



**INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN
EN TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIÓN**

**DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS**

**“PROPUESTA DE LÍNEAS GENERALES DE
ACCIÓN PARA PRESERVAR LA
CONFIDENCIALIDAD DE LA INFORMACIÓN
ESTADÍSTICA Y GEOGRÁFICA A TRAVÉS
DEL CIFRADO Y ANONIMIZACIÓN”**

PROPUESTA DE INTERVENCIÓN
Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS
DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Luis Martín Clemente Aréchiga

Asesor:

Mtra. Evelyn Téllez Carvajal

Ciudad de México, a 25 de octubre de 2019.



AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA
MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y
COMUNICACIÓN

Ciudad de México, 25 de octubre de 2019
INFOTEC-DAIC-GCH-SE-0329/19.

La Gerencia de Capital Humano / Gerencia de Investigación hacen constar que el trabajo de titulación intitulado

PROPUESTA DE LÍNEAS GENERALES DE ACCIÓN PARA PRESERVAR LA
CONFIDENCIALIDAD DE LA INFORMACIÓN ESTADÍSTICA Y GEOGRÁFICA A
TRAVÉS DEL CIFRADO Y ANONIMIZACIÓN

Desarrollado por el alumno **Luis Martín Clemente Aréchiga** y bajo la asesoría de la **Mtra. Evelyn Téllez Carvajal**; cumple con el formato de biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Asimismo se hace constar que no debe material de la biblioteca de INFOTEC.

Vo. Bo.


Mtra. Julieta Alcibar Hermsillo
Coordinadora de biblioteca

***Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.**

Agradecimientos

A Dios por su infinita bondad y misericordia.

A mi familia por su apoyo incondicional.

A la maestra Evelyn Telléz Carvajal por su guía, paciencia y dirección para lograr concluir este proyecto.

A las autoridades de INFOTEC que me otorgaron su confianza para incorporarme en la maestría.

A mis compañeras y compañeros que compartieron este proyecto y sus conocimientos.

Tabla de contenido

Introducción.....	1
Capítulo 1: Marco contextual y conceptual de la información estadística y geográfica y la confidencialidad	4
1.1 La captación de información estadística y geográfica.....	5
1.1.1 Antecedentes de la captación de la información estadística y geográfica	5
1.1.2 Evolución de la captación de la información estadística y geográfica en México.....	7
1.2 Propuesta de intervención.....	10
1.2.1 Diagnóstico	11
1.2.2 Planteamiento de la propuesta.....	15
1.3 El Sistema Nacional de Información Estadística y Geográfica (SNIEG) 16	16
1.3.1 Conformación del SNIEG	18
1.3.2 El INEGI como coordinador del SNIEG	19
1.4 La información en el INEGI	19
1.4.1 Tipos de información en el INEGI.....	20
1.4.2 Conceptos básicos sobre información.....	22
1.4.3 Importancia de la información estadística y geográfica.....	25
1.5 El proceso estadístico y geográfico.....	26
1.5.1 Los informantes del Sistema, las actividades estadísticas y geográficas y el programa de información.....	26
1.5.2 Objetivos de las fases del proceso estadístico y geográfico	27
1.6 La confidencialidad de la información estadística y geográfica	30
1.6.1 La privacidad y la confidencialidad.....	30
1.6.2 Los principios estadísticos de confidencialidad.....	31
1.6.3 El control de la divulgación indebida	32
1.6.4 La anonimización y el cifrado	34
Capítulo 2: Referencias del marco regulatorio internacional y mexicano sobre la confidencialidad de la información.....	37
2.1 Referencias del marco regulatorio internacional sobre la confidencialidad de la información	37
2.1.1 Pacto Internacional de Derechos Civiles y Políticos (PIDCP)	38
2.1.2 Convenio No. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108).....	40
2.1.3 Reglamento (CE) No. 223/2009 del Parlamento Europeo y del Consejo (Reglamento 223/2009).....	41
2.1.4 Código de Buenas Prácticas de las Estadísticas Europeas.....	43
2.1.5 Código Regional de Buenas Prácticas en Estadísticas para América Latina y el Caribe	45
2.1.6 Principios Fundamentales de las Estadísticas Oficiales.....	46

2.1.7 Recomendación del Consejo de la OCDE sobre buenas prácticas de estadística	47
2.1.8 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (Reglamento General de Protección de Datos).....	48
2.2 Referencias del marco regulatorio mexicano sobre la confidencialidad de la información	50
2.2.1 La confidencialidad desde las leyes de transparencia y protección de datos personales.....	51
2.2.2 La confidencialidad desde la Ley del Sistema Nacional de Información Estadística y Geográfica (Ley del SNIEG)	52
Capítulo 3: El cifrado y la anonimización de la información como medidas para preservar la confidencialidad de la información.....	56
3.1 La anonimización.....	56
3.1.1 Principios de privacidad por diseño en la anonimización	57
3.1.2 Riesgos de la anonimización.....	58
3.1.3 Técnicas de anonimización	59
3.2 El cifrado	62
3.2.1 Clasificación del cifrado.....	62
3.2.2 Procedimientos básicos de cifrado: sustitución y transposición	63
3.2.3 Riesgos en el cifrado.....	64
3.2.4 Algoritmos de cifrado.....	66
Conclusiones.....	70
Bibliografía.....	74
Anexo: Propuesta de líneas generales de acción para preservar la confidencialidad de la información estadística y geográfica a través del cifrado y anonimización.....	81
I. Introducción	81
Capítulo I. Líneas generales	82
Capítulo II. Líneas de acción sobre anonimización	86
Capítulo III. Líneas de acción sobre cifrado	87

Índice de cuadros

Cuadro 1. Características, principios rectores y objetivos del SNIEG	9
Cuadro 2. Marco regulatorio del INEGI que aborda aspectos de Seguridad de la Información.....	12
Cuadro 3. Documentos regulatorios con objeto distinto a la seguridad de la información y que coadyuvan en la regulación de la confidencialidad de la información.....	13

Siglas y abreviaturas

AES: Estándar de Cifrado Avanzado.

ANSI: Instituto Nacional Americano de Estándares.

DEA: Algoritmo de Cifrado de Datos.

ECC: Criptografía de Curva Elíptica.

IEC: Comisión Electrotécnica Internacional.

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos.

INEGI: Instituto Nacional de Estadística y Geografía.

ISO: Organización Internacional para la Estandarización.

NIST: Instituto Nacional de Estándares y Tecnología Norteamericano.

RSA: Rivest, Shamir y Adleman.

SECG: Grupo de Estándares para la Criptografía Eficiente.

SNIEG: Sistema Nacional de Información Estadística y Geográfica.

SSI: Sistema de Seguridad de la Información.

TDEA: Algoritmo de Cifrado de Datos Triples.

Introducción

En el presente documento se aborda el análisis y propuesta del cifrado y la anonimización como mecanismos para preservar la confidencialidad de la información estadística y geográfica.

Para preservar la confidencialidad de la información estadística y geográfica se puede utilizar la tecnología como una herramienta para evitar la identificación de las personas físicas y morales a las que está asociada la información, sin embargo, se debe considerar que la tecnología es falible, por lo que también es necesario identificar las vulnerabilidades de cada tecnología y a partir de ello definir la combinación de tecnologías que otorgan los mejores resultados en la preservación de la confidencialidad. El proyecto aporta un acercamiento conceptual sobre el manejo tecnológico de las técnicas de anonimización y cifrado de datos, centrándose en establecer una propuesta para regular su uso y para contribuir a la preservación de la confidencialidad de la información estadística y geográfica.

El proyecto está conformado por tres capítulos, las conclusiones y el anexo en el cual se plasma la propuesta de líneas de acción para preservar la confidencialidad de la información estadística y geográfica a través del cifrado y la anonimización.

En el primer capítulo se describe y analiza el marco contextual y conceptual de la información estadística y geográfica, en el que se aportan referencias sobre la relevancia de la generación de la información, la evolución de su captación en México, los subsistemas que conforman el Sistema Nacional de Información Estadística y la función del INEGI como ente coordinador, así como las fases que constituyen el proceso de producción de información estadística y geográfica, el cual representa el marco de referencia en el que se situará la propuesta. Se incluye la revisión de los conceptos de privacidad, confidencialidad, cifrado y anonimización.

En el segundo capítulo se realiza una revisión del marco regulatorio internacional y mediano sobre la confidencialidad de la información. En el plano

internacional la revisión incluye el *Pacto Internacional de Derechos Civiles y Políticos*, el *Convenio No. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, el *Reglamento Número 223/2009 del Parlamento Europeo y del Consejo de Europa*, así como referencias de buenas prácticas estadísticas de la Organización para la Cooperación y el Desarrollo Económico, europeas, de América Latina y el Caribe, el *Reglamento 2016/679 del Parlamento Europeo y del Consejo*, así como de los principios fundamentales de las estadísticas oficiales de la Organización de las Naciones Unidas.

En el tercer capítulo se abordan los principios de privacidad por diseño enfocados desde la anonimización como una forma de aportar una visión sistémica de la protección de la confidencialidad. Se describen los tres riesgos que son inherentes a la anonimización: la singularización, la vinculabilidad y la inferencia. Posteriormente se detallan las técnicas de anonimización, en el que se resaltan las fortalezas de cada técnica. Finalmente se describen los tipos de cifrado y la forma general en la que funciona y sus riesgos. La revisión del capítulo concluye con la descripción de los algoritmos principales de cifrado de datos.

En el apartado de conclusiones se resalta la identificación del derecho a la privacidad como origen de la confidencialidad de la información y sus implicaciones, es decir, se busca evitar la identificación directa e indirecta de los informantes del Sistema, en el que la sustancia reside en evitar que se dé a conocer la información que fue conferida, lo cual está relacionado directamente con el derecho a la privacidad, ya que ello implica obligaciones de no revelar lo que fue informado.

En el anexo único se incluye la propuesta de líneas generales de acción para preservar la confidencialidad de la información estadística y geográfica a través del cifrado y la anonimización.



Capítulo 1

Marco contextual y conceptual de la información estadística y geográfica y la confidencialidad



Capítulo 1: Marco contextual y conceptual de la información estadística y geográfica y la confidencialidad

En el presente capítulo se abordan los temas de: captación de la *información estadística*¹ y *geográfica*;² la descripción del diagnóstico y el planteamiento de la propuesta de mejora; los elementos contextuales y conceptuales a tener en cuenta en el análisis de la propuesta, como es el *Sistema Nacional de Información Estadística y Geográfica*,³ los tipos de *información*⁴ en el INEGI,⁵ el proceso de generación de información estadística y geográfica y la *confidencialidad*⁶ de la información estadística y geográfica; temas que en su conjunto, permiten focalizar la obligación que tiene el INEGI de emitir las reglas generales de confidencialidad señaladas en el artículo 47 de la Ley del Sistema Nacional de Información

1 Información estadística es el “conjunto de resultados cuantitativos o datos que se obtienen de las Actividades Estadísticas y Geográficas en materia estadística, tomando como base los datos primarios obtenidos de los Informantes del Sistema sobre hechos que son relevantes para el conocimiento de los fenómenos económicos, gobierno, seguridad pública e impartición de justicia; demográficos y sociales, así como sus relaciones con el medio ambiente y el espacio territorial”. Ver Cámara de Diputados del H. Congreso de la Unión, *Ley del Sistema Nacional de Información Estadística y Geográfica*, 2018, artículo 2, fracción III, pp. 1-2, consultada el 10 de enero de 2019 en http://www.diputados.gob.mx/LeyesBiblio/pdf/LSNIEG_250618.pdf.

2 Información geográfica es el “conjunto organizado de datos espaciales georreferenciados, que mediante símbolos y códigos genera el conocimiento acerca de las condiciones físico-ambientales, de los recursos naturales y de las obras de naturaleza antrópica del territorio nacional”. Ver artículo 2, fracción IV, *Ley del Sistema Nacional de Información Estadística y Geográfica*, *ibídem*, p. 2.

3 El Sistema Nacional de Información Estadística y Geográfica o Sistema es el “conjunto de Unidades organizadas a través de los Subsistemas, coordinadas por el Instituto y articuladas mediante la Red Nacional de Información, con el propósito de producir y difundir la Información de Interés Nacional”. Ver artículo 2, fracción XIII, de la *Ley del Sistema Nacional de Información Estadística y Geográfica*, *ídem*.

4 Son los “datos útiles en un contexto particular. El contexto permite que los datos adquieran significado y puedan representar un mensaje determinado, hecho o fenómeno. Incluye información estadística y geográfica”. Ver Junta de Gobierno del INEGI, *Norma técnica del proceso de producción de información estadística y geográfica para el Instituto Nacional de Estadística y Geografía*, 2018, p. 5, consultada el 10 de enero de 2019 en http://sc.inegi.org.mx/repositorioNormateca/O_05Sep18.pdf.

5 Cámara de Diputados del H. Congreso de la Unión, ver artículo 2, fracción VIII, de la *Ley del Sistema Nacional de Información Estadística y Geográfica*, *op. cit.*, nota 1.

6 Es el “atributo de Seguridad de la Información que indica que la información sólo es revelada a individuos autorizados”. Ver Junta de Gobierno del INEGI, *Políticas para la Seguridad de la Información del Instituto Nacional de Estadística y Geografía*, 2014, p. 6, consultada el 10 de enero de 2019 en http://sc.inegi.org.mx/repositorioNormateca/Pod_17Dic14.pdf.

Estadística y Geográfica y sobre la cual se realizará la propuesta de líneas generales de acción para preservar la confidencialidad.

El primer tema a desarrollar corresponde a la captación de la información estadística y geográfica, en el que se abordan los antecedentes de la captación de la información estadística y geográfica, se mencionan los primeros países que realizaron actividades de captación de información y el uso que se hacía de ésta.

1.1 La captación de información estadística y geográfica

La información es la base para la toma de decisiones, aseveración que suena lógica y obvia, sin embargo, en algún momento de la historia se comenzó a utilizar la información para decidir sobre los temas del Estado y sobre la generación de inversiones.

En el siguiente tema se describen los antecedentes de la captación de la información estadística y geográfica, los propósitos de su captación y las fuentes de información.

1.1.1 Antecedentes de la captación de la información estadística y geográfica

“Censo es la recolección total de una población estadística”⁷ y es el antecedente de la recolección de los *datos*⁸ geográficos, económicos y demográficos realizados en la actualidad por las diferentes instancias gubernamentales de los países.

La historia de la captación de información estadística y geográfica señala que desde el año 3,050 a. C. en Egipto, se realizaban censos; en el año 3,000 a. C. en Babilonia se utilizaban tablillas de arcilla que servían para registrar y captar información sobre la producción agrícola. Aproximadamente en el año 2,200 a. C. en China, se organizaban censos para captar información sobre el comercio; hacia

7 Alvarado Valencia, *et al.*, *Fundamentos de inferencia estadística*, Colombia, Editorial Pontificia Universidad Javeriana, 2008, p. 70.

8 Son “valores que representan una ocurrencia de los hechos u objetos que se recopilaron o derivaron”. Ver Junta de Gobierno del INEGI, Norma técnica... *op. cit.*, nota 4, artículo 3, fracción XI.

el año 500 a. C. en Roma se realizó un censo que permitió conocer la cantidad de la población en ese momento en dicha ubicación.

En el año 762 se realizó el registro de las propiedades y bienes que pertenecían a Carlomagno y a la Iglesia católica; en el año 1482, en España se realizó el censo de hogares de la provincia de Castilla, que tenía como propósito identificar las necesidades de armamento y aprovisionamiento, con el fin de formar un ejército.

Históricamente los datos de las actividades comerciales, de los sucesos biológicos y de la naturaleza se han registrado, contabilizado para ser utilizados en la toma de decisiones en diferentes ámbitos de la sociedad, fuera para detectar necesidades de alimentación, identificar los requerimientos de armamento o para conocer la cantidad de habitantes de una población para con ello establecer decisiones de gobierno en las distintas regiones conforme a las propias características sociales, económicas y geográficas.

El siguiente tema aborda la evolución de la captación de la información estadística y geográfica en México, desde la contabilización de la población migrante de las tribus chichimecas, hasta la fecha actual en la que el tema está regulado a nivel constitucional y en el que se define la obligatoriedad de la población mexicana de proporcionar la información, así como de las diferentes instancias de gobierno de proporcionar los datos contenidos en los *registros administrativos*⁹ propios de la actividad que éstos realizan.

9 Es un “conjunto de Datos que fueron generados con fines operacionales o como parte de las funciones de una institución pública o privada sobre un tipo de objeto, sujeto, acción, hecho o evento, y obtenidos sistemáticamente con base en un formato específico ya sea impreso, digital u otro y bajo un marco de funciones y facultades formalmente establecidas en instrumentos jurídicos o reglamentarios”. *Ibidem*, artículo 3, fracción XXXIV, p. 6.

1.1.2 Evolución de la captación de la información estadística y geográfica en México

En el caso de México, los antecedentes¹⁰ se remontan al año 1116, en el que se registró la información correspondiente a la migración de las tribus chichimecas; la dinámica consistió en que cada persona arrojaba una piedra a un montículo, que posteriormente sería contabilizada; los datos se registraban en códigos, como en el caso de la Matrícula de Tributos, que permitió contabilizar el pago de los tributos de los pueblos que tenían bajo su dominio, con fines utilitarios.

A partir del año 1571 se integró la información¹¹ referente a la cuantificación utilitaria económica, geográfica y social, como el informe del Arzobispo Fray Alonso Montúfar; las llamadas Relaciones Geográficas de los años 1579 a 1584; las Nóminas de cabildos y algunos padrones poblacionales realizados a finales del siglo XVI; las Memorias y noticias sacras y reales del Imperio de las Indias Occidentales, realizado en el siglo XVII y que reseña los datos relevantes de la Nueva España.

En el siglo XVIII la captación de información estadística y geográfica continuó, con el registro de: Asuntos de Conventos y Colegios, y Hospital Real de Naturales, empadronamientos del consumo de maíz, carne y trigo de la Ciudad de México, datos sobre los obispados, curatos y pueblos, la actualización de las Relaciones Geográficas y Estadísticas, el Censo de Revillagigedo realizado entre los años 1790 y 1793, el cual recopiló datos de: población por sexo, edad, estado civil, casta y ocupación.¹²

Los trabajos de captación de información estadística y geográfica del territorio mexicano continuaron¹³ después de la independencia del país y se llegó a

10 Ver Instituto Nacional de Estadística, Geografía e Informática, Estadísticas Históricas de México, Tomo I, 1994, consultado el 15 de abril de 2019 en http://internet.contenidos.inegi.org.mx/contenidos/productos/prod_serv/contenidos/espanol/bvinegi/productos/integracion/pais/historicas/EHM1.pdf.

11 Ver Instituto Nacional de Estadística y Geografía, *Estadísticas históricas de México 2014*, México, 2015, pp. 11 y 12, consultado el 15 de abril de 2019 consultado en http://internet.contenidos.inegi.org.mx/contenidos/productos/prod_serv/contenidos/espanol/bvinegi/productos/nueva_estruc/HyM2014/EHM2014.pdf.

