a lo indicado en los numerales 6.1.2.1 y 6.1.2.2 del presente documento de análisis.

Con lo anterior se garantizará que los titulares tengan conocimiento -por escrito- del tratamiento que se le da a sus datos y realicen un ejercicio informado de sus derechos con relación a dichos datos, así como el otorgamiento del consentimiento a la Unidad o área productora que corresponda para el tratamiento mencionado.

6.1.5 Procesamiento.

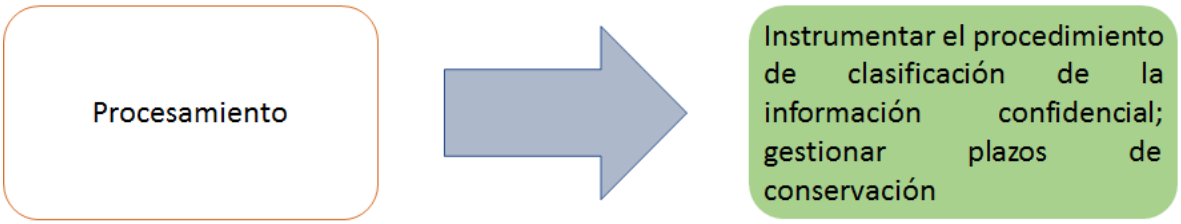

Figura 7

6.1.5.1 Clasificación de los datos personales.

a) Objetivo.

Instrumentar los procedimientos para clasificar los datos personales como información confidencial, así como de disociación de datos y de conservación.

b) Justificación y descripción.

Tomando en cuenta que de acuerdo con el GSBPM en el subproceso 5.1, así como en el artículo 25 fracción I de la Norma Técnica del INEGI en esta fase se integran los datos de una o más fuentes, se considera que las Unidades y áreas productoras de información deben instrumentar un procedimiento de clasificación para que los datos personales sean considerados información confidencial incorporando una etiqueta a los mismos, a fin de posibilitar su adecuada identificación y tratamiento.

Es necesario establecer e instrumentar un procedimiento de clasificación de la información confidencial, derivado del cual las unidades productoras identifican y determinan formalmente cuál es la información que tiene el carácter de confidencial y por ende, respecto de la cual se desplegarán las medidas de protección respectivas.

Cuando un documento contenga partes o secciones reservadas o confidenciales, las unidades productoras, podrán elaborar una versión pública en la que se testen las partes o secciones clasificadas, indicando su contenido de manera genérica y fundando y motivando su clasificación; en el apartado 6.2 se incluye lo relativo a la integración de las Versiónes Públicas.

6.1.5.2 Gestionar plazos de conservación.

a) Objetivo.

Dar certidumbre a las Unidades productoras, estableciendo criterios estandarizados respecto de la temporalidad en la cual deben conservar la información.

b) Justificación y descripción.

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento; se deberán considerar los aspectos administrativos e históricos de los datos personales.

Los plazos de conservación deberán estar incorporados en el Catálogo de Disposición Documental que corresponda y deberá observarse la normatividad que aplicable a cada Unidad del Estado; en el caso del INEGI los Lineamientos para la Organización y Conservación de los Archivos publicados en la siguiente liga electrónica de la Normateca Institucional: http://sc.inegi.org.mx/repositorioNormateca/Lrm_07Feb18.pdf.

6.1.6 Análisis de la producción.

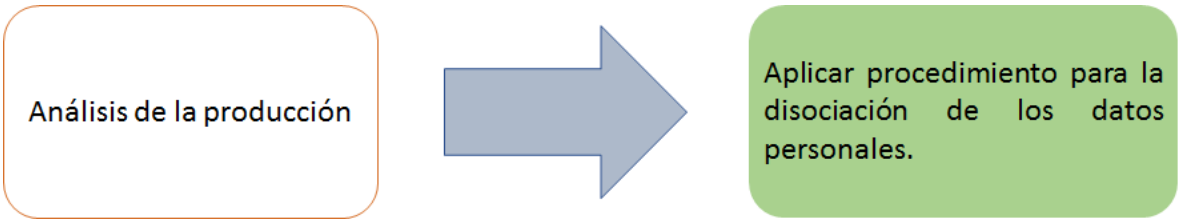

Figura 8

6.1.6.1 Instrumentación del procedimiento para la disociación de los datos personales.

a) Objetivo.

Ejecutar el mecanismo diseñado para que los datos personales no puedan asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación la identificación del mismo.

b) Justificación y descripción.

El subproceso 6.4 del GSBPM se refiere a la aplicación del control de divulgación, el cual asegura que los datos (y metadatos) difundidos no violen las reglas de confidencialidad; por su parte, la Norma Técnica INEGI, en su artículo 28 fracción III, establece dentro de las actividades a ejecutar asegurar que los datos y metadatos que se difundirán observen los principios de confidencialidad y reserva previstos en la LSNIEG.

Es por lo anterior, que en esta fase previa a la difusión, la Unidad o Área productora de la información deberá ejecutar el procedimiento previamente elaborado, de acuerdo con lo previsto en el apartado 6.1.2.4 de este documento para la disociación de los datos personales.

Con lo anterior se permitirá que los datos personales no se asocien al titular, impidiendo que por su estructura, contenido o grado de desagregación, se lleve a cabo la identificación del mismo.

Es importante destacar que la LSNIEG en su artículo 100 establece que el Instituto, siguiendo las mejores prácticas internacionales, pondrá a disposición de quien lo solicite, los microdatos de las encuestas nacionales y muestras representativas de los operativos censales que realice con la mayor desagregación posible, sin violar la confidencialidad y reserva de la información básica establecidas en la LSNIEG.

La anterior previsión es parte de las correspondientes al Servicio Público de Información Estadística y Geográfica, por lo que resulta esencial la ejecución del procedimiento aludido para prestar el

Servicio Público mencionado, en lo que respecta a la puesta a disposición de los microdatos sin violentar la confidencialidad de los datos personales.

6.1.7 Difusión.

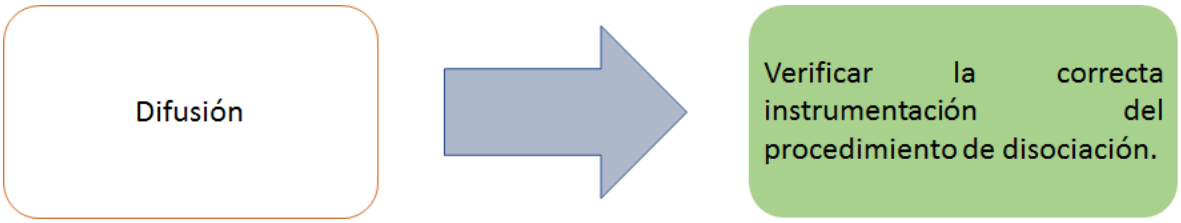

Figura 9

6.1.7.1 Verificar la instrumentación del procedimiento de disociación.

a) Objetivo.

Verificar la correcta instrumentación del procedimiento de disociación de datos personales, previamente a la publicación de los productos de información y de la puesta a disposición de los microdatos.

b) Justificación y descripción.

El Subproceso 7.3 del GSBPM se refiere a la Gestión de la publicación de productos de difusión y en este se asegura que los elementos a ser publicados están en su lugar e incluye gestionar el momento en el que serán publicados; en el mismo subproceso se indica inclusive que en ocasiones, una organización debe retirar un producto (por ejemplo, si se descubre un error).

En razón de lo anterior, se considera que el área encargada de la difusión de los productos de información deberá verificar o validar que en efecto, se instrumentó de manera adecuada el procedimiento de disociación y que consecuentemente es posible realizar la publicación de la información o, en su caso, puesta a disposición de microdatos sin que se comprometa la confidencialidad de los datos personales.

6.1.7.2 Previsiones normativas para el Servicio Público de información y acciones de difusión.

a) Objetivo.

Se estima importante que el INEGI, en su carácter de instancia normativa del SNIEG emita disposiciones tendientes a garantizar la confidencialidad y protección de datos personales en la prestación del Servicio Público de Información[13], así como para las actividades de difusión de información estadística y geográfica que realice el propio INEGI.

b) Justificación y descripción.

