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

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

"GUÍA DE CUMPLIMIENTO PARA LA ATENCIÓN DEL MAAGTICSI Y PROTECCIÓN DE LA INFORMACIÓN DE LA LEY GENERAL DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS"

IMPLEMENTACIÓN DE UN PROYECTO LABORAL

Que para obtener el grado de MAESTROS EN DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Presenta:

Margarita Landaverde Casanova
Facundo Carlos Sarmiento Álvarez

Asesor:
Dr. Federico César Lefranc Weegan

Ciudad de México, junio de 2018.

Autorización de Impresión

C4

AUTORIZACIÓN DE IMPRESIÓN

Ciudad de México, 14 de junio de 2018

La Gerencia de Capital Humano/ Gerencia de Investigación hacen constar que el proyecto terminal titulado:

"Guía de cumplimiento para la atención del MAAGTICSI y protección de la información de la ley General de datos personales en posesión de sujetos obligados"

Desarrollada por los alumnos

Nombre: **Margarita**	Nombre: **Facundo Carlos**
Apellido paterno: **Landaverde**	Apellido paterno: **Sarmiento**
Apellido materno: **Casanova**	Apellido materno: **Alvarez**

Desarrollado bajo la asesoría del:

Dr. Federico César Lefranc Weegan

Ha sido revisado y aprobado por miembro del Núcleo Académico Básico (NAB).

Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Vo. Bo.

Mtra. Patricia Ávila Muñoz
Gerencia de Capital Humano

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

Agradecimientos

A mis papas y hermanos, por mostrarme el camino hacia la superación continua.

A mi colaborador y amigo Facundo, por elergir trabajar conmigo.

A mis compañeros de trabajo Alfredo, Laura, Omar y Danko a quienes agradezco su apoyo.

margott

Agradezco a toda mi familia por su siempre incondicional apoyo, especialmente a mi amada esposa Ale por su invaluable paciencia y cariño.

También le agradezco enormemente a mi querida amiga Margarita por compartir sus conocimientos y sobre todo su amistad.

Carlos Facundo

Un agradecimiento especial al Dr. Federico Lefranc por su apoyo y asesoría a lo largo del posgrado y en la elaboración de este trabajo tesis.

Tabla de contenido

Contenido

Introducción 1

Capítulo 1: Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información. 4

1.1 Antecedentes 5

1.2 Estructura del MAAGTICSI 14
1.2.1 Proceso de Planeación Estratégica (PE) 18
1.2.2 Administración del Presupuesto y las Contrataciones (APCT) 19
1.2.3 Proceso de Administración de Servicios (ADS) 19
1.2.4 Proceso de Administración de la Configuración (ACNF) 20
1.2.5 Proceso de Administración de la Seguridad de la Información (ASI) 20
1.2.6 Proceso de Administración de Proyectos (ADP) 21
1.2.7 Proceso de Administración de Proveedores (APRO) 21
1.2.8 Proceso de Administración de Operación (AOP) 22
1.2.9 Operación de Controles de Seguridad de la Información y del ERISC (OPEC) 22

1.3 Aplicación Actual del Manual 23

Capítulo 2: Ley General de Datos Personales en Posesión de Sujetos Obligados y Lineamientos Generales de Protección de Datos Personales para el Sector Público. 25

2.1 Antecedentes 26
2.1.1 Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental 27
2.1.2 Constitución Política de los Estados Unidos Mexicanos (CPEUM) 30
2.1.3 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) 33
2.1.4 Lineamientos Generales de Protección de Datos Personales para el Sector Público. 34

2.2 Estructura de la Ley 35
2.2.1 Disposiciones Generales 36
2.2.2 Principios y Deberes 37
2.2.3 Derechos de los titulares 39
2.2.4 Relación del responsable y encargado 40
2.2.5 Comunicación de Datos Personales 41
2.2.6 Acciones Preventivas 42
2.2.7 Responsables en materia de protección de datos personales en posesión de los Sujetos Obligados. 42
2.2.8 Organismos Garantes 43
2.2.9 Procedimientos de impugnación en materia de protección de datos personales en posesión de sujetos obligados 44
2.2.10 Facultad de Verificación del Instituto y los organismos garantes 44
2.2.11 Medidas de Apremio y responsabilidad 44

2.3 Elementos Básicos en la Seguridad Informática 45
2.3.1 Sistema de Gestión de la Seguridad de la Información 47
2.3.2 MAAGTICSI - ASI 48
2.3.3 MAAGTICSI - OPEC 48

2.4 Problemática Actual en la Protección de Datos Personales 49

Capítulo 3: Análisis comparado entre el MAAGTICSI y la Ley General. *53*

Tema 1: Objeto **53**

Tema 2: Ámbito de aplicaciones **53**

Tema 3: Responsable **54**

Tema 4: Borrado seguro **55**

Tema 5: Cómputo en la nube **56**

Tema 6: Interoperabilidad **57**

Tema 7: Dominio tecnológico **58**

Tema 8: Desarrollo **58**

Tema 9: Seguridad **60**

Tema 10: Tratamiento y baja **60**

Tema 11: Internet- seguridad de la información **62**

Tema 12: Almacenamiento **63**

Tema 13: Responsables de la información **64**

Tema 14: Medidas de seguridad físicas **64**

Tema 15: Bases de datos **65**

Tema 16: Inventario **66**

Tema 17: Plataformas **66**

Tema 18: Seguridad Nacional **67**

Capítulo 4. Propuesta de procesos básicos que permite el cumplimiento del MAAGTICSI y la Ley General. *70*

4.1 Diagramas de flujo en el que convergen el MAAGTICSI y la Ley General. **70**

1. **Diagrama de flujo de Proceso de Borrado Seguro** 71
2. **Diagrama de flujo de Proceso de Computo en la Nube** 72
3. **Diagrama de flujo de Proceso de Interoperabilidad** 73
4. **Diagrama de flujo de Proceso de Dominio Tecnológico** 74
5. **Diagrama de flujo de Proceso de Desarrollo** 75
6. **Diagrama de flujo de Proceso de Seguridad** 76
7. **Diagrama de flujo de Proceso Tratamiento y Baja** 77
8. **Diagrama de flujo de Proceso Internet-Seguridad de la Información** 78
9. **Diagrama de flujo de Proceso de almacenamiento** 79
10. **Diagrama de flujo de responsables de la información** 80
11. **Diagrama de flujo de Proceso de Medidas de seguridad física** 81
12. **Diagrama de flujo de Proceso de Bases de Datos** 82
13. **Diagrama de Flujo de Inventario** 83
14. **Diagrama de flujo de plataformas** 84
15. **Diagrama de flujo de seguridad nacional** 85

Conclusiones *86*

Fuentes consultadas *89*

Índice de figuras

Figura 1. Marco rector de procesos, MAAGTIC 2010..... 8

Figura 2 Marco rector de procesos, MAAGTIC 2011..... 10

Figura 3 Marco rector de procesos, MAAGTICSI 2011 13

Figura 4. Diagrama de organización de procesos, MAAGTICSI..... 18

Figura 5. Principios normativos 29

Figura 6. Derechos ARCO..... 31

Figura 8. Nueve títulos de los Lineamientos Generales de Protección de Datos Personales para el Sector Público..... 35

Figura 9. Principios rectores, *LGPDPPSO*..... 38

Figura 10. Deberes, LGPDPPSO 39

Figura 11. Derechos ARCO, LGPDPPSO..... 40

Siglas y abreviaturas

APF. - Administración Pública Federal

CNTSE. - Catálogo Nacional de Trámites y Servicios del Estado

EDN. - Estrategia Digital Nacional

EIDA. - Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal

ERISC. - Equipo de respuesta a incidentes de seguridad en TIC en la Institución

MAAGMAASSP. - El Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público

MAAGTICSI. - Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información

PETIC. - Conjunto de proyectos que elaboran las Instituciones, conformado por un máximo de 7 proyectos estratégicos

SEGOB. - Secretaría de Gobernación;

SFP. - Secretaría de la Función Pública;

SHCP. - Secretaría de Hacienda y Crédito Público

TIC. - Tecnologías de Información y Comunicaciones

UPCP. - Unidad Política de Control Presupuestario de la SHCP

UTIC. - Unidad de Tecnologías de Información y Comunicaciones o área responsables de las TIC en la Institución

LFPDPPP – Ley Federal de Protección de Datos Personales en Posesión de Particulares

LGPDPPSO – Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

ASI – Administración de la Seguridad de la Información

LFTAIPG – Ley Federal de Transparencia y Acceso a la Información Pública

INAI – Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

IFAI – Instituto Federal de Acceso a la Información y Protección de Datos

CPEUM – Constitución Política de los Estados Unidos Mexicanos

OPEC – Operación de Controles de Seguridad de la Información

Introducción

El presente trabajo tiene por objetivo contribuir con el cumplimiento a dos normas reguladoras enfocadas, al resguardo y seguridad de la información aplicable a las dependencias y entidades de la Administración Pública Federal (APF).

Ambos postulantes trabajamos en la APF y tenemos conocimiento acerca de la problemática que se vive en el ámbito gubernamental, ya que, como Servidores Públicos, tenemos la obligación de dar cumplimiento al marco normativo que aplique.

En ese sentido, nos dimos a la tarea de analizar y armonizar el "Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el manual administrativo de aplicación general en dichas materias", conocido como "MAAGTICSI", y la "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados"[1] , en adelante "Ley", en lo referente a la Seguridad de la Información.

Dentro de nuestra vida laboral, nos percatamos de que algunas de las cosas que señala la Ley de observancia obligatoria, ya se realizaba por la APF, a través del cumplimiento al MAAGTICSI, toda vez que este surgió al amparo del "Acuerdo por el que se instruye a las dependencias y entidades de la Administración Pública Federal, así como a la Procuraduría General de la República a abstenerse de emitir regulación en las materias que se indican", publicado en el Diario Oficial de la Federación (DOF) el 10 de agosto de 2010, y tenía entre otras cosas el objetivo de eliminar, reducir y simplificar las disposiciones administrativas en diversas materias, al interior de las dependencias y entidades, y que si existían diversas normativas, homologarlas todas en 9 manuales que serían de aplicación general, y no que cada una de las dependencias y entidades tuviesen un instrumento diferente.

[1] La cual, por su reciente creación, está siendo implementada en la APF

En ese sentido, uno de los 9 manuales instruidos por el Ejecutivo Federal en ese entonces, fue el correspondiente a Tecnologías de la Información y Comunicaciones.

Este trabajo de tesis constituye una propuesta que busca simplificar y consolidar los procesos operativos en los que convergen la Ley General y el MAAGTICSI para la administración de la seguridad de la información y el resguardo y protección de los datos personales en posesión de los sujetos obligados en la APF, proponemos una serie de diagramas en los cuales buscamos empatar los puntos de coincidencia de ambas normativas generando un solo producto que facilitará el cumplimiento de ambos instrumentos vinculantes para la APF.

El propósito principal de esta investigación es plasmar de manera clara y concisa los puntos de convergencia de la Ley y MAAGTICISI, y que como resultado se tenga una guía de cumplimiento para que pueda ser un referente para las áreas involucradas dentro de cada institución de la APF, y así lograr de manera sencilla y puntual el cumplimento de ambas normativas.

Capítulo 1

Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información.

Capítulo 1: Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información.

Uno de los asuntos que más se han discutido entre los expertos en tecnologías de la información y comunicaciones, en la última década, ha sido la estandarización y formalización de prácticas comunes en dicha disciplina.

El **13 de julio de 2010**, se publicó en el DOF[2] por parte de la Secretaría de la Función Pública, el "Acuerdo por el que se expide el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones" denominado "MAAGTIC", el cual establece las disposiciones administrativas en materia de tecnologías de la información y comunicaciones que se deberán observar en el ámbito de la APF y, en lo conducente, en la Procuraduría General de la República, como parte de la estrategia de Gobierno Digital orientada a coordinar las políticas y programas en esa materia, con el principal objetivo de homologar, armonizar reglas y acciones definidas, así como contar con procesos uniformes para el aprovechamiento y aplicación eficiente de las tecnologías de la información y comunicaciones.

Sin embargo, construir desde cero un Acuerdo, respecto de cómo se deben hacer las cosas, basado en un modelo de gestión[3] de una disciplina joven –en un

[2]Diario Oficial de la Federación consultado en http://dof.gob.mx/nota_detalle.php?codigo=5151475&fecha=13/07/2010 el 10 de diciembre de 2017.

[3] *Un modelo de gestión es un esquema o marco de referencia para la administración de una entidad. Los modelos de gestión pueden ser aplicados tanto en las empresas y negocios privados como en la administración pública. Esto quiere decir que los gobiernos tienen un modelo de gestión en el que se basan para desarrollar sus políticas y acciones, y con el cual pretenden alcanzar sus objetivos.*

El modelo de gestión que utilizan las organizaciones públicas es diferente al modelo de gestión del ámbito privado. Mientras el segundo se basa en la obtención de

entorno, que cambia muy rápido, y que abarca el cómputo, las comunicaciones, la ingeniería en sistemas, la administración y seguridad de la información, no fue un asunto trivial.