12 *Ídem*

13 *Ibidem*, pp. 12 y 13.

una formalización: en el decreto de diciembre del año 1821 se solicitaba la preparación de los trabajos en la materia; en abril del año 1822 se decretó la formación de la Estadística General del Imperio, en ese mismo año se presentó el Análisis Estadístico de Michoacán, que representó el primer trabajo estadístico del México independiente; en el año 1831 se decretó el levantamiento del Censo General de la República, en el cual se estimó la población de varias entidades por carecer de información; en el año 1833 se estableció el Instituto Nacional de Geografía y Estadística.

En el año 1882 se fundó la Dirección General de Estadística,¹⁴ instancia que organizó el Primer Censo General de Población del año 1895. En el periodo¹⁵ de 1976 a 1983 ocurrieron eventos significativos en el contexto de la estadística nacional. En 1976 se creó la Secretaría de Programación y Presupuesto y en 1977 se creó la Coordinación General del Sistema Nacional de Información y en 1980 se convirtió en la Coordinación General de los Servicios Nacionales de Estadística, Geografía e Informática, año en el que se emitió la Ley de Información Estadística y Geográfica con el objetivo de centralizar la coordinación y regulación de la información estadística y geográfica.

En el año de 1983 se creó el Instituto Nacional de Estadística, Geografía e Informática, responsable de coordinar los Sistemas Nacionales, Estadístico y de Información Geográfica. En abril de 2006, con la reforma del artículo 26 constitucional se creó el Sistema Nacional de Información Estadística y Geográfica (en adelante SNIEG o solamente Sistema), que proporcionaría información para el Sistema Nacional de Planeación Democrática de México. En abril de 2008 se emitió la Ley del Sistema Nacional de Información Estadística y Geográfica, que dotó de autonomía¹⁶ al INEGI con el nombre de Instituto Nacional de Estadística y Geografía, responsable de coordinar y normar al SNIEG.

Conforme se establece en la Ley del SNIEG, artículo 2, fracción XIII, Sistema es el “conjunto de Unidades organizadas a través de los Subsistemas, coordinadas

14 *Ibidem*, p. 14

15 *Ibidem*, p. 15.

16 *Ibidem*, pp.17-18.

por el Instituto y articuladas mediante la Red Nacional de Información, con el propósito de producir y difundir la Información de Interés Nacional".¹⁷

Las Unidades referidas en el párrafo anterior, conforme se establece en la Ley del SNIEG, artículo 2, fracción XV, son:

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 de:

- a) Las dependencias y entidades de la Administración Pública Federal, incluyendo a las de la Presidencia de la República y de la Procuraduría General de la República;
- b) Los poderes Legislativo y Judicial de la Federación;
- c) Las entidades federativas, los municipios y las demarcaciones territoriales de la Ciudad de México;
- d) Los organismos constitucionales autónomos, y
- e) Los tribunales administrativos federales.¹⁸

El SNIEG tiene como finalidad proporcionar a la sociedad y al Estado información con determinadas características, basado en principios rectores, para cumplir con objetivos puntuales, los cuales se integran en el siguiente cuadro.

Características	Principios rectores	Objetivos
Calidad	Accesibilidad	Producir información
Pertinente	Transparencia	Difundir oportunamente la información a través de mecanismos que faciliten su consulta
Veraz	Independencia	Promover el conocimiento
Oportuna	Objetividad	Conservar la información

Cuadro 1. Características, principios rectores y objetivos del SNIEG

Fuente: Página oficial del SNIEG.¹⁹

En la actualidad, en países como España, Estados Unidos de Norteamérica y México, en sus constituciones se establece la obligatoriedad de realizar censos que permitan conocer información sobre sus territorios y muchos tienen oficinas encargadas de la generación de información estadística.

17 Cámara de Diputados del H. Congreso de la Unión, *Ley del Sistema Nacional de Información Estadística y Geográfica*, op. cit., nota 1, p. 2.

18 *Ibidem*, pp. 2 y 3.

19 Página oficial del SNIEG, consultado el 4 de marzo de 2019 en <https://www.snieg.mx/>.

México tienen una amplia historia en la generación y procesamiento de la información estadística y geográfica, y su evolución permite identificar que el tema es de la mayor relevancia para el Estado, situación que se puede confirmar con el hecho de que el tema está regulado a nivel constitucional y coordinado por el INEGI, organismo dotado de autonomía para operar.

La propuesta de líneas generales de acción para preservar la confidencialidad de la información cubre el ámbito de aplicación del INEGI y del SNIEG, ya que es el ámbito de creación de la información estadística y geográfica, razón por la cual se incluye el tema de su conformación como parte de los elementos de análisis contextual y conceptual.

En el siguiente tema se aborda el diagnóstico respecto del manejo regulatorio de la confidencialidad de la información estadística y geográfica en el INEGI, en el que se incluirán los documentos normativos que regulan el tema, con el fin de contar con los elementos que permitan identificar los aspectos que ya están regulados. También, de manera general, se aborda el planteamiento de la propuesta de líneas generales de acción para preservar la confidencialidad de la información estadística y geográfica.

1.2 Propuesta de intervención

La propuesta de intervención a realizar consiste en el análisis de la regulación existente respecto de las reglas generales de confidencialidad de la información y la generación de una propuesta de líneas generales de acción para preservar la confidencialidad de la información estadística y geográfica a través del cifrado y la anonimización, mismas que son aplicables en el almacenamiento, transmisión y difusión de la información.

A continuación, se aborda el diagnóstico que contextualiza la regulación de la confidencialidad de la información estadística y geográfica en el INEGI.

1.2.1 Diagnóstico

El punto de origen es la obligación de regulación definida en la Ley del Sistema Nacional de Información Estadística y Geográfica (Ley del SNIEG), artículo 47, referente a que los “datos proporcionados”²⁰ por los informantes del Sistema serán confidenciales conforme a los términos de la Ley del SNIEG y de las reglas generales que emita el INEGI, respecto de la confidencialidad de la Información Estadística y la Información Geográfica, como “organismo con autonomía técnica y de gestión, personalidad jurídica y patrimonio propios, con las facultades necesarias para regular la captación, procesamiento y publicación de la información que se genere y proveer a su observancia”,²¹ conforme lo definido en la Constitución Política de los Estados Unidos Mexicanos, artículo 26, Apartado B.

La confidencialidad de la información es uno de los tres atributos que constituyen la *Seguridad de la Información*,²² además de la *integridad*²³ y la *disponibilidad*,²⁴ tema sobre el cual el INEGI tiene un marco regulatorio que abarca diferentes documentos regulatorios, y con los que se abarca tanto a la *información de la gestión administrativa*,²⁵ como a la *información estadística y geográfica*.

20 Los informantes del Sistema están obligados a proporcionar los datos e informes que les soliciten las autoridades competentes para fines estadísticos, censales y geográficos. Ver Cámara de Diputados del H. Congreso de la Unión, *Ley del Sistema Nacional de Información Estadística y Geográfica*, *op. cit.*, nota 1, artículo 45, p. 15.

21 Cámara de Diputados del H. Congreso de la Unión, *Constitución Política de los Estados Unidos Mexicanos*, México, 2018, p. 26, consultado el 12 de abril de 2019 en http://www.diputados.gob.mx/LeyesBiblio/pdf/1_120419.pdf.

22 Es la “capacidad de preservar la confidencialidad, Integridad y disponibilidad de la Información a partir de la implementación de medidas técnicas y organizativas”. Ver Junta de Gobierno del INEGI, *Políticas para la Seguridad de la Información...* *op. cit.*, nota 6, p. 7.

23 Es el “atributo de Seguridad de la Información referente a que la información está completa y sin alteraciones”. *Ídem*.

24 Es el “atributo de Seguridad de la Información que consiste en que la información puede ser accedida por el personal cuando éste lo requiere”. *Ibidem*, p. 6.

25 Es la que “corresponde a la gestión administrativa del Instituto, contenida en documentos generados, obtenidos, adquiridos, transformados o conservados por cualquier título, por sus servidores públicos, Unidades y Áreas Administrativas, exceptuando la Información Estadística y Geográfica, así como el material de apoyo y consulta de los servidores públicos cuya clasificación y difusión no correspondan al Instituto en su carácter de sujeto obligado”. Ver Junta de Gobierno del Instituto Nacional de Estadística y Geografía, *Reglamento de Transparencia y Acceso a la Información Pública del INEGI*, México, 2015, p. 4, consultado el 12 de marzo de 2019 en http://sc.inegi.org.mx/repositorioNormateca/RT_Ago15.pdf.

Dados los dos tipos de información que se manejan en el INEGI, a cada tipo de información le aplica un marco regulatorio respecto del manejo de la confidencialidad, de tal manera que a la información de la gestión administrativa le aplica el marco regulatorio concerniente a temas como transparencia, archivos, protección de datos personales, propiedad industrial y derecho de autor; en el caso de la información estadística y geográfica, el manejo de la confidencialidad se rige por la Ley del SNIEG y el marco regulatorio que en materia de seguridad de la información emite el INEGI.

En la siguiente tabla se enlistan los documentos regulatorios que abordan la confidencialidad de la información desde la seguridad de la información en el INEGI.

Documentos Regulatorios
Políticas para la Seguridad de la Información del Instituto Nacional de Estadística y Geografía
Lineamientos para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales
Protocolo Institucional de Respuesta a Incidentes de Seguridad de la Información
Criterios para la Documentación de Incidentes de Seguridad de la Información
Criterios para asignar prioridad a los eventos de Seguridad de la Información
Criterios para definir requerimientos de redundancia tecnológica en procesos y proyectos institucionales
Criterios para definir áreas de acceso restringido
Criterios para la calificación de activos de información
Criterios generales para la protección y resguardo de la información con base en sus contenidos

Cuadro 2. Marco regulatorio del INEGI que aborda aspectos de Seguridad de la Información

Fuente: Basado en el marco regulatorio contenido en la Normateca del INEGI.

Además de los documentos regulatorios señalados en el cuadro anterior, existen otros documentos regulatorios que coadyuvan en la regulación de la confidencialidad de la información, los cuales se enlistan en el siguiente cuadro.

Marco Regulatorio
Reglas de Operación del Laboratorio de Microdatos del INEGI
Políticas para la Seguridad Informática
Reglas para la integración y administración del Acervo de Información de Interés Nacional
Reglas para la Prestación del Servicio Público de Información Estadística
Principios y Buenas Prácticas para las Actividades Estadísticas y Geográficas del SNIEG
Norma para la Difusión y Promoción del Acceso, Conocimiento y Uso de la Información Estadística y Geográfica que Genera el Instituto Nacional de Estadística y Geografía

Cuadro 3. Documentos regulatorios con objeto distinto a la seguridad de la información y que coadyuvan en la regulación de la confidencialidad de la información

Fuente: Basado en el marco regulatorio contenido en la Normateca del INEGI.

El INEGI cuenta con un marco regulatorio que aborda el manejo de la confidencialidad de la información, tanto de manera directa como de manera coyuntural, más no supe la obligatoriedad señalada en el artículo 47 de la Ley del SNIEG, respecto de las reglas generales referentes al manejo de la confidencialidad de la información estadística y geográfica.

El cuidado de la confidencialidad de la información es un reto en un mundo en el que las tecnologías de la información y la comunicación han posibilitado una plataforma para el libre flujo de ideas, información, conocimiento, así como del procesamiento de grandes volúmenes de información, se trata de un contexto en el que la tecnología y el derecho enfrentan retos que están en el cruce de ambas áreas, de tal manera que el uso de la tecnología es una variable que requiere ser regulada en favor del ser humano y de la construcción de las sociedades, con el fin de disminuir los riesgos de la pérdida de la confidencialidad de la información y las consecuencias asociadas con el tipo y criticidad de la información.

En la captación de la información se utilizan cuestionarios en papel, vía internet y mediante dispositivos móviles, los cuales se definen como:

aparatos o dispositivos pequeños que cuentan con capacidades de procesamiento, conexión permanente o intermitente a una red, memoria

limitada, diseños específicos para una función principal y versatilidad para el desarrollo de otras funciones. Tanto su posesión como su operación se asocia al uso individual de una persona, quien puede configurarlo a su necesidad y a su gusto.²⁶

Las fuentes que sirven de consulta de la información han cambiado en el transcurso del tiempo: en un principio se utilizaban los códigos, matrículas de tributos, memorias de gobierno, relaciones geográficas y libros sacramentales, todos ellos constituyen una forma de los actuales registros administrativos:

realizados por instituciones gubernamentales y eclesiásticas (ministerios, secretarías, contadurías, consulados, autoridades provinciales y locales, arzobispado, obispados y parroquias) sobre acontecimientos demográficos, sociales y económicos (nacimiento, bautismo y fallecimiento de las personas, tributación, cobro de impuestos, producción económica, exportación e importación de mercancías, migración internacional, hechos judiciales, ingresos a centros escolares y de salud, así como registros catastrales, entre otros).²⁷

Se pasó de las fuentes de consulta en la que información estaba contenida en papel a los medios digitales, del envío en físico de los cuestionarios a la transmisión de los datos por internet.

El uso de la tecnología en el proceso de generación de información estadística y geográfica trajo consigo cambios en la forma de vulnerar²⁸ la confidencialidad de la información, como lo es: la revelación, divulgación o uso indebido de información obtenida en una intervención de comunicación privada, la modificación, destrucción o provocación de pérdida de información, sin autorización, contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se conozca o copie, sin autorización, la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.

26 González Melgarejo, Grecia en Escobar Martínez, Jorge Iván y Quinto Rojas, Luis Carlos, "Vulnerabilidad en dispositivos móviles con sistema operativo Android", *Cuaderno Activa*, núm., 7, 2015, p. 57, consultado el 7 de abril de 2019 en ojs.tdea.edu.co/index.php/cuadernoactiva/article/download/248/240/.

27 INEGI, *Catálogo de Documentos Históricos de la Estadística en México (Siglos XVI-XIX)*, México, 2005, p. 5, consultado el 8 de abril de 2019 en <http://tjay.org.mx/wp-content/uploads/2013/05/Catalogo-de-documentacion-historica-INEGI-1.pdf>.

28 Ver el Título Noveno, Revelación de secretos y acceso ilícito a sistemas y equipos de informática, del *Código Penal Federal*, consultado el 10 de abril de 2019 en http://www.diputados.gob.mx/LeyesBiblio/pdf/9_051118.pdf.

De lo expresado anteriormente se identifica que el INEGI cuenta con múltiples documentos que regulan la confidencialidad de la información estadística y geográfica, lo cual se fortalecería con la emisión de las reglas generales sobre el manejo confidencial de la información señalada en la Ley del SNIEG.²⁹

La pérdida de la confidencialidad de los datos que proporcionan los informantes del Sistema para generar la información estadística y geográfica puede tener diversas implicaciones a nivel nacional en los ámbitos político, social y económico, además de las implicaciones legales cuando ello sea causa de alguno de los delitos mencionados en el Título Noveno del Código Penal Federal, así como la disminución de la credibilidad en el INEGI respecto del cuidado de la información que le es proporcionada.

A continuación, se aborda el planteamiento general de la propuesta de líneas generales para preservar la confidencialidad de la información estadística y geográfica mediante el uso de las tecnologías de cifrado y anonimización de la información.

1.2.2 Planteamiento de la propuesta

Ante la situación planteada, se pretende proporcionar a los miembros del *Comité del Sistema de Seguridad de la Información del Instituto Nacional de Estadística y Geografía*³⁰ (Comité del SSI), una propuesta de líneas generales para preservar la confidencialidad de la información estadística y geográfica a través del cifrado y anonimización, que contribuyan a la construcción de las reglas generales de confidencialidad de la información que tiene que emitir el INEGI como parte de la

29 Cámara de Diputados del H. Congreso de la Unión, *Ley del Sistema Nacional... op. cit.*, p. 16,

30 Es el “Órgano Colegiado en materia de Seguridad de la Información, instaurado en cumplimiento a lo establecido por las Políticas para la Seguridad de la Información del Instituto Nacional de Estadística y Geografía, para realizar acciones tendientes a la coordinación de los trabajos que se emprendan por las Unidades Administrativas del Instituto en el fortalecimiento de la Seguridad de la Información”. Ver Comité del Sistema de Seguridad de la Información, *Manual de Integración y Funcionamiento del Comité del Sistema de Seguridad de la Información*, México, 2015, p. 6, consultado el 12 de abril de 2019 en <http://sc.inegi.org.mx/repositorioNormateca/Manual%20IFCdeSSI.pdf>.

regulación que se orienta a la preservación de la confidencialidad de la información, aplicable tanto en el INEGI como en el SNIEG.

El cifrado de la información no evita el robo o copia de la información, así como tampoco impide el acceso no autorizado a los sistemas informáticos, pero sí evita que personas que no tienen la clave puedan transformar en legible la información. El caso de la anonimización es similar al del cifrado en cuanto a que no evita el robo o copia de la información ni evita el acceso no autorizado a los sistemas informáticos, pero sí disminuye el riesgo de que se pueda identificar a los individuos a los que se refiere ésta.

Un principio en materia de seguridad de la información es, que no existe un sistema completamente seguro, por lo cual, se aborda el tema a manera de ayudar a disminuir los riesgos de la pérdida de la confidencialidad de la información mediante una propuesta de regulación del cifrado y la anonimización de la información que está contenida en los sistemas informáticos y que es transmitida por medio de internet de tal manera que, la propuesta de líneas generales para preservar la confidencialidad de la información estadística y geográfica tiene su objeto en la información transmitida por internet y contenida en sistemas informáticos, tanto del INEGI como de algún otro miembro del SNIEG.

A continuación, se aborda la conformación del SNIEG y al INEGI como instituto coordinador y encargado de normar al SNIEG, teniendo presente que la propuesta de líneas generales para preservar la confidencialidad de la información estadística y geográfica será un aporte para la regulación del tema de la confidencialidad tanto en el INEGI como en el SNIEG.

1.3 El Sistema Nacional de Información Estadística y Geográfica (SNIEG)

Por mandato constitucional, el Estado mexicano cuenta con un “Sistema Nacional de Información Estadística y Geográfica cuyos datos serán considerados oficiales. Para la Federación, las entidades federativas, los Municipios y las demarcaciones

territoriales de la Ciudad de México, los datos contenidos en el Sistema serán de uso obligatorio en los términos que establezca la ley”³¹.

Con la publicación, en 2008, en el Diario Oficial de la Federación (DOF), del Decreto por el cual se expidió la Ley del Sistema Nacional de Información Estadística y Geográfica (Ley del SNIEG), se reglamentó el apartado B del artículo 26 de la Constitución Política de los Estados Unidos Mexicanos. La Ley del SNIEG es de *orden público*,³² de *interés social*³³ y de *observancia general*³⁴ en toda la República y regula lo siguiente:

- 1) El SNIEG;
- 2) Los derechos y obligaciones de los informantes del Sistema;
- 3) La organización, funcionamiento, autonomía y responsabilidad de normar y coordinar el SNIEG, del Instituto Nacional de Estadística y Geografía (INEGI), y
- 4) Las faltas administrativas y el medio de defensa administrativo frente a los actos o resoluciones del INEGI.

En el siguiente punto se aborda a detalle la conformación del SNIEG, sus integrantes, así como los subsistemas que lo componen, con el fin de tener en

31 Constitución Política de los Estados Unidos Mexicanos, *op. cit.*, nota 21, p. 26.

32 Orden público es el conjunto de principios, normas y disposiciones legales en que se apoya el régimen jurídico para preservar los bienes y valores que requieren de su tutela, por corresponder éstos a los intereses generales de la sociedad, mediante la limitación de la autonomía de la voluntad, y de hacer así prevalecer dichos intereses sobre los de los particulares. Ver Domínguez Martínez, Jorge Alfredo, *Orden público y autonomía de la voluntad*, s/f, p. 83, consultado el 8 de abril de 2019 en <https://archivos.juridicas.unam.mx/www/bjv/libros/8/3834/9.pdf>.