Dentro de los aspectos que consideramos deben ser definidos normativamente por el INEGI en las actividades del Servicio Público de Información, así como en las de difusión de información, se encuentran los siguientes:

[13] De acuerdo con el artículo 98 de la LSNIEG, el Servicio Público de Información Estadística y Geográfica consiste en poner a disposición de los usuarios, sujeto a las normas que al efecto dicte la Junta de Gobierno, la totalidad de la Información de Interés Nacional.

- No se requerirá el consentimiento de los particulares titulares de la información confidencial, en el supuesto de que la información se encuentre en registros públicos o fuentes de acceso público, que por ley tenga el carácter de pública o cuando sea transmitida entre las unidades del Estado.
- En las plantillas de los metadatos de la Información se deberá hacer referencia a aquellas disposiciones en razón de las cuáles, en su caso, la información relacionada con los mismos tiene el carácter de reservado, confidencial o cuenta con alguna restricción de difusión.
- Ejecución del procedimiento de disociación cuando se deba divulgar información; estableciendo condiciones que permitan garantizar la no identificación del titular.
- Regular un procedimiento formal para la atención y respuesta a solicitudes relacionadas con información estadística y geográfica; a través de este procedimiento se dejará constancia tanto de las solicitudes de información generadas por los particulares, como de las respuestas a las mismas, las cuales deben encontrarse debidamente fundadas y motivadas.

6.1.8 Evaluación del proceso.

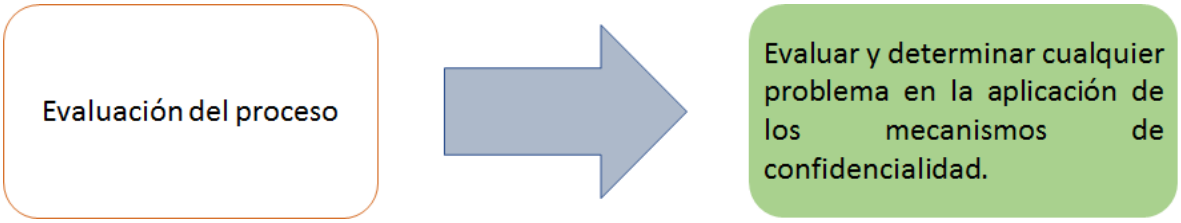

Figura 10

6.1.8.1 Evaluar y determinar cualquier problema en la aplicación de los mecanismos de confidencialidad.

a) Objetivo.

Detectar cualquier desviación en la generación y aplicación de los mecanismos de confidencialidad y protección de datos que deben instrumentar las Unidades o áreas productoras de información con motivo de la ejecución del proceso de producción de información estadística y geográfica.

b) Justificación y descripción.

Conforme al GSBPM esta fase implica evaluar el éxito de una instancia específica del proceso, tomando información cuantitativa y cualitativa e identificando y priorizando mejoras potenciales; de acuerdo con el artículo 35 fracción II de la Norma Técnica INEGI, en esta fase se considera dentro de las actividades analizar los insumos de evaluación y sintetizarlos en un reporte de evaluación, el cual debe resaltar cualquier problema que sea específico a este Proceso y debe identificar y priorizar las mejoras potenciales, así como emitir recomendaciones.

Dentro de la evaluación a realizarse debe encontrarse una revisión y análisis de la implementación de los mecanismos de confidencialidad y protección de datos, a fin de detectar posibles desviaciones, incluirlas en el reporte respectivo y, en su caso, generar las recomendaciones que resulten procedentes y realizar las correcciones que correspondan al proceso.

6.2 Mecanismos y pautas de carácter transversal.

A continuación se hace referencia a los mecanismos que con independencia de la ejecución del proceso de producción de información estadística y geográfica, así como de las fases que lo integran deben ser instrumentados en forma transversal, con el propósito de garantizar la confidencialidad y protección de los datos personales.

En la figura 11 se enlistan los mecanismos transversales que deben ser regulados e instrumentados para los efectos anteriores y posteriormente se realiza una descripción general de cada uno de ellos.

Figura 11; mecanismos de carácter transversal.

6.2.1 Definición de información Datos personales ¿Cuáles son? ¿Qué información debe ser considerada como confidencial?

a) Objetivo.

Tener claridad de cuáles son los datos personales que deben ser protegidos y que tienen el carácter de información confidencial.

b) Justificación y descripción.

Es imprescindible que se cuente con una definición conceptual de “datos personales” y que se conceptualicen a su vez los datos personales sensibles, con el propósito de que el personal que interviene en su tratamiento tenga claridad sobre cuál es la información a que deben aplicar las medidas de seguridad y confidencialidad establecidas.

la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados define datos personales como “*Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información*”.

El mismo ordenamiento conceptualiza datos sensibles como "*Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual*".

Ambos conceptos deben estar definidos en forma precisa en la normatividad del SNIEG para tener claridad respecto del ámbito material de aplicación de la normatividad que se emitan en materia de confidencialidad y protección de datos personales.

6.2.2 Inventario de los datos personales y de los sistemas de tratamiento

a) Objetivo.

Identificar la información básica de los datos personales; esto servirá para establecer y mantener las medidas de seguridad para la protección de los datos personales.

b) Justificación y descripción.

El inventario podría incluir lo siguiente, con el propósito de aportar elementos que coadyuven al establecimiento de las diversas medidas de seguridad de carácter general -es decir, aplicables a cualquier línea de producción- para la protección de los datos personales:

- Catálogo de medios físicos y electrónicos en que se obtienen los datos.
- Finalidades de cada tratamiento de datos.
- Catálogo de los distintos tipos de datos personales; identificando los sensibles[14].
- Formatos de almacenamiento y ubicación de los datos personales.
- Listado de servidores públicos con acceso a los datos y sistemas de tratamiento.
- Transferencias de datos personales y finalidades.
- Ciclo de vida de los datos:
    - Obtención.
    - Almacenamiento.
    - Uso.
    - Divulgación.
    - Bloqueo.
    - Cancelación, supresión o destrucción.

Los datos personales se pueden agrupar en las siguientes categorías:

- **Nivel estándar:** Esta categoría considera información de identificación, contacto, datos laborales y académicos de una persona física identificada o identificable, tal como: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo, experiencia laboral, datos de

[14] La Ley General de Protección de Datos Personales en posesión de sujetos obligados considera como datos sensibles los siguientes: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.

- **Nivel sensible:** Esta categoría contempla los datos que permiten conocer la ubicación física de la persona, tales como la dirección física e información relativa al tránsito de las personas dentro y fuera del país. También son datos de nivel sensible aquéllos que permitan inferir el patrimonio de una persona, que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores y fianzas. Incluye el número de tarjeta bancaria de crédito y/o débito. Son considerados también los datos de autenticación con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica y cualquier otro que permita autenticar a una persona.

  Dentro de esta categoría se toman en cuenta los datos jurídicos tales como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

  Finalmente, se contemplan los datos personales sensibles de la Ley, es decir, aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste; en esta categoría se encuentran los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

- **Nivel especial:** Esta categoría corresponde a los datos cuya naturaleza única, o bien debido a un cambio excepcional en el contexto de las operaciones usuales de la organización, pueden causar daño directo a los titulares, por ejemplo la Información adicional de tarjeta bancaria que considera el número de la tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido en la misma, por ejemplo fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN); probablemente en el caso de la información estadística no aplique esta categoría.

6.2.3 Análisis de brecha de medidas de seguridad.

a) **Objetivo**.

Contar con un análisis en el que se identifiquen las medidas de seguridad existente, así como aquellas que deberían establecerse.

b) Justificación y descripción.

La realización del análisis de brecha es indispensable con el objeto de establecer y mantener las medidas de seguridad de carácter general -aplicables a cualquier ciclo de producción- para la protección de los datos personales en la organización (o Unidad del Estado de que se trate).

Este análisis considera:

- Medidas de seguridad existentes.

- Medidas de seguridad existentes que operan correctamente.
- Medidas de seguridad faltantes.
- Nuevas medidas de seguridad que puedan reemplazar a uno o más controles implementados actualmente.

6.2.4 Análisis de riesgos.

a) Objetivo.