Tal vez por ello, el MAAGTIC debe su origen más inmediato a las iniciativas presidenciales de tala regulatoria y regulación base cero[4], enfocadas a reducir la carga administrativa interna del gobierno y a mejorar el servicio al ciudadano.

De esta forma, el MAAGTIC en su primera versión establece un marco rector de procesos, fundamentados en las mejores prácticas de Tecnologías de la Información y Comunicaciones (TIC), que traduce a las condiciones operativas del gobierno federal mexicano, las buenas prácticas internacionales en la gestión de las TIC; para simplificar, agilizar y hacer más efectivos los procesos bajo los cuales deben operar las dependencias públicas federales hacia el interior y para con los ciudadanos.

1.1 Antecedentes

El Plan Nacional de Desarrollo 2007-2012, estableció como estrategia para lograr el objetivo 10 del Eje Rector "Estado de Derecho y Seguridad", la ampliación de los programas de simplificación administrativa y mejora regulatoria en toda la administración pública, procurando que los cambios tengan un impacto directo en el combate a la discrecionalidad, la arbitrariedad o la corrupción[5].

---

ganancias económicas, el primero pone en juego otras cuestiones, como el bienestar social de la población." Consultado en https://definicion.de/modelo-de-gestion/ el 10 de diciembre de 2017.

[4] Véase, Tala regulatoria, Página de la Secretaría de la Función Pública consultada en http://2006-2012.funcionpublica.gob.mx/index.php/unidades-administrativas/ssfp/mejor-gobierno/tala.html el 11 de diciembre de 2017.

[5] Véase, Plan Nacional de Desarrollo. Estado de Derecho y Seguridad. Confianza en las Instituciones Públicas. Estrategia 10.3 Reducir los trámites burocráticos con la finalidad de abatir la discrecionalidad. Consultado en

En ese sentido, el Programa Especial de Mejora de la Gestión en la Administración Pública Federal 2008-2012[6], en su estrategia 2.3 “Simplificar la regulación que rige a las instituciones y su interacción con la sociedad”, establecía como una línea de acción, mejorar el marco normativo de las instituciones a través del proceso de calidad regulatoria para lograr mayor agilidad, certidumbre y menores costos de operación para la institución y los particulares.

Por ello para mejorar la gestión de las instituciones, fue necesario reformar el marco regulatorio de aplicación obligatoria a toda la APF, mediante las estrategias tendientes a simplificar la regulación que rige a las instituciones y su interacción con la sociedad, así como a mejorar las políticas, normas y disposiciones de carácter general que emiten las dependencias globalizadoras [7]o instituciones coordinadoras de sector.

Bajo ese tenor, el Ejecutivo Federal, en su mensaje dirigido a la nación con motivo de la presentación al H. Congreso de la Unión del Tercer Informe de Gobierno, se comprometió a llevar a cabo un proceso de desregulación a fondo de la normatividad de la APF, con el objetivo de reducir y simplificar al máximo las disposiciones administrativas, eliminar toda aquella regulación, requisitos, duplicidad de información y trámites innecesarios que permitan consolidar una mayor certeza jurídica, en donde la plena eficacia de las normas aplicables a

---

http://pnd.calderon.presidencia.gob.mx/index.php?page=confianza-en-las-instituciones-publicas el 11 de diciembre de 2017.

[6] Véase Programa Especial de Mejora de la Gestión en la Administración Pública Federal 2008-2012, consultado en dof.gob.mx/nota_to_doc.php?codnota=5059570 el 12 de diciembre de 2017.

[7] Dependencias Globalizadoras: Aquellas que emiten disposiciones de cumplimiento general para las demás Dependencias y Entidades de la Administración Pública Federal.

particulares y a gobernantes, les garantice el ejercicio pleno de sus derechos y libertades.

En este sentido, el Ejecutivo Federal instruyó a la Secretaría de la Función Pública, para emitir, por sí o con la participación de las dependencias competentes, disposiciones, políticas o estrategias, acciones o criterios de carácter general y procedimientos uniformes para la APF y, en lo conducente, para la Procuraduría General de la República en materia de auditoría; adquisiciones, arrendamientos y servicios del sector público; control interno; obra pública y servicios relacionados con la misma; recursos humanos; recursos materiales; recursos financieros; **tecnologías de la información y comunicaciones**; de transparencia y rendición de cuentas. Adicionalmente que las dependencias y entidades, así como la citada Procuraduría procedan a dejar sin efectos todas aquellas disposiciones, lineamientos, oficios circulares, procedimientos, así como demás instrumentos normativos emitidos al interior de sus instituciones, en esas materias;

El MAAGTIC contiene un marco rector de la forma en la que se deben llevar a cabo los procesos de las Unidades de Tecnologías de la Información y Comunicaciones (UTIC) de cada dependencia. En el se contemplaron la conjugación de mejores prácticas y estándares internacionales tales como: Balanced Score Card, TOGAF, ISO 9001, VAL IT, PMBOK, CMMI, MOPROSOFT, ITIL, RISK IT e ISO 27001.El denominado marco rector de procesos proporcionó una guía descriptiva de las actividades, roles y productos de los procesos, mediante la ejecución de factores críticos para la; Dirección, Control, Gestión y Operación de una UTIC; así como un esquema de indicadores que permitirá medir los resultados, efectividad y eficiencia de los procesos al interior de la misma.

Además, se compuso de 11 grupos de procesos, ubicados en 4 niveles de gestión que detallan el enfoque que debe cuidarse en cada uno de ellos: Gobierno, Organización y Estrategia, Ejecución y Entrega, Soporte.

Estos 11 grupos de procesos se subdividieron en otros 30 procesos que buscan cubrir todos los aspectos del funcionamiento de una UTIC. En la Figura 1

se muestra el marco rector de procesos del MAAGTIC, aplicable para la versión del 13 de julio de 2010.

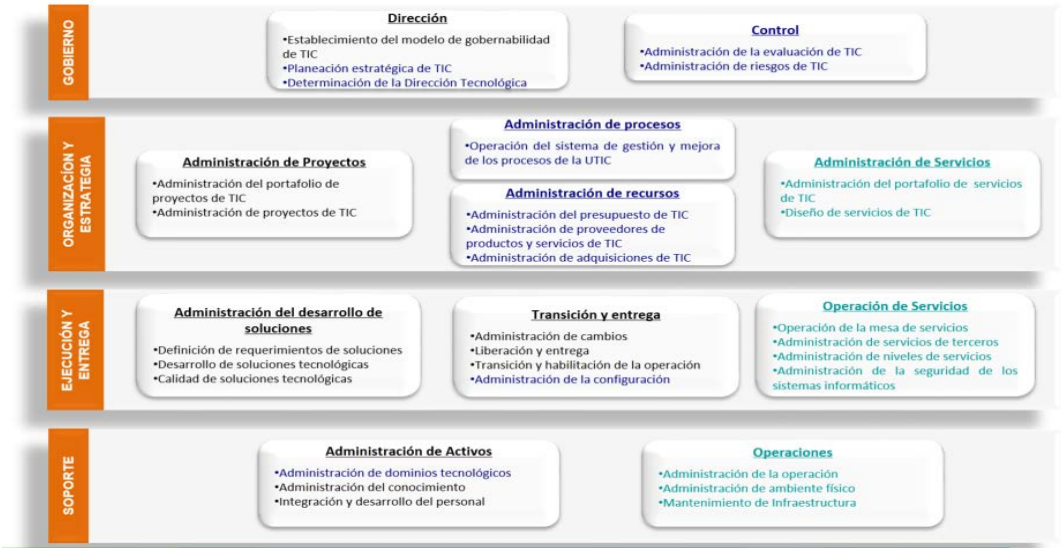


Figura 1. Marco rector de procesos, MAAGTIC 2010.[8]

Fuente: Elaboración propia con base en información de MAAGTIC vigente el 13 de julio de 2010.

El grupo de Dirección se conforma de los procesos de: Establecimiento del modelo de gobernabilidad de TIC, Planeación estratégica de TIC y Determinación de la dirección tecnológica.

El grupo de Control se conforma de los procesos de: Administración de la evaluación de TIC y Administración de riesgos de TIC.

El grupo de Administración de Proyectos se conforma de los procesos de: Administración del portafolio de proyectos de TIC y Administración de proyectos de TIC.

El grupo de Administración de Procesos se conforma del proceso de: Operación del sistema de gestión y mejora de los procesos de la UTIC.

[8] Diario Oficial de la Federación. 13 de julio de 2010. Consultado en http://dof.gob.mx/nota_detalle.php?codigo=5151475&fecha=13/07/2010 el 12 de diciembre de 2017.

El grupo de Administración de Recursos se conforma de los procesos de: Administración del presupuesto de TIC, Administración de proveedores de productos y servicios de TIC y de Administración de adquisiciones de TIC.

El grupo de Administración de Servicios se conforma de los procesos de: Administración del portafolio de servicios de TIC y Diseño de servicios de TIC.

El grupo de Administración y Desarrollo de Soluciones se conforma de los procesos de: Definición de requerimientos de soluciones, Desarrollo de soluciones tecnológicas y Calidad de soluciones tecnológicas.

El grupo de Transición y Entrega se conforma de los procesos de: Administración de cambios, Liberación y entrega, Transición y habilitación de la operación y de Administración de la configuración.

El grupo de Operación de Servicios se conforma de los procesos de: Operación de la mesa de servicios, Administración de servicios de terceros, Administración de niveles de servicio y Administración de la seguridad de los sistemas informáticos.

El grupo de Administración de Activos se conforma de los procesos de: Administración de dominios tecnológicos, Administración del conocimiento e Integración y desarrollo del personal.

El grupo de Operaciones se conforma de los procesos de: Administración de la operación, Administración de ambiente físico y Mantenimiento de infraestructura.

Como parte de la revisión y actualización de los procesos y procedimientos del MAAGTIC, previsto en el artículo octavo del Acuerdo del 13 de julio de 2010; el **6 de septiembre de 2011**, se publica en el mismo diario oficial, el *"ACUERDO por el que se modifica el diverso por el que se expide el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, y se establecen las disposiciones administrativas en esa materia"*[9].

[9] Véase Diario Oficial de la Federación. 06 de septiembre de 2011. Consultado en http://dof.gob.mx/nota_detalle.php?codigo=5208012&fecha=06/09/2011 el 13 de diciembre de 2017.

En este manual modificado, las adecuaciones realizadas al MAAGTIC se enfocaron en agregar mayor claridad y precisión sobre la ejecución de las actividades por parte de los responsables definidos para cada proceso, la estructura de grupos de procesos se mantiene en lo general y se pasa de un modelo de 30 procesos a uno de 29, al ser reformadas parte de las actividades del proceso de Administración de servicios de terceros del grupo de Operación de Servicios.

En la Figura 2 se muestra el marco rector de procesos del MAAGTIC, aplicable para la versión del 6 de septiembre de 2011.

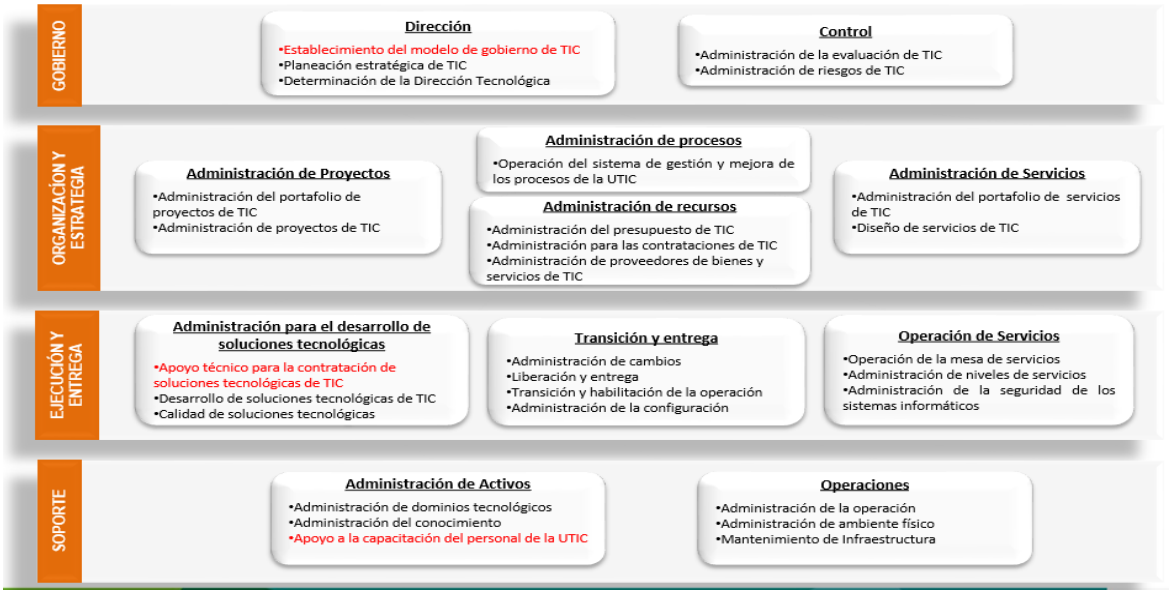


Figura 2 Marco rector de procesos, MAAGTIC 2011.[10]

Fuente: Elaboración propia con base en información de MAAGTIC vigente el 6 de septiembre de 2011.