El vocablo “orden” hace referencia a la idea de un mandato que debe ser obedecido. En el contexto de lo público, es decir, de orden público, puede entenderse como un deber de los gobernados de no alterar la organización del cuerpo social. Ver Tribunales Colegiados de Circuito, Novena Época, *Semanario Judicial de la Federación y su Gaceta*, Tomo XXI, 2005, p. 1515, consultado el 8 de abril de 2019 en <http://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/178/178594.pdf>.

33 El vocablo “interés” implica nociones como bien, beneficio, utilidad, valor de algo, importancia, conveniencia y trascendencia. Cuando se ubica en el ámbito social, debe tratarse de un beneficio, utilidad, valor, importancia, conveniencia o trascendencia o bien para la comunidad o sociedad. *Ídem*.

34 Se refiere a las normas abstractas, es decir, las que no se refieren a personas individuales designadas, ni a un grupo cerrado, sino a categorías de personas. Ver Secretaría de Gobernación, *Doctrina y Lineamientos para la redacción de textos jurídicos, su publicación y divulgación*, México, 2005, p. 448, consultado el 8 de abril de 2019 en <http://www.ordenjuridico.gob.mx/Publicaciones/okDoctrinas.pdf>.

cuenta impacto de la propuesta de líneas generales para preservar la confidencialidad de la información.

1.3.1 Conformación del SNIEG

El SNIEG está integrado por:

- a) Un Consejo Consultivo Nacional, que es el “órgano colegiado de participación y consulta, encargado de opinar y proponer a la Junta de Gobierno del INEGI temas o asuntos relacionados con Información Estadística o Geográfica que contribuya al desarrollo nacional”.³⁵
- b) Subsistemas Nacionales de Información, son los componentes del SNIEG enfocados a producir, integrar y difundir información de una determinada clase o respecto de temas específicos, de su competencia.

Conforme se establece en la Ley del SNIEG, artículo 17, la creación de los Subsistemas es una atribución que tiene la Junta de Gobierno del INEGI, en la que se requiere previamente que el Consejo Consultivo Nacional haya emitido opinión favorable al respecto. Actualmente existen los Subsistemas Nacionales de Información:

- 1) Demográfica y Social;
- 2) Económica;
- 3) Geográfica, Medio Ambiente, Ordenamiento Territorial y Urbano, y
- 4) Gobierno, Seguridad Pública e Impartición de Justicia.

c) INEGI.

En el siguiente apartado se aborda la atribución del INEGI como ente coordinador y encargado de normar el SNIEG, ello considerando que la propuesta de líneas generales para la preservación de la confidencialidad de la información contribuirá a la generación de las reglas generales de confidencialidad, mismas que forman parte de la atribución en cuestión.

35 Página oficial del SNIEG, Preguntas frecuentes sobre el Sistema Nacional de Información Estadística y Geográfica, consultado el 12 de abril de 2019 en <https://www.snieg.mx/Contenidos/espanol/portal/faq.htm>.

1.3.2 El INEGI como coordinador del SNIEG

Conforme se establece en la Ley del SNIEG, artículo 55, fracciones I a la V, el INEGI como coordinador del SNIEG tiene las atribuciones siguientes:

- I. Normar y coordinar el Sistema, así como fomentar las acciones que permitan mantener su operación eficiente;
- II. Normar y coordinar las actividades que lleven a cabo las Unidades, tomando en cuenta los estándares nacionales e internacionales, así como las mejores prácticas en la materia;
- III. Solicitar a las Unidades información relativa a sus actividades, para la integración de los anteproyectos de los programas a los que hace referencia el artículo 9 de esta Ley;
- IV. Solicitar a las Unidades la Información que éstas hayan obtenido en el ámbito de sus respectivas competencias y sea necesaria para el Sistema;
- V. Las demás que correspondan conforme a la Ley del SNIEG.

De las atribuciones del INEGI señaladas en los numerales anteriores, para el propósito que se persigue en el presente documento, resalta la atribución correspondiente a normar y coordinar las actividades que realicen las Unidades del Estado, pues la regulación del manejo confidencial de la información tiene un alcance al interior del INEGI, con proyección a las Unidades del Estado que conforman el SNIEG.

En el siguiente punto se aborda el tema de la información en el INEGI, ello permite identificar una primera clasificación de la información conforme al marco regulatorio que le es aplicable, lo que permite profundizar en el contexto y los conceptos necesarios para comprender la propuesta de líneas generales de acción para preservar la confidencialidad de la información estadística y geográfica.

1.4 La información en el INEGI

En los siguientes puntos se integran los conceptos básicos que describen los tipos de información que se utiliza en el INEGI como órgano autónomo encargado de producir la información estadística y geográfica, considerando que también utiliza

información propia de su gestión administrativa, en la que se ubican los datos personales.

La diferenciación de los tipos de información que se manejan en el INEGI es básica para comprender que la propuesta de líneas generales de acción para preservar la confidencialidad de la información se focaliza en la información estadística y geográfica dado el marco regulatorio que le es aplicable.

En el siguiente punto se abordan los tipos de la información que se utiliza en el INEGI, identificando tanto la información de la gestión administrativa como a la información estadística y geográfica.

1.4.1 Tipos de información en el INEGI

En el INEGI se manejan dos tipos de información, la información de la gestión administrativa (sujeta a las leyes de transparencia y protección de datos personales) y la información estadística y geográfica (sujeta a la Ley del SNIEG).

La *Información de la gestión administrativa* se define en el Reglamento de Transparencia y Acceso a la Información Pública del Instituto Nacional de Estadística y Geografía, en el artículo 2, fracción XXVI, como:

aquella que corresponde a la gestión administrativa del Instituto, contenida en documentos generados, obtenidos, adquiridos, transformados o conservados por cualquier título, por sus servidores públicos, Unidades y Áreas Administrativas, exceptuando la Información Estadística y Geográfica, así como el material de apoyo y consulta de los servidores públicos cuya clasificación y difusión no correspondan al Instituto en su carácter de sujeto obligado.³⁶

Tanto la información estadística como la información geográfica se definen en la Ley del SNIEG, artículo 2, fracciones III y IV, respectivamente y también existe una definición para un subconjunto de ambas, la información de interés nacional, conceptos que se describen a continuación.

Información estadística es el:

36 Ver Junta de Gobierno del Instituto Nacional de Estadística y Geografía, *Reglamento de Transparencia... op. cit., nota 25.*

conjunto de resultados cuantitativos o datos que se obtienen de las Actividades Estadísticas y Geográficas en materia estadística, tomando como base los datos primarios obtenidos de los Informantes del Sistema sobre hechos que son relevantes para el conocimiento de los fenómenos económicos, gobierno, seguridad pública e impartición de justicia; demográficos y sociales, así como sus relaciones con el medio ambiente y el espacio territorial.³⁷

Información geográfica es el “conjunto organizado de datos espaciales georreferenciados, que mediante símbolos y códigos genera el conocimiento acerca de las condiciones físico-ambientales, de los recursos naturales y de las obras de naturaleza antrópica del territorio nacional”.³⁸

Información de interés nacional es la información correspondiente a temas señalados en el artículo 59 de Ley del SNIEG, como:

- a) Censos nacionales;
- b) El sistema de cuentas nacionales;
- c) Los índices nacionales de precios:
 - i. Índice Nacional de Precios al Consumidor, e
 - ii. Índice Nacional de Precios Producto.

Así como la que determine la Junta de Gobierno del INEGI con base en los cuatro criterios siguientes, señalados en la Ley del SNIEG, artículo 78, fracciones I a la IV:

- 1) Se trate de los siguientes temas, grupos de datos o indicadores: población y dinámica demográfica; salud; educación; empleo; distribución de ingreso y pobreza; de gobierno, seguridad pública e impartición de justicia; vivienda; sistema de cuentas nacionales; información financiera; precios; trabajo; ciencia y tecnología; telecomunicaciones y radiodifusión; atmósfera; biodiversidad; agua; suelo; flora; fauna; residuos peligrosos y residuos sólidos; marco de referencia geodésico; límites costeros, internacionales, estatales y municipales; datos de relieve continental, insular y submarino; datos catastrales, topográficos, de recursos naturales y clima, y nombres

37 Cámara de Diputado del H. Congreso de la Unión, Ley del Sistema..., *op. cit.*, nota 1, artículo 2, fracción III, pp. 1 y 2.

38 *Ibidem*, artículo 2, fracción IV, p. 2.

- geográficos, o bien se trate de temas que sean aprobados por unanimidad por el Consejo Consultivo Nacional, incluyendo aquéllos que se generen como parte de la creación de un nuevo Subsistema;
- 2) Resulte necesaria para sustentar el diseño y la evaluación de las políticas públicas de alcance nacional;
 - 3) Sea generada en forma regular y periódica, y
 - 4) Se elabore con base en una metodología científicamente sustentada.

En términos del mismo artículo 78, también se incluye la información que “...resulte necesaria para prevenir y, en su caso, atender emergencias o catástrofes originadas por desastres naturales, y aquella que se deba generar en virtud de un compromiso establecido en algún tratado internacional”.³⁹

A partir de lo anteriormente descrito se pueden identificar los conceptos de información estadística y geográfica, que constituye la información a la cual se le aplicará el cifrado y anonimización para ayudar a preservar la confidencialidad de la información.

A continuación, se abordan conceptos referentes de la información estadística y geográfica que permitirá ampliar el marco conceptual manejado en el contexto del INEGI y del SNIEG.

1.4.2 Conceptos básicos sobre información

En el contexto de la información estadística y geográfica, en el INEGI se manejan conceptos como dato, microdato, registro administrativo, registro estadístico o geográfico, los cuales se describen sus definiciones a continuación.

Existe diversidad de conceptos sobre microdatos, dato e información, desde las más básicas encontradas en los diccionarios hasta las técnicas y legales referidas en guías y marcos legales; los conceptos que se abordan a continuación se tomaron del marco regulatorio del SNIEG y del INEGI, ello con el fin de establecer

39 *Ibidem*, artículo 78, p. 24.

congruencia conceptual entre la propuesta a realizar y el marco conceptual propio de la INEGI, por ser la institución a la que se dirige la propuesta.

El dato suele referirse como un elemento de la información, en el contexto del INEGI, *dato* “es un valor que representa una ocurrencia de los hechos u objetos que se recopilaron o derivaron”.⁴⁰

En el INEGI, los resultados de la información recabada en ejercicios censales o de encuestas, se pone a disposición de la sociedad en diferentes niveles de agregación, preservando en todo momento la confidencialidad de la información, el nivel de mayor desagregación de la información corresponde a los *microdatos*, que son “los valores de las variables asociadas a cada una de las unidades de observación”.⁴¹

Los conceptos de registro administrativo y registro estadístico y geográfico, ambos definidos en la Norma Técnica del Proceso de Producción de Información Estadística y Geográfica para el Instituto Nacional de Estadística y Geografía, artículo 3, fracciones XXXIV y XXXV, respectivamente, son parte de los conceptos asociados con la información estadística y geográfica que son descritos a continuación para profundizar en el marco conceptual que permite comprender la propuesta.

Registro administrativo es un:

conjunto de Datos que fueron generados con fines operacionales o como parte de las funciones de una institución pública o privada sobre un tipo de objeto, sujeto, acción, hecho o evento, y obtenidos sistemáticamente con base en un formato específico ya sea impreso, digital u otro y bajo un marco de funciones y facultades formalmente establecidas en instrumentos jurídicos o reglamentarios.⁴²

Registro estadístico o geográfico es una:

lista estructurada, completa y exhaustiva de las unidades de una Población cuyo mantenimiento, evaluación de su calidad y actualización se lleva a cabo con fines estadísticos o geográficos. Entre los fines estadísticos o geográficos

40 Junta de Gobierno del Instituto Nacional de Estadística y Geografía, Norma Técnica..., *op. cit.*, nota 4, p. 5.

41 INEGI, Reglas de Operación del Laboratorio de Microdatos del INEGI, 2015, p. 5, consultado el 10 de febrero de 2019 en http://sc.inegi.org.mx/repositorioNormateca/Or_03sep15.pdf.

42 Junta de Gobierno del Instituto Nacional de Estadística y Geografía, Norma..., *op. cit.*, nota 4, p. 5.

están: servir como marco de muestreo y de base en el diseño y planeación de otros Programas de Información; ser una fuente de datos para generar información estadística o geográfica; y servir como referencia para la integración de otras fuentes de datos como registros administrativos.⁴³

De acuerdo con lo señalado en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 3, fracción IX, *datos personales* son “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”.⁴⁴ Para efectos del presente documento se integra el concepto con el fin de brindar un contexto amplio de la información que se utiliza en el INEGI, más cabe señalar que este tipo de información no es el objeto de la propuesta que se realizará.

Un subconjunto de los datos personales, son los *datos personales sensibles* y son:

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.⁴⁵

Al igual que en el caso de los datos personales, los datos personales sensibles forman parte de la información de la gestión administrativa, misma que no es objeto de la propuesta que se realizará, sin embargo, se integra el concepto con el fin de ampliar el contexto sobre el manejo de la información en el INEGI.

Conforme se establece en la Norma Técnica del Proceso de Producción de Información Estadística y Geográfica para el Instituto Nacional de Estadística y Geografía, artículo 3, fracción XV, *información* son los “datos útiles en un contexto particular. El contexto permite que los datos adquieran significado y puedan

43 *Ídem.*

44 Cámara de Diputados del H. Congreso de la Unión, *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, México, 2017, p. 3, consultado el 11 de febrero de 2019 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>.

45 *Ídem.*

representar un mensaje determinado, hecho o fenómeno. Incluye información estadística y geográfica”.⁴⁶

Diferenciar entre dato, microdato, información, información de interés nacional, dato personal, dato personal sensible resulta básico para comprender el nivel de protección que se requiere respecto del manejo de la confidencialidad de la información.

Lo descrito en los dos anteriores puntos, permite generar una aproximación a la importancia de la información estadística y geográfica, tanto para la sociedad, como para el Estado mexicano, lo cual se describe mayor profundidad en el siguiente punto.

1.4.3 Importancia de la información estadística y geográfica

La importancia de la información estadística y geográfica reside en que ésta, muestra la situación de la sociedad y del Estado, a partir de la cual, se pueden derivar múltiples análisis orientados a proporcionar los insumos para la toma de decisiones y la creación de políticas de Estado o la generación de inversiones por parte del sector empresarial.

Algunos de los principales temas de los que se genera información estadística y geográfica son:

- 1) Pobreza;
- 2) Hambre;
- 3) Salud y bienestar;
- 4) Educación de calidad;
- 5) Igualdad de género;
- 6) Agua limpia y saneamiento;
- 7) Energía asequible y no contaminante;
- 8) Trabajo decente y crecimiento económico;
- 9) Industria, innovación e infraestructura;

46 Junta de Gobierno del Instituto Nacional de Estadística y Geografía, Norma..., *op. cit*, nota 4, p. 5.

10) Reducción de las desigualdades.

Temas que suelen estar en la lista de los asuntos de mayor relevancia, sobre todo, en la agenda de los países en vías de desarrollo, ya que implica la determinación de políticas para combatir la pobreza, la población ubicada en zonas geográficas de alto riesgo ante desastres naturales, los sectores de la población que tienen alguna discapacidad, sobre requerimiento de planeación estratégica.

Lo cierto es que toda la información estadística y geográfica se desarrolla dentro del proceso estadístico, cuyas fases se describen a continuación y retoman especial importancia para posteriormente identificar las actividades en las que se puede aplicar el cifrado y la anonimización de la información, así como las tecnologías que son utilizadas.

1.5 El proceso estadístico y geográfico

El proceso estadístico y geográfico se describe en la Norma Técnica del Proceso de Producción de Información Estadística y Geográfica para el Instituto Nacional de Estadística y Geografía. Antes de abordar las fases del citado proceso, se abordan los conceptos de informantes del Sistema y de actividades estadísticas y geográficas, ambos conceptos están directamente relacionados con la identificación de las actividades en las que se aplicaría el cifrado y anonimización, así como la razón por la cual se busca preservar la confidencialidad de la información estadística y geográfica, es decir, que al final de cuentas, la información a detalle se refiere a los llamados informantes del Sistema.

1.5.1 Los informantes del Sistema, las actividades estadísticas y geográficas y el programa de información

La información que el INEGI capta, independientemente de la forma en la que lo realice, se relaciona con un informante del Sistema, ello implica que, aunque no se capturen sus *datos personales*, es posible que a nivel de registro: administrativo, estadístico o geográfico se pueda identificar a quién pertenece, poniendo en riesgo la privacidad del informante.

Conforme se establece en la Ley del SNIEG, artículo 2, fracción VII, los informantes del Sistema son “las personas físicas y morales, a quienes les sean solicitados datos estadísticos y geográficos”⁴⁷ en términos de la Ley del SNIEG.

En el mismo artículo 2, fracción I, de la Ley del SNIEG, se definen las *actividades estadísticas y geográficas* como “las relativas al diseño, captación, producción, actualización, organización, procesamiento, integración, compilación, publicación, divulgación y conservación de la Información de Interés Nacional”.⁴⁸

El *programa de información* es el “conjunto de actividades, que se pueden repetir, que describen el propósito y contexto de un conjunto de Procesos que se llevarán a cabo cada periodo de tiempo para producir información”.⁴⁹

De los conceptos integrados hasta ahora, cobran especial relevancia: registro administrativo, registro estadístico o geográfico, microdatos, informantes del Sistema y actividades estadísticas y geográficas, ya que es en éstos, son en los que se focaliza operativamente la preservación de la confidencialidad de la información, es decir en los que se opera el cifrado y anonimización de la información (registros administrativos, registros estadísticos o geográficos y microdatos), así como en el caso de los informantes del Sistema es en el que se vincula la privacidad y en las actividades estadísticas y geográficas en las que se ubican las actividades en las que se aplicaría directamente el cifrado y anonimización de la información.

1.5.2 Objetivos de las fases del proceso estadístico y geográfico

Previo a la descripción de los objetivos de cada una de las fases del proceso de producción de información estadística y geográfica se requiere la descripción de algunos conceptos que permitirán contextualizar el lenguaje de procesos utilizados, todos ellos obtenidos de la Norma Técnica del Proceso de Producción de Información Estadística y Geográfica para el Instituto Nacional de Estadística y Geografía, artículo 3, fracciones V, X, XXII, XXVI, XXIX y XXXI.

47 Cámara de Diputado del H. Congreso de la Unión, Ley del Sistema..., *op. cit.*, nota 1, p. 2.

48 *Ibídem*, p. 1.