Realizar una identificación y análisis de los riesgos a que se encuentran expuestos los datos personales en la Unidad del Estado que corresponda, con el propósito de minimizar su impacto.

b) Justificación y descripción.

La seguridad se basa en el entendimiento de la naturaleza del riesgo al que están expuestos los datos personales, el riesgo no se puede erradicar completamente, pero sí se puede minimizar a través de la mejora continua.

La organización deberá determinar las características del riesgo que mayor impacto puede tener sobre los datos personales que tratan, con el fin de que prioricen y tomen la mejor decisión respecto a los controles más relevantes e inmediatos a implementar.

Este análisis deberá incluir:

- Identificación de Activos.-
- Identificación de amenazas.
- Identificación de vulnerabilidades.
- Identificar Escenarios de Vulneración y Consecuencias.

6.2.5 Manejo de incidentes de seguridad.

a) Objetivo.

Establecer acciones y actividades uniformes que deben realizarse ante una vulneración[15] en la seguridad de los datos personales.

b) Justificación y descripción.

El responsable de los datos personales en la organización deberá analizar las causas por las cuales se presentó la vulneración e implementar en un plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

El responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

Se deberá informar a la instancia que se determine de la Unidad del Estado, así como al titular de los datos personales el incidente ocurrido.

[15] La Ley General de Protección de Datos Personales en posesión de sujetos obligados, en su artículo 38 considera de las vulneraciones de la seguridad de los datos personales, al menos lo siguiente: I. La pérdida o destrucción no autorizada; II. El robo, extravío o copia no autorizada; III. El uso, acceso o tratamiento no autorizado, o IV. El daño, la alteración o modificación no autorizada.

6.2.6 Transferencia de datos personales.

a) Objetivo.

Establecer condiciones esenciales para que la transferencia de datos personales se realice en un marco de certidumbre y legalidad.

b) Justificación y descripción.

Respecto de las transferencias de datos personales que realicen las Unidades productoras de información, deberán observarse las siguientes condiciones:

- Toda transferencia deberá formalizarse mediante la suscripción de instrumentos contractuales, convenios de colaboración o cualquier otro instrumento jurídico.
- El receptor de los datos personales deberá tratar los datos personales, comprometiéndose a garantizar su confidencialidad y únicamente los utilizará para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad.
- El responsable de los datos personales deberá comunicar al receptor de los datos personales el aviso de privacidad conforme al cual se tratan los datos personales.
- El titular de los datos personales debe dar su consentimiento para la realización de la transferencia.

6.2.7 Mecanismos de destrucción y borrado seguro de información.

a) Objetivo.

Un elemento esencial en la protección y confidencialidad de los datos personales lo constituye el contar con mecanismos para destruir la información de manera segura, de tal manera que se garantice que los referidos datos no serán recuperados una vez que ha concluidos el plazo de conservación respectivo.

b) Justificación y descripción.

Cuando los datos personales han dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos.

Se debe asegurar que una vez que han concluido los plazos de conservación respectivos, los datos personales no podrán ser recuperados con fines no autorizados, por lo que es necesaria la implementación de mecanismos de borrado seguro de información tanto en medios físicos como electrónicos.

Se considera necesario dejar constancia de la aplicación de los referidos mecanismos, a través de actas, fotografías, reportes y certificados; algunos de los mecanismos para el borrado seguro de la información son los siguientes:

b.1 Medios de almacenamiento físico.

- Trituración.
- Incineración.
- Incineración.
- Uso de químicos.

b.2 Medios de almacenamiento electrónico.

- Destrucción.
- Desmagnetización.
- Sobre-escritura.

La Guía para el Borrado Seguro de Datos Personales, publicada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales establece algunas pautas que pueden ser consultadas como referencia para la definición de los mecanismos homogéneos para el borrado seguro de los datos personales; la referida Guía puede ser consultada en la siguiente liga electrónica: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf.

6.2.8 Instancia de supervisión y seguimiento.

a) Objetivo.

Establecer una instancia que cuente con facultades para realizar la supervisión y el seguimiento de los mecanismos establecidos para la confidencialidad y protección de los datos personales.

b) Justificación y descripción.

Se considera imprescindible que para la debida implementación de los mecanismos de confidencialidad y protección de los datos personales se cuente con una instancia facultada para llevar a cabo la supervisión y seguimiento respectivos y con ello asegurar su instrumentación.

La instancia que podría ejercer las funciones de supervisión y seguimiento es el Comité de Transparencia de cada Unidad del Estado; en el caso del INEGI, por lo que hace a la información derivada de su gestión administrativa, el referido Comité es el que realiza las funciones referidas.

Conforme al artículo 83 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, cada responsable contará con un Comité de Transparencia, el cual se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.

El artículo 84 fracción I de la Ley General mencionada establece como función del referido Comité coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable.

En ese sentido, tenemos que las funciones de dicho Comité son consistentes con las relativas a la supervisión y seguimiento de los mecanismos de confidencialidad y protección de datos personales que establezca el INEGI en su carácter de instancia normativa del SNIEG, en lo que respecta a la información estadística, por lo que a fin de evitar duplicidades de funciones y aprovechando las estructuras ya existentes, ese órgano colegiado podría realizar las acciones en cuestión.

6.2.9 Derechos ARCO.

a) Objetivo.

Garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales con que cuentan los titulares de dichos datos.

b) Justificación y descripción.

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, en su segundo párrafo establece que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición (Derechos ARCO), de tal manera que se trata de derechos de los que goza toda persona en el territorio nacional.

Como se ha advertido en este documento, todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos, de acuerdo con lo previsto en el artículo 1 constitucional, en su tercer párrafo.

En ese sentido, resulta imprescindible que el INEGI establezca los mecanismos tanto de carácter jurídico-normativo, como operativo para que se garantice el ejercicio de los aludidos derechos por parte los titulares de los datos personales que le son proporcionados, siempre con una debida armonización con respecto al enfoque que debe darse a dichos mecanismos, tratándose de datos que son utilizados para la realización de actividades estadísticas.

El marco jurídico mexicano regula el ejercicio de los derechos mencionados en la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados; dicho ordenamiento establece diversas previsiones para tales efectos, destacándose las siguientes en razón de que podrían ser consideradas en la definición de los mecanismos relativos en el SNIEG:

- En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen (Artículo 43).
- El titular tendrá derecho de acceder a sus datos personales que obren en posesión del
- responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento (Artículo 44).
- El titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados (Artículo 45).
- El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

Habrá que analizar la forma en que serán ejercidos los derechos de rectificación y cancelación, ya que si bien es cierto que se trata de derechos fundamentales que pueden ejercer los titulares de los datos personales, también lo es que en un contexto estadístico, dichos datos son captados para la producción de información estadística, por lo que se podrían afectar los resultados contenidos en los diversos programas estadísticos.

- El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:
    - Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular, y
    - 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 del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

Sobre estas previsiones relativas a la oposición al tratamiento de datos personales, es preciso comentar que de acuerdo con la LSNIEG en su artículo 37, los datos que proporcionen para fines estadísticos los Informantes del SNIEG son estrictamente confidenciales y bajo ninguna circunstancia pueden utilizarse para otro fin que no sea el estadístico.

Para el ejercicio de estos derechos resulta indispensable que se cuente con una ventanilla y un procedimiento para la presentación de las solicitudes por parte de los titulares de los datos personales; estos deberán estar señalados en el aviso de privacidad respectivo. Como parte del procedimiento aludido deberán indicarse los requisitos y el contenido que debe corresponder a las solicitudes que formulen los solicitantes de los datos.

Conforme al octavo párrafo del artículo 52 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia del responsable; en ese sentido, a fin de evitar duplicidad de funciones y a efecto de aprovechar las estructuras existentes en las Unidades del Estado, las Unidades de Transparencia respectivas podrían fungir como ventanillas para la presentación, seguimiento y atención para la gestión de las solicitudes aludidas.

6.2.10 Programa de Contingencia.

a) Objetivo.

Contar con un documento en el que se plantee la estrategia, el recurso humano de la Unidad del Estado, los activos y las actividades requeridas, para recuperar por completo o parcialmente un servicio o proceso relacionado con datos personales, en caso de presentarse un desastre o la materialización de un riesgo.

b) Justificación y descripción.