No obstante, que el marco rector de procesos del MAAGTIC contaba de origen con procesos enfocados a la seguridad de los sistemas informáticos, en virtud del desarrollo y utilización cada vez mayor de las tecnologías de la información y comunicaciones en la operación de los diferentes trámites y servicios públicos que proporciona la APF, revistió particular importancia el establecimiento de procesos uniformes y de acciones y medidas coordinadas en materia de

[10] *Ídem.*

seguridad de la información, que permitan a partir de la identificación de la infraestructura de tecnologías de la información y comunicaciones y de aquélla otra vinculada o asociada con ésta que se considere crítica, fortalecer la gestión de la seguridad de la información, para lograr el uso seguro de equipos y servicios, así como una respuesta oportuna ante situaciones de emergencia, y contribuir a la seguridad de la nación ante amenazas materializadas a través del uso de tecnologías de la información y comunicaciones.

Por su parte el Programa para la Seguridad Nacional 2009-2012[11], en su objetivo específico 1. "Fortalecer estructuralmente el sistema de seguridad nacional", en su línea estratégica 1.2. "Establecer un sistema integral de información para la preservación de la seguridad nacional", prevé como una de sus líneas de acción, la 1.2.4., "Desarrollar instrumentos y tecnología que garanticen la protección y confidencialidad de la información de seguridad nacional, así como su transmisión segura".

Por tal motivo, el Ejecutivo Federal acordó en el seno del Consejo de Seguridad Nacional, diversos lineamientos generales de seguridad de la información; y su incorporación en el Acuerdo y en el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones.

La definición de los procesos, acciones y medidas que en materia de seguridad de la información se contempló incorporar en las disposiciones del Acuerdo y del Manual en materia de Tecnologías de la Información y Comunicaciones, tuvo una participación preponderante el Grupo Técnico Intersecretarial Especializado en Seguridad de la Información (GTECSI), establecido por el Consejo de Seguridad Nacional con objeto de coordinar los trabajos para el desarrollo de una política general de seguridad de la información.

De esta forma el **29 de noviembre de 2011**, se publica en el DOF el *"ACUERDO por el que se reforma y adiciona el diverso por el que se establecen las*

---

[11] Diario Oficial de la Federación. Consultado en http://dof.gob.mx/nota_detalle_popup.php?codigo=5106082 el 13 de diciembre de 2017.

disposiciones administrativas en materia de tecnologías de la información y comunicaciones, y se expide el Manual Administrativo de Aplicación General en esa materia y en la de Seguridad de la Información", denominado "MAAGTICSI"[12].

Cuidando la armonización y enfoque de procesos, de la versión previamente publicada en septiembre de 2011, reviste en la importancia en la nueva versión reformada del 29 de noviembre de 2011 del MAAGTICSI, sobre el reforzamiento en los temas de seguridad de la información (SI), y de aquella considera de seguridad nacional.

Las adecuaciones al marco rector de procesos, para dar cabida a los 2 nuevos procesos del MAAGTICSI; **Administración de la Seguridad de la Información** y **Operación de los Controles de Seguridad de la Información y del ERISC**, manteniendo el marco rector de 29 procesos; reforma los procesos de la versión de septiembre de 2011, en lo que se refiere a la Administración de riesgos de TIC y la Administración de la seguridad de los sistemas informáticos.

En la Figura 3 se muestra el marco rector de procesos del MAAGTICSI, aplicable para la versión del 29 de noviembre de 2011.

[12] Véase Diario Oficial de la Federación. 29 de noviembre de 2011. Consultado en http://www.dof.gob.mx/nota_detalle.php?codigo=5221649&fecha=29/11/2011 el 13 de diciembre de 2017.

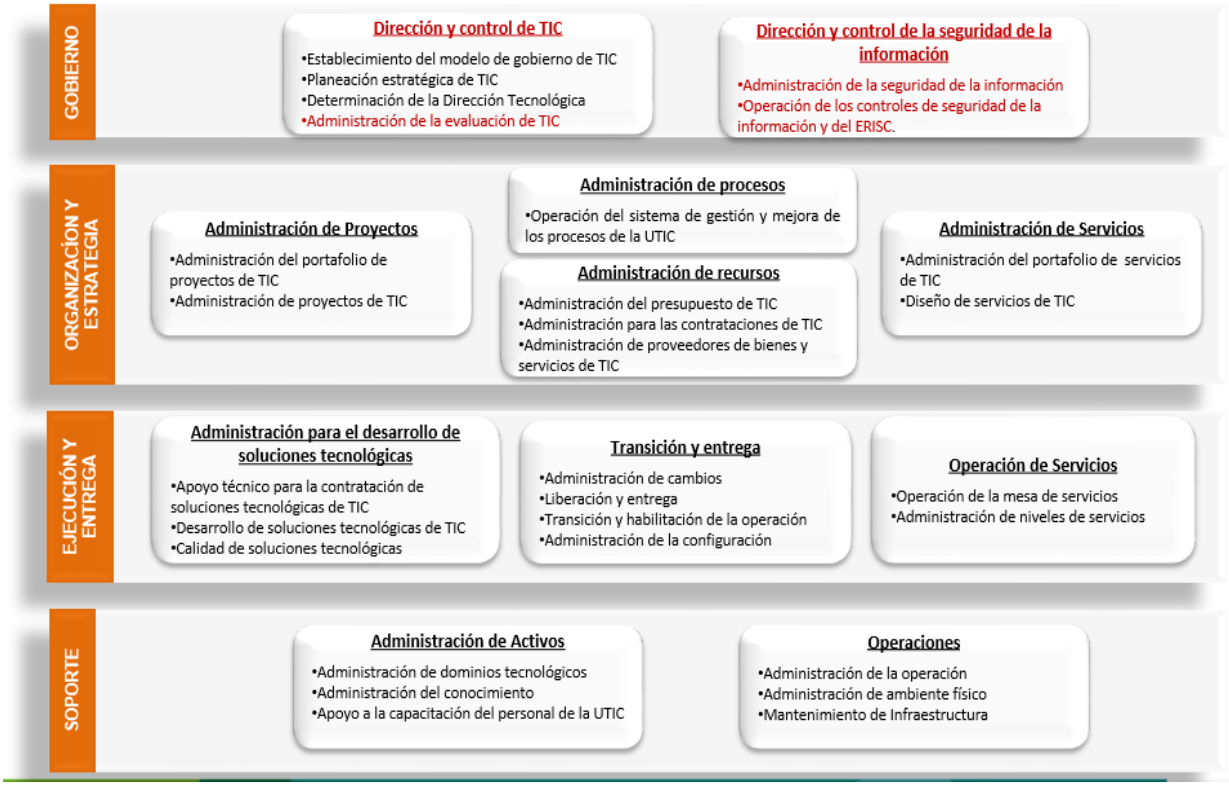


Figura 3 Marco rector de procesos, MAAGTICSI 2011[13]

Fuente: Elaboración propia con base en información de MAAGTICSI vigente el 29 de noviembre de 2011

Mediante los acuerdos publicados en el referido órgano de difusión oficial en fechas 6 de septiembre y 29 de noviembre de 2011, incorporando en el último de dichos acuerdos las disposiciones administrativas y procesos en materia de seguridad de la información, el **22 de agosto de 2012**, en términos de lo establecido por el artículo octavo de las disposiciones administrativas en materia de tecnologías de la información y comunicaciones y de seguridad de la información, tales disposiciones, así como los procesos contenidos en el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información fueron revisados, por la Secretaría de

[13] Véase Diario Oficial de la Federación. 29 de noviembre de 2011. Consultado en http://www.dof.gob.mx/nota_detalle.php?codigo=5221649&fecha=29/11/2011 el 13 de diciembre de 2017.

Gobernación, a través del Centro de Investigación y Seguridad Nacional, y por la Secretaría de la Función Pública, por conducto de la Unidad de Gobierno Digital, para efectos de su actualización, y durante el proceso de revisión a que hace referencia el considerando que antecede, en el seno del Comité Especializado en Seguridad de la Información (CESI), establecido por acuerdo del Consejo de Seguridad Nacional, se advirtió la necesidad de precisar y aclarar algunos aspectos de las disposiciones relativas a la materia de seguridad de la información.

De esta nueva publicación, el marco rector de 29 procesos del MAAGTICSI, no sufrió modificaciones a los mismos, permitiendo a las dependencias y entidades, madurar en las tareas de implementación y operación de los procesos al interior de las UTIC; basados en un enfoque operativo y de cultura de seguridad de la información, bajo la aplicación de actividades, factores críticos y directrices fundamentadas en el modelo de un Sistema de Gestión de Seguridad de la Información y la implementación, operación y evaluación de controles de seguridad.

1.2 Estructura del MAAGTICSI

Evolucionar en la gestión de las TIC para las dependencias del estado mexicano ha sido un gran reto, independientemente de los cambios naturales de toda Administración Pública, el Plan Nacional de Desarrollo 2013-2018[14], aprobado por Decreto publicado en el DOF el 20 de mayo de 2013, propone dentro de la estrategia transversal “Un Gobierno Cercano y Moderno”, el establecer una Estrategia Digital Nacional para fomentar la adopción y el desarrollo de las TIC, e impulsar un gobierno eficaz que inserte a México en la Sociedad de la Información y del Conocimiento.

[14] Véase Plan Nacional de Desarrollo 2013-2018. Consultado en http://pnd.gob.mx/ el 14 de diciembre de 2017.

El Programa para un Gobierno Cercano y Moderno 2013-2018[15], aprobado por Decreto publicado en el DOF el 30 de agosto de 2013, indica que para alcanzar dicha estrategia transversal, es fundamental reconocer que las nuevas TIC son una herramienta básica que brinda amplias oportunidades para mejorar la eficiencia del gobierno, por lo que en este sentido, en su Objetivo 5 "Establecer una Estrategia Digital Nacional que acelere la inserción de México en la Sociedad de la Información y del Conocimiento", indica que este impulso se efectuará mediante el uso de las TIC, lo cual permitirá el desarrollo de la modernización del gobierno y la mejora de los servicios y bienes públicos, lo que supone contar con habilitadores digitales como la conectividad, asequibilidad, inclusión y alfabetización digital, la interoperabilidad y el uso de datos abiertos, así como el marco jurídico adecuado para tales efectos.

El *"Decreto que establece las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal"*, publicado el 10 de diciembre de 2012 en el DOF[16], prevé en materia de TIC, que se deberán establecer programas de optimización, sistematización y digitalización de procesos administrativos; que los nuevos sistemas consolidarán la operación e integración de diferentes sistemas y bases de datos; que se deberán adoptar las políticas de la Estrategia Digital Nacional, la cual fomentará dentro de sus objetivos un cambio de cultura para que el gobierno utilice

---

[15] Véase Diario Oficial de la Federación. Consultado en http://www.dof.gob.mx/nota_detalle.php?codigo=5312420&fecha=30/08/2013 el 14 de diciembre de 2017.

[16] Decreto que establece las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal. Consultado en https://www.gob.mx/cms/uploads/attachment/file/143509/DECRETO_que_establece_las_medidas_para_el_uso_eficiente.pdf el 14 de diciembre de 2017.

las TIC y con ello ofrezca servicios gubernamentales transparentes y de mayor calidad con posibilidad de interoperabilidad a través de conexiones rápidas y seguras, y que se deberán implementar las recomendaciones que se emitan en materia de política de Estrategia Digital Nacional, respecto a las contrataciones de bienes o servicios en materia de TIC, así como las mejores prácticas susceptibles de desarrollarse e instrumentarse a través de proyectos estratégicos.

A su vez, los *"Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal"*, difundidos en el DOF el 30 de enero de 2013, disponen la necesidad de privilegiar la unificación e integración de aplicaciones para su optimización, homologación y estandarización, a fin de consolidar los sistemas y servicios de TIC y disminuir los costos de mantenimiento de los portafolios de aplicaciones.

Como resultado de la revisión de las disposiciones administrativas en materia de TIC y de seguridad de la información, así como del Manual Administrativo de Aplicación General en esas materias, establecidos en el Acuerdo del 13 de julio de 2010 y sus reformas publicadas el 6 de septiembre y 29 de noviembre de 2011, así como el 22 de agosto de 2012; se observó la necesidad de homologar los procesos contenidos en dicho manual a la Estrategia Digital Nacional, para agilizar y optimizar su gestión al interior de las dependencias y entidades de la APF y en la Procuraduría General de la República, por lo que el **8 de mayo de 2014**, se da a conocer el *"ACUERDO que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias"*[17].

[17] Diario Oficial de la Federación. Consultado en http://www.dof.gob.mx/nota_detalle.php?codigo=5343881&fecha=08/05/2014 el 14 de diciembre de 2017.