49 Junta de Gobierno del Instituto Nacional de Estadística y Geografía, Norma Técnica..., *op. cit.*, nota 4, p. 6.

Ciclo de Programa, es un “conjunto de actividades para investigar características de una determinada población para un período de referencia determinado”.⁵⁰

Conjunto de Información, son “colecciones organizadas de contenido estadístico o geográfico generados en la Fase de Análisis para ser insumo de la Fase de Difusión”.⁵¹

Metadatos, son “datos estructurados que describen las características del contenido, captura, procesamiento, calidad, condición, acceso y distribución de la información estadística o geográfica”.⁵²

Necesidades estructuradas de información, es la “necesidad de información para la que se han definido el objetivo de la información, los conceptos a ser medidos, la población objeto de estudio, los dominios de estudio y la periodicidad con la que se requiere”.⁵³

Presentación, es la “forma en la que datos y metadatos obtenidos de un Conjunto de Información se incorporan para formar un elemento de un Producto”.⁵⁴

Producto, es el “resultado final de un proceso que se pone a disposición de un usuario. Un Producto incluye un conjunto de Presentaciones para un usuario”.⁵⁵

El proceso de producción de información estadística y geográfica del INEGI se desarrolla en ocho fases y en cada una de ellas se tiene un objetivo puntual, mismo que tiene relevancia para verificar si se trata de una fase en la que se deban aplicar medidas de cifrado y anonimización de información.

A continuación, se describen los objetivos de cada una de las fases que comprende el proceso de producción de información estadística y geográfica del INEGI.

50 *Ibidem*, p. 4.

51 *Ibidem*, p. 5.

52 *Ídem*.

53 *Ibidem*, p. 6.

54 *Ídem*.

55 *Ídem*.

Fase 1: Documentación de necesidades, el objetivo es documentar las necesidades de información que sustentan al Programa de Información.

Fase 2: Diseño, tiene por objeto diseñar los productos de información estadística o geográfica que atenderán las necesidades estructuradas de información determinadas de acuerdo con los elementos documentales recabados en la fase de documentación de necesidades.

Fase 3: Construcción, tiene por objeto la construcción y prueba de la infraestructura informática, los componentes, aplicaciones y servicios de software, para crear un ambiente operacional completo que permita ejecutar la producción de información, así como la ejecución de pruebas que lo acrediten.

Fase 4: Captación, tiene por objeto captar los datos necesarios, incluyendo la obtención de metadatos, para la generación de productos de información estadística y geográfica.

Fase 5: Procesamiento, tiene por objeto preparar los datos captados para el análisis.

Fase 6: Análisis de la producción, tiene por objeto asegurar que la información producida es apta para su propósito.

Fase 7: Difusión, tiene por objeto poner a disposición de los usuarios el conjunto de información a través del producto de información y sus diversas presentaciones.

Fase 8: Evaluación del proceso, tiene por objeto decidir si el siguiente ciclo de producción de información debe llevarse a cabo utilizando las mismas especificaciones de necesidades, diseño y construcción o si se requiere implementar alguna mejora en el mismo.

Conforme los objetivos descritos de cada una de las fases del proceso de generación de información estadística y geográfica, se identifica que el cifrado y anonimización de la información debe tenerse en cuenta desde la Fase de Diseño hasta la Fase de Evaluación del Proceso. Cabe señalar que en la Fase de Diseño se deben tomar en cuenta las necesidades de cifrado y anonimización de la

información que se aplicaran en el Producto de información y sus Presentaciones, así como en la construcción y prueba de la estructura informática que soporta el proceso de generación de información estadística y geográfica.

1.6 La confidencialidad de la información estadística y geográfica

En este apartado se aborda el tema de la confidencialidad, así como de la privacidad, sin embargo, no se trata de un enfoque desde el derecho, ya que ese enfoque será abordado en el capítulo II, correspondiente al marco regulatorio internacional y nacional.

1.6.1 La privacidad y la confidencialidad

El diccionario de la Real Academia de la Lengua Española, en su versión en línea, define privacidad como “cualidad de privado” y como el “ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión”.⁵⁶ Los conceptos de privacidad son variados y en algunos casos lo vinculan con la intimidad y la protección de datos personales. El alcance de este capítulo es mostrar algunos de los conceptos más comunes sobre los términos referidos; la identificación de los límites y vinculaciones entre privacidad e intimidad exceden el objetivo del presente capítulo.

También puede entenderse por privacidad como “el respeto y control de los datos íntimos, así como el secreto de las comunicaciones y de las circunstancias en las que se producen, el control de otros datos públicos que dan acceso a la intimidad”.⁵⁷ De la definición anterior resalta la mención al control de datos públicos que dan acceso a la intimidad, situación que refleja el sentido de preservar la confidencialidad de la información estadística y geográfica proporcionada por los informantes del Sistema.

56 Real Academia Española, *Diccionario de la lengua española*, modalidad en línea, actualización 2018, consultado el 10 de febrero de 2019 en <https://dle.rae.es/?id=UD4g0KW>.

57 Megías Quirós, José Justo, *Privacidad e internet: intimidad, comunicaciones y datos personales*, Sociedad de la Información, en RCE, 2002, p. 523, consultado el 2 de agosto de 2019 en <https://revistas.ucm.es/index.php/ANDH/article/download/.../20978>.

El concepto de confidencialidad está definido en el marco regulatorio del INEGI y pertenece a uno de los atributos de la *Seguridad de la Información*, entendida ésta como la “capacidad de preservar la confidencialidad, Integridad y disponibilidad de la Información a partir de la implementación de medidas técnicas y organizativas”⁵⁸. Se entiende, *confidencialidad*, como el “atributo de Seguridad de la Información que indica que la información sólo es revelada a individuos autorizados”⁵⁹.

En el contexto de la definición de Seguridad de la información, la propuesta solamente tiene el alcance sobre la confidencialidad de la información, deja de lado la *integridad* (“atributo de Seguridad de la Información referente a que la información está completa y sin alteraciones”⁶⁰) y la *disponibilidad* (“atributo de Seguridad de la Información que consiste en que la información puede ser accedida por el personal cuando éste lo requiere”⁶¹).

De la revisión anterior respecto de los conceptos de privacidad y confidencialidad se puede concluir que mientras que la privacidad se refiere a un derecho de la persona, la confidencialidad se refiere a las acciones que se realizan para proteger la privacidad, de tal manera que se evite identificar a la persona a la que pertenece la información. En el siguiente punto se describen los principios estadísticos de confidencialidad que se siguen en el tratamiento de la información estadística y geográfica en el ámbito del SNIEG.

1.6.2 Los principios estadísticos de confidencialidad

Los Principios y Buenas Prácticas para las Actividades Estadísticas y Geográficas del SNIEG, contienen los *principios estadísticos de confidencialidad*,⁶² establecidos de la siguiente forma:

58 Junta de Gobierno del INEGI, Políticas para la Seguridad..., *op. cit.*, nota 6, p. 7.

59 *Ibidem*, p. 6.

60 *Ibidem*, p. 7.

61 *Ibidem*, p. 6.

62 Junta de Gobierno del INEGI, *Principios y Buenas Prácticas para las Actividades Estadísticas y Geográficas del SNIEG*, México, 2015, p. 13, consultado el 2 de agosto de 2019 en https://www.snieg.mx/DocumentacionPortal/Normatividad/vigente/Principios_Buenas_Practicas_Es_Geo_SNIEG.pdf.

Las Unidades del Estado garantizan la confidencialidad y reserva de los datos que los informantes proporcionan:

- a) Los datos que proporcionan los informantes del SNIEG se utilizan sólo para fines estadísticos y geográficos y son estrictamente confidenciales.
- b) Se cuida la información personal generada por la utilización de los sistemas geográficos (georreferenciación) o por la combinación de dos o más bases de datos.
- c) Se cuenta con procedimientos y protocolos de control para los usuarios externos que acceden a los microdatos con fines de investigación.

Los principios estadísticos de confidencialidad señalados anteriormente representan una guía que se debe seguir para evitar que se pueda reconocer a quien corresponde la información proporcionada por los informantes del Sistema, lo cual se deberá considerar de manera puntual al elaborar la propuesta de líneas generales de acción para preservar la confidencialidad de la información estadística y geográfica a través del cifrado y anonimización.

1.6.3 El control de la divulgación indebida

La divulgación de la información pertenece a la fase 7, difusión, del proceso de producción de información estadística y geográfica para el INEGI, fase en la que se pone a disposición de la sociedad y el Estado la información estadística y geográfica y en la que la información tiene diferentes vistas, sea en gráficas, cuadros estadísticos o archivos de microdatos. El control de la divulgación indebida es una forma de preservar la confidencialidad de la información y los métodos utilizados pertenecen al rubro de la anonimización de la información. A continuación, se describen a detalle.

Control de divulgación indebida “son las medidas adoptadas para proteger los datos estadísticos de manera que no se vulneren las normas de confidencialidad prescritas o promulgadas”.⁶³

El Departamento de Asuntos Económicos y Sociales de la Organización de las Naciones Unidas (ONU), señala que los *métodos*⁶⁴ del inciso a) al c), (incisos que se mencionan a continuación), permiten reducir el riesgo de divulgación de información confidencial en cuadros estadísticos y que los métodos señalados en los incisos d) y e) siguientes, son útiles para controlar el riesgo de divulgación de información confidencial en los archivos de microdatos:

- a) Supresión de valores individuales, o supresión de casillas, aplicando un criterio de “sensibilidad” para determinar las casillas del cuadro que presentan un riesgo elevado de divulgación de información confidencial;
- b) Rediseño de los cuadros, modificando las definiciones de filas y columnas mediante la fusión de categorías o la reagrupación de los valores de las categorías;
- c) Distorsión de datos mediante la adición de ruido a los microdatos utilizados para generar el cuadro o a los datos tabulares;
- d) Métodos de reducción de datos, como el muestreo, la utilización de poblaciones suficientemente grandes para determinados grupos, la utilización de categorías de variables más toscas, la codificación superior e inferior, la eliminación de algunas de las variables correspondientes a algunos encuestados, y la eliminación de los encuestados del archivo;
- e) Métodos de modificación de datos, como la adición de ruido aleatorio a los microdatos, los canjes de datos, la sustitución de pequeños grupos por valores medios, y la sustitución de información sobre algunos encuestados por valores imputados.

63 Organización de las Naciones Unidas, Departamento de Asuntos Económicos y Sociales, *Guía de elaboración de estadísticas sobre el empleo del tiempo para medir el trabajo remunerado y no remunerado*, Nueva York, 2006, p. 188, consultada el 2 de agosto de 2019 en https://unstats.un.org/unsd/demographic-social/Standards-and-Methods/files/Handbooks/time-use/SeriesF_93-S.pdf.

64 *Ídem*.

Los métodos señalados anteriormente son aplicables en la fase de difusión de la información, dichos métodos son referentes básicos a considerar en la construcción de la propuesta de líneas generales para preservar la confidencialidad de la información por medio del cifrado y la anonimización de la información, conceptos que se describen en el siguiente punto.

1.6.4 La anonimización y el cifrado

El cifrado, la anonimización y disociación son métodos que coadyuvan a preservar la confidencialidad de la información, cada uno de estos métodos tiene sus particularidades, lo cuales serán abordados en el capítulo III, en este apartado únicamente se describe el concepto con el fin de brindar los elementos conceptuales que permitan comprender el desarrollo de la propuesta.

El *cifrado* o *encriptado* “implica alterar los datos, generalmente mediante el uso de una clave, de modo que no sean legibles para quienes no posean dicha clave. Luego, a través del proceso de descifrado, aquellos que sí poseen la clave podrán utilizarla para obtener la información original”.⁶⁵

De acuerdo con la Agencia Española de Protección de Datos, *anonimización* es un “proceso mediante el cual se reduce al mínimo los riesgos de identificación de los datos anonimizados, al tiempo que se mantiene la veracidad de los resultados del tratamiento de los mismos, es decir, evita que se pueda identificar a quién pertenece la información”.⁶⁶

Disociación es 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”.⁶⁷

65 ESET, *Cifrado de la información, Guía corporativa*, 2014, p. 6, consultado el 2 de agosto de 2019 en https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014v2.pdf.

66 Agencia Española de Protección de Datos, *Orientaciones y garantías en los procedimientos de anonimización de datos*, 2016, p. 2, consultado el 2 de agosto de 2019 en <https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf>.

67 Cámara de Diputados del H. Congreso de la Unión, *Ley General de Protección de Datos...*, *op. cit.*, nota 44, p.3.

Tanto la anonimización como el cifrado manejan algoritmos para lograr el objetivo buscado; de manera general un algoritmo es una secuencia de instrucciones que basadas en un modelo de análisis dan como resultado la solución a la problemática planteada.

En los dos casos, anonimización y cifrado, el método implica el uso de un algoritmo que permita codificar los datos y decodificarlos, así mismo, existen diferentes técnicas o variaciones de algoritmos en cada caso, mismas que serán abordadas en el capítulo III, pues corresponde al detalle de la revisión de los aspectos técnicos y tecnológicos.

Tanto el contexto como los conceptos revisados en el presente capítulo permiten fundamentar, conceptualmente, el desarrollo de la propuesta de líneas generales para preservar la confidencialidad de la información estadística y geográfica. La aplicación de la propuesta se identifica en las fases de Diseño a Evaluación del Proceso para la generación de información estadística y geográfica, fases en las que el uso de las tecnologías de información y comunicaciones son básicas para la captación, almacenamiento, transmisión, procesamiento y difusión de la información, de tal forma que el cifrado y anonimización de la información, por lo que el cifrado y la anonimización de la información pueden considerarse como opciones para preservar la confidencialidad de la información.



Capítulo 2

Referencias del marco regulatorio internacional y mexicano sobre la confidencialidad de la información



Capítulo 2: Referencias del marco regulatorio internacional y mexicano sobre la confidencialidad de la información

El capítulo 2 describe los fundamentos legales de los que deriva la preservación de la confidencialidad, con atención en el tratamiento de la información estadística y geográfica.

La primera parte del capítulo 2 incluye una revisión del marco regulatorio internacional, tanto de los instrumentos que tienen carácter vinculatorio para el Estado Mexicano, como de los que solamente son una referencia en la materia.

A continuación, se aborda la descripción del marco regulatorio internacional que de una forma directa o indirecta refiere a la preservación de la confidencialidad de la información.

2.1 Referencias del marco regulatorio internacional sobre la confidencialidad de la información

En los siguientes siete subtemas se abordan las referencias internacionales sobre el manejo de la confidencialidad de la información, con especial énfasis en el ámbito de la generación de estadísticas oficiales.

El análisis incluye las siguientes referencias regulatorias:

1. Pacto Internacional de Derechos Civiles y Políticos (PIDCP);
2. Convenio No. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108);
3. Reglamento (CE) No. 223/2009 del Parlamento Europeo y del Consejo (Reglamento 223/2009);
4. Código de buenas prácticas de las estadísticas europeas;
5. Código regional de buenas prácticas en estadísticas para América Latina y el Caribe;
6. Principios fundamentales de las Estadísticas Oficiales;

7. Recomendación del Consejo de la OCDE sobre buenas prácticas de estadística;
8. Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo (Reglamento General de Protección de Datos).

Cabe señalar que se excluyeron del análisis las siguientes referencias:

- a) Directiva 2002/58/CE del Parlamento europeo y de Consejo. No se incluye dado que se trata de una referencia en el manejo de la confidencialidad para el sector de las telecomunicaciones y en el presente caso se analizan las referencias en el ámbito de la generación de las estadísticas oficiales;
- b) Directiva 95/46/CE del Parlamento europeo y de Consejo. No se incluye dado que esta directiva fue derogada por el Reglamento General de Protección de Datos Personales, el cual sí se analiza.
- c) Normas Especiales para la Divulgación de Datos del Fondo Monetario Internacional. No se incluye dado que solamente establece los elementos que se deben incluir en la divulgación de los datos, más no en lo que se refiere al manejo de la confidencialidad de éstos.

A continuación, se aborda el análisis del Pacto Internacional de Derechos Civiles y Políticos, el cual se puede considerar como el primer referente de un documento legalmente vinculante a nivel internacional y que aborda el derecho a la privacidad de las personas, del cual se deriva el manejo confidencial, tanto de los datos personales como de los datos que son recabados por las instituciones de estadística para tales fines.

2.1.1 Pacto Internacional de Derechos Civiles y Políticos (PIDCP)

Adoptado⁶⁸ por la Asamblea General de las Naciones Unidas el 16 de diciembre de 1966, en vigor desde el 23 de marzo de 1976, con *adhesión*⁶⁹ de México desde el

68 Ver Asamblea General de las Naciones Unidas, *Pacto Internacional de Derechos Civiles y Políticos*, 1966, consultado el 19 de abril de 2019 en <https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx>.

69 Es el "acto mediante el cual un Estado acepta la oferta o la oportunidad de convertirse en parte de un tratado ya negociado y firmado por otros Estados. Tiene el mismo efecto legal que la

24 de marzo de 1981, con carácter *vinculante*,⁷⁰ el PIDCP deriva del reconocimiento de la dignidad inherente de toda persona humana y de sus derechos iguales e inalienables, señalados en la *Declaración Universal de los Derechos Humanos*,⁷¹ con lo que se busca contribuir a que los Estados generen las condiciones que permita a cada persona gozar de sus derechos civiles y políticos.

El PIDCP aborda su contenido en seis partes:⁷² el derecho de todos los pueblos a la libre determinación; las condiciones generales de su aplicación; los derechos que son la esencia del PIDCP; la vigilancia y conformación del órgano de monitoreo; la relación entre las obligaciones contenidas en el PIDCP y las definidas en la Carta de las Naciones Unidas, y lo relacionado con la firma, entrada en vigor y modificaciones.

Referente al derecho a la intimidad, el PIDCP en el artículo 17 establece lo siguiente:

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

ratificación. La adhesión generalmente ocurre después de que el tratado ha entrado en vigor. El Secretario General de las Naciones Unidas, en su función de depositario, también ha aceptado adhesiones a algunas convenciones antes de su entrada en vigor. Las condiciones bajo las cuales puede ocurrir la adhesión y el procedimiento involucrado dependen de las disposiciones del tratado. Un tratado puede prever la adhesión de todos los demás Estados o para un número limitado y definido de Estados. En ausencia de tal disposición, la adhesión solo puede ocurrir cuando los Estados negociadores fueron acordados o posteriormente lo acordaron en el caso del Estado en cuestión". Ver, Organización de las Naciones Unidas, Glosario de términos relativos a los procedimientos de los tratados, consultado el 19 de abril de 2019 en https://treaties.un.org/pages/Overview.aspx?path=overview/glossary/page1_en.xml#accession.

70 "Los instrumentos vinculantes, suponen, por parte de los Estados, un reconocimiento de obligación legal. De acuerdo con el principio de primacía de la ley internacional sobre la ley nacional, los Estados Parte tienen el deber de adaptar sus legislaciones nacionales al tratado en cuestión y de introducir toda medida relevante en sus sistemas legales para implementar sus obligaciones respecto al tratado". Ver Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, *Más sobre la naturaleza y el estatus de los instrumentos legales y programas*, consultado el 19 de abril de 2019 en <http://www.unesco.org/new/es/social-and-human-sciences/themes/advancement/networks/larno/legal-instruments/nature-and-status/>.

71 En específico lo referente a la vida privada. Ver Asamblea General de las Naciones Unidas, *Declaración Universal de los Derechos Humanos*, artículo 12, 1948, p. 4, consultado el 19 de abril de 2019 en https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf.