Ante la posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de Tecnologías de la Información y Comunicaciones, las infraestructuras de información y activos de información, incluyendo los datos personales de los informantes de la Unidad del Estado de que se trate, consideramos necesaria la generación de un Programa de Contingencia en el que se plantee la estrategia, el recurso humano de la Unidad del Estado, los activos y las actividades requeridas, para recuperar por completo o parcialmente los referidos activos e infraestructura.

7. Conclusiones y recomendaciones.

Derivado de los antecedentes regulatorios y prácticas nacionales e internacionales abordados en el presente análisis, así como de los riesgos que han sido identificados, se llega a las siguientes conclusiones y recomendaciones:

- El marco jurídico vigente del SNIEG tiene un alto nivel de abstracción y promueve la discrecionalidad, respecto de los mecanismos de confidencialidad y protección de datos personales.

- El marco normativo nacional e internacional ha evolucionado en forma significativa en los últimos años, en respuesta al creciente tratamiento de datod personales, con motivo de relaciones comerciales, sociales y de gobierno.
- Es conveniente establecer un marco de referencia para las Unidades del Estado, incluído el INEGI, que garantice la aplicación de mecanismos para salvaguardar la confidencialidad y la protección de los datos que son tratados con motivo de las actividades estadísticas y geográficas.
- Se propone evaluar la conveniencia de desarrollar las Reglas especificadas en el Art. 47 de la LSNIEG y demás normatividad que sea necesaria con el propósito de materializar el cumplimiento de los dispuesto en la LSNIEG en lo que respecta a la confidencialidad y reserva.

Anexo I; Marco normativo relativo a la confidencialidad y protección de datos en el SNIEG.

Conforme al artículo 37 de la LSNIEG, los datos que proporcionen para fines estadísticos los Informantes del Sistema a las Unidades, en términos de la presente Ley, serán estrictamente confidenciales y en ninguna circunstancia podrán utilizarse para otro fin que no sea el estadístico; el Instituto no deberá proporcionar a persona alguna, los datos a que se refiere este artículo para fines fiscales, judiciales, administrativos o de cualquier otra índole.

Por su parte, el artículo 38 dispone que los datos e informes que los Informantes del Sistema proporcionen para fines estadísticos y que provengan de registros administrativos, serán manejados observando los principios de confidencialidad y reserva, por lo que no podrán divulgarse en ningún caso en forma nominativa o individualizada, ni harán prueba ante autoridad judicial o administrativa, incluyendo la fiscal, en juicio o fuera de él.

El mismo numeral indica que cuando se deba divulgar la información, ésta deberá estar agregada de tal manera que no se pueda identificar a los Informantes del Sistema y, en general, a las personas físicas o morales objeto de la información; así también se menciona que el Instituto expedirá las normas que aseguren la correcta difusión y el acceso del público a la Información.

El Acuerdo por el que se aprueba la Norma Técnica para el acceso y publicación de Datos Abiertos de la Información Estadística y Geográfica de Interés Nacional, publicado en el Diario Oficial de la Federación el 4 de diciembre de 2014, en su artículo 7 regula la confidencialidad y reserva de los datos abiertos y establece que corresponderá a las Unidades del Estado garantizar que la Información que generen y sea publicada como Datos Abiertos, protejan la confidencialidad de la información y datos personales, en términos de lo dispuesto por la Ley del Sistema.

Conforme al mismo numeral, las Unidades del Estado deberán cumplir con el principio de máxima publicidad que establece el artículo 6o. Constitucional y las excepciones de reserva y confidencialidad establecidas en las leyes correspondientes; al hacer referencia a leyes correspondientes se entiende aquellos instrumentos legales aplicables a cada unidad del estado.

El artículo 46 de la LSNIEG establece la obligación de las Unidades de Estado, consistente en respetar la confidencialidad y reserva de los datos que para fines estadísticos proporcionen los Informantes del Sistema.

Por su parte el artículo 47 prevé que los datos que proporcionen los Informantes del Sistema, serán confidenciales en términos de esta Ley y de las reglas generales que conforme a ella dicte el Instituto.

Este último artículo, además de reiterar el carácter confidencial de los datos que proporcionen los Informantes del Sistema, otorga una potestad normativa al INEGI para emitir reglas generales en la materia (Confidencialidad de datos); al día de hoy, no se tiene evidencia de la emisión de alguna regla para regular la confidencialidad de los datos que proporcionen los informantes.

En su segundo párrafo, el numeral en cuestión señala que la Información no queda sujeta a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, sino que se dará a conocer y se conservará en los términos previstos en la presente Ley.

Dentro de los supuestos o causales que implica la excepción de observancia a la entonces Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, se destaca lo referente a las siguientes actividades:

- Dar a conocer la Información (Servicio Público de Información y solicitudes de información).
- Conservación de la Información (Acervo de Información).

No se omite mencionar que la referida excepción también aplica para los demás aspectos regulados en la Ley Federal abrogada, como es el caso de causales de información reservada y confidencial, cuotas de acceso, la sujeción al procedimiento de acceso a la información, por destacar algunos.

El artículo 102 fracción I de la LSNIEG indica que el Instituto no está obligado a proporcionar aquella información que tenga en virtud de cualquier disposición legal el carácter de confidencial, clasificada, reservada o de cualquier otra forma se encuentre restringida su difusión.

Derivado de este numeral, tenemos que la propia LSNIEG reconoce las regulaciones en materia de clasificación y reserva de la información de otros instrumentos legales específicos, al establecer la prohibición de proporcionar información que tenga las características mencionadas.

El artículo 104, fracción I de la LSNIEG prevé como infracción imputable a los servidores públicos del Instituto o a los servidores públicos de las Unidades la revelación de datos confidenciales; **aspecto que suma relevancia a la necesidad de establecer reglas claras que definan la forma y términos en que los servidores públicos mencionados cumplirán con los principios de confidencialidad y reserva de los datos e información que tienen bajo su posesión.**

Los Lineamientos de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Instituto Nacional de Estadística y Geografía, publicados en el Diario Oficial de la Federación el pasado 19 de abril de 2018, tienen por objeto *establecer criterios, procedimientos institucionales y responsabilidades de los servidores públicos y órganos colegiados del Instituto Nacional de Estadística y Geografía (Instituto) en materia de transparencia a efecto de garantizar el derecho de acceso a la información pública que posee el Instituto, de conformidad con la Ley General de Transparencia y Acceso a la Información Pública, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley Federal de Transparencia y Acceso a la Información Pública y demás disposiciones legales y normativas aplicables*.

Conforme al artículo 2, fracción XX de los citados Lineamientos, la información estadística y geográfica no se encuentra sujeta a la legislación en materia de transparencia y acceso a la información; en ese sentido, para efectos de la normatividad en cita, se considera información y queda sujeta a su ámbito de aplicación, aquella que corresponde a la gestión administrativa del Instituto.

Al respecto, es de destacar que al existir la excepción en cuestión, la información de carácter administrativo y en general, toda aquella con que cuente el Instituto, que no sea estadística o geográfica cuenta con mayores niveles de protección, pues a esta sí le aplican las disposiciones tendientes a garantizar su confidencialidad, integridad y disponibilidad.

Por otra parte, es de destacarse, que las Políticas para la Seguridad de la Información del INEGI (http://sc.inegi.org.mx/repositorioNormateca/Pod_17Dic14.pdf), en su numeral IV, apartado A, indican que todos los servidores públicos del Instituto son responsables de conservar y resguardar la Información que por razón de su empleo, cargo o comisión, tengan bajo su cuidado, sea Información estadística, geográfica o de la gestión administrativa, generada por el Instituto o entregada por

terceros; así mismo deben aplicar los mecanismos de protección establecidos por los responsables de los procesos y así como aquellos que se determinen en el marco del Sistema de Seguridad de la Información, para brindar la protección de la confidencialidad, integridad y disponibilidad de la Información.

En el apartado D del mismo numeral, se indica que para la protección de la Información estadística y geográfica corresponderá a cada Unidad Administrativa, en su ámbito de competencia, establecer mecanismos que garanticen de manera particular la confidencialidad de los datos personales de los informantes, en las actividades de captación, producción, actualización, organización, procesamiento, integración, compilación, publicación, divulgación, conservación y destrucción, en cumplimiento a lo previsto por la LSNIEG .