Esta nueva versión del MAAGTICSI, se basa en un enfoque orientado a la productividad de las UTIC y pasa de un modelo de gestión de un marco rector de 29 procesos a 9 procesos agrupados en 3 grupos de procesos: Gobernanza, Organización y Entrega.

Dentro del grupo de Gobernanza, se agrupan los procesos de: Planeación Estratégica (PE) y Administración del Presupuesto y las Contrataciones (APCT).

En el grupo de Organización, se agrupan los procesos de: Proceso de Administración de Servicios (ADS), Proceso de Administración de la Configuración (ACNF) y Proceso de Administración de la Seguridad de la Información (ASI).

Finalmente, en el grupo de Entrega fueron agrupados los procesos de: Administración de Proyectos (ADP), Administración de Proveedores (APRO), Administración de la Operación (AOP) y Operación de Controles de Seguridad de la Información y del ERISC (OPEC).

Por último, en esta ruta evolutiva del MAAGTICSI y tomando en consideración la importancia de seguir consolidando el desarrollo de las TIC en el Gobierno Federal, así como la necesidad de seguir simplificando y automatizando procesos en atención a las prioridades que en materia de austeridad y eficiencia presupuestal ha establecido el propio gobierno, resultó necesario actualizar las políticas y disposiciones para la Estrategia Digital Nacional contenidas en el Acuerdo del 8 de mayo de 2014, de manera que con ello se continúe combatiendo el rezago tecnológico en el que se encontraba la APF, así como para simplificar y clarificar el citado documento y los procesos que integra en su manual, dando pie a la publicación en dicho órgano oficial el **4 de febrero de 2016**, del *"ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias"*[18].

[18] Diario Oficial de la Federación. Consultado en http://dof.gob.mx/nota_detalle.php?codigo=5424367&fecha=04/02/2016 el 18 de diciembre de 2017.

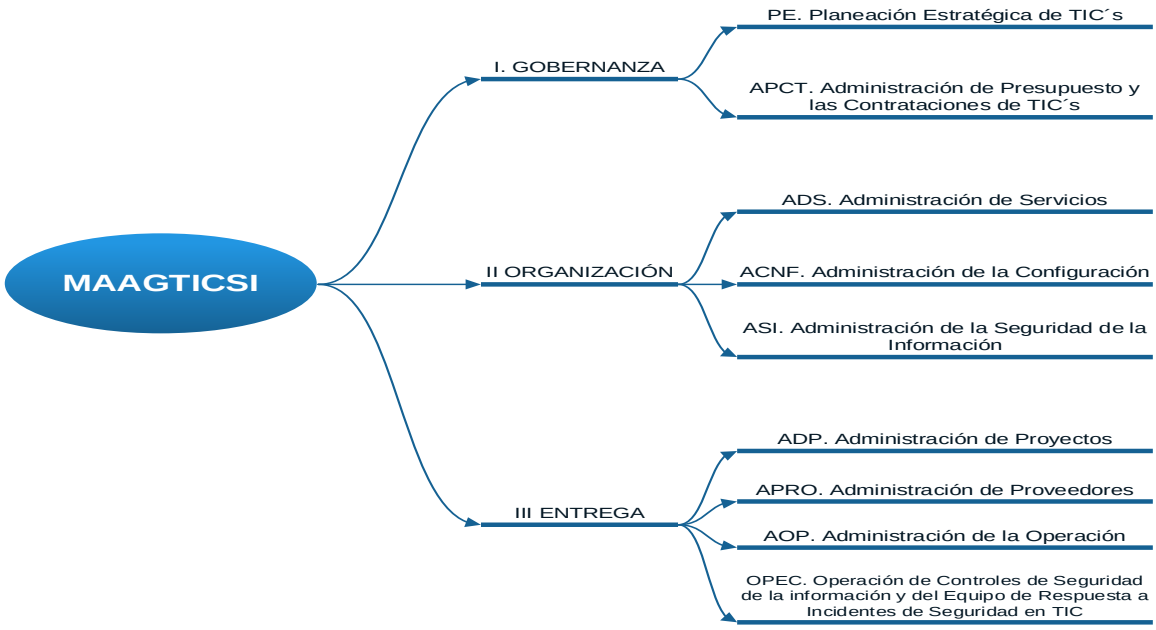


Figura 4. Diagrama de organización de procesos, MAAGTICSI[19]

Fuente: Elaboración propia con base en información de MAAGTICSI 2011.

1.2.1 Proceso de Planeación Estratégica (PE)

Objetivo General:

Mantener la operación de un modelo de gobierno de TIC en la Institución, para efectuar, entre otras acciones, el análisis de las oportunidades de aprovechamiento de las TIC, la planeación estratégica de TIC y asegurar la adecuada organización al interior de la UTIC para la gestión de sus procesos y vinculación ordenada con sus usuarios.

Objetivos Específicos:

1. Promover que los mandos medios y los titulares de las unidades administrativas de la Institución, coadyuven con la UTIC en la toma de decisiones para la dirección y control de las TIC, así como para la entrega efectiva y eficiente de los sistemas y servicios de TIC.

2. Prever que la Institución cuente con una Cartera Ejecutiva de Proyectos TIC, con el objeto de establecer líneas de acción en materia de TIC y su

[19] *Ídem.*

seguimiento, alineadas a los objetivos institucionales, al Plan Nacional de Desarrollo 2013-2018, a los programas sectoriales y especiales que resulten aplicables, así como al Decreto, el Programa, las Bases de colaboración que haya celebrado la Institución y las líneas de acción de la EDN.

1.2.2 Administración del Presupuesto y las Contrataciones (APCT)

Objetivo General:

Coordinar las acciones para el ejercicio del presupuesto destinado a las TIC, a fin de maximizar su aplicación en las contrataciones de TIC requeridas por la institución, así como las acciones para efectuar el acompañamiento necesario a las unidades facultadas para realizar los procedimientos de contrataciones, de manera que se asegure su ejecución en tiempo y forma, alineado al presupuesto autorizado; así como el seguimiento a los contratos que se celebren.

Objetivos Específicos:

1. Elaborar el listado de bienes y servicios de TIC que la UTIC requiera contratar en cada ejercicio fiscal, considerando las directrices de la Institución, así como las disposiciones que en materia presupuestaria, de adquisiciones, arrendamientos y servicios resulten aplicables.

2. Proporcionar al área contratante, el apoyo y los elementos técnicos necesarios para llevar a cabo los procedimientos de contratación de TIC y participar en los mismos de acuerdo con su ámbito de atribuciones.

1.2.3 Proceso de Administración de Servicios (ADS)

Objetivo General:

Definir los compromisos y costos de los servicios de TIC necesarios para mantener el adecuado funcionamiento de la Institución, así como identificar iniciativas de servicios de TIC que aporten beneficios importantes en el cumplimiento de los objetivos estratégicos de la Institución, con apego a la EDN y efectuar su instrumentación.

Objetivos Específicos:

1. Diseñar y mantener actualizada la arquitectura empresarial de los servicios de TIC y definir las especificaciones técnicas para satisfacer las necesidades actuales y proyectadas de la Institución, considerando que se deben incluir las definiciones de los niveles de seguridad, capacidad, disponibilidad y continuidad de la operación de TIC

2. Identificar y administrar riesgos, desde el diseño de los servicios de TIC, para que puedan ser eliminados, transferidos o mitigados y de ser el caso, aceptados.

1.2.4 Proceso de Administración de la Configuración (ACNF)

Objetivo General:

Establecer y actualizar un repositorio de configuraciones, en el que se integren las soluciones tecnológicas y sus componentes, así como la información funcional y técnica de los mismos y la relativa a los diversos ambientes y arquitecturas tecnológicas de la UTIC, como elementos de configuración, con la finalidad de facilitar su acceso a los involucrados en los procesos de la UTIC, cuando éstos así lo requieran para la operación del proceso respectivo.

Objetivos Específicos:

1. Identificar, registrar, controlar y verificar los datos de los elementos de configuración, así como la información relacionada con los mismos.

2. Mantener actualizada la información contenida en el repositorio de configuraciones y disponible para los Servidores Públicos de la UTIC involucrados en los diversos procesos.

1.2.5 Proceso de Administración de la Seguridad de la Información (ASI)

Objetivo General:

Establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Institución, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos de la Institución o constituir una amenaza para la Seguridad Nacional.

Objetivos Específicos:

1. Establecer, operar y mantener un modelo de gobierno de seguridad de la información.

2. Efectuar la identificación de Infraestructuras de información esenciales y, en su caso, críticas, así como de activos clave de la Institución, y elaborar el catálogo respectivo.

3. Establecer los mecanismos de administración de riesgos que permitan identificar, analizar, evaluar, atender y monitorear los riesgos.

4. Establecer un SGSI que proteja los activos de información de la Institución, con la finalidad de preservar su confidencialidad, integridad y disponibilidad.

5. Establecer mecanismos para la respuesta inmediata a incidentes a la seguridad de la información.

6. Vigilar los mecanismos establecidos y el desempeño del SGSI, a fin de prever desviaciones y mantener una mejora continua.

7. Fomentar una cultura de seguridad de la información en la Institución.

1.2.6 Proceso de Administración de Proyectos (ADP)

Objetivo General:

Administrar la Cartera Operativa de proyectos de TIC, a fin de optimizar la aplicación de los recursos y obtener mayores beneficios para la Institución.

Objetivos Específicos:

1. Establecer la gobernabilidad de la Cartera Operativa de Proyectos de TIC.

2. Establecer las directrices y visión para administrar la cartera operativa de proyectos TIC.

1.2.7 Proceso de Administración de Proveedores (APRO)

Objetivo General:

Establecer un mecanismo que permita verificar el cumplimiento de las obligaciones derivadas de los contratos celebrados para la adquisición, arrendamiento o servicios de TIC.

Objetivos Específicos:

1. Identificar hallazgos, desviaciones y riesgos en el cumplimiento de los contratos en materia de TIC.
2. Proponer acciones preventivas y correctivas que propicien el adecuado cumplimiento del proveedor a sus obligaciones contractuales.

1.2.8 Proceso de Administración de Operación (AOP)

Objetivo General:

Entregar a los usuarios los servicios de TIC, conforme a los niveles de servicio acordados y con los controles de seguridad definidos.

Objetivos Específicos:

1. Operar la infraestructura y servicios de TIC, de manera que puedan resistir fallas, ataques deliberados o desastres y, se recuperen los servicios de TIC de manera ágil y segura.
2. Asegurar la estabilidad y continuidad de la operación de la infraestructura de TIC en la aplicación de cambios y la solución de problemas e Incidentes, la implementación de aplicativos de cómputo, soluciones tecnológicas y nuevos servicios de TIC.

1.2.9 Operación de Controles de Seguridad de la Información y del ERISC (OPEC)

Objetivo General:

Implementar y operar los controles de seguridad de la información de acuerdo con el programa de implementación del SGSI, así como los correspondientes a la capacidad de respuesta a incidentes.

Objetivo Específico:

1. Implementar las mejoras recibidas del Proceso de Administración de la Seguridad de la Información (ASI), para el fortalecimiento del SGSI, tanto de sus guías técnicas como de los controles de seguridad de la información en operación.

1.3 Aplicación Actual del Manual

En similitud a las versiones que anteceden al MAAGTICSI, la versión vigente del 4 de febrero de 2016, tiene influencia de mejores prácticas y estándares internacionales tales como: Balanced Score Card, TOGAF, Cobit, ISO 9001, VAL IT, PMBOK, CMMI, ITIL, RISK IT e ISO 27001, 27005 y 31000, PRINCE 2, ARCHIMATE, así como el uso de Normas Oficiales Mexicanas como; NMX-I-38500-NYCE-2009 y MX-I-20000-1-NYCE-2010.

Por tal motivo, y una vez identificado los antecedentes del MAAGTICSI, así como su estructura, procesos y regulación normativa aplicable a las dependencias y entidades de la APF, podemos intuir que su implementación ha servido a las mismas a llevar acabo un control en lo que respecta a la Seguridad de la Información en materia de TIC.

Con el fin de complementar la presente investigación, a continuación, se abordarán diversos aspectos de la Ley General de Datos Personales en Posesión de Sujetos Obligados, con el fin de analizar los procedimientos regulatorios que se establecen en la misma.

Capítulo 2

Ley General de Datos Personales en Posesión de Sujetos Obligados y Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Capítulo 2: Ley General de Datos Personales en Posesión de Sujetos Obligados y Lineamientos Generales de Protección de Datos Personales para el Sector Público.

En la historia de la humanidad siempre han estado presentes los datos personales, de alguna manera el ser humano siempre ha buscado reservar información que no quiere divulgar y/o considera sensible, si bien es cierto que antes del siglo XX la protección de los datos personales no era una preocupación importante, el surgimiento de nuevas tecnologías ha planteado con mayor intensidad una serie de retos y problemáticas respecto al uso de los datos personales que impacta directamente en la vida de las personas.