72 Ver Barrena, Guadalupe, *El Pacto Internacional de Derechos Civiles y Políticos* (Fascículo 3), 2015, México, Comisión Nacional de los Derechos Humanos, consultado el 19 de abril de 2019 en <https://archivos.juridicas.unam.mx/www/bjv/libros/10/4890/13.pdf>.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.⁷³

En relación con lo señalado en el anterior punto uno, cabe señalar que los datos proporcionados por los informantes del sistema y utilizados para fines estadísticos, censales y geográficos no son producto de injerencias arbitrarias ni ilegales, ya que su captación está regulada en la *Ley del SNIEG*.⁷⁴ En lo que se refiere a lo señalado en el anterior punto dos, el INEGI cuenta con la facultad⁷⁵ para regular la captación, procesamiento y publicación de la información estadística y geográfica, así como para emitir las reglas⁷⁶ que permitan la protección de la confidencialidad los datos proporcionados por los informantes del sistema.

A continuación, se aborda el análisis del Convenio 108, documento que es legalmente vinculante para los Estados que lo firmaron y los que se adhirieron a éste. Del Convenio 108, en lo referente al manejo confidencial de la información, se hace énfasis en la protección de los datos personales, tanto en su acceso, modificación como en su divulgación.

2.1.2 Convenio No. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108)

Firmado el 28 de enero de 1981 por los Estados miembros del *Consejo de Europa*⁷⁷, el Convenio 108 entró en vigor el 1 de octubre de 1985. México se adhirió⁷⁸ y le es

73 Asamblea General de las Naciones Unidas, Pacto Internacional de Derechos Civiles y Políticos, *op. cit.*, nota 68.

74 Ver Cámara de Diputados del H. Congreso de la Unión, *Ley del Sistema...*, *op. cit.*, nota 1, p.15.

75 Ver Cámara de Diputados del H. Congreso de la Unión, *Constitución Política...*, *op. cit.*, nota 21, artículo 26, sección B.

76 Ver Cámara de Diputados del H. Congreso de la Unión, *Ley del Sistema...*, *op. cit.*, nota 1, artículo 45.

77 Creado el 5 de mayo de 1949, el Consejo de Europa está integrado por 47 países europeos, su objetivo principal es la defensa, protección y promoción de los derechos civiles y políticos, la democracia y el Estado de Derecho. Ver página de internet del Consejo de Europa, consultado el 21 de abril de 2019 en <https://www.coe.int/en/web/commissioner>.

78 La adhesión de México se dio en términos de lo señalado en el artículo 23, numeral 1, del Convenio 108, que permite la adhesión de Estados no miembros del Consejo de Europa. Ver Consejo de Europa, *Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal*, 1981, p. 9, consultado el 21 de abril de 2019 en <https://rm.coe.int/16806c1abd>.

aplicable desde el 1 de octubre de 2018. El Convenio 108 tiene carácter vinculante y tiene como fin: “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 («protección de datos»)”.⁷⁹

Referente a la seguridad de los datos, el Convenio 108 establece en el artículo 7, lo siguiente: “Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados”.⁸⁰

La propuesta de líneas generales de acción está orientada a preservar la confidencialidad de la información, tanto la que se almacena de manera digital como la que se transmite por medio de internet, por lo que se puede decir que la propuesta coadyuva al cumplimiento, en el ámbito de la información estadística y geográfica, de lo establecido en el artículo 7 del Convenio 108.

A continuación, se analiza el manejo de la confidencialidad de la información estadística bajo lo que se establece en el Reglamento No. 223/2009, documento que no es vinculante legalmente para el Estado Mexicano, pero que representa un referente en lo relativo a la generación, procesamiento y divulgación de las estadísticas oficiales y en el que se hace mención del manejo confidencial de la información recabada para fines estadísticos.

2.1.3 Reglamento (CE) No. 223/2009 del Parlamento Europeo y del Consejo (Reglamento 223/2009)

Relativo a la estadística europea, aprobado por el Parlamento Europeo y el Consejo de la Unión Europea el 11 de marzo de 2009, en vigor el 1 de abril de 2009; deroga el Reglamento (CE, Euratom) no 1101/2008 relativo a la transmisión a la Oficina

79 *Ibidem*, p. 2.

80 *Ibidem*, p. 4.

Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico, el Reglamento (CE) no 322/97 del Consejo sobre la estadística comunitaria y la Decisión 89/382/CEE, Euratom del Consejo por la que se crea un Comité del Programa Estadístico de las Comunidades Europeas. Para el Estado Mexicano no tiene carácter vinculante, solamente se trata de una referencia en la materia.

El Reglamento 223/2009 tiene por objeto⁸¹ establecer un marco jurídico para desarrollar, elaborar y difundir estadísticas europeas y en el capítulo V se aborda la protección, transmisión y acceso de los *datos confidenciales*.⁸²

En lo que se refiere al manejo confidencial se rige por el *secreto estadístico*, definido como la “protección de los datos confidenciales relativos a unidades estadísticas individuales que se obtienen directamente con fines estadísticos o indirectamente de fuentes administrativas u otras, lo que implica prohibir la utilización con fines no estadísticos de los datos obtenidos y su revelación ilegal”.⁸³ De la definición de anterior se identifican dos orientaciones en la protección de los datos:

1. Referente a los *datos confidenciales* que permiten la *identificación directa*⁸⁴ e *indirecta*⁸⁵ de las *unidades estadísticas*⁸⁶ individuales, y
2. La prohibición del uso del uso de los datos obtenidos con fines no estadísticos y su revelación ilegal.

81 Parlamento Europeo y Consejo de la Unión Europea, Reglamento (CE) no 223/2009 del Parlamento Europeo y del Consejo, artículo, 1, 2009, p. 2, consultado el 25 de abril de 2019 en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02009R0223-20150608&from=LT>.

82 *Ibidem*, p. 4. *Dato confidencial*, es un dato que permite identificar, directa o indirectamente, a las unidades estadísticas y divulgar, por tanto, información sobre particulares; para determinar si una unidad estadística es identificable, deberán tenerse en cuenta todos los medios pertinentes que razonablemente podría utilizar un tercero para identificar a la unidad estadística.

83 *Ibidem*, p. 3.

84 *Ídem*. La *identificación directa*, es la identificación de una unidad estadística por su nombre o apellidos, su domicilio o un número de identificación públicamente accesible.

85 *Ídem*. La *identificación indirecta*, es la identificación de una unidad estadística por otros medios que los de la identificación directa.

86 *Ibidem*, p. 4. Unidad estadística, unidad básica de observación, a saber, una persona física, un hogar, una empresa u otro tipo de operador al que se refieren los datos.

Conforme lo señalado en el anterior punto uno, se identifica que las acciones de confidencialidad están orientadas a preservar la privacidad de las unidades de estadística, sea por medio de los datos que los identifican directamente (entre ellos los datos personales, cuando se refiere a las personas físicas), así como de los datos que de manera indirecta permiten identificar al informante.

En el caso de la identificación directa las acciones de confidencialidad pueden incluir: el no captar los datos de identificación directa, el cifrado, el ofuscamiento, la anonimización y la disociación, entre otros. Mientras que para evitar la identificación indirecta incluye el uso de métodos como: supresión de valores individuales mediante la aplicación de un criterio de sensibilidad, el rediseño de cuadros estadísticos, la distorsión de datos en los cuadros estadísticos, la reducción de datos y la modificación de datos.

A continuación, se analiza el manejo de la confidencialidad desde la perspectiva de lo establecido en el Código de Buenas Prácticas de las Estadísticas Europeas, documento que es un referente para las autoridades estadísticas de los Estados, aunque su alcance está centrado en la Comunidad Europea.

2.1.4 Código de Buenas Prácticas de las Estadísticas Europeas

El Código de Buenas Prácticas de las Estadísticas Europeas adoptado, por primera vez en 2005 por el Comité del Programa Estadístico, modificado y adoptado en 2011 y 2017 por el Comité del Sistema Estadístico Europeo, dirigido a las autoridades estadísticas y comunitarias de la Unión Europea (para el Estado Mexicano no tiene carácter vinculante, solamente se trata de una referencia en la materia), tiene por objetivos:

- Aumentar la confianza en la independencia, la integridad y la responsabilidad de las autoridades nacionales de estadística y de Eurostat, así como en la credibilidad y la calidad de las estadísticas que elaboran y difunden;
- Promover la aplicación de los mejores principios, métodos y prácticas entre todos aquellos que elaboran las estadísticas europeas a fin de aumentar su calidad.⁸⁷

87 Ver página oficial del Instituto de Estadística del Comunidad de Madrid, consultado el 27 de abril de 2019 en <http://www.madrid.org/iestadis/fijas/otros/codigobucoeu.htm>.

El Código de Buenas Prácticas de las Estadísticas Europeas contiene tres secciones: “Entorno institucional, Procesos estadísticos y Producción estadística”,⁸⁸ en los cuales se describen dieciséis principios en la materia que deben seguir las autoridades nacionales y comunitarias europeas. El principio número cinco, confidencialidad y protección de datos, señala lo siguiente:

- a) Confidencialidad debe estar garantizada por ley;
- b) Firma del personal de un compromiso jurídico al momento de su contratación;
- c) Establecimiento de sanciones ante el incumplimiento deliberado de la confidencialidad estadística;
- d) Orientación e instrucción sobre la protección de la confidencialidad estadística en todos los procesos estadísticos, así como la disponibilidad de la política de confidencialidad al público;
- e) Adopción de medidas reguladoras, administrativas, técnicas y organizativas para proteger la seguridad e integridad de los datos estadísticos, y
- f) Aplicación de protocolos para el acceso de usuarios externos a los microdatos estadísticos.

La propuesta que comprende el presente documento toma como referencia lo señalado en el anterior inciso e), ya que en su más amplio sentido se busca emitir líneas generales de acción que permitan ayudar a preservar la confidencialidad de la información estadística y geográfica por medio del cifrado y la anonimización.

A continuación, se analiza lo que establece en términos del manejo de la confidencialidad de la información desde el Código regional de buenas prácticas en estadísticas para América Latina y el Caribe, región a la que pertenece el Estado Mexicano, por lo que se trata de una referencia directa en la materia.

88 Unión Europea, Código de Buenas Prácticas de las Estadísticas Europeas, 2018, consultado el 27 de abril de 2018 en https://www.ine.es/ine/codigobp/codigo_2017.pdf.

2.1.5 Código Regional de Buenas Prácticas en Estadísticas para América Latina y el Caribe

Aprobado en 2011 por la Comisión Económica para América Latina y el Caribe (CEPAL), constituye una referencia para los institutos de estadística de la región (no es un documento legalmente vinculante).

Dividido en tres secciones: Entorno institucional y Coordinación; Proceso estadístico y Producción estadística, describe diecisiete principios y ochenta y cuatro criterios de cumplimiento, en su principio número cuatro, señala lo siguiente: “Confidencialidad estadística: La oficina nacional de estadística y los demás miembros del sistema estadístico nacional deben garantizar la protección y confidencialidad de la información con la que se producen las estadísticas oficiales, así como evitar la identificación de las fuentes”.⁸⁹

El principio señalado contiene siete criterios de cumplimiento, de los cuales el criterio número tres señala que deben existir normas que regulen la confidencialidad, establece lo siguiente: “Deben existir normas y compromisos jurídicos de confidencialidad de información establecidos para el personal involucrado en la generación de estadísticas oficiales, que estipulan sanciones por incumplimiento”.⁹⁰

En general el Código Regional de Buenas Prácticas en Estadísticas para América Latina y el Caribe, respecto del manejo de la confidencialidad de la información, tiene la misma orientación y rubros que el Código de Buenas Prácticas de las Estadísticas Europeas.

La propuesta de líneas generales de acción para preservar la confidencialidad de la información estadística y geográfica está enmarcada en lo establecido en el principio número 4, confidencialidad estadística y en el criterio de

89 Comisión Económica para América Latina y el Caribe, Código regional de buenas prácticas en estadísticas para América Latina y el Caribe, 2011, p. 7, consultado el 28 de abril de 2019 en https://repositorio.cepal.org/bitstream/handle/11362/16422/FILE_148023_es.pdf?sequence=1&isAllowed=y.

90 *Ibidem*, pp. 7y 8.

cumplimiento número 3 (señalado anteriormente), ya que contribuirá a la regulación del manejo de la confidencialidad de la información estadística y geográfica.

A continuación, se describe lo que señala en lo referente al manejo de la confidencialidad en las Estadísticas Oficiales la Organización de las Naciones Unidas.

2.1.6 Principios Fundamentales de las Estadísticas Oficiales

Aprobados por la Asamblea General de las Naciones Unidas en 2014, dirigido a los Estados miembros de la ONU y a sus autoridades estadísticas, establece diez principios que sirven como referencia para establecer el marco jurídico e institucional que permita mantener la confianza de la sociedad y la credibilidad en las instituciones de estadística. Se trata de un documento que no es vinculante jurídicamente, es decir, representa una referencia a considerar, más no es obligatorio su cumplimiento.

El principio número seis indica el manejo de la confidencialidad de los datos recabados para fines estadísticos, mismo que a continuación se cita: “Principio 6. Los datos individuales que reúnan los organismos de estadística para la compilación estadística se refieran a personas naturales o jurídicas, deben ser estrictamente confidenciales y utilizarse exclusivamente para fines estadísticos”.⁹¹

Lo señalado en el anterior principio está en concordancia con lo que se establece, respecto del manejo de la confidencialidad de los datos proporcionados por los informantes, en los Códigos de Buenas Prácticas Estadísticas Europeas y de Estadísticas para América Latina y el Caribe, la diferencia es que no proporciona criterios de cumplimiento u otra información que permita su aplicación.

A continuación, se describe lo que establece la Recomendación del Consejo de la OCDE sobre buenas prácticas de estadística, el foco de atención es el manejo

91 Asamblea General de las Naciones Unidas, *Principios Fundamentales de las Estadísticas Oficiales*, 2014, p. 2, consultado el 29 de abril de 2019 en <https://unstats.un.org/unsd/dnss/gp/FP-New-S.pdf>.

de la confidencialidad de la información estadística, por ser el contexto en el que se sitúa la presente propuesta.

2.1.7 Recomendación del Consejo de la OCDE sobre buenas prácticas de estadística

Aprobado por el Consejo de la OCDE en 2015, es un documento que no es legalmente vinculante, se trata de una referencia para la operación de los institutos nacionales de estadística.

Las recomendaciones abordan los siguientes temas:

- a) Requisitos institucionales, jurídicos y de recursos que permiten que los sistemas estadísticos funcionen;
- b) Los métodos, la calidad y los procesos de producción estadística;
- c) Difusión;
- d) Coordinación, cooperación e innovación estadística.

La confidencialidad es parte de las recomendaciones comprendida como parte de los requisitos institucionales, jurídicos y de recursos que permiten que los institutos estadísticos funcionen, la cual señala lo siguiente: “4. Protejan la privacidad de los proveedores de datos (incluyendo individuos, hogares, empresas, administraciones, y todos los niveles de gobierno) y garantizar por ley la confidencialidad de la información personal proporcionada y su uso exclusivo para fines estadísticos”.⁹²

La recomendación emitida por el Consejo de la OCDE en lo referente a la preservación de la confidencialidad de los proveedores de datos es consistente con lo que se establece para tal fin en el *Código de Buenas Prácticas de las Estadísticas Europeas*, el *Código Regional de Buenas Prácticas en Estadísticas para América Latina y el Caribe*, así como de los *Principios Fundamentales de las Estadísticas*

92 Consejo de la OCDE, *Recomendación del Consejo de la OCDE sobre buenas prácticas estadísticas*, 2015, p. 11, consultado el 28 de abril de 2019 en https://www.oecd.org/statistics/good-practice-toolkit/Brochure-Recommendation%20of%20the%20OECD%20Council%20on%20Good%20Statistical%20Practice_SPANISH.pdf.

Oficiales de la ONU, que se revisaron anteriormente, documentos son una referencia para la elaboración de la propuesta del presente documento.

Finalmente, se aborda lo que se establece en el Reglamento General de Protección de Datos Personales respecto del manejo confidencial de la información, en este caso sobre los datos personales.

2.1.8 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (Reglamento General de Protección de Datos)

Aprobado por el Parlamento Europeo y el Consejo de la Unión Europea el 27 de abril de 2016, aplicable a partir del 25 de mayo de 2018, deroga la Directiva 95/46/CE. Para el Estado Mexicano no tiene carácter vinculante, solamente se trata de una referencia en la materia.

El Reglamento General de Protección de Datos tiene por objeto:

1. Establecer 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.
2. Proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.
3. Establecer la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.⁹³

En los siguientes artículos del Reglamento General de Protección de Datos se aborda el manejo de la confidencialidad de los datos personales:

- a) Artículo 5, numeral 1, inciso f, “tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)⁹⁴”.
- b) Artículo 32, numerales 1, 2, 3 y 4:

93 Parlamento Europeo y Consejo de la Unión Europea, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 2016, artículo, 1, p. 32, consultado el 22 de abril de 2019 en <https://www.boe.es/doue/2016/119/L00001-00088.pdf>.

94 *Ibidem*, p. 36.

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales sólo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.⁹⁵

El Reglamento señala el uso de medidas técnicas, organizativas, además de las legales para mantener la confidencialidad de los datos personales, entre las medidas que señala es la *seudonimización*⁹⁶ como una forma de que se procese la información preservando la privacidad de las personas a las que está asociada la información. También menciona los criterios a tomar en cuenta para considerar que se establecen medidas de seguridad razonables, de los cuales se hace mención en el artículo 32, numeral 1, del citado Reglamento.

Otros elementos a considerar en el establecimiento de medidas de protección que ayudan a mantener la confidencialidad de la información es el establecimiento

95 *Ibidem*, pp. 51 y 52.

96 Definida como “el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable”. *Ibidem*, p. 33.

de procesos de verificación, evaluación y valoración de la eficacia de las medidas establecidas, así como la evaluación de los riesgos, lo cual permite identificar las amenazas y vulnerabilidades con el fin de determinar medidas de protección, tanto preventivas como correctivas.

La revisión de los referentes regulatorios internacionales y el enfoque desde el cual se maneja el derecho a la privacidad y el establecimiento de medidas que contribuyen a preservar la confidencialidad, tanto de la información estadística como de los datos personales, contribuyen a delinear la orientación en la elaboración de la presente propuesta.

En los siguientes subtemas se describe el marco regulatorio mexicano teniendo presente como foco de atención el derecho a la privacidad y la protección de los datos personales en lo referente a la confidencialidad, el énfasis estará en la Ley del Sistema Nacional de Información Estadística y Geográfica, así como en el marco regulatorio interno del INEGI, por ser el ámbito al que se dirige la propuesta y en el cual se pretende contribuir.

2.2 Referencias del marco regulatorio mexicano sobre la confidencialidad de la información

En el marco regulatorio mexicano se encuentra referida la preservación de la confidencialidad de la información desde el ámbito de las telecomunicaciones, tema que no es objeto de análisis del presente documento, ya que la atención está en la preservación de la confidencialidad de la información estadística y geográfica, en la que se puede encontrar datos que permitan la identificación directa o indirecta de los informantes del SNIEG, de tal manera que el análisis comprende una visión tangencial desde las leyes de transparencia y acceso a la información pública y de la protección de los datos personales y de manera directa desde la Ley del SNIEG.

A continuación, se aborda el tema de la confidencialidad desde la visión referida en las leyes de transparencia y protección de datos personales.