Anexo II; Marco jurídico mexicano relativo a la Protección de los datos personales y confidencialidad en el SNIEG.

II.1 Antecedentes constitucionales; la confidencialidad de la información como derecho fundamental.

Conforme a Decreto publicado en el Diario Oficial de la Federación el 20 de julio de 2007, la Constitución Política de los Estados Unidos Mexicanos, establece en su artículo 6, apartado A, fracción II, que *la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.*

Mediante publicación en el Diario Oficial de la Federación de fecha 1 de junio de 2009, se adiciona el segundo párrafo vigente al artículo 16 de nuestra Carta Magna, para establecer que ***Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos****, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros*.

El 7 de febrero de 2014 se publicó en el Diario Oficial de la Federación la reforma constitucional en la cuál se amplia el catálogo de sujetos obligados y se establece la creación de un organismo autónomo responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a **la protección de datos personales en posesión de los sujetos obligados** (http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_215_07feb14.pdf); hasta antes de esa reforma, la autoridad responsable en esa materia era un órgano de la Administración Pública Federal, el Instituto Federal de Acceso a la Información y Protección de Datos.

De esta forma, el derecho de acceso a la información y el de protección de los datos personales son derechos reconocidos en la Constitución Política de los Estados Unidos Mexicanos y en los tratados internacionales de la materia. En ese sentido, el artículo 1º, párrafo primero, de nuestra Carta Magna señala que: "*En los Estados Unidos Mexicanos* ***todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección****, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece*."

En relación con lo anterior, el mismo artículo 1º, en su tercer párrafo, establece que todas las autoridades del Estado, **en el ámbito de sus competencias**, **tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad**. En consecuencia, el Estado deberá **prevenir**, investigar, sancionar y reparar **las violaciones a los derechos humanos**, en los términos que establezca la ley.

Respecto de esta obligación constitucional relacionada con la protección de los derechos humanos, la Primera Sala de la Suprema Corte de Justicia de la Nación, en la tesis de jurisprudencia 1a./J. 85/2017 (10a.), ha establecido que el principio de progresividad al que se alude en el artículo 1º de la Constitución "*…ordena ampliar el alcance y la protección de los derechos humanos en la mayor medida posible* ***hasta lograr su plena efectividad****, de acuerdo con las circunstancias fácticas y jurídicas*." Asimismo, en dicha tesis se señala que, en el caso de las autoridades que, como el INEGI,

cuentan con atribuciones para la crear normas y aplicarlas, se traduce en "…*la **obligación de ampliar el alcance y la tutela de los derechos humanos**; y para el aplicador, el deber de interpretar las normas de manera que se amplíen, en lo posible jurídicamente, esos aspectos de los derechos.*"

A mayor abundamiento, el Poder Judicial de la Federación ha establecido, mediante la tesis de jurisprudencia Tesis: XXVII.3o. J/25 (10a.), que:

> *El párrafo tercero del artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos dispone como obligaciones generales de las autoridades del Estado Mexicano las consistentes en: i) Respetar; ii) Proteger; iii) Garantizar; y, iv) Promover los derechos humanos, de conformidad con los principios rectores de universalidad, interdependencia, indivisibilidad y progresividad.* ***De ahí que para determinar si una conducta específica de la autoridad importa violación a derechos fundamentales, debe evaluarse si se apega o no a la obligación de protegerlos. Ésta puede caracterizarse como el deber que tienen los órganos del Estado, dentro del margen de sus atribuciones, de prevenir violaciones a los derechos fundamentales, ya sea que provengan de una autoridad o de algún particular y, por ello, debe contarse tanto con mecanismos de vigilancia como de reacción ante el riesgo de vulneración del derecho, de forma que se impida la consumación de la violación.*** *En este último sentido, su cumplimiento es inmediatamente exigible, ya que como la conducta estatal debe encaminarse a resguardar a las personas de las interferencias a sus derechos provenientes de los propios agentes del Estado como de otros particulares, este fin se logra, en principio, mediante la actividad legislativa y de vigilancia en su cumplimiento y, si esto es insuficiente, mediante las acciones necesarias para impedir la consumación de la violación a los derechos.* ***De ahí que, una vez conocido el riesgo de vulneración a un derecho humano, el Estado incumple su obligación si no realiza acción alguna, sobre todo, porque, en el caso de sus propios agentes, está obligado a saber todo lo que hacen****.*

II.2 Legislación.

La LSNIEG, publicada en el Diario Oficial de la Federación (DOF) el 16 de abril de 2008 protege los datos y la información que proporcionen los informantes del Sistema, así como de las personas físicas y morales objeto de información, impidiéndose la divulgación nominativa e individualizada.

Así también, en la LSNIEG, específicamente en su artículo 47, se estableció originalmente una excepción a la aplicación de la entonces Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), publicada en el DOF el 11 de junio de 2002 (http://www.diputados.gob.mx/LeyesBiblio/abro/lftaipg/LFTAIPG_abro.pdf), ordenamiento que fue abrogado por la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), publicada en el DOF el 9 de mayo de 2016 (http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf)[16].

[16] La LFTAIP (Vigente), deriva de la publicación en el Diario Oficial de la Federación el 4 de mayo de 2015 de la Ley General de Transparencia y Acceso a la Información Pública; la cuál tiene dentro de sus objetivos distribuir competencias entre los Organismos garantes de la Federación y las Entidades Federativas, en materia de transparencia y acceso a la información, así como establecer las bases mínimas que regirán los procedimientos para garantizar el ejercicio del derecho de acceso a la información y regular el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; esta Ley General, en su artículo 68 prevé algunas pautas generales que deberán ser observadas por los sujetos obligados, con motivo de los datos personales que tienen en posesión.

La LFTAIPG (Abrogada), tenía como finalidad proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal; estableció como autoridad en la materia al Instituto Federal de Acceso a la Información y Protección de Datos, el cuál era un órgano de la Administración Pública Federal.

Entre otros aspectos, dicho ordenamiento reguló lo siguiente:

- Obligación de los sujetos obligados de publicar cierta información.
- Supuestos para la clasificación de información reservada.
- Supuestos para la clasificación de información confidencial.
- Plazos de reserva.
- Protección de datos personales; para lo cual se destinaron siete artículos de la Ley (del 20 al 26), con un considerable nivel de abstracción, ya que se incluyeron algunas obligaciones a cargo de los sujetos obligados, sin que se abundara en la forma o mecanismos en que estas debían ser observadas; a los datos personales se les dio la categoría de información confidencial.
- Unidades de enlace y Comités de Información.
- Procedimiento para el acceso a la información: cabe destacar que se consideró, en el caso de los órganos constitucionales autónomos -entre otros-, que estos establecieran mediante reglamentos o acuerdos de carácter general, los órganos, criterios y procedimientos institucionales para proporcionar a los particulares el acceso a la información.
- Recurso de revisión para el caso de negativa a solicitud de acceso a la información.

La LFTAIP (vigente), tiene por objeto proveer lo necesario en el ámbito federal, para garantizar el derecho de acceso a la Información Pública en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos federales o realice actos de autoridad.

Dentro de sus objetivos tenemos proveer lo necesario para que todo solicitante pueda tener acceso a la información, mediante procedimientos sencillos y expeditos; transparentar la gestión pública mediante la difusión de la información oportuna, verificable, inteligible, relevante e integral y consolidar la apertura de las instituciones del Estado mexicano, mediante iniciativas de gobierno abierto.

La LFTAIP reitera el carácter autónomo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI); lo cuál es un aspecto medular, ya que anteriormente el IFAI tenía el carácter de órgano de la Administración Pública Federal; ello implicaba un sesgo considerable respecto de su competencia, con relación con los órganos constitucionales autónomos, así como otros sujetos obligados como es el caso del Poder Judicial de la Federación.