El derecho a la protección de los datos personales se ha ido configurando a lo largo de los años, su precedente más remoto e internacional lo podemos ubicar en el desarrollo y evolución del derecho a la privacidad a finales de la Segunda Guerra Mundial (1939-1945) con la creación de la Organización de las Naciones Unidas[20] (1945) mediante el documento llamado Declaración Universal de los Derechos Humanos[21] (1948), en su artículo 12 que define;

> "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de*

[20] Las Naciones Unidas nacieron oficialmente el 24 de octubre de 1945, después de que la mayoría de los 51 Estados Miembros signatarios del documento fundacional de la Organización, la Carta de la ONU, la ratificaran. En la actualidad, 193 Estados son miembros de las Naciones Unidas, que están representados en el órgano deliberante, la Asamblea General. Consultado en http://www.un.org/es/about-un/ el 25 de noviembre de 2017.

[21] Asamblea general de la ONU. "Declaración Universal de los Derechos Humanos." "Naciones Unidas," 217 (III) A, 1948, París, Consultado en http://www.un.org/es/universal-declaration-human-rights/index.html el 26 de noviembre de 2017.

ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."[22]

2.1 Antecedentes

Las últimas dos décadas han representado un largo camino para la conformación de un marco normativo para la protección de datos personales en México, podemos identificar los primeros esfuerzos a partir del año 2001, dichos esfuerzos fueron infuenciados por factores como la globalización, el amplio uso de las nuevas tecnologías como Internet, el marco normativo para la protección de datos personales en Europa con el Convenio 108 del Consejo de Europa, la Directiva 95/46/CE y la Carta de Derechos Fundamentales de la Unión Europea, y el derecho a la privacidad en Estados Unidos de América.

A partir de ese año se inician una serie de trabajos legislativos que a lo largo del tiempo fueron dando contenido para la formulación de leyes que en una primer instancia no eran específicas para la protección de datos personales, sin embargo, fueron esfuerzos importantes que significaron las bases para la posterior formulación y promulgación de leyes específicas para garantizar la protección de los datos personales. Es importante mencionar que el desarrollo constante de nuevas tecnologías como Big Data, Internet de las Cosas, Inteligencia Artifical, etc, representan un gran reto para el campo del Derecho, ya que día a día plantea nuevas situaciones a resolver y por ello es importante adecuar los marcos normativos ante la aparición de nuevas tecnologías o las nuevas formas de uso de tecnologías existentes, en este último aspecto, también identificamos que la Seguridad Informática juega un papel sustancial en la consecución de la protección de datos personales.

---

[22] Organización de las Naciones Unidas, Declaración Universal de los Derechos Humanos 1948. Consultado en http://www.un.org/es/universal-declaration-human-rights/ el 26 de noviembre de 2017.

2.1.1 Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

Un primer acercamiento hacia la Protección de los Datos Personales en México, en el año 2002 el Congreso Mexicano aprobó la promulgación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) – actualmente abrogada - con el objetivo principal de garantizar el derecho de acceso a la información pública buscando transparentar las actividades del gobierno y aumentar la confianza de la población, la Ley en comento no tenía por objeto principal la protección de datos personales, si estableció aspectos básicos para la protección de los mismos iniciando en la fracción II del artículo 3 de la LFTAIPG que define lo que son los datos personales[23], lo que permitió tener un bien jurídico tutelado que quedará bajo la responsabilidad del Sujeto Obligado[24], el cual es definido en la fracción XIV del artículo 3 de la LFTAIPG. Como mencionamos anteriormente, la Ley no era específica para la protección de los datos personales, de manera general si contenía un objetivo referente a nuestro tema principal establecido en la fracción III del artículo 4 de esta Ley; "Garantizar la protección de los datos personales en posesión de los sujetos obligados".

---

[23] Según la LFPDPPP, datos personales: Cualquier información concerniente a una persona física identificada o identificable. Consultada en http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf el 2 de diciembre de 2017.

[24] Sujetos obligados: a) El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República; b) El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos; c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal; d) Los órganos constitucionales autónomos; e) Los tribunales administrativos federales, y f) Cualquier otro órgano federal. Consultado en http://inicio.ifai.org.mx/LFTAIPG/LFTAIPG.pdf el 2 de diciembre de 2017.

Uno de los aspectos más relevantes de la LFTAIPG respecto a la Protección de Datos Personales, se centra en su capítulo IV relativo a disposiciones específicas para garantizar el derecho a la protección de datos personales, en el cual se establece responsabilidades y limitantes de los sujetos obligados, derechos de los interesados, procedimientos de acceso y corrección de datos personales; desde los artículos 20 al 26 de la citada Ley. Otro aspecto de vital importancia establecido en la multicitada Ley para la protección de los datos personales en México, fue la creación del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) y que actualmente es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Es importante resaltar que la LFTAIPG solo era aplicable a los sujetos obligados que de manera general los podemos definir como la APF, sin embargo, quedaba en el vacío la regulación del tratamiento de los datos personales en el sector privado, que en su momento tendría que ser atendido por otros instrumentos jurídicos, y que finalmente fue regulado mediante la promulgación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en el año 2010.

Una vez creado y establecido el IFAI, para el año 2005 publicó los Lineamientos Generales de Protección de Datos Personales para el sector público, como instrumento administrativo de carácter general, para una correcta aplicación de la LFTAIPG, con el objeto de establecer las políticas generales y procedimientos que deberán atender las dependencias y entidades de la APF, con el propósito de asegurar el adecuado tratamiento de los datos personales.

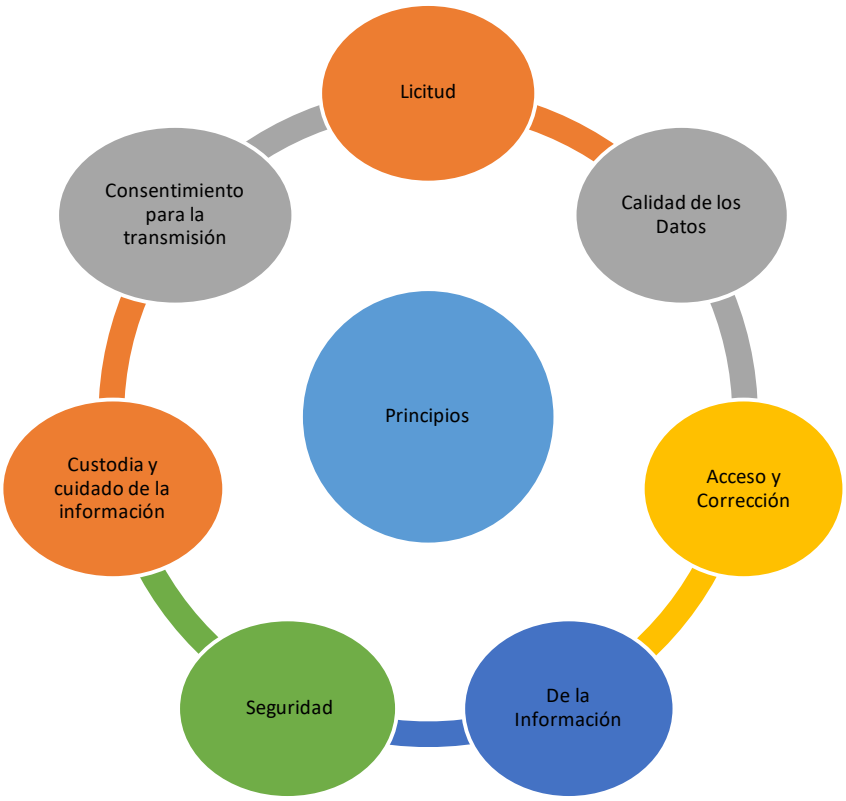


Figura 5. Principios normativos

Fuente: Elaboración propia con base a los Lineamientos Generales de Protección de Datos Personales para el sector público vigente en 2005.

Derivado de sus atribuciones el entonces IFAI en el año 2006 publicó las "*Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales*"[25] para establecer las políticas generales para el manejo, mantenimiento, seguridad y protección de datos personales, que estén en posesión de las dependencias y entidades de la APF, en dicho documento hace énfasis en que se debe se debe tomar en cuenta los avances tecnológicos, la naturaleza de los datos y los riesgos a los que estén expuestos.

[25] Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales. Consultado en https://www.gob.mx/cms/uploads/attachment/file/83122/MODELOS_Y_GU_AS_17.pdf el 20 de diciembre de 2017.

2.1.2 Constitución Política de los Estados Unidos Mexicanos (CPEUM)

En México a razón de que a nivel internacional la protección de datos personales se considera como un derecho fundamental[26], en el año 2007 se realiza una reforma al artículo 6° constitucional en el que se adicionan 7 fracciones, entre las que se hace de manifiesto en las fracciones II y III la protección de los datos personales de manera clara y explícita.

> *II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.*
> *III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.*

Como lo menciona la Dra. Peschard, *"Las fracciones II y III de la CPEUM, tiene la virtud de ser las primeras menciones constitucionales que hacen un reconocimiento del derecho a la protección de datos personales, dando continuidad a la labor iniciada por el legislador ordinario a través de la Ley Federal de Transparencia"*.[27]

Sin embargo, no fue sino hasta el año 2009 donde nuevamente a través de una reforma constitucional al artículo 16 se garantiza la protección de los datos

---

[26] Del Derecho fundamental a la Protección de Datos de Carácter Personal, Consultado en https://www.agpd.es/portalwebAGPD/common/FOLLETO.pdf el 22 de diciembre de 2017.

[27] Peschard Mariscal Jacqueline, 2013, "El Derecho Fundamental a la Protección de Datos Personales en México", Tirant Lo Blanch eds, La Protección de Datos Personales en México, p. 29.

personales reconociéndolo como un "derecho distinto y fundamental"[28] (Ornelas Lina, 2013, p.68), así como dotarlo de contenido mediante las adiciones de los siguientes párrafos:

> *"Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la Ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros."*[29]

La adición del segundo párrafo al artículo 16 constitucional contiene 3 aspecto principales:

- El establecimiento del derecho a la protección de datos personales a nivel constitucional,
- El establecimiento de los derechos de acceso, rectificación, cancelación y oposición (ARCO)[30], y las excepciones a los principios que rigen el tratamiento de datos personales.

Figura 6. Derechos ARCO
Fuente: Elaboración propia con base en información del Diario Oficial de la Federación del 9 de diciembre de 2015.

[28] Ornelas Lina, "La recepción del derecho a la protección de datos en México: breve descripción de su origen y estatus legislativo", Protección de Datos Personales, 2013, p.68.

[29] Consultado en http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf el 20 de noviembre de 2017.

[30] Acuerdo mediante el cual se aprueban los lineamientos de los procedimientos de protección de derechos, de investigación y verificación, y de imposición de sanciones. Consultado en http://dof.gob.mx/nota_detalle.php?codigo=5419449&fecha=09/12/2015 el 25 de noviembre de 2017.

Y finalmente en la misma reforma constitucional se adiciona la fracción XXIX-O del artículo 73 de la CPEUM, que otorga la facultad al Congreso de la Nación para legislar en materia de protección de datos personales en posesión de particulares.

Si bien este trabajo de titulación está enfocado específicamente a la Protección de Datos Personales en Posesión de Sujetos Obligados, no podemos dejar de mencionar la importancia de la publicación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares[31], expedida en el año 2010 cuyo objeto es la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Rescataremos la reforma constitucional de 2014 en materia de transparencia, al INAI – en su momento IFAI -, mediante la cual lo dota de atribuciones importantes al otorgarle autonomía constitucional y al señalar que sus determinaciones tienen el carácter de definitivas e inatacables.

Es sumamente relevante esta reforma ya que amplía su alcance no solo de manera vertical (tres órdenes de gobierno[32]) sino también de manera horizontal, al ampliar el grupo de sujetos obligados[33].

---

[31] Ley Federal de Protección de Datos Personales en Posesión de Particulares, Consultada en http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf el 20 noviembre de 2017

[32] Tres niveles de gobierno: federal, estatal y municipal.

[33] Con este nuevo marco, la sociedad podrá conocer la información de los Poderes Ejecutivo, Legislativo y Judicial; órganos autónomos; partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física o moral, incluidos los sindicatos, que reciban y ejerzan recursos públicos o realicen actos de autoridad en el ámbito federal, estatal o municipal. Consultado en

2.1.3 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)

La gestión gubernamental se ha transformado notablemente en la última década, buscando ofrecer más y mejores servicios a la población que ha iniciado un cambio hacia un entorno más automatizado, donde la tecnología juega un papel muy importante, si bien es cierto que esto representa una gran oportunidad para hacer más eficientes los procesos operativos y de servicio a la sociedad, también representan un reto para el aseguramiento de la información en general y la protección de datos personales en particular, por ello el Congreso mexicano se dio a la tarea de establecer un paraguas general de protección de datos personales para la administración pública que marcará los lineamientos mínimos a cumplir por parte de los sujetos obligados. Por ello, en enero de 2017 se promulga la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, iniciando así:

> *Artículo 1º- La presente Ley es de orden público y de observancia general en toda la República […]*
> *Tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.*
> […]

La promulgación de LGPDPPSO establece un marco normativo claro y específico para la protección de datos personales cuando los responsables son los sujetos obligados, así mismo se le otorgan mecanismos importantes al ciudadano

---

https://www.gob.mx/cms/uploads/attachment/file/66464/13_Transparencia.pdf el 20 de noviembre de 2017.

para el ejercicio de sus derechos ARCO. Sin embargo, si bien la Ley es observancia general y vinculante, hasta el mes de agosto de 2017 se tenían reconocidos solo a 24 estados con Ley de protección de datos personales, las 8 entidades restantes deberán aplicar de manera directa las disposiciones de la Ley General[34].