2.2.1 La confidencialidad desde las leyes de transparencia y protección de datos personales

La Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), publicada en mayo de 2015, así como la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), cuya última reforma corresponde a enero de 2017, regulan el derecho de acceso a la información y en ambos casos se caracteriza a la información confidencial en los términos siguientes:

- I. La que contiene datos personales concernientes a una persona física identificada o identificable;
- II. Los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos, y
- III. Aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales.⁹⁷

Cabe la similitud de la orientación de los términos usados en la LGTAIP y la LFTAIP con lo referido en el Reglamento 223/2009, respecto de la información confidencial y los datos confidenciales, mientras que en las leyes de transparencia mexicanas se utilizan los términos identificada o identificable, en el citado reglamento europeo se utilizan los términos identificación directa e indirecta para referirse a qué se debe cuidar la confidencialidad tanto de los datos personales (los que identifican directamente (como el nombre y el domicilio), como de los que permiten identificar o hacen identificable a una persona.

En el caso de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO), publicada en enero de 2017, se hace explícita en la definición de datos personales la referencia sobre la identificación directa e indirecta, el cual se cita a continuación: “Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es

97 Cámara de Diputados del H. Congreso de la Unión, Ley Federal de Transparencia y Acceso a la Información Pública, artículo 113, p. 52, 2017, consultado el 02 de mayo de 2019 en http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf.

identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información”.⁹⁸

La LGPDPPSO señala tres tipos de medidas⁹⁹ para la protección de los datos personales: administrativas, físicas y técnicas, además señala la *disociación*¹⁰⁰ como una opción para evitar la asociación de los datos personales con su titular, de manera que se preserva la confidencialidad de los datos personales.

Cabe señalar que en ninguna de las leyes (LGTAIP, LFTAIP y LGPDPPSO) contiene la definición del concepto confidencialidad, aunque sí caracterizan lo que debe ser considerado como información confidencial; únicamente en el caso de la LGPDPPSO se mencionan medidas explícitas del cuidado de la confidencialidad, como es la disociación para evitar la identificación del titular de los datos personales.

Las leyes mencionadas anteriormente sirven como referencia de la protección de la confidencialidad en el marco regulatorio mexicano. Para el caso específico de la información estadística y geográfica corresponde la Ley del Sistema Nacional de Información Estadística y Geográfica, misma que se aborda a continuación desde el enfoque del cuidado de la confidencialidad.

2.2.2 La confidencialidad desde la Ley del Sistema Nacional de Información Estadística y Geográfica (Ley del SNIEG)

Publicada en el DOF en abril de 2008 y con última reforma en junio de 2018, tiene por objeto regular: el SNIEG, los derechos y obligaciones de los informantes del SNIEG, la organización y funcionamiento del INEGI, así como las faltas administrativas y el medio de defensa administrativo frente a los actos o resoluciones del INEGI.

El artículo 37 de la Ley del SNIEG establece que los datos proporcionados para fines estadísticos por los informantes del SNIEG serán estrictamente

98 Cámara de Diputados del H. Congreso de la Unión, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 3, fracción IX, *op. cit.*, nota 44, p. 3.

99 *Ibidem*, artículo 3, fracciones XXI, XXII y XXIII, pp. 3 y 4.

100 Es “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”, *ibidem*, artículo 3, fracción, XIII, p. 3.

confidenciales, lo mismo ocurre con los datos e informes que provengan de registros administrativos, de acuerdo con lo establecido en el artículo 38 de la Ley del SNIEG, en el que se menciona la prohibición de que no se puedan difundir de manera nominativa o individualizada, de tal forma que su divulgación se hará de manera que no se pueda identificar a los informantes del SNIEG, para lo cual el INEGI expedirá las normas que aseguren la correcta difusión y el acceso del público a la información.

El artículo 47 de la Ley del SNIEG señala que los datos proporcionados por los informantes del SNIEG son confidenciales en los términos de la citada ley y de las reglas generales que emita el INEGI.

El artículo 100 de la Ley del SNIEG señala que la Junta de Gobierno del INEGI establecerá los procedimientos y condiciones para facilitar el acceso a los microdatos, de tal manera que se preserve la confidencialidad y reserva de la información.

Se identifica en los cuatro artículos anteriormente referidos el deber de preservar la confidencialidad de la información estadística y geográfica, así como la facultad para emitir la regulación concerniente, de manera tal que la confidencialidad se debe preservar a través de todo el proceso de generación de la información estadística y geográfica. Es en ese sentido que se considera la propuesta de líneas generales de acción que coadyuven a preservar la confidencialidad de la información por medio del cifrado y anonimización.

A manera de conclusión del capítulo 2 se identifica que la confidencialidad es una obligación derivada de una medida legislativa, como lo es el secreto estadístico o los principios de confidencialidad estadística, que busca dar cumplimiento al derecho de las personas sobre la privacidad¹⁰¹ y a la protección de datos personales, los cuales son referidos en el artículo 16 constitucional, así mismo

101 Sobre el fundamento del derecho a la privacidad en los instrumentos internacionales en los que México está adherido hay que referirse a: la Convención Americana sobre Derechos Humanos, artículo 11; la Declaración Americana de los Derechos y Deberes del Hombre, artículo V; la Declaración Universal de los Derechos Humanos, artículo 12, y el Pacto Internacional de Derechos Civiles y Políticos, artículo 17.

permite dar cumplimiento al derecho de acceso a la información pública sin menoscabo de la privacidad y de la protección de los datos personales. En tal sentido se hace explícita la importancia de preservar la confidencialidad de los datos que se hayan captado con fines estadísticos dado el impacto sobre los derechos de los informantes del SNIEG ante la identificación directa o indirecta de éstos.



Capítulo 3

El cifrado y la anonimización como medidas para preservar la confidencialidad de la información



Capítulo 3: El cifrado y la anonimización de la información como medidas para preservar la confidencialidad de la información

El capítulo 3 describe las técnicas de anonimización y los algoritmos de cifrado como medidas que ayudan a la preservación de la confidencialidad.

El capítulo se divide en dos partes. La primera parte incluye una revisión de los principios de privacidad por diseño y su aplicación en la anonimización, los riesgos de la anonimización y las técnicas utilizadas para anonimizar la información.

En la segunda parte del capítulo se aborda el cifrado de datos, en el que se describe la clasificación del cifrado, los procedimientos básicos en el cifrado, los riesgos generales asociados con el cifrado y las características a considerar en los algoritmos de cifrado siguientes: TDEA, AES, RSA y ECC.

A continuación, se aborda la descripción de la anonimización.

3.1 La anonimización

En esta sección se abordan los principios de privacidad por diseño aplicables en la anonimización como una medida que coadyuva a preservar la confidencialidad de la información y con ello a mantener la privacidad de los informantes. También se describen los riesgos asociados de manera general con la anonimización, por lo que su aplicación puede implicar la combinación de técnicas de anonimización y de aplicación conforme cada caso particular. Finalmente se analizan las técnicas de anonimización siguientes: adición de ruido, permutación, privacidad diferencial, agregación, anonimato k , diversidad l y proximidad t .

A continuación, se describen los principios de privacidad por diseño, enfocados desde su aplicación en la anonimización como una medida que permite mantener la confidencialidad de la información y con ello preservar la privacidad de los informantes.

3.1.1 Principios de privacidad por diseño en la anonimización

La privacidad por diseño se define como “la filosofía y el enfoque de incorporar la privacidad en el diseño de las diferentes tecnologías”,¹⁰² lo cual facilita una visión sistémica en el cuidado de la confidencialidad dado que se considera el proceso completo de la anonimización, lo que permite minimizar los riesgos de pérdida de confidencialidad y se basa en los siguientes principios:¹⁰³

1. Proactivo, no reactivo, implica el análisis de riesgos y el establecimiento de medidas para disminuir las brechas de seguridad desde la planeación y la identificación de necesidades, de manera que se analice la posibilidad de que se pueda identificar la correspondencia de los datos con la persona a quien pertenecen;
2. Privacidad como configuración predeterminada, requiere que de manera inicial las medidas estén habilitadas para preservar la privacidad, es decir, que durante la operación no se deba realizar acción adicional para que las medidas de protección funcionen, de tal forma que si no se realiza ninguna acción la privacidad se mantiene;
3. Privacidad integrada en el diseño, para ello se debe considerar la protección de la privacidad como un complemento esencial de la funcionalidad sin disminuirla, no debe ser adicional a la operación, sino parte de ésta;
4. Funcionalidad completa, su aplicación implica evitar dicotomías, como seguridad frente a privacidad, es decir se debe cumplir con todos los objetivos buscados y no quitar uno para cumplir otro;
5. Privacidad en el ciclo de vida de la información, considera que las medidas de privacidad funcionan desde antes de que se capta la información hasta su destrucción, de tal manera que la privacidad se preserva durante todo el ciclo de vida de la información;

102 Ver Cavoukian, Ann, *Privacy By Design*, Information and Privacy Commissioner of Ontario, Ontario, 2009, consultado el 27 de mayo de 2019 en <http://www.ontla.on.ca/library/repository/mon/23002/289982.pdf>.

103 Cavoukian, Ann, *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*, Information and Privacy Commissioner of Ontario, Ontario, consultado el 29/05/2019 en https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

6. Visibilidad y transparencia, su aplicación implica asegurar que las tecnologías y las prácticas funcionan conforme a los objetivos y requerimientos planteados y que se puede verificar su operación, la cual es visible tanto para usuarios como para proveedores, y
7. Respeto por la privacidad del usuario, implica poner en primer plano los intereses de las personas y a partir de ello establecer las medidas de privacidad adecuadas.

La privacidad por diseño aplicada en la anonimización contribuye a crear una visión sistémica con orientación al establecimiento de medidas proactivas, comprendidas como parte de la funcionalidad de las tecnologías y de las prácticas de negocio, con el fin de minimizar los riesgos de pérdida de la confidencialidad de la información, de tal manera que se mantenga la privacidad de los informantes.

Al aplicar la anonimización, además de considerar la privacidad por diseño, también conviene conocer los riesgos que de manera general están asociados con la anonimización, mismos que se describen a continuación.

3.1.2 Riesgos de la anonimización

La anonimización, de manera general, tiene riesgos¹⁰⁴ que son inherentes a ésta, mismos que a continuación se describen:

- a) Singularización: la posibilidad de extraer de un conjunto de datos algunos registros (o todos los registros) que identifican a una persona;
- b) 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, y
- c) 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.

104 Ver Grupo de Trabajo sobre Protección de Datos del Artículo 29, Dictamen 05/2014 sobre técnicas de anonimización, 2014, p. 12, consultado el 30 de mayo de 2019 en https://gahazas.files.wordpress.com/2018/10/wp216_es_-tc3a9cnicas-de-anonimizacic3b3n.pdf.

La materialización de alguno de los riesgos antes señalados conlleva a la identificación directa o indirecta del informante, es decir, que al perderse la confidencialidad de la información se afecta la privacidad del informante, por lo que es necesario considerar las particularidades de cada una de las técnicas de anonimización con el fin de identificar fortalezas y debilidades de cada una y a partir de ello elegir la técnica conveniente conforme a cada caso particular.

A continuación, se describen las técnicas de anonimización, agrupadas conforme al enfoque de cada una de éstas, sea que corresponda a la aleatorización o a la generalización, así como las implicaciones que tiene su uso conforme los riesgos antes señalados.

3.1.3 Técnicas de anonimización

De manera general las técnicas de anonimización, conforme a su enfoque, se dividen en aleatorización y generalización. Las técnicas correspondientes al enfoque de aleatorización que se describen en el presente documento son: adición de ruido, permutación y privacidad diferencial; en cuanto al enfoque de generalización, las técnicas que se describen son: agregación, anonimato k , diversidad l y proximidad t .

La aleatorización es un enfoque de anonimización centrado en la modificación de los datos, con el fin de eliminar el vínculo entre los datos y la persona a la que identifican, lo que implica la pérdida de la veracidad de los datos. Entre las técnicas comprendidas en este enfoque están:

- a) Adición de ruido, consiste en modificar los datos originales, de tal forma que éstos sean inexactos y que conserven su distribución general. Dado que existen algunos atributos que son obvios y facilitarían la identificación a pesar de la aplicación de la adición de ruido, se suele utilizar de manera combinada con técnicas que eliminen determinados atributos. Las modificaciones (agregación de ruido) dependerán de la cantidad y tipo de información requerida. En cuanto a los riesgos, es posible que se pueda realizar la singularización de registros de una persona, aunque con datos

inexactos; el riesgo de vinculabilidad es posible, pero con datos no fiables; en el caso del riesgo de inferencia su probabilidad disminuye.

- b) Permutación, “consiste en mezclar los valores de los atributos en una tabla para que algunos de ellos puedan vincularse artificialmente a distintos interesados”,¹⁰⁵ esta técnica permite conservar la distribución de cada atributo en el conjunto de datos y se combina con la eliminación de atributos obvios para obtener la anonimización. Se combina con la eliminación de atributos obvios para obtener la anonimización. Para obtener beneficios su aplicación debe centrarse en datos que puedan facilitar la identificación del informante. Con el uso de esta técnica los riesgos de singularización, vinculabilidad e inferencia se mantienen, aunque con datos inexactos.
- c) Privacidad diferencial, su uso permite identificar cuánto ruido se debe añadir, y en qué forma, para preservar la privacidad ante la respuesta a un conjunto de consultas, de tal forma que se agrega ruido antes de entregar los resultados que dan respuesta a las consultas realizadas. Su aplicación evita el riesgo de la singularización, aunque los riesgos de vinculabilidad e inferencia son posibles en caso de que se generen varias consultas sobre el mismo conjunto de datos, por lo que el análisis de protección de privacidad debe realizarse en el contexto de las consultas que se han recibido sobre un conjunto determinado de datos.

La generalización se basa en la modificación de los datos para eliminar el vínculo entre los datos y la persona a la que identifican, ello implica la modificación de las respectivas escalas u órdenes de magnitud, con lo que se evita la singularización, en el caso de los riesgos de vinculabilidad e inferencia se requiere combinar enfoques cuantitativos. Entre las técnicas comprendidas en este enfoque están:

- a) Agregación y Anonimato k, su objetivo es impedir la singularización por medio de la agrupación en un conjunto con k datos, de tal forma que dentro del conjunto todos tienen el mismo valor. Al aplicar las técnicas de

105 *Ídem.*

agregación y anonimato k se evita el riesgo de singularización. La probabilidad del riesgo de vinculabilidad disminuye. Para quienes sus datos están dentro del conjunto k es factible que pueden inferir a la correspondencia entre los valores y a quién pertenecen. Un aspecto a considerar en la aplicación de la técnica de anonimato k es que el valor del conjunto k es directamente proporcional a la garantía de privacidad que se ofrece.

b) Diversidad l y Proximidad t . En el caso de la diversidad l se busca crear conjuntos con al menos l valores diferentes con el fin de limitar que existan conjuntos con variabilidad escasa entre sus valores. La proximidad t busca crear conjuntos equivalentes con la misma distribución inicial que los datos no agrupados. Además de que en cada conjunto existan al menos l valores diferentes se busca que cada valor esté presente tantas veces como sea necesario para reflejar la distribución inicial de los datos. Su aplicación evita los riesgos de singularización e inferencia, pero permanece el riesgo de vinculabilidad.

En la preservación de la privacidad se pueden utilizar diferentes técnicas de anonimización, cada una de ellas permite disminuir la probabilidad de ocurrencia de los riesgos asociados con la anonimización, lo cual debe considerarse en la elección de la o las técnicas de anonimización a utilizar con el fin de preservar la privacidad y al mismo tiempo evaluar la utilidad de la información que se obtiene posterior a la aplicación de las técnicas de anonimización.

Además de la anonimización también se puede utilizar el cifrado como medida para mantener la confidencialidad de la información y con ello contribuir a preservar la privacidad de los informantes, tema que se aborda a continuación.

3.2 El cifrado

Conforme se definió en la sección I, el cifrado corresponde a la alteración por medio de métodos matemáticos¹⁰⁶ de los datos mediante una clave para hacerlos ilegibles a quienes no posean la clave, de tal forma que para hacer legible la información corresponde realizar un proceso de descifrado haciendo uso de la clave con la que se cifró.

En esta sección se describe la clasificación del cifrado, los procedimientos básicos de cifrado: sustitución y transposición, los riesgos que existen en su uso y los algoritmos de cifrado.

A continuación, se aborda la clasificación de los tipos de cifrado.

3.2.1 Clasificación del cifrado

El cifrado se puede clasificar según el tipo de clave utilizada, es decir si se utiliza una sola clave tanto para cifrar como para descifrar los datos, o si por el contrario se utilizan dos claves, una para cifrar los datos y otra para descifrarlos: cifrado asimétrico (de dos claves) y cifrado simétrico (de una clave).

Los métodos de cifrado que utilizan una sola clave para cifrar y descifrar los datos se denominan de *cifrado simétrico*. Cuando se utiliza este método es conveniente tomar medidas de protección para asegurar que la clave solamente será conocida por las partes que intervienen en la comunicación, lo cual conlleva la necesidad de establecer acuerdos sobre la forma de cuidar la clave tanto por el emisor como del receptor, o en su caso que se tomen las medidas pertinentes para establecer una forma de dar a conocer la clave por medio de un medio de comunicación seguro.

El cifrado simétrico conforme el tratamiento que se le da a los datos se subdivide en:

106 La criptografía estudia las técnicas matemáticas, algoritmos, protocolos y sistemas que se utilizan para mantener la seguridad de la información.

- a. *Cifrado en bloque*, en este tipo de cifrado la alteración de los datos “se aplica sobre un grupo (bloque) de símbolos del alfabeto en el que está escrito el mensaje original dando lugar a un bloque de texto cifrado”.¹⁰⁷ El tamaño del bloque a cifrar depende del algoritmo utilizado.
- b. *Cifrado en flujo*, en este tipo de cifrado la alteración de los datos “se aplica sobre cada símbolo del alfabeto en el que está escrito el mensaje original”.¹⁰⁸

En el cifrado asimétrico la clave de cifrado es diferente de la clave de descifrado. A la clave de cifrado se le conoce como clave pública y no se requiere de restricciones para que se conozca. Situación contraria ocurre con la clave de descifrado, ésta solamente es conocida por la parte interesada y no debe compartirla con nadie con el fin de preservar la confidencialidad de los datos que se cifraron. Cabe señalar que el uso del cifrado asimétrico no enfrenta el riesgo del cuidado en la distribución de la clave.

Al cifrado simétrico también se le conoce como cifrado de clave secreta y al cifrado asimétrico se le conoce como cifrado de clave pública.

Es de resaltar que las clasificaciones mencionadas anteriormente permiten identificar las características genéricas de los algoritmos de cifrado, así como las acciones de administración que se deben realizar sobre la clave de cifrado, lo cual constituye información a considerar en el análisis en la decisión sobre el algoritmo a utilizar para cifrar los datos.

A continuación, se describen los procedimientos básicos de cifrado.

3.2.2 Procedimientos básicos de cifrado: sustitución y transposición

En general el cifrado de los datos constituye un intercambio de símbolos para que los datos solamente sean legibles para quien tiene la clave que permite identificar

107 Centro Criptológico Nacional, *Guía de Seguridad de la TIC. CCN-STIC 807. Criptología de empleo en el Esquema Nacional de Seguridad*, p. 26, 2017, consultado el 12 de julio de 2019 en <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html>.