Dentro de los aspectos que son regulados por el ordenamiento jurídico en cuestión, se destacan los siguientes:

- Obligaciones de los sujetos obligados, dentro de las que se destaca la protección y resguardo de la información clasificada como reservada y confidencial, así como la de publicar cierta información.
- Se prevé la obligación de publicar información particular o específica por parte de los órganos constitucionales autónomos, incluyendo al INEGI, de la cuál se destaca los programas estratégico, nacional y anual de estadística y geografía, así como las clasificaciones, catálogos y cuestionarios y las metodologías, documentos técnicos y proyectos estadísticos.
- Clasificación de la información (Procedimiento)[17].
- Supuestos para la clasificación de información reservada.
- Supuestos para la clasificación de información confidencial[18].
- Plazos de reserva.
- Unidades de Transparencia y Comités de Transparencia.
- Información confidencial; supuestos en que no es necesario el consentimiento de los particulares para permitir el acceso a información confidencial; por ejemplo, cuando se transmite entre sujetos obligados.
- Versiones públicas[19].
- Procedimiento para el acceso a la información.
- Recurso de revisión para el caso de negativa a solicitud de acceso a la información.

Es importante apuntar, que la LFTAIP (Vigente), ya no destina un capitulado específico a la protección de datos personales, como sí lo hacía la LFTAIPG (Abrogada), únicamente se reitera la obligación de los sujetos obligados de proteger los datos personales (Artículo 9) y se considera a dichos datos como información confidencial (Artículo 113 fracción I).

El 26 de enero de 2017 se publicó en el DOF la Ley General de Protección de Datos Personales en posesión de los sujetos obligados; en la exposición de motivos del referido ordenamiento legal, se establece lo siguiente:

> *"… una ley general de protección de datos personales para el ámbito público, que desarrolle sustantivamente este derecho a partir de los principios, deberes y derechos que internacionalmente han sido reconocidos, de manera que* ***la protección de datos personales se vea emancipada del derecho de acceso a la información****, y en ese sentido deje de visualizársele como un accesorio de ese derecho. A partir de esta consideración,* ***el derecho a la protección de datos deberá considerarse en un esquema de igualdad con el acceso a la información y el resto de los derechos fundamentales que establece nuestra Carta Magna****."*

[17] Se entiende por clasificación de la información el proceso mediante el cual el sujeto obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad que prevé la Ley (Art. 97 LFTAIP)

[18] Se considera información confidencial, aquella que contiene datos personales concernientes a una persona física identificada o identificable (Art. 113 fracción I de la LFTAIP).

[19] Cuando un documento o expediente contenga partes o secciones reservadas o confidenciales, los sujetos obligados a través de sus áreas, para efectos de atender una solicitud de información, deberán elaborar una versión pública en la que se testen las partes o secciones clasificadas, indicando su contenido de manera genérica, fundando y motivando su clasificación (Artículo 118 de la LFTAIP).

Con dicho ordenamiento se desvincula la materia de protección de datos personales del derecho de acceso a la información, regulado por la Ley Federal de Transparencia y Acceso a la Información Pública.

Se destacan las siguientes regulaciones incorporadas en la Ley General de referencia:

- Bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.
- Aviso de privacidad.
- Tratamiento de datos personales: obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia.
- Consentimiento de los titulares para el tratamiento de sus datos personales.
- Medidas de seguridad para la protección de los datos personales:
    - Administrativas.
    - Físicas.
    - Técnicas.
- Documento de seguridad:
    - Inventario de datos personales y sistemas de tratamiento.
    - Funciones y obligaciones de las personas que traten datos personales.
    - Análisis de riesgos.
    - Análisis de brecha.
    - Plan de trabajo.
    - Monitoreo y revisión de medidas de seguridad.
    - Capacitación.
- Derechos de Acceso, Rectificación, Cancelación y Oposición (Derechos ARCO).
- Encargado (o tercero) que realiza el tratamiento de datos personales por nombre y cuenta del responsable.
- Evaluación de impacto de datos personales.
- Transferencias y Remisiones de Datos Personales.
- Acciones preventivas en materia de protección de datos personales.
- Tratamiento intensivo o relevante de datos personales.
    - Riesgos inherentes a los datos personales a tratar.
    - Se traten datos personales sensibles.
    - Se efectúen o pretendan efectuar transferencias de datos personales.
- Comité de transparencia como instancia de coordinación y supervisión; este se encarga entre otras cosas, 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 ARCO, así como dar vista al Órgano Interno respectivo sobre probables irregularidades en el tratamiento de datos personales.
- Unidad de Transparencia; tiene dentro de sus facultades la gestión de las solicitudes para el ejercicio de los derechos ARCO, así como auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, como órgano garante de la federación en materia de protección de datos personales; tiene dentro de sus facultades garantizar el ejercicio del derecho a la protección

de datos personales en posesión de sujetos obligados; interpretar la Ley General en el ámbito administrativo; conocer y resolver los recursos de revisión que interpongan los titulares, y vigilar y verificar el cumplimiento de las disposiciones contenidas en la Ley.

- Recursos de Revisión y Recursos de Inconformidad.

Como conclusión de este apartado, y en razón de los expuesto, pese a una excepción, prevista en la Ley del SNIEG respecto a la aplicación normatividad existente al momento de su expedición (Abril 2008) en materia de transparencia, el marco normativo ha evolucionado considerablemente, a partir de la expedición de dos Leyes Generales, reguladoras por un lado de la transparencia y acceso a la información pública y por el otro de la protección de datos personales.

II.3 Disposiciones administrativas.

El INAI como instancia normativa en ambas materias (transparencia y acceso a la información pública y protección de datos personales), con la especialización técnica correspondiente, ha emitido múltiple normatividad, guías y demás documentos de apoyo para la debida aplicación de los criterios y controles necesarios a fin de proteger la información personal o confidencial en posesión de las instituciones públicas.

Tal es el caso de los siguientes instrumentos (Normativos y no normativos), que consideramos incorporan aspectos que deberíamos considerar en el manejo de los datos personales que proporcionan los informantes del SNIEG:

A) En materia de datos personales:

- Lineamientos Generales de Protección de Datos Personales para el Sector Público (D.O.F. 26-I-2018); http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf .
- Recomendaciones para el manejo de incidentes de seguridad de datos personales (http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf).
- Recomendaciones sobre protección de datos personales contenidos en la Credencial para Votar (http://inicio.inai.org.mx/DocumentosdeInteres/RecomendacionesCredencialV.pdf).
- Guía para el borrado seguro de datos personales (http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf).

B) En materia de acceso a la información:

- Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas (D.O.F. 15-IV-2016); http://www.dof.gob.mx/nota_detalle.php?codigo=5433280&fecha=15/04/2016.

Mediante los Lineamientos Generales de Protección de Datos Personales para el Sector Público, enlistados en el apartado A que antecede, el órgano garante de la Federación (INAI) desarrolla las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados en lo relativo al ámbito Federal y son aplicables a cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, entre otros.

Entre otros aspectos, se particulariza y detalla el contenido de la Ley General de la materia y se regulan aspectos específicos en lo que respecta a lo siguiente:

- Consentimiento otorgado por el titular de datos personales.
- Supresión de datos personales.
- Características, difusión y consulta del aviso de privacidad.
- Mecanismos y medios para el ejercicio de los derechos ARCO.
- Deber de seguridad.
- Inventario de datos personales.
- Ciclo de vida de los datos personales.
- Análisis de riesgos.
- Análisis de brecha; entre las medidas de seguridad existentes y las faltantes.
- Monitoreo y supervisión.
- Vulneraciones de seguridad.
- Inexistencia de los datos personales.
- Relación entre el responsable de los datos personales y el encargado (o tercero en el tratamiento).
- Transferencias de datos personales.
- Acciones preventivas.
- Medios de impugnación.
- Verificación por parte del Instituto e investigaciones sobre probables incumplimientos.
- Auditorías voluntarias.

Por lo que hace a las recomendaciones sobre el manejo de seguridad de datos personales y las relativas al borrado seguro de dichos datos, constituyen buenas prácticas emitidas por un ente especializado técnicamente en la materia y que pueden ser observadas por las Unidades del Estado de manera voluntaria u obligatoria sí así lo determinara el Instituto en el ejercicio de sus facultades normativas, relacionadas con la información estadística y geográfica.