2.1.4 Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Conforme a lo establecido en la promulgación de la LGPDPPSO, el INAI público los Lineamientos Generales de Protección de Datos Personales para el Sector Público, con esto, se busca que exista un solo instrumento normativo donde se concentren las obligaciones establecidas en la Ley, teniendo como finalidad "facilitar y hacer más comprensible y simple el conocimiento y la exigibilidad del derecho a la protección de datos personales en el sector público federal" [35]

Los Lineamientos publicados se conforman de 9 títulos en los cuales se desarrollan con más detalle aspectos señalados en los capítulos de la Ley, con esto se busca dar mayor cuerpo a la misma.

Título	Nombre	Descripción
Primero	Disposiciones Generales	Se establece el objetivo y los ámbitos de validez subjetivo y objetivo de este ordenamiento
Segundo	Principios y deberes	Desarrolla los principios y deberes de protección de datos personales a que se refiere la Ley

[34]Gobierno de Zacatecas, 8 de agosto de 2017, Cuentan 24 estados con Ley de Protección de Datos Personales en posesión de sujetos obligados. Consultado en http://transparencia.zacatecas.gob.mx/cuentan-24-estado-con-ley-de-proteccion-de-datos-personales-en-posesion-de-sujetos-obligados/ el 28 de diciembre de 2017.

[35] Lineamientos Generales de Protección de Datos Personales para el Sector Público, consultado en http://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018, el 15 de febrero de 2018.

Tercero	Derechos de los Titulares y su Ejercicio	Se regulan los derechos ARCO y las reglas generales para su efectivo ejercicio
Cuarto	Relación del responsable y Encargado	Reglas aplicables a la figura del encargado
Quinto	Transferencia de datos personales	Establece disposiciones específicas en materia de transferencias nacionales e internacionales de los datos personales
Sexto	Acciones preventivas en materia de protección de datos personales	Se desarrollan las acciones preventivas en materia de protección de datos personales
Séptimo	Medios de impugnación	Se establecen reglas muy puntuales en torno al procedimiento de sustanciación de los recursos de revisión e inconformidad
Octavo	Facultad de verificación del instituto	Reglas que deberán regir los procedimientos de investigaciones previas y verificación del cumplimiento de las disposiciones previstas en la Ley, así como auditorías voluntarias.
Noveno	De las medidas de apremio y responsabilidades administrativas	Se desarrollan las medidas de apremio y el régimen de responsabilidades administrativas.

Figura 7. Nueve títulos de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Fuente: Elaboración propia con base en información del Diario Oficial de la Federación del 26 de enero de 2018.

Los Lineamientos Generales destacan su importancia al señalar con mayor detalle los puntos finos de la Ley, considerados una guía general que define el ¿qué? deben atender los sujetos obligados, sin embargo, no establece el ¿cómo? lo deben hacer, con esto se da una completa libertad a las instituciones de la APF a adoptar los mecanismos acordes a cada institución siempre y cuando se atiendan los deberes de la Ley.

2.2 Estructura de la Ley

Con la reciente promulgación de la LGPDPPSO, se actualiza y complementa el marco regulatorio nacional respecto a la protección de datos personales en el sector público, establece las bases mínimas que regirán el tratamiento de los datos personales en la administración pública, así como diversos aspectos importantes como la ampliación del grupo de Sujetos Obligados, e incorpora elementos como la

Evaluación de Impacto, tratamiento intensivo, datos personales sensibles, transferencia y remisión, entre otros. No es tema de esta investigación hacer un análisis profundo de cada artículo de la Ley, pero si plasmar los elementos más relevantes de la misma, mediante la descripción de sus capítulos.

2.2.1 Disposiciones Generales

- *La Ley se expide con la finalidad de establecer un marco mínimo de cumplimiento en la protección de datos para los sujetos obligados, ya sea armonizando sus Leyes locales a la Ley General o bien realizar la aplicación directa de la LGPDPPSO.*
  - *Tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.*
  - *Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.*

Objetivo

- *Tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.*

Ámbito de aplicación.

Artículo 1º- La presente Ley es de orden público y de observancia general en toda la República […]

2.2.2 Principios y Deberes[36]

Mediante los principios y deberes establecidos en la Ley se busca que el tratamiento de los datos personales en todo su ciclo sea de manera legítima, el responsable y encargado deberá cumplir con los mismos para poder hacer uso de los datos personales que su organización este tratando. También notaremos que existe una diferencia importante en la definición y número de principio establecidos en la LGPDPPSO y la actualmente abrogada LFTAIPG.

a) Principios

Los principios son regulados o están incluidos en el art. 16 de la LGPDPPSO, el cual señala lo que se transcribe a continuación:

> *"Artículo 16. El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales".*

[36] Guía para titulares de los Datos Personales Volumen 2. Consultado en http://inicio.ifai.org.mx/GuiasTitulares/Guia%20Titulares-02_PDF.pdf el 29 de diciembre de 2017

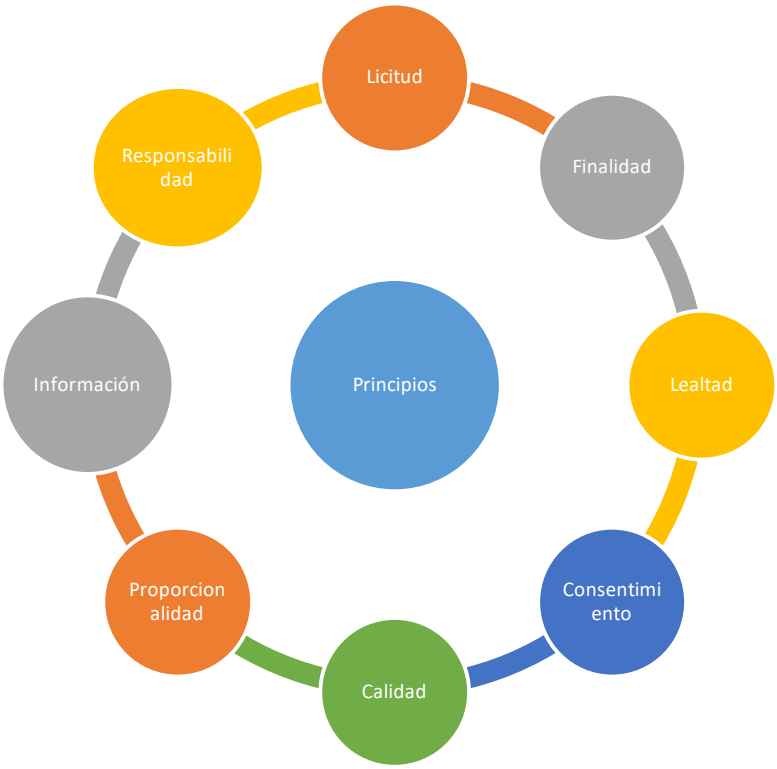


Figura 8. Principios rectores, *LGPDPPSO*

Fuente: Elaboración propia con base en información del Diario Oficial de la Federación del 26 de enero de 2017.

b) Deberes

Con relación a los deberes el Art. 31 de la LGPDPPSO señala lo siguiente[37]…:

> *"Artículo 31. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se*

[37] Guía para titulares de los Datos Personales Volumen 2, Consultado en http://inicio.ifai.org.mx/GuiasTitulares/Guia%20Titulares-02_PDF.pdf el 28 de noviembre de 2017.

efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad".

Figura 9. Deberes, LGPDPPSO

Fuente: Elaboración propia con base en información del Diario Oficial de la Federación del 26 de enero de 2017.

2.2.3 Derechos de los titulares

La Ley busca dotar de mecanismos eficientes a los titulares de datos personales mediante el ejercicio de sus derechos ARCO y mediante el órgano garante como lo es el INAI, se busca tener medios eficientes para el ejercicio de los mismos.

a) Derechos[38]

"Artículo 43. En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le

[38] Guía para Titulares de los Datos Personales Volumen 3. Consultado en http://inicio.ifai.org.mx/GuiasTitulares/Guia%20Titulares-03_PDF.pdf el 20 de diciembre de 2017.

conciernen, de conformidad con lo establecido en el presente Título. El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro".

Figura 10. Derechos ARCO, LGPDPPSO

Fuente: Elaboración propia con base en información del Diario Oficial de la Federación del 26 de enero de 2017.

2.2.4 Relación del responsable y encargado

Si bien es cierto que las figuras jurídicas de responsable y encargado de protección de datos personales puede ser la misma persona física o moral, también pueden ser dos entes independientes, por ello es importante indicar que la Ley establece las obligaciones de cada una de ellas de manera independiente.

a) Responsable

Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales.

"Artículo 1

[...]

Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito

federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.
En todos los demás supuestos diferentes a los mencionados en el párrafo anterior, las personas físicas y morales se sujetarán a lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

b) Encargado

La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable."

2.2.5 Comunicación de Datos Personales

Las transferencias y remisiones de información siguen estando sujetas a lo establecido en la Ley, por ello las dependencias sujetas a la LGPDPPSO, deben cumplir con lo estipulado la misma para poder hacer uso de las ventajas de la tecnología como el computo en la nube, para poder enviar los datos personales de los ciudadanos en servidores hospedados fuera del territorio nacional.

Acorde a la definición de la Ley, una transferencia es:
"Artículo 3 – Fracción XXXII
Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado; "
"Artículo 65. Toda transferencia de datos personales sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de esta Ley".
"Artículo 71. Las remisiones nacionales e internacionales de datos personales que se realicen entre responsable y encargado no requerirán ser informadas al titular, ni contar con su consentimiento".

2.2.6 Acciones Preventivas

El riesgo de vulnerabilidades de seguridad en los sistemas informáticos siempre es latente, por ello es importante que los responsables adopten esquemas que permitan en primera instancia minimizar el impacto de las brechas de seguridad y en segundo lugar reaccionar lo más pronto posible en caso de una afectación.

> *"Artículo 72. Para el cumplimiento de las obligaciones previstas en la presente Ley, el responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas que tengan por objeto: ".*

> *"Artículo 1. fracción XVI.*
> *Evaluación de impacto en la protección de datos personales: Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable; ".*

2.2.7 Responsables en materia de protección de datos personales en posesión de los Sujetos Obligados.

Es importante que el responsable en la protección de datos personales no sea solo una persona, es conveniente que sea un comité que tenga facultades para establecer los lineamientos internos a seguir para el cumplimiento de la Ley.

"Artículo 83. Cada responsable contará con un Comité de Transparencia, el cual se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable. El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales".

2.2.8 Organismos Garantes

Las dependencias y entidades de la APF deben atender las disposiciones de Ley y dar cumplimiento a lo que establecen los órganos locales de protección de datos personales en cada estado, así como al órgano garante nacional INAI.

"Artículo 88. En la integración, procedimiento de designación y funcionamiento del Instituto y del Consejo Consultivo se estará a lo dispuesto por la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública y demás normativa aplicable".

"Artículo 3 – fracciones XVII y XXIV

XVIII. Instituto: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados;

XXIV. Organismos garantes: Aquellos con autonomía constitucional especializados en materia de acceso a la información y protección de datos personales, en términos de los artículos 6o. y 116, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos".

2.2.9 Procedimientos de impugnación en materia de protección de datos personales en posesión de sujetos obligados

El medio de impugnación que tiene el titular o el representante es el que se señala en el Art. 94 de la Ley, el cual a la letra dice:

> *Artículo 94. El titular o su representante podrá interponer un recurso de revisión o un recurso de inconformidad ante el Instituto o los Organismos garantes, según corresponda, o bien, ante la Unidad de Transparencia, […]*

2.2.10 Facultad de Verificación del Instituto y los organismos garantes

La Ley concede la facultad a el Instituto como a los Organismos garantes para realizar la verificación de cumplimiento de las disposiciones de la Ley, de ahí que se derive la necesidad de evidenciar dicho cumplimiento. Lo anterior, se encuentra plasmado en el Art. 146 de la Ley, como se indica a continuación:

> *"Artículo 146. El Instituto y los Organismos garantes, en el ámbito de sus respectivas competencias, tendrán la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente Ley y demás ordenamientos que se deriven de ésta."*

2.2.11 Medidas de Apremio y responsabilidad

En la Ley se dan medidas para poder sancionar a los sujetos Obligados de resguardar los datos personales, es importante señalar que este es un GRAN cambio, ya que anteriormente en las normas que aplicaban a los Servidores Públicos, no se preveía estas medidas de apremio.