108 *Ibidem*, p. 25.

la forma en la que se intercambiaron los símbolos. El intercambio de los símbolos se puede realizar por medio de los procedimientos¹⁰⁹ de sustitución o transposición de éstos.

La *sustitución* “consiste en establecer una correspondencia entre las letras del alfabeto en el que está escrito el mensaje original y los elementos de otro conjunto, que puede ser el mismo o distinto alfabeto”¹¹⁰. En la sustitución el intercambio entre los símbolos es uno a uno tanto en el cifrado como en el descifrado.

La *transposición* utiliza los mismos símbolos contenidos en los datos a cifrar, pero los coloca en un orden distinto al original, de tal forma que su contenido resulta incomprensible. Se puede decir que la transposición “consiste en «barajar» los símbolos del mensaje original colocándolos en un orden distinto”¹¹¹, el descifrado implica que se conoce la clave que permite ordenar los datos y hacerlos legibles.

Los métodos de cifrado pueden combinar el uso de la sustitución y de la transposición, para lo cual se utiliza algún método matemático para generar las claves mediante operaciones llamadas “de una sola vía”, que son operaciones matemáticas simples en su cálculo pero que resultan difícil de revertir¹¹², sin embargo ello no implica que no exista el riesgo de que se pueda conocer la clave de cifrado.

A continuación, se describen los riesgos relacionados con el cifrado.

3.2.3 Riesgos en el cifrado

En el caso del cifrado simétrico el principal riesgo reside en que alguna persona no autorizada conozca la clave utilizada, por lo que se vuelve un tema relevante la

109 “Dos procedimientos de cifrado básicos se han ido repitiendo sistemáticamente a lo largo de los siglos hasta llegar a nuestros días. Son los principios de sustitución y transposición”, *Ibidem*, p. 26

110 *Ibidem*, p. 26

111 *Ibidem*, p.26

112 Ver Cordoba, Diego y Méndez-Garabetti, Miguel, “Criptografía Post Cuántica”, consultado el 12/07/2019 en http://sedici.unlp.edu.ar/bitstream/handle/10915/62685/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

forma en la que se da a conocer la misma a las partes interesadas, así como las medidas que se toman para administrarla.

En el caso del cifrado asimétrico el riesgo al que se enfrenta es que se pueda conocer la clave probando las combinaciones posibles hasta que se encuentra la que permite el acceso, lo cual se le conoce como ataque de fuerza bruta.

Respecto del riesgo asociado con el control de la clave de cifrado las medidas para contrarrestarlo implican, tanto medidas tecnológicas para administrar las claves, como medidas administrativas y legales en las que se regule la actuación de las personas que están relacionadas con el manejo de las claves.

En el caso del riesgo asociado con los ataques de fuerza bruta, la solución es utilizar algoritmos de cifrado que estén certificados por algún organismo de estandarización. En México es la Dirección General de Normas de la Secretaría de Economía la encargada de coordinar el sistema de normalización. A nivel internacional se puede citar los siguientes organismos:

- a. Instituto Nacional Americano de Estándares (American National Standards Institute, ANSI);
- b. Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC);
- c. Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers, IEEE);
- d. Organización Internacional para la Estandarización (International Organization for Standardization, ISO);
- e. Instituto Nacional de Estándares y Tecnología norteamericano (National Institute of Standards and Technology, NIST);
- f. Grupo de Estándares para la Criptografía Eficiente (Standards for Efficient Cryptography Group, SECG).

Es importante considerar a la seguridad en términos de su administración, con el fin de emprender acciones que permitan evitar, disminuir y controlar los riesgos.

3.2.4 Algoritmos de cifrado

Existen varios algoritmos de cifrado de datos, los cuales proveen determinado *nivel de seguridad*¹¹³ de que la clave de cifrado no podrá ser identificada por medio de criptoanálisis.¹¹⁴ A continuación se describen¹¹⁵ los tamaños de clave sugeridos por el Centro Criptológico Nacional de España para los algoritmos de cifrado siguientes: TDEA, AES, RSA y ECC.

- a. TDEA, es un algoritmo simétrico de bloque que consiste en la concatenación de tres algoritmos DEA (Data Encryption Algorithm, algoritmo de cifrado en bloque cuya longitud de bloque es de 64 bits, de los cuales 8 se utilizan como medio de detección de errores y 56 bits para genera la clave, lo que significa que existen 2^{56} claves diferentes).¹¹⁶ Existen tres variantes del TDEA, conforme a las claves que se utilizan:
 - i. Variante 1: las tres claves son iguales. La seguridad efectiva es de 56 bits y la longitud real de clave es 56 bits (más 8 que se utilizan como medio de detección de errores);
 - ii. Variante 2: la primera y tercera claves son iguales mientras que la segunda es diferente e independiente de las otras. La seguridad efectiva es de 80 bits y la longitud real de clave es 112 bits (más 16 bits que se utilizan como medio de detección de errores);

113 El nivel de seguridad de un algoritmo de cifrado se da generalmente como el número de operaciones necesarias para que un adversario rompa con éxito la seguridad proporcionada por el algoritmo y el número de operaciones está relacionado con el número de bits (un bit es la unidad mínima de información en informática y puede tomar dos valores: 0 y 1) utilizados para generar la clave. Ver Grupo de Trabajo de Criptografía SOG-IS, Esquema de evaluación criptográfica SOG-IS. Mecanismos criptográficos convenidos, p. 9, 2018, consultado el 13 de julio de 2019 en <https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.1.pdf>.

114 El Criptoanálisis es el conjunto de técnicas que se utilizan para identificar las claves generadas a partir de la criptografía.

115 Se enlistan los algoritmos de cifrado simétricos y asimétricos acreditados por dos instancias: el Centro Criptológico Nacional de España y el sistema de certificación europeo del Grupo de Altos Funcionarios de Seguridad de Sistemas de Información (SOG-IS), ya que se considera que las referencias técnicas son actuales. En el caso del Centro Criptológico el documento de referencia se emitió en abril de 2017 y para el caso de SOG-IS se emitió en junio de 2018. Ver sitios oficiales de internet: <https://www.ccn-cert.cni.es/> y <https://www.sogis.eu/>, respectivamente.

116 El resultado de elevar el número 2 a la 256 potencia es 72,057,594,037,927,900. El número 2 corresponde a los dos valores posibles que puede tomar un bit: 0 y 1, mientras que el número 56 corresponde a la cantidad de bits que son utilizados para genera la clave de cifrado.

- iii. Variante 3: las tres claves son diferentes e independientes entre sí. La seguridad efectiva es de 112 bits, la longitud real de clave es 168 bits (más 24 bits que se utilizan como medio de detección de errores).

En caso de requerirse de un nivel de seguridad mayor de deben utilizar algoritmos con claves de seguridad efectiva comprendida entre 128 y 256 bits.

- b. AES, es un algoritmo simétrico de bloque en el que se pueden establecer claves de 128, 192 o 256 bits, con un nivel efectivo de seguridad para cualquier tamaño de clave. En el caso de que se necesite mantener archivos cifrados por más de una década la sugerencia es que se utilice una clave con longitud de 256 bits, ello con el fin de prever que puedan crearse innovaciones que afecten la seguridad de las claves que se generan a partir de 128 y 196 bits;
- c. RSA, se trata de un algoritmo en el que tanto la clave privada como la clave pública sirven para cifrar y descifrar por igual. Se recomienda establecer claves con longitud igual o mayor a los 2048 y 3072 bits, con lo que se obtendría un nivel de seguridad efectivo de 112 y 128 bits respectivamente;
- d. ECC, se trata de un algoritmo de cifrado asimétrico en el que se recomienda establecer claves con longitud igual o mayor a los 256 y 384 bits, con lo que se obtendría un nivel de seguridad efectivo de 128 y 192 bits respectivamente.

El cifrado de los datos permite establecer una medida de seguridad que orientada a preservar la confidencialidad de la información tanto en la transmisión como en su almacenamiento, aun cuando existen riesgos de que se logre identificar las claves de cifrado, cabe resaltar que el tiempo de cómputo requerido para procesar las operaciones, el conocimiento necesario y los recursos de cómputo actuales para realizarlo son significativos, es decir, no están fuera del alcance la mayoría de la población, por lo que su uso es recomendable para preservar la confidencialidad de la información.

En el caso de la anonimización resulta conveniente su uso, tanto en el almacenamiento como en la difusión y coyunturalmente en la transmisión, ya que, aunque no evita que se conozca la información que se transmite, su diseño sí disminuye la posibilidad de que se logre la identificación directa e indirecta del informante.

La combinación de las medidas de anonimización y cifrado de la información ayudan a incrementar el nivel de confidencialidad sobre la información, ya que las medidas de anonimización, la privacidad por diseño y el cifrado son aplicables directamente a los datos, es decir, son medidas que van directo al objeto de protección, disminuyendo con ello los riesgos de pérdida de la confidencialidad.



Conclusiones



Conclusiones

En el desarrollo del documento se abordaron los siguientes temas: Marco contextual y conceptual de la información estadística y geográfica y la confidencialidad. Referencias del marco regulatorio internacional y mexicano sobre la confidencialidad de la información, y el cifrado y la anonimización como medidas para preservar la confidencialidad de la información, de los cuales a continuación se presentan las conclusiones obtenidas de cada uno de los temas.

Referente al marco contextual y conceptual de la información estadística y geográfica y la confidencialidad se concluye lo siguiente:

1. La información estadística y geográfica es la base para la toma de decisiones en la construcción del Estado Mexicano, información que históricamente se ha captado con el fin de identificar los recursos con los que se cuenta y la forma en la que están distribuidos geográficamente, de cuyo análisis se pueden crear las políticas públicas sobre las que se sustente el desarrollo social y económico;
2. La captación de los datos proviene de censos, encuestas y registros administrativos, con lo que se ha cubierto las necesidades de información para la generación de las estadísticas sociodemográficas, de gobiernos, seguridad pública, justicia, económicas, geográficas y del medio ambiente.
3. Actualmente se realizan análisis estadísticos a partir de datos que se registran en internet, ampliando con ello las fuentes de información para la generación de la estadística;
4. La preservación de la confidencialidad de la información es un reto que requiere del establecimiento de: medidas físicas, como el establecimiento de áreas de acceso restringido; medidas legales y administrativas como la firma acuerdos de preservación de la confidencialidad, así como de medidas tecnológicas, entre éstas el establecimiento de nombre de usuario y contraseña para otorgar el acceso a recursos digitales;
5. Mantener la confidencialidad de la información estadística y geográfica implica la participación de diferentes áreas y en cada una de ellas con un

enfoque particular, de tal manera que los riesgos asociados con la pérdida y el robo de la información pueden tener diferente origen y con una misma consecuencia: la afectación de la privacidad de los informantes del Sistema y con ello la disminución de la confianza que la sociedad ha depositado en el INEGI;

6. El uso de dispositivos tecnológicos en el proceso de producción de información estadística y geográfica ha incrementado las formas en las que se puede vulnerar la confidencialidad de la información, aunque también se han incrementado las medidas de protección que se pueden utilizar para preservarla;
7. La pérdida de la confidencialidad estadística y geográfica puede tener repercusiones de diferente índole, dependiendo del tipo y cantidad de información sobre la que se haya vulnerado la confidencialidad, de tal forma que sus impactos pueden repercutir en el ámbito económico, político y social del país;
8. El INEGI tiene múltiples medidas que están orientadas a la preservación de la confidencialidad de la información, medidas que se aplican en todas las fases del proceso de producción de información estadística y geográfica.

Las conclusiones obtenidas de la revisión de las referencias del marco regulatorio internacional y mexicano sobre la confidencialidad de la información son:

1. En el ámbito de la generación de la información estadística y geográfica, la confidencialidad de la información es un mecanismo que permite dar cumplimiento al derecho a la privacidad;
2. Resulta relevante identificar el origen del que se deriva la obligación de preservar la confidencialidad. En el caso de la información estadística y geográfica, en su forma se busca evitar la identificación directa e indirecta de los informantes del Sistema y la identificación directa se realiza por medio de los datos personales o de los datos de la razón social, sin embargo, la sustancia reside en evitar que se dé a conocer la información que fue conferida, lo cual está relacionado directamente con el derecho a la

privacidad, ya que ello implica obligaciones de no revelar lo que fue informado;

3. La confidencialidad de la información estadística y geográfica está estrechamente vinculada con la reserva de la información, la cual implica que la información solamente sea utilizada para fines estadísticos;
4. La preservación de la confidencialidad de la información estadística y geográfica contribuye a mantener la confianza que la sociedad confiere a las oficinas que generan la estadística oficial.

Finalmente, del contenido analizado sobre el cifrado y la anonimización como medidas para preservar la confidencialidad de la información se obtuvieron las conclusiones siguientes:

1. La anonimización es una medida que contribuye a preservar la confidencialidad de la información estadística y geográfica, la cual puede ser aplicada desde la fase del diseño del proceso de producción de información estadística y geográfica y dar resultados en todo el proceso;
2. El cifrado es una medida que contribuye a preservar la confidencialidad de la información, en el proceso de la información estadística y geográfica su aplicación se realiza a partir de la fase de captación y tiene especial relevancia en el almacenamiento y transmisión de la información, ya que se requiere de conocer la clave para poder descifrar la información que fue cifrada;
3. La aplicación de los principios de privacidad por diseño enfocados en el proceso de anonimización facilita la identificación de una visión sistémica en el cuidado de la confidencialidad de la información, de tal manera que se puedan establecer medidas proactivas desde el diseño, la configuración de los sistemas informáticos y durante todo el ciclo de vida de la información;
4. Al seleccionar las técnicas de anonimización se deben tener presentes los riesgos inherentes a cada uno de ellos, de tal forma que se puedan complementar con otras medidas de privacidad por diseño para preservar la confidencialidad;

5. Al evaluar los riesgos de pérdida de confidencialidad se debe conocer la información que se ha publicado anteriormente o que se ha otorgado por medio de consultas específicas, así como la información que otras fuentes han publicado respecto de la misma temática, ello con el fin de evitar la identificación indirecta de los informantes del Sistema;
6. Los métodos de cifrado basan su nivel de seguridad en la cantidad de posibles combinaciones que existen para generar una clave, sin embargo, los avances tecnológicos incrementan la capacidad de cómputo rápidamente, por lo que se deberá mantener una verificación periódica con el fin de verificar que los algoritmos de cifrado seleccionados continúan siendo seguros;
7. Independientemente del algoritmo de cifrado que se elija es necesario realizar una gestión adecuada de las claves de cifrado, ya que al conocerse la clave la seguridad se rompe completamente.

Bibliografía

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Orientaciones y garantías en los procedimientos de anonimización de datos*, España, 2016, en <https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf>.
- ALVARADO VALENCIA, Jorge Andrés y OBAGI ARAÚJO, Juan José, *Fundamentos de inferencia estadística*, 2008, Colombia, Editorial Pontificia Universidad Javeriana, 2008.
- ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, *Declaración Universal de los Derechos Humanos*, 1948, en https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf.
- ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, *Pacto Internacional de Derechos Civiles y Políticos*, 1966, en <https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx>.
- ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, *Principios Fundamentales de las Estadísticas Oficiales*, 2014, en <https://unstats.un.org/unsd/dnss/gp/FP-New-S.pdf> <https://unstats.un.org/unsd/dnss/gp/FP-New-S.pdf>.
- BARRENA, Guadalupe, *El Pacto Internacional de Derechos Civiles y Políticos* (Fascículo 3), México, 2015, México: Comisión Nacional de los Derechos Humanos, en <https://archivos.juridicas.unam.mx/www/bjv/libros/10/4890/13.pdf>.
- CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, *Código Penal Federal*, México, Diario Oficial de la Federación, 14 de abril de 2019, en http://sc.inegi.org.mx/repositorioNormateca/Lmj2_SNIEG.pdf.
- CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, *Constitución Política de los Estados Unidos Mexicanos*, México, 2018, en http://www.diputados.gob.mx/LeyesBiblio/pdf/1_120419.pdf.
- CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, *Ley del Sistema Nacional de Información Estadística y Geográfica*, México, Diario Oficial de la Federación, 16 de junio de 2018, en http://www.diputados.gob.mx/LeyesBiblio/pdf/LSNIEG_250618.pdf.

CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, *Ley Federal de Transparencia y Acceso a la Información Pública*, México, Diario Oficial de la Federación, 9 de mayo de 2017, en http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf.

CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, México, Diario Oficial de la Federación, 26 de enero de 2017, en <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>.

CAVOUKIAN, Ann, "Privacy By Design", Information and Privacy Commissioner of Ontario, Canadá, en <http://www.ontla.on.ca/library/repository/mon/23002/289982.pdf>.

CENTRO CRIPTOLÓGICO NACIONAL, *Guía de Seguridad de la TIC. CCN-STIC 807. Criptología de empleo en el Esquema Nacional de Seguridad*, España, Ministerio de Hacienda y Función Pública, p.26, 2017, en <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html>.

COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE, *Código regional de buenas prácticas en estadísticas para América Latina y el Caribe*, Conferencia Estadística de las Américas de la CEPAL, República Dominicana, 2011, en https://repositorio.cepal.org/bitstream/handle/11362/16422/FILE_148023_es.pdf?sequence=1&isAllowed=y.

COMITÉ DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN, *Manual de Integración y Funcionamiento del Comité del Sistema de Seguridad de la Información*, México, INEGI, Dirección General de Integración, Análisis e Investigación, 2015, en <http://sc.inegi.org.mx/repositorioNormateca/Manual%20IFCdeSSI.pdf>.

CONSEJO DE EUROPA, Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal, Estrasburgo, Serie de Tratados Europeos núm. 108, 1981, en <https://rm.coe.int/16806c1abdhttps://rm.coe.int/16806c1abd>.

CONSEJO DE EUROPA, Página de internet del Consejo de Europa, en <https://www.coe.int/en/web/commissioner>.

CONSEJO DE LA OCDE, Recomendación del Consejo de la OCDE sobre buenas prácticas estadísticas, Traducción no oficial del Instituto Nacional de Estadística e Informática (INEI) de Perú, 2015, en https://www.oecd.org/statistics/good-practice-toolkit/Brochure-Recommendation%20of%20the%20OECD%20Council%20on%20Good%20Statistical%20Practice_SPANISH.pdf.

CORDOBA, Diego y MÉNDEZ-GARABETTI, Miguel, “*Criptografía Post- Cuántica integrada en SSL/TLS y HTTPS*”, XXI Workshop de Investigadores en Ciencias de la Computación, Facultad de Ciencias Exactas, Físicas y Nucleares, Argentina, Universidad de San Juan, en Repositorio Institucional de la Universidad Nacional de la Plata en http://sedici.unlp.edu.ar/bitstream/handle/10915/62685/Documento_completo.pdf-PDFA.pdf?sequence=1&isAll.

DOMÍNGUEZ MARTÍNEZ, Jorge Alfredo, “Orden público y autonomía de la voluntad”, en SÁNCHEZ BARROSO, José Antonio (coord.), *Cien años de Derecho Civil en México, 1910-2010, Conferencias en homenaje a la Universidad Nacional Autónoma de México por su centenario*, México, Colegio de Profesores de Derecho Civil de la Facultad de Derecho de la UNAM, 2011 en <https://archivos.juridicas.unam.mx/www/bjv/libros/8/3834/9.pdf>.