Anexo III; Consideraciones a partir de la controversia constitucional interpuesta por el INEGI

Los argumentos jurídicos que se han hecho valer en la demanda de controversia constitucional interpuesta por el INEGI, en contra del Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI) esencialmente consisten en lo siguiente:

- Se ha presentado una invasión de competencias del INEGI por parte del INAI, en relación con la resolución de un recurso de revisión presentado por un particular, con motivo de una solicitud de acceso a la información.
- No hay disposición alguna que le otorgue al INAI competencia en materia de información estadística o geográfica.
- El INEGI es el órgano constitucional autónomo con facultades en materia de información estadística y geográfica, mientras que en el caso del INAI, su ámbito de competencia comprende toda la información pública.
- Lo relativo a la información estadística y geográfica, es competencia exclusiva del INEGI, con exclusión de otros órganos del Estado mexicano, como el INAI.
- El artículo 47 de la Ley del Sistema, subsiste hoy en día ya que sigue respondiendo al marco constitucional aplicable, por el cual se responsabiliza al INEGI de la información estadística y geográfica, por lo cual es el único facultado por la CPEUM en materia de estadística y geografía.
- Es claro que el principio de confidencialidad del INEGI se encuentra establecido expresamente en la Ley del Sistema justamente para respetar los derechos de sus informantes, situación que pone en riesgo el INAI, al pretender conocer sobre la Información Estadística y Geográfica, pues invade la competencia del INEGI en el tratamiento de la Información Estadística y Geográfica que este Instituto clasifica como confidencial y/o reservada.

Sobre este último punto surgen el cuestionamiento ¿Cómo se debe clasificar la información?, toda vez que no se ha emitido normatividad sobre ese particular.

Con independencia de la falta de competencia por parte del INAI que se ha argumentado con respecto de la información estadística y geográfica, el Instituto, por conducto de la Junta de Gobierno, en nuestra consideración debe tomar las determinaciones que resultan necesarias y pertinentes a fin de garantizar la protección de la información confidencial, relacionada con la IIN, para garantizar el cumplimiento y observancia de la prerrogativa constitucional de todo ciudadano, consistente en la protección de sus datos personales.

Derivado de lo expuesto, resulta necesaria la definición de criterios normativos respecto de la forma y términos en que se cumplirá con la confidencialidad de la información proporcionada por los informantes y aquella de personas físicas y morales, a fin de determinar la normatividad que deben seguir las unidades del Estado para cumplir con sus obligaciones de confidencialidad.

Anexo IV; Cuestionamientos que surgen a partir del marco jurídico existente en materia de confidencialidad y protección de datos.

Derivado de las consideraciones de hecho y de derecho expuestas en el presente análisis, así como de la evolución que ha tenido el marco normativo en materia de confidencialidad y protección de datos personales, así como de acceso a la información, podrían surgir los siguientes cuestionamientos por parte de las Unidades del Estado:

- *¿Las previsiones de la LSNIEG son suficientes para garantizar la observancia del derecho de protección de datos personales proporcionados por los informantes del SNIEG?*
- *¿Cuáles serían los mecanismos y métodos para proteger los datos personales referidos?*
- *¿Pese a que la protección de datos personales ha sido emancipada del derecho de acceso a la información, la excepción prevista en el artículo 47 de la LSNIEG, continúa siendo aplicable, pese a que esta se refiere en forma exclusiva a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental?*
- *¿Cuál es el procedimiento con el que cuentan los particulares para acceder a la información estadística y geográfica o generar solicitudes de acceso?*
- *¿Qué se entiende por información confidencial para efectos del SNIEG?*
- *¿Cuál es el procedimiento que deben seguir las Unidades del Estado para clasificar la información confidencial?*
- *¿Cuál es la unidad o área responsable encargada de coordinar la aplicación y observancia de los principios de confidencialidad y reserva previstos en la LSNIEG, así como de la normatividad que se emita?*
- *¿Cuáles son los mecanismos que deben observarse para que el Presidente y las Direcciones Generales del INEGI cumplan con la siguiente atribución, establecida en diversos numerales del Reglamento Interior del INEGI:*
    - *Guardar los principios de confidencialidad y reserva que la Ley establece respecto de los datos que los informantes del Sistema proporcionen para fines estadísticos al Instituto, así como, respecto de la información de carácter confidencial que provenga de registros administrativos de las Unidades del Estado*
- *¿Es jurídicamente viable la transmisión de información confidencial sin el consentimiento de su titular entre unidades del Estado o entre unidades administrativas? ¿Cuál es el sustento?*
- *¿Qué pasa sí un documento o base de datos contiene información pública e información confidencial? ¿Existe el sustento para la generación de versiones públicas?*
- *¿Qué medidas de seguridad deben seguir las unidades responsables de datos personales proporcionados por informantes del SNIEG? ¿Dónde están reguladas?*
- *¿Cómo garantizo el cumplimiento y observancia de los derechos ARCO?*

Anexo V; Modelo Tipo de Aviso de Privacidad.

Nota preliminar: Este modelo tipo deberá ser adaptado al contexto del SNIEG y deberán preservarse únicamente los contenidos que resulten aplicables.

AVISO DE PRIVACIDAD

[*Nombre completo del responsable si se trata de una persona física, o denominación o razón social en caso de ser una persona moral. En su caso, se sugiere incluir el nombre comercial*], con domicilio en [*indicar calle, número, colonia, ciudad, municipio o delegación, código postal y entidad federativa del domicilio para oír y recibir notificaciones*], es el responsable del uso y protección de sus datos personales, y al respecto le informamos lo siguiente:

¿Para qué fines utilizaremos sus datos personales?

Los datos personales que recabamos de usted, los utilizaremos para las siguientes finalidades que son necesarias para el servicio que solicita:

- Finalidad principal A
- Finalidad principal B
- Finalidad principal C

De manera adicional, utilizaremos su información personal para las siguientes finalidades que no son necesarias para el servicio solicitado, pero que nos permiten y facilitan brindarle una mejor atención:

- Finalidad secundaria A
- Finalidad secundaria B

En caso de que no desee que sus datos personales sean tratados para estos fines adicionales, desde este momento usted nos puede comunicar lo anterior, [*descripción del mecanismo que tenga implementado el responsable. Nota, el mecanismo de que se trate deberá permitir al titular negar su consentimiento previo a que sus datos personales sean tratados para estas finalidades]*.

La negativa para el uso de sus datos personales para estas finalidades no podrá ser un motivo para que le neguemos los servicios y productos que solicita o contrata con nosotros.

¿Qué datos personales utilizaremos para estos fines?

Para llevar a cabo las finalidades descritas en el presente aviso de privacidad, utilizaremos los siguientes datos personales: [*listado de datos personales o sus categorías. Para ejemplos de categorías ver el Glosario*].

Además de los datos personales mencionados anteriormente, para las finalidades informadas en el presente aviso de privacidad utilizaremos los siguientes datos personales considerados como sensibles, que requieren de especial protección: [*listado de datos personales sensibles o sus categorías. Para ejemplo de categorías ver el Glosario*].

¿Con quién compartimos su información personal y para qué fines?

Le informamos que sus datos personales son compartidos dentro y fuera del país con las siguientes personas, empresas, organizaciones y autoridades distintas a nosotros, para los siguientes fines:

Destinatario de los datos personales	País (opcional)	Finalidad
Nombre del tercero receptor o sector al que pertenece		Descripción de la finalidad
Nombre del tercero receptor o sector al que pertenece		Descripción de la finalidad*
Nombre del tercero receptor o sector al que pertenece		Descripción de la finalidad*

Le informamos que para las transferencias indicadas con un asterisco (*) requerimos obtener su consentimiento. Si usted no manifiesta su negativa para dichas transferencias, entenderemos que nos lo ha otorgado [*Ésto sólo aplica para consentimiento tácito*].

No autorizo que mis datos personales sean compartidos con los siguientes terceros *[NOTA, este ejemplo de cláusula corresponde a un consentimiento tácito. Para ejemplos de cláusulas en las que se requiera el consentimiento expreso y expreso y por escrito ver numeral 7 de la sección III*]:

[Transferencia 1].

[Transferencia 2].