> *"Artículo 152. Para el cumplimiento de las resoluciones emitidas por el Instituto o los Organismos garantes, según corresponda, estos organismos y el responsable, en su caso, deberán observar lo dispuesto en el Capítulo VI del Título Octavo de la Ley General de Transparencia y Acceso a la Información Pública*

"Artículo 153. El Instituto y los Organismos garantes podrán imponer las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones:

I. La amonestación pública, o

II. La multa, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización.

El incumplimiento de los sujetos obligados será difundido en los portales de obligaciones de transparencia del Instituto y los Organismos garantes y considerados en las evaluaciones que realicen éstos.

En caso de que el incumplimiento de las determinaciones del Instituto y los Organismos garantes implique la presunta comisión de un delito o una de las conductas señaladas en el artículo 163 de la presente Ley, deberán denunciar los hechos ante la autoridad competente. Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos."

2.3 Elementos Básicos en la Seguridad Informática

Inmersos en la revolución digital y en la transición hacia una Sociedad de la Información y Conocimiento, la generación de datos y/o información en los últimos años ha tenido una transformación y crecimiento sin precedentes. De acuerdo con el Informe de Business Software Alliance (BSA)[39] "*se destaca la manera en que la*

[39] BSA, The Software Alliance es el principal defensor de la industria global del software ante los gobiernos y el mercado internacional. Se trata de una asociación de empresas de clase mundial que invierten miles de millones de dólares al año para crear soluciones de software que promueven a la economía y mejoran la vida moderna.

emergente economía impulsada por los datos afecta a varios sectores, como la producción, el transporte, la energía, la agricultura, la educación y la salud, más del 90% de los datos del planeta se crearon solo en los últimos dos años, y ahora estamos duplicando la velocidad con que se producen cada dos años."

En el ámbito gubernamental, la masificación de datos se observa como una excelente oportunidad para obtener datos de múltiples fuentes y canales. Al combinar estos datos, de forma inteligente y eficiente, se puede revelar fenómenos que de otra manera no hubiera sido posible identificar.

Al ser los datos un activo valioso para las organizaciones, los delincuentes cibernéticos han proliferado con herramientas más sofisticadas mediante las cuales buscan sacar provecho de las vulnerabilidades de los sistemas informáticos y/o bases de datos donde se encuentra almacenada la información, por eso es importante que las organizaciones tanto públicas como privadas, cuenten con una Estrategia de Seguridad Informática alineada a los objetivos de la organización, con el fin de garantizar la protección de la información en general y en específico de los datos personales, tema principal de este trabajo.

La BSA sirve como la principal organización de lucha contra la piratería de todo el mundo y como un líder respetado para conformar políticas públicas que promueven la innovación tecnológica e impulsan el crecimiento económico.

A través de las relaciones gubernamentales, la observancia de la propiedad intelectual y de actividades educativas en el mundo, la BSA protege la propiedad intelectual y fomenta la innovación; trabaja para abrir mercados y garantizar la competencia justa; y construye confianza y seguridad en las tecnologías de información para los consumidores, empresas y gobiernos por igual. ¿Por qué son tan importantes los datos?, Consultada en http://data.bsa.org/wp-content/uploads/2015/10/BSADataStudy_es.pdf, el 15 de abril de 2017.

Cómo se abordará en el siguiente punto, la Ley no establece la obligatoriedad de contar con un Sistema de Gestión de la Seguridad de la Información (SGSI)[40], sin embargo, su importancia radica en que permita llevar de manera planificada, organizada y documentada, las tareas relacionadas con la administración de la seguridad de la información.

2.3.1 Sistema de Gestión de la Seguridad de la Información

Seguridad de la Información no es un tema nuevo para las organizaciones, sin embargo, ha tomado mayor relevancia en los últimos años por ser un elemento sustancial para la protección de la información en un entorno digitalizado y conectado a Internet.

Por eso identificamos como una necesidad la implementación de un SGSI para minimizar los riesgos de vulnerabilidades de los sistemas de información y diversos elementos que lo conforman, y utilizar el SGSI como un elemento que nos permita dar cumplimiento a los deberes establecidos por la Ley respecto a los encargados de los datos personales.

Como se abordó en el Capítulo 1, nos centraremos en el *Manual Administrativo de Aplicación General en las materias de Tecnologías de la*

---

[40] SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI Consultada en http://www.iso27000.es/download/doc_sgsi_all.pdf , el 13 de marzo de 2018.

Información y Comunicaciones de Seguridad de la Información[41] (MAAGTICSI), por ser el marco normativo en materia de Tecnologías de la Información y Comunicación para la administración pública y específicamente en los procesos de *Administración de la Seguridad de la Información (ASI) y* Operación de Controles de Seguridad de la Información y del ERISC *(OPEC), al tratarse de los temas de Seguridad de la Información (SI).*

2.3.2 MAAGTICSI - ASI

Retomando el objetivo principal del proceso de Administración de la Seguridad de la Información, según el manual es:

Establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Institución, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos de la Institución o constituir una amenaza para la Seguridad Nacional.[42]

El objetivo del proceso ASI de MAAGTICSI se alinea perfectamente a lo dispuesto en el artículo 34 de la LGPDPPSO:

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

2.3.3 MAAGTICSI - OPEC

Por su parte, el objetivo principal del proceso de Operación de Controles de Seguridad de la Información y del ERISC es el siguiente según el manual:

---

[41] Política TIC/MAAGTICSI 2017. Consultada en https://www.gob.mx/cidge/acciones-y-programas/politica-tic-maagticsi-2017 el 9 de marzo de 2018.

[42] Definición de los 9 procesos MAAGTICSI, Consultado en https://www.gob.mx/cms/uploads/attachment/file/58682/Definicion_de_los_9_procesos_MAAGTICSI.pdf el 9 de marzo de 2018.

Implementar y operar los controles de seguridad de la información de acuerdo con el programa de implementación del SGSI, así como los correspondientes a la capacidad de respuesta a incidentes.[43]

Este proceso materializa el resultado del proceso ASI, es la parte técnica operativa que mediante un marco de referencia como ISO 27001 y herramientas tecnológicas se concreta lo establecido en el proceso de ASI.

2.4 Problemática Actual en la Protección de Datos Personales

La dependencia que tenemos con respecto a la tecnología es incuestionable, la utilización de esta ha transformado cualquier aspecto de nuestro entorno ya sea como individuos, sectores de la sociedad o como una sola sociedad en conjunto.

El Internet es un claro ejemplo, una tecnología disruptiva que ha derrumbado barreras de espacio y tiempo, que ha permitido que las organizaciones y las personas estén conectadas alrededor mundo, así mismo es el medio más importante para el flujo de información en las últimas décadas, asociado al Internet podemos ubicar otra tecnología importante como lo es Big Data, el cual tiene como instrumento primordial a, ***los datos***, lo que permite que tengan y/o generen valor para las organizaciones privadas como públicas.

Por otra parte, es importante reflexionar acerca de los retos y problemas que esto representa. El uso intensivo de la tecnología como el teléfono inteligente, las tabletas, y ahora con el auge del Internet de las Cosas en las que casi cualquier objeto puede estar conectado a la red, hace que la información pueda estar accesible a casi cualquiera, lo cual pone en riesgo la información de las personas (datos personales) afectando contundentemente la privacidad de las mismas.

---

[43] Disposiciones de la Estrategia Digital Nacional en materia de Tecnologías de la Información y Comunicaciones, consultado en https://www.gob.mx/cms/uploads/attachment/file/59534/MAAGTICSI_compilado_04_02_2016.pdf el 9 de marzo de 2018.

Si bien es cierto, en el ámbito nacional se han realizado esfuerzos significativos para garantizar la protección de los datos personales, sin embargo, en el contexto actual de nuestra sociedad se sigue planteando nuevos retos que deberán ser considerados no solo desde la visión tecnológica con mejores sistemas informáticos para asegurar la integridad y confidencialidad de la información, sino también deberán considerarse aspectos culturales, económicos, sociales y jurídicos. Por tal motivo, planteamos una serie de retos que la protección de datos personales debe enfrentar.

Retos

- Marcos regulatorios flexibles para no bloquear el desarrollo de las organizaciones en su modelo de negocios basados en los datos
- Asignación de presupuesto para contar con una estrategia de Seguridad de la Información alienada al cumplimiento de los nuevos marcos jurídicos
- Educación y concientización
- Economía basada en datos
- Protección de los niños en la era de la información
- Privacidad desde el diseño
- Privacidad por defecto
- Big Data - Anonimización
- Computo en la nube - ¿Dónde están nuestros datos?
- Transferencias internacionales

Solventar las problemáticas inherentes a la evolución tecnológica, la globalización y la transformación digital en la ahora conocida Sociedad de la Información y Conocimiento, no es una tarea fácil de conseguir y al parecer no tiene fin en el contexto cambiante de nuestra sociedad, sin embargo, siempre se deberán realizar esfuerzos constantes para la construcción de un entorno adecuado en la utilización de la información.

Indudablemente vemos esfuerzos significativos en materia legislativa referente a la generación de un marco jurídico para la protección de los datos personales en

posesión de particulares y sujetos obligados, con ello se busca generar un entorno adecuado que garantice la protección de los datos personales en todo el tratamiento.

Hoy en día con la transformación digital de todo nuestro entorno, la APF está adoptando modelos de gestión y operación con el apoyo de las tecnologías, por ello es importante que las entidades públicas que son sujetas de la LGPDPPSO tengan alineados sus procesos operativos con las disposiciones que marca la Ley a fin de evitar duplicidad de actividades, discrepancias operativas y hasta incumplimientos de la misma.

Finalmente es importante que las áreas de TIC de la APF estén orientadas a los objetivos estratégicos de la institución, lo cual permitirá dar cumplimiento a los objetivos institucionales aunado a las obligaciones de Ley, por ello la razón de este trabajo de investigación, el cual busca empatar las obligaciones señalas por la LGPDPPSO con el modelo de referencia MAAGTICSI.

Capítulo 3

Análisis comparado entre el MAAGTICSI y la Ley General

Capítulo 3: Análisis comparado entre el MAAGTICSI y la Ley General.

En el presente capítulo se abordará un Análisis Comparado entre el **Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información (MAAGTICSI)** en el proceso **ASI** y la **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley)**, con el objetivo es determinar las convergencias entre los deberes establecidos en cada normatividad, con la finalidad de identificar su aplicabilidad en la APF.

Con dicho estudio, analizaremos las semejanzas y diferencias entre las normatividades y de acuerdo al resultado que se obtenga, se podrá señalar que disposiciones de MAAGTICSI dan cumplimiento a los deberes de la Ley, y viceversa, si se cumple con algunas cosas de la Ley se seguirá dando cumplimiento a lo señalado en el MAAGTICSI, y de esta forma simplificaremos y consolidaremos tareas y actividades para el cumplimiento de ambas normas.

Tema 1: Objeto

Acuerdo: Tiene por objeto emitir políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias, contenido en su Anexo Único, Artículo 1.

Ley: Tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados, Artículo 1ro. Tercer párrafo

Análisis: Objetos diferentes.

Tema 2: Ámbito de aplicaciones

Acuerdo:

Artículo 1. Observancia obligatoria en la Administración Pública Federal y en la Procuraduría General de la República.

Ley:

Artículo 1. Primer y cuarto párrafo. Todas las disposiciones de esta Ley General, según corresponda, y en el ámbito de su competencia, son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal.

Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Análisis: El Acuerdo es de observancia para la APF, mientras que la Ley es de orden federal, estatal y municipal.

Tema 3: Responsable

Acuerdo:

Artículo 3. La aplicación de las políticas y disposiciones contenidas en el presente Acuerdo y su Anexo Único, corresponde a los Titulares de las unidades administrativas o áreas responsables de las TIC en las Instituciones, así como a los Servidores Públicos cuyas atribuciones o funciones estén relacionadas con la planeación, contratación y administración de bienes y servicios de TIC y con la seguridad de la información.

Ley:

Artículo 1. Cuarto párrafo. Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Análisis: Los Servidores Públicos encargados de la aplicación del Acuerdo son los Titulares de las unidades administrativas o áreas responsables de las TIC en las Instituciones; y para la Ley son los sujetos obligados de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Tema 4: Borrado seguro

Acuerdo:

Artículo 2. Para los efectos del presente Acuerdo, se entiende por:

Borrado Seguro: el proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital;

Artículo 14.- En las contrataciones relacionadas con los servicios de correo electrónico, las Instituciones deberán prever en las convocatorias a la licitación pública, en las invitaciones a cuando menos tres personas o las solicitudes de cotización, o bien en los contratos que celebren con otros entes públicos, según corresponda, lo siguiente:

IV. Al término del plazo señalado en la fracción anterior, y no habiendo aclaraciones pendientes de resolver, el proveedor contará con 10 días naturales para entregar evidencias auditables de no conservar información alguna utilizando métodos de borrado seguro.

Artículo 27.- Las Instituciones mantendrán los componentes de software y de seguridad de los dominios tecnológicos actualizados para evitar vulnerabilidades, de acuerdo a lo que se establece en el MAAGTICSI, para lo cual implementarán, entre otros, elementos de seguridad de la información, los siguientes:

III. Mantener, evidencia auditable del proceso de borrado seguro; Artículo 2, 14 y 27

Ley:

Artículo 3. Para los efectos de la presente Ley se entenderá por:

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

XXX. Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción

de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable; Artículo 3, fracción XXI y XXX.