GONZÁLEZ, G. en ESCOBAR MARTÍNEZ, Jorge Iván. y QUINTO ROJAS, Luis Carlos, “Vulnerabilidad en dispositivos móviles con sistema operativo Android”, *Cuaderno Activa*, núm. 7, 2015, en ojs.tdea.edu.co/index.php/cuadernoaactiva/article/download/248/240/.

ESET, *Cifrado de la información, Guía corporativa*, 2014, en https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014v2.pdf.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 05/2014 sobre técnicas de anonimización, 2014, en https://gahazas.files.wordpress.com/2018/10/wp216_es_-tc3a9cnicas-de-anonimizacic3b3n.pdf.

INSTITUTO DE ESTADÍSTICA DEL COMUNITAT DE MADRID, Pàgina de internet oficial, en <http://www.madrid.org/iestadis/fijas/otros/codigobucoeu.htm>.

INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, *Estadísticas históricas de México* 2014, 2015, en http://internet.contenidos.inegi.org.mx/contenidos/productos/prod_serv/contenidos/espanol/bvinegi/productos/nueva_estruc/HyM2014/EHM2014.pdf.

INSTITUTO NACIONAL DE ESTADÍSTICA, GEOGRAFÍA E INFORMÁTICA, *Catálogo de Documentos Históricas de la Estadística en México (Siglos XVI-XIX)*, 2005, <http://tjay.org.mx/wp-content/uploads/2013/05/Catalogo-de-documentacion-historica-INEGI-1.pdf>.

INSTITUTO NACIONAL DE ESTADÍSTICA, GEOGRAFÍA E INFORMÁTICA, *Estadísticas Históricas de México*, Tomo I, 1994, en http://internet.contenidos.inegi.org.mx/contenidos/productos/prod_serv/contenidos/espanol/bvinegi/productos/integracion/pais/historicas/EHM1.pdf.

INSTITUTO NACIONAL DE ESTADÍSTICA, GEOGRAFÍA E INFORMÁTICA, *Reglas de Operación del Laboratorio de Microdatos del INEGI*, 2015, en http://sc.inegi.org.mx/repositorioNormateca/Or_03sep15.pdf.

JUNTA DE GOBIERNO DEL INEGI, Norma técnica del proceso de producción de información estadística y geográfica para el Instituto Nacional de Estadística y Geografía, 2018, en http://sc.inegi.org.mx/repositorioNormateca/O_05Sep18.pdf.

JUNTA DE GOBIERNO DEL INEGI, *Políticas para la Seguridad de la Información del Instituto Nacional de Estadística y Geografía*, 2014, en http://sc.inegi.org.mx/repositorioNormateca/Pod_17Dic14.pdf.

JUNTA DE GOBIERNO DEL INEGI, *Principios y Buenas Prácticas para las Actividades Estadísticas y Geográficas del SNIEG*, 2015, en https://www.snieg.mx/DocumentacionPortal/Normatividad/vigente/Principios_Buenas_Practicas_Es_Geo_SNIEG.pdf.

JUNTA DE GOBIERNO DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, *Reglamento de Transparencia y Acceso a la Información Pública del INEGI*, 2015, en http://sc.inegi.org.mx/repositorioNormateca/RT_Ago15.pdf.

- JUNTA DE GOBIERNO DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, Norma Técnica del Proceso de Producción de Información Estadística y Geográfica para el Instituto Nacional de Estadística y Geografía, 2018, en http://sc.inegi.org.mx/repositorioNormateca/O_05Sep18.pdf.
- MEGÍAS QUIRÓS, José Justo, "Privacidad e internet: intimidad, comunicaciones y datos personales", Anuario de Derechos Humanos. Nueva Época, vol. 3, 2002, en <https://revistas.ucm.es/index.php/ANDH/article/view/ANDH0202110515A/20978>.
- ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA EDUCACIÓN, LA CIENCIA Y LA CULTURA, Página de internet oficial de la UNESCO, *Más sobre la naturaleza y el estatus de los instrumentos legales y programas*, en <http://www.unesco.org/new/es/social-and-human-sciences/themes/advancement/networks/lamo/legal-instruments/nature-and-status/>.
- ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Departamento de Asuntos Económicos y Sociales, Guía de elaboración de estadísticas sobre el empleo del tiempo para medir el trabajo remunerado y no remunerado*, 2006.
- ORGANIZACIÓN DE LAS NACIONES UNIDAS, Página de internet oficial, *Glosario de términos relativos a los procedimientos de los tratados*, en https://treaties.un.org/pages/Overview.aspx?path=overview/glossary/page1_en.xml#accession.
- PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA, Reglamento (CE) no 223/2009 del Parlamento Europeo y del Consejo, 2009, en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02009R0223-20150608&from=LT>.
- PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 2016, en <https://www.boe.es/doue/2016/119/L00001-00088.pdf>.
- REAL ACADEMIA ESPAÑOLA, *Diccionario de la lengua española*, modalidad en línea, actualización 2018, en <https://dle.rae.es/?id=UD4g0KW>.
- SECRETARÍA DE GOBERNACIÓN, *Doctrina y Lineamientos para la redacción de textos jurídicos, su publicación y divulgación*, México, 2005, 19 en <http://www.ordenjuridico.gob.mx/Publicaciones/okDoctrinas.pdf>.

TRIBUNALES COLEGIADOS DE CIRCUITO. Novena Época. *Semanario Judicial de la Federación y su Gaceta*, Tomo XXI, 2005, en <http://sjf.scjn.gob.mx/sjsist/Documentos/Tesis/178/178594.pdf>.

UNIÓN EUROPEA, *Código de buenas prácticas de las estadísticas europeas*, 2018, consultado el 27/04/2018 en https://www.ine.es/ine/codigobp/codigo_2017.pdf.



Anexo



Propuesta de líneas generales de acción para preservar la confidencialidad de la información estadística y geográfica a través del cifrado y anonimización

I. Introducción

Conforme se establece en la Constitución Política de los Estados Unidos Mexicanos, el Instituto Nacional de Estadística y Geografía (INEGI), es un organismo con autonomía técnica y de gestión, personalidad jurídica y patrimonio propios, con las facultades necesarias para regular la captación, procesamiento y publicación de la información que se genere y proveer a su observancia.

El INEGI con el fin de coadyuvar al desarrollo nacional proporciona a la sociedad y el Estado Mexicano información estadística y geográfica de calidad, pertinente, veraz y oportuna, en cuyo proceso de generación debe asegurar la confidencialidad de los datos que proporcionan los informantes del Sistema Nacional de Información Estadística y Geográfica conforme lo establecido en la ley en la materia, así como en el sexto principio fundamental de las Naciones Unidas sobre Estadística Oficial y en el cuarto principio del Código Regional de Buenas Prácticas en Estadísticas para América Latina y el Caribe.

Preservar la confidencialidad de los datos que proporcionan los informantes del Sistema como la de los datos individualizados es uno de los pilares sobre los que se mantiene la confianza que la sociedad deposita en el INEGI, por lo que en todas las fases del proceso de producción de información estadística y geográfica se deben establecer acciones que coadyuven a la preservación de la confidencialidad de la información estadística y geográfica, en tal sentido se proponen las siguientes:

Líneas generales de acción para preservar la confidencialidad de la información estadística y geográfica a través del cifrado y anonimización

Capítulo I. Líneas generales

I. Las presentes Líneas de acción tienen por objeto establecer las disposiciones a partir de las cuales las Unidades y Áreas Administrativas del INEGI, al amparo de su ámbito de competencia, instrumentarán las medidas técnicas y organizativas para preservar la confidencialidad de la información estadística y geográfica.

II. Las presentes líneas de acción, son de observancia obligatoria para las Unidades Administrativas del INEGI que desarrollen actividades para producir información estadística y geográfica, de conformidad con lo dispuesto por el Reglamento Interior del Instituto Nacional de Estadística y Geografía. Corresponde a los Titulares implementarlas y promover su cumplimiento en su respectivo ámbito de competencia.

III. Para los efectos de las presentes líneas de acción se entenderá por:

- a. Actor: Servidor público que desempeña diversas actividades en relación con un Rol determinado;
- b. Anonimización: proceso mediante el cual se reduce al mínimo los riesgos de identificación de los datos anonimizados, al tiempo que se mantiene la veracidad de los resultados del tratamiento de los mismos, es decir, evita que se pueda identificar a quién pertenece la información;
- c. Cifrado o encriptado: corresponde a la alteración, por medio de una clave generada a través de métodos matemáticos, de los datos para hacerlos ilegibles para quienes no posean la clave;
- d. Clasificación: Conjunto de categorías que pueden ser asignadas a una o más variables de un conjunto de datos. Las categorías para cada nivel de la estructura de clasificación deben ser mutuamente excluyentes y en su conjunto exhaustivas, es decir, a cada una de las unidades de una población se le puede asignar una y sólo una categoría;

- e. Confidencialidad estadística y geográfica: Atributo de la información estadística y geográfica que evita la identificación directa e indirecta de los informantes del Sistema;
- f. Conjunto de Datos: Datos organizados. Incluyen Metadatos Estructurales a través de los cuales estos datos se vinculan entre sí y se agrupan dentro de una misma unidad temática;
- g. Dato: Un valor que representa una ocurrencia de los hechos u objetos que se recopilaron o derivaron;
- h. Dato confidencial: aquel que por motivos éticos, morales o por obligación legal no puede difundirse o publicarse;
- i. 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;
- j. Dato sensible: aquél que no siendo confidencial permite identificar individualmente de manera directa o indirecta al informante del Sistema;
- k. Fases del Proceso de Producción de Información Estadística y Geográfica: se refiere a las fases de Documentación de necesidades, Diseño, Construcción, Captación, Procesamiento, Análisis de la producción, Difusión y Evaluación del Proceso;
- l. Identificación directa: es la identificación individual de los informantes del Sistema por medio de sus datos personales o datos relacionados con la razón social;
- m. Identificación indirecta: es la identificación individual de los informantes del Sistema por otros medios que los de la identificación directa.
- n. Información: Datos útiles en un contexto particular. El contexto permite que los datos adquieran significado y puedan representar un mensaje determinado, hecho o fenómeno. Incluye información estadística y geográfica;
- o. Información Estadística: Al conjunto de resultados cuantitativos o datos que se obtienen de las Actividades Estadísticas y Geográficas en materia

- estadística, tomando como base los datos primarios obtenidos de los informantes del Sistema sobre hechos que son relevantes para el conocimiento de los fenómenos económicos, gobierno, seguridad pública e impartición de justicia; demográficos y sociales, así como sus relaciones con el medio ambiente y el espacio territorial;
- p. Información Geográfica: Al conjunto organizado de datos espaciales georreferenciados, que mediante símbolos y códigos genera el conocimiento acerca de las condiciones físico ambientales, de los recursos naturales y de las obras de naturaleza antrópica del territorio nacional;
 - q. Informantes del Sistema: a las personas físicas y morales, a quienes les sean solicitados datos estadísticos y geográficos en términos de la Ley del Sistema Nacional de Información Estadística y Geográfica;
 - r. Instituto o INEGI: Instituto Nacional de Estadística y Geografía, organismo público con autonomía técnica y de gestión, personalidad jurídica y patrimonio propios.
 - s. Ley: Ley del Sistema Nacional de Información Estadística y Geográfica;
 - t. Metadatos: Datos estructurados que describen las características del contenido, captura, procesamiento, calidad, condición, acceso y distribución de la información estadística o geográfica;
 - u. Metadatos Estructurales: Datos que definen la estructura de un conjunto de datos, actuando como identificadores y descriptores de los mismos;
 - v. Presentación: La forma en la que datos y metadatos obtenidos de un Conjunto de Información se incorporan para formar un elemento de un Producto;
 - w. Proceso: Conjunto de actividades, recursos humanos, datos e infraestructura relacionadas lógicamente para producir un resultado;
 - x. Proceso de Producción de Información Estadística y Geográfica: Conjunto de actividades, recursos humanos, datos e infraestructura relacionadas lógicamente para producir información estadística y geográfica por medio de las fases de documentación de necesidades, diseño, construcción,

- captación, procesamiento, análisis de la producción, difusión y evaluación del proceso;
- y. Producto: Resultado final de un proceso que se pone a disposición de un usuario. Un Producto incluye un conjunto de Presentaciones para un usuario;
 - z. Programa de Información o Programa: Conjunto de actividades, que se pueden repetir, que describen el propósito y contexto de un conjunto de Procesos que se llevarán a cabo cada periodo de tiempo para producir información;
 - aa. Registro Administrativo: Conjunto de Datos que fueron generados con fines operacionales o como parte de las funciones de una institución pública o privada sobre un tipo de objeto, sujeto, acción, hecho o evento, y obtenidos sistemáticamente con base en un formato específico ya sea impreso, digital u otro y bajo un marco de funciones y facultades formalmente establecidas en instrumentos jurídicos o reglamentarios;
 - bb. Rol: La función o actividades de un actor, relativas a su participación en un Proceso determinado;
 - cc. Sistema Nacional de Información Estadística y Geográfica o Sistema (SNIEG): al conjunto de Unidades organizadas a través de los Subsistemas, coordinadas por el Instituto y articuladas mediante la Red Nacional de Información, con el propósito de producir y difundir la Información de Interés Nacional;
 - dd. Subsistemas Nacionales de Información o Subsistemas: a los componentes del Sistema enfocados a producir información de una determinada clase o respecto de temas específicos;
 - ee. Unidades Administrativas: Aquellas enlistadas en el artículo 3o. del Reglamento Interior del Instituto Nacional de Estadística y Geografía que desarrollen actividades para producir información estadística y geográfica, sea o no de Interés Nacional.

IV. Las acciones que se emprendan para preservar la confidencialidad de la información estadística y geográfica no excluye la aplicación otras medidas de seguridad de la información.

Capítulo II. Líneas de acción sobre anonimización

V. El proceso de anonimización comprende tres etapas: Diseño de la anonimización, Aplicación de la anonimización y Control de la anonimización.

VI. La etapa de Diseño de la anonimización está comprendida dentro de la fase de Diseño en el Proceso de Producción de Información Estadística y Geográfica. En la etapa de Diseño de la anonimización, para cada Producto de Información estadístico o geográfico se debe:

- a. Identificar y clasificar los datos y metadatos que hacen posible la identificación directa o indirecta de los informantes del Sistema y que será incluida en el proceso de anonimización;
- b. Seleccionar la o las técnicas adecuadas de anonimización conforme a las características del conjunto de datos de cada caso particular;
- c. Identificar los riesgos de identificación asociados con el conjunto de datos y con las técnicas de anonimización seleccionadas;
- d. Identificar y seleccionar a los actores necesarios y asignar la responsabilidad a cada uno de ellos para ejecutar las acciones correspondientes a la etapa de diseño de la anonimización;
- e. Definir las acciones a realizar en caso de existir algún riesgo de identificación directa o indirecta de los informantes del Sistema una vez que se haya publicado la información estadística y geográfica;
- f. Definir la información mínima que cada actor requiere para realizar sus funciones y establecer los controles de acceso a datos e información correspondientes;

VII. En la clasificación de los datos y metadatos que hacen posible la identificación directa e indirecta se debe tomar en cuenta las categorías siguientes:

- a. Datos de identificación geográfica;
- b. Datos de identificación directa;
- c. Datos confidenciales;

- d. Datos sensitivos.

VIII. La etapa de Aplicación de la anonimización está comprendida dentro de las fases Construcción, Captación, Procesamiento, Análisis de la Producción y Difusión en el Proceso de Producción de Información Estadística y Geográfica. En la etapa de Aplicación de la anonimización, para cada Producto de Información estadístico o geográfico se debe:

- e. Implementar las técnicas de anonimización seleccionadas;
- f. Realizar las pruebas necesarias para verificar que las técnicas de anonimización aplicadas preservan la confidencialidad de la información estadística y geográfica, para lo cual se debe considerar la información disponible al público de otras fuentes;
- g. Aprobar las técnicas de anonimización a utilizar;
- h. Supervisar la aplicación de las técnicas de anonimización.

IX. La etapa de Control de la anonimización está comprendida dentro de la fase de Evaluación del proceso en el Proceso de Producción de Información Estadística y Geográfica. En la etapa de Control de la anonimización, para cada Producto de Información estadístico o geográfico se debe:

- a. Definir los controles y la periodicidad de su aplicación, para verificar la vigencia y efectividad de la anonimización aplicada;
- b. Identificar y revisar la información de la temática correspondiente al Producto de Información estadístico y geográfico publicado y que está disponible en registros administrativos.
- c. Considerar las tecnologías y métodos de reciente creación y que pueden ser utilizados tanto para hacer la identificación de los informantes del Sistema como para evitar la materialización de los riesgos de identificación.

Capítulo III. Líneas de acción sobre cifrado

X. El cifrado de información comprende tres etapas: Detección de necesidades de cifrado, aplicación y gestión de cifrado y control del cifrado.

XI. La etapa de detección de necesidades de cifrado está comprendida dentro de la fase de Diseño en el proceso de producción de información estadística y geográfica.

En la etapa de detección de necesidades de cifrado, para cada programa de información se debe:

- a. Identificar el volumen de los datos y los medios de transmisión a cifrar;
- b. Identificar si los dispositivos de almacenamiento son móviles o fijos, así como los medios que se utilizarán para transmitir la información;
- c. Seleccionar los algoritmos de cifrado a utilizar, para lo cual se debe considerar el nivel de seguridad proporcionado por cada algoritmo;
- d. Identificar los riesgos de seguridad asociados con el conjunto de datos y los algoritmos de cifrado seleccionados;
- e. Identificar y seleccionar a los actores necesarios y asignar la responsabilidad a cada uno de ellos para ejecutar las acciones correspondientes a la etapa de detección de necesidades de cifrado;
- f. Definir las acciones a realizar en caso de pérdida o robo de datos o información estadística y geográfica cifrada;
- g. Definir la información mínima que cada actor requiere para realizar sus funciones y establecer los controles de acceso a datos e información correspondientes;

XII. La etapa de aplicación y gestión del cifrado está comprendida dentro de las fases de Construcción, Captación, Procesamiento, Análisis de la producción y Difusión en el proceso de producción de información estadística y geográfica. En la etapa de aplicación y gestión del cifrado, para cada programa de información se debe:

- a. Realizar las pruebas necesarias para verificar el nivel de seguridad que se obtiene con los algoritmos de cifrado seleccionados;
- b. Aprobarse los algoritmos de cifrado a utilizar;
- c. Aplicar los algoritmos de seguridad seleccionados;
- d. Gestionar las claves de cifrado generadas.

XIII. En la gestión de las claves de cifrado considerar:

- a. Los requisitos a cumplir en la generación de la clave;
- b. Asociar las claves con el actor que las utilizará;
- c. La forma en la que se distribuirá entre los actores que la utilizarán;

- d. Las medidas de protección a utilizar para evitar la revelación o sustitución no autorizados;
- e. El establecimiento de tiempo de caducidad para las claves;
- f. Las acciones a realizar en caso de que las claves sean conocidas por personas no autorizadas.

XIV. La etapa de control del cifrado está comprendida dentro de la fase de Evaluación del proceso en el proceso de producción de información estadística y geográfica. En la etapa de control de la anonimización, para cada programa de información se debe:

- a. Definir los controles y la periodicidad de su aplicación, para verificar la vigencia y efectividad de los algoritmos de cifrado;
- b.** Considerar las tecnologías y métodos de reciente creación que pueden ser utilizados para identificar la clave de cifrado.