¿Cómo puede acceder, rectificar o cancelar sus datos personales, u oponerse a su uso?

Usted tiene derecho a conocer qué datos personales tenemos de usted, para qué los utilizamos y las condiciones del uso que les damos (Acceso). Asimismo, es su derecho solicitar la corrección de su información personal en caso de que esté desactualizada, sea inexacta o incompleta (Rectificación); que la eliminemos de nuestros registros o bases de datos cuando considere que la misma no está siendo utilizada conforme a los principios, deberes y obligaciones previstas en la normativa

(Cancelación); así como oponerse al uso de sus datos personales para fines específicos (Oposición). Estos derechos se conocen como derechos ARCO.

Para el ejercicio de cualquiera de los derechos ARCO, usted deberá presentar la solicitud respectiva en [*Describir los medios*].

Para conocer el procedimiento y requisitos para el ejercicio de los derechos ARCO, usted podrá llamar al siguiente número telefónico [...]; ingresar a nuestro sitio de Internet [...] a la sección [...], o bien ponerse en contacto con nuestro Departamento de Privacidad, que dará trámite a las solicitudes para el ejercicio de estos derechos, y atenderá cualquier duda que pudiera tener respecto al tratamiento de su información. Los datos de contacto del Departamento de Privacidad son los siguientes:

[Domicilio, teléfono, correo electrónico del departamento de datos o de la persona].

¿Cómo puede revocar su consentimiento para el uso de sus datos personales?

Usted puede revocar el consentimiento que, en su caso, nos haya otorgado para el tratamiento de sus datos personales. Sin embargo, es importante que tenga en cuenta que no en todos los casos podremos atender su solicitud o concluir el uso de forma inmediata, ya que es posible que por alguna obligación legal requiramos seguir tratando sus datos personales. Asimismo, usted deberá considerar que para ciertos fines, la revocación de su consentimiento implicará que no le podamos seguir prestando el servicio que nos solicitó, o la conclusión de su relación con nosotros.

Para revocar su consentimiento deberá presentar su solicitud en [Describir los medios].

Para conocer el procedimiento y requisitos para la revocación del consentimiento, usted podrá llamar al siguiente número telefónico [...]; ingresar a nuestro sitio de Internet [...] a la sección [...], o bien ponerse en contacto con nuestro Departamento de Privacidad.

¿Cómo puede limitar el uso o divulgación de su información personal?

Le informamos que en nuestra página de Internet utilizamos cookies, web beacons y otras tecnologías a través de las cuales es posible monitorear su comportamiento como usuario de Internet, así como brindarle un mejor servicio y experiencia de usuario al navegar en nuestra página.

Los datos personales que obtenemos de estas tecnologías de rastreo son los siguientes: [*descripción de datos personales*], mismos que utilizamos para [*descripción de finalidades*]. Asimismo, le informamos que compartiremos estos datos con:

Destinatario de los datos personales	País (opcional)	Finalidad

Nombre del tercero receptor o sector al que pertenece		Descripción de la finalidad
Nombre del tercero receptor o sector al que pertenece		Descripción de la finalidad
Nombre del tercero receptor o sector al que pertenece		Descripción de la finalidad

Estas tecnologías podrán deshabilitarse siguiendo los siguientes pasos: [*descripción del procedimiento*].

Para mayor información sobre el uso de estas tecnologías, puede consultar el sitio de Internet [...]

¿Cómo puede conocer los cambios a este aviso de privacidad?

El presente aviso de privacidad puede sufrir modificaciones, cambios o actualizaciones derivadas de nuevos requerimientos legales; de nuestras propias necesidades por los productos o servicios que ofrecemos; de nuestras prácticas de privacidad; de cambios en nuestro modelo de negocio, o por otras causas.

Nos comprometemos a mantenerlo informado sobre los cambios que pueda sufrir el presente aviso de privacidad, a través de [descripción del medio].

El procedimiento a través del cual se llevarán a cabo las notificaciones sobre cambios o actualizaciones al presente aviso de privacidad es el siguiente: [descripción del procedimiento].

Última actualización [día/mes/año].

Anexo VI; Definición de términos.

En el presente Anexo se incorpora la definición conceptual de las principales expresiones que son empleadas en el documento de análisis, lo cual posibilita una utilización uniforme y entendimiento estandarizados de las mismas.

Activo de información:

Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Fuente: Disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información , así como el Manual de Aplicación General en dichas materias.

Amenaza:

A cualquier posible acto que pueda causar algún tipo de daño a los activos de información de la Institución.

Fuente: Disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información , así como el Manual de Aplicación General en dichas materias.

Análisis de riesgos:

El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a las infraestructuras de información esenciales y/o críticas o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Fuente: Disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información , así como el Manual de Aplicación General en dichas materias.

Anonimizar:

A) Expresar un dato relativo a entidades o personas, eliminando la referencia a su identidad.
B) Resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación. En este proceso, los responsables del tratamiento deben considerar distintos aspectos y valorar todos los medios que puedan utilizarse «razonablemente» para la identificación de los datos (ya sea por el responsable del tratamiento o por terceros); estudios y legislaciones posteriores le han dado el carácter irreversible al término “Disociación”.

Fuente: A) Real Academia de la Lengua Española; B) Dictamen 05/2014 sobre técnicas de anonimización; adoptado en abril de 2014 por el Grupo de Trabajo del Parlamento Europeo sobre protección de las personas

Aviso de privacidad:

Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos

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

Bases 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.

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

Borrado Seguro:

Proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital.

Fuente: Disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información , así como el Manual de Aplicación General en dichas materias.

Confidencialidad:

A) Que se hace o se dice en la confianza de que se mantendrá la reserva de lo hecho o lo dicho; por excelencia, tienen estos carácter aquellos datos que se refieren a la esfera íntima o privada de las personas.
B) En el ámbito específico de Seguridad de la Información se le define como "*Atributo de Seguridad de la Información que indica que la información sólo es revelada a individuos autorizados*".

Fuente: A) Real Academia de la Lengua Española y Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; B) Disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información , así como el Manual de Aplicación General en dichas materias.

Consentimiento:

Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

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

Cyber seguridad

Es la disciplina encargada de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable, enfocada en la protección de la infraestructura computacional, especialmente la información contenida a través de las redes.

Datos personales:

Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

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

Datos personales sensibles:

Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

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

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

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

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

Disociación:

El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo; algunos autores y legislaciones, como es el caso de la española le dan el carácter de absolutamente irreversible.

Fuente: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; https://gahazas.com/tag/disociar/; la legislación europera emplea la expresión anonimización.

Disponibilidad:

Atributo de Seguridad de la Información que consiste en que la información puede ser accedida por el personal cuando éste lo requiere.

Fuente: Políticas de Seguridad de la Información del INEGI.

Incidente de Seguridad de la Información:

Hecho que sucede de manera inesperada, materializando un riesgo que afecta a la Seguridad de la Información;

Fuente: Políticas de Seguridad de la Información del INEGI.

Infraestructura de TIC:

El hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC.

Fuente: Disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información , así como el Manual de Aplicación General en dichas materias.

Integridad:

Atributo de Seguridad de la Información referente a que la información está completa y sin alteraciones.

Fuente: Políticas de Seguridad de la Información del INEGI.

Medidas de seguridad:

Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

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

Medidas de seguridad administrativas:

Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

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

Medidas de seguridad físicas:

Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

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

Medidas de seguridad técnicas:

Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

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

Riesgo de Seguridad de la Información:

Es el efecto de la incertidumbre respecto al mantenimiento de la Seguridad de la Información; .

Fuente: Políticas de Seguridad de la Información del INEGI.

Seguridad de la Información:

Capacidad de preservar la confidencialidad, Integridad y disponibilidad de la Información a partir de la implementación de medidas técnicas y organizativas.
Fuente: Políticas de Seguridad de la Información del INEGI y Disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información , así como el Manual de Aplicación General en dichas materias.

Sistema informático:

El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

Fuente: Disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información , así como el Manual de Aplicación General en dichas materias.

Tratamiento:

Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

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

Vulnerabilidades:

Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a las infraestructuras de información esenciales y/o críticas, así como a los activos de información.

Fuente: Disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información , así como el Manual de Aplicación General en dichas materias.