Artículo 23. El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

…

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser **suprimidos,** previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Análisis: En esta parte la Ley prevé de forma general el borrado seguro de la información, pero resulta importante precisar que el borrado de la información se encuentra previsto en el Acuerdo y se dan los mecanismos para hacerlo, siendo algo que las dependencias y entidades cubren al dar cumplimiento al Acuerdo en mención.

Tema 5: Cómputo en la nube

Acuerdo:

Artículo 5, fracción I. El Portafolio de Proyectos de TIC se sujetará al artículo anterior, para lo cual atenderá lo siguiente:

I. Favorecer el uso del cómputo en la nube para el aprovechamiento de la economía de escala, eficiencia en la gestión gubernamental, fomentando la utilización de las TIC, los estándares abiertos y teniendo en consideración la seguridad de la información y la protección de datos personales.

Ley:

Artículo 63. El responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los

principios y deberes establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

En su caso, el responsable deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.

Análisis: Ambas normatividades prevén el uso del cómputo en la nube, solo que el Acuerdo lo prevé como una forma de aprovechamiento de la economía de escala, eficiencia en la gestión gubernamental, y la Ley como una opción de almacenamiento.

Tema 6: Interoperabilidad

Acuerdo:

Artículo 5, fracción VIII. Establecer estrategias de interoperabilidad al interior de la propia Institución y con otras Instituciones que requieran compartir datos que obren en su posesión, puedan o no formar parte de un mismo proceso, y…

Ley:

Artículo 57. Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.

El Sistema Nacional establecerá mediante lineamientos los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales. Artículo 57.

Artículo 70. El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los siguientes supuestos:

I. Cuando la transferencia esté prevista en esta Ley u otras Leyes, convenios o Tratados Internacionales suscritos y ratificados por México;

Análisis: El Acuerdo refiere una interoperabilidad al interior de la Institución y fuera de ella, estableciendo estrategias, y la Ley se refiere a la trasferencia en formatos estructurados.

Tema 7: Dominio tecnológico

Acuerdo:

Artículo 8. Las Instituciones deberán compartir recursos de infraestructura, bienes y servicios en todos los dominios tecnológicos, utilizando soluciones tecnológicas comunes a nivel institucional, sectorial y de la Administración Pública Federal, conforme a las directrices que emita la Unidad, teniendo en consideración la seguridad de la información, la privacidad y protección de datos personales.

Ley:

Artículo 32, fracción III Las medidas de seguridad adoptadas por el responsable deberán considerar:

El desarrollo tecnológico;

Análisis: El Acuerdo plantea la forma de implementar los recursos de infraestructura, así como los medios, y la Ley solo prevé el desarrollo tecnológico como una medida a considerar.

Tema 8: Desarrollo

Acuerdo:

Artículo 10, fracción II. En las contrataciones relacionadas con los servicios de desarrollo, implementación, soporte a la operación y mantenimiento de aplicativos de cómputo, las Instituciones deberán prever en las convocatorias a la licitación pública, en las invitaciones a cuando menos tres personas o las solicitudes de cotización, o bien en los contratos que se celebren con otros entes públicos, según corresponda, lo siguiente:

Incluir el diseño detallado del aplicativo que se vaya a desarrollar, considerando por lo menos, requerimientos del negocio, de seguridad de la información, de privacidad y protección de datos personales, técnicos, casos de uso, módulos, matriz de trazabilidad y protocolos de pruebas; así como el uso de la Identidad digital y, en su caso, lo dispuesto en artículo 19 fracción IV y artículo 26 del presente Acuerdo; considerando las guías o disposiciones que emita la Unidad a través de su portal;

Ley:

Artículo 3. Para los efectos de la presente Ley se entenderá por:

XVI. Evaluación de impacto en la protección de datos personales: Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable;

Artículo 30. Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:

VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y

VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.

Análisis: El Acuerdo establece las medidas a tomar para el desarrollo, mientras que la Ley prevé una evaluación de impacto en la protección de datos personales en programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales que se pretenda modificar.

Tema 9: Seguridad

Acuerdo:

Artículo 10. VII. Prever que la transferencia de datos se realice sobre canales seguros en donde se favorezca el cifrado y la integridad de los datos críticos, confidenciales sensibles, en concordancia con el MAAGTICSI, en lo referente a Seguridad de la Información;

Ley: Artículo 31. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Análisis: El Acuerdo hace referencia a la transferencia de datos por canales seguros y la Ley menciona que el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, de esto puede observarse que el Acuerdo prevé los mecanismos que, de considerarse, se estaría dando cumplimiento al Artículo 31 de la Ley.

Tema 10: Tratamiento y baja

Acuerdo:

Artículo 11. Con respecto a las redes de telecomunicaciones, las Instituciones deberán observar lo siguiente:

II. Contar con mecanismos estándares de cifrado de datos, de acuerdo a lo que se establece en las reglas del proceso de administración de servicios del MAAGTICSI, considerando la criticidad de los datos en sus etapas de tratamiento, especialmente en su transmisión a través de redes de telecomunicaciones.

Ley:

Articulo 3. XXI. Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;

XXX. Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable; Artículo 3 fracción XXI y XXX.

Artículo 23. El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

Artículo 24. El responsable deberá establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos, de conformidad con lo dispuesto en el artículo anterior de la presente Ley.

En los procedimientos a que se refiere el párrafo anterior, el responsable deberá incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales.

Análisis: El Acuerdo refiere con respecto al cifrado de datos refiere contar con mecanismos estándares de cifrado de datos considerando la criticidad de los datos en sus etapas de tratamiento y la Ley refiere sobre la baja archivística; el primero prevé todos las etapas y la Ley solo prevé una etapa que es la de baja.

Tema 11: Internet- seguridad de la información

Acuerdo:

Artículo 12. En las contrataciones relacionadas con los servicios de Internet, las Instituciones deberán prever en las convocatorias a la licitación pública, en las invitaciones a cuando menos tres personas o las solicitudes de cotización, o bien en los contratos que celebren con otros entes públicos, según corresponda, que los servicios cuenten con lo siguiente:

I. Mecanismos de protección a ataques de denegación de servicios, desde la propia red del proveedor e independientemente de los controles de seguridad de la información que implemente la Institución, debiendo atenderse mediante las actividades que se señalan en el MAAGTICSI para el establecimiento de controles de seguridad de la información, y

Ley: No especifica.

Análisis: Solo el Acuerdo prevé mecanismos de seguridad de la información respecto a los servicios de internet, pero no especifica datos personales, solo información en general.

Tema 12: Almacenamiento

Acuerdo:

Artículo 13. En el caso de servicios de Centros de Datos, las Instituciones, deberán observar lo siguiente:

II. Evaluar la conveniencia de contratar servicios de Centro de Datos, tomando en cuenta el beneficio económico, eficiencia, privacidad, seguridad de los datos y de la información, en comparación con la de utilizar un Centro de Datos propio o compartido con otra Institución;

VIII. En la contratación de servicios de hospedaje, gestión u operación de Centro de Datos, deberán asegurarse se establezca el acceso irrestricto a la información y datos propiedad de la Institución, durante la vigencia del mismo, así como la devolución de la información y datos al término del servicio.

Ley:

Artículo 3. XX. Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

Artículo 4. La presente Ley será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Artículo 81. En el tratamiento de datos personales, así como en el uso de las bases de datos para su almacenamiento, que realicen los sujetos obligados competentes de las instancias de seguridad, procuración y administración de justicia deberá cumplir con los principios establecidos en el Título Segundo de la presente Ley.

Análisis: El Acuerdo advierte la posibilidad de contratar Centro de Datos para beneficio económico, eficiencia, privacidad, seguridad de los datos y de la información y la Ley solo contempla de forma general atender medidas de seguridad.

Tema 13: Responsables de la información

Acuerdo:

Artículo 13. VII. Establecer la infraestructura y administración de la seguridad de la información en zonas de seguridad física y lógica, considerando identidad, perfiles y privilegios, incluyendo en éstas las necesarias para el personal involucrado, conforme a los controles de seguridad de la información que se definan atendiendo a lo previsto en el MAAGTICSI, y Artículo 13, fracción VII.

Ley:

Artículo 3. XXIII. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales; Artículo 3.

Análisis: Ambas normatividades prevén mecanismos y perfiles para el personal que tendrá acceso a la información.

Tema 14: Medidas de seguridad físicas

Acuerdo:

Artículo 15.- En las contrataciones relacionadas con servicios de plataformas de procesamiento de datos…

II. La administración e infraestructura esté clasificada en zonas de seguridad basadas en funciones, tipo de datos y requerimientos de acceso a los espacios de almacenamiento. Artículo 15, fracción II.

Ley:

Artículo 3. XXII. Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad; Artículo 3.

Análisis: El Acuerdo prevé el acceso a espacios de almacenamiento con relación a los servicios de procesamiento de datos y la Ley es más específica con respecto a las acciones a tomar.

Tema 15: Bases de datos

Acuerdo:

Artículo 16.- Las Instituciones, respecto de componentes de bases de datos, deberán observar lo siguiente:

III. Salvaguardar los derechos de la propiedad intelectual, portabilidad y recuperación de los datos generados y procesados de acuerdo al ciclo de vida de la información, incluyendo el borrado seguro. Artículo 16, fracción III.

Ley:

Artículo 81. En el tratamiento de datos personales, así como en el uso de las bases de datos para su almacenamiento, que realicen los sujetos obligados competentes de las instancias de seguridad, procuración y administración de justicia deberá cumplir con los principios establecidos en el Título Segundo de la presente Ley…

Artículo 82. Los responsables de las bases de datos a que se refiere este Capítulo, deberán establecer medidas de seguridad de nivel alto, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Análisis: El Acuerdo indica que, para las bases de datos, deberá observarse salvaguardar aspectos como recuperación de datos y borrado seguro, la Ley prevé principios para garantizar la integridad, disponibilidad y confidencialidad de la información.

Tema 16: Inventario

Acuerdo:

Artículo 16. I. Contar con el inventario institucional de bases de datos en las que se identifique cuáles tienen interacción con otras bases de datos.

Ley:

Artículo 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

III. Elaborar un inventario de datos personales y de los sistemas de tratamiento; Artículo 33.

Análisis: El Acuerdo establece un inventario de bases de datos, en las que se podrían comprender datos personales, mientras que la Ley prevé un inventario de los datos personales.

Tema 17: Plataformas

Acuerdo:

Artículo 19.- Las Instituciones, por lo que respecta a las plataformas digitales de páginas web, deberán observar lo siguiente:

VI. Cumplir con las disposiciones aplicables en materia de datos abiertos, protección de datos personales, seguridad de la información y derechos de autor.

Ley:

Artículo 30. Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:

VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.

Análisis: Ambas normatividades solo refieren dar cumplimiento a las obligaciones previstas en otro ordenamiento que resulte aplicable.

Tema 18: Seguridad Nacional

Acuerdo:

Artículo 28.- Las Instancias de Seguridad Nacional observarán las disposiciones siguientes:

I. La información relacionada con la seguridad nacional, generada o custodiada, que pretendan diseminar, deberá identificarse previamente, mediante la asignación de alguno de los niveles de diseminación que a continuación se indican:

a) "AAA": se asignará este nivel cuando se trate de información requerida para el proceso de decisiones políticas fundamentales, esto es, para la adopción de decisiones sobre riesgos y amenazas a la seguridad nacional, por parte del Presidente de la República, previa consideración del Consejo de Seguridad Nacional, cuya revelación no autorizada pueda dañar la integridad, estabilidad o permanencia del Estado mexicano;

b) “AA”: este nivel se asignará a la información resultante del ejercicio de atribuciones sustantivas, cuya revelación no autorizada pueda actualizar o potenciar un riesgo o amenaza a la seguridad nacional en términos de la Ley de la materia, o bien, comprometer su operación, las condiciones de seguridad de las instalaciones estratégicas o la integridad física de su personal, y

c) "A": se asignará este nivel a aquella información que derive del cumplimiento de las disposiciones jurídicas en materia de ejercicio del gasto, transparencia y rendición de cuentas, cuya revelación no autorizada pueda comprometer su operación, las condiciones de seguridad de las instalaciones estratégicas o la integridad física de su personal

Ley:

Artículo 6. El Estado garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente.

El derecho a la protección de los datos personales solamente se limitará por razones de seguridad nacional, en términos de la Ley en la materia, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Artículo 80. La obtención y tratamiento de datos personales, en términos de lo que dispone esta Ley, por parte de los sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en las bases de datos establecidas para tal efecto.

Las autoridades que accedan y almacenen los datos personales que se recaben por los particulares en cumplimiento de las disposiciones legales correspondientes, deberán cumplir con las disposiciones señaladas en el presente Capítulo.

Análisis: Ambas normatividades contemplan la Seguridad Nacional, solo que el Acuerdo lo encamina a niveles de diseminación.

Capítulo 4

Propuesta de procesos básicos que permite el cumplimiento del MAAGTICSI y la Ley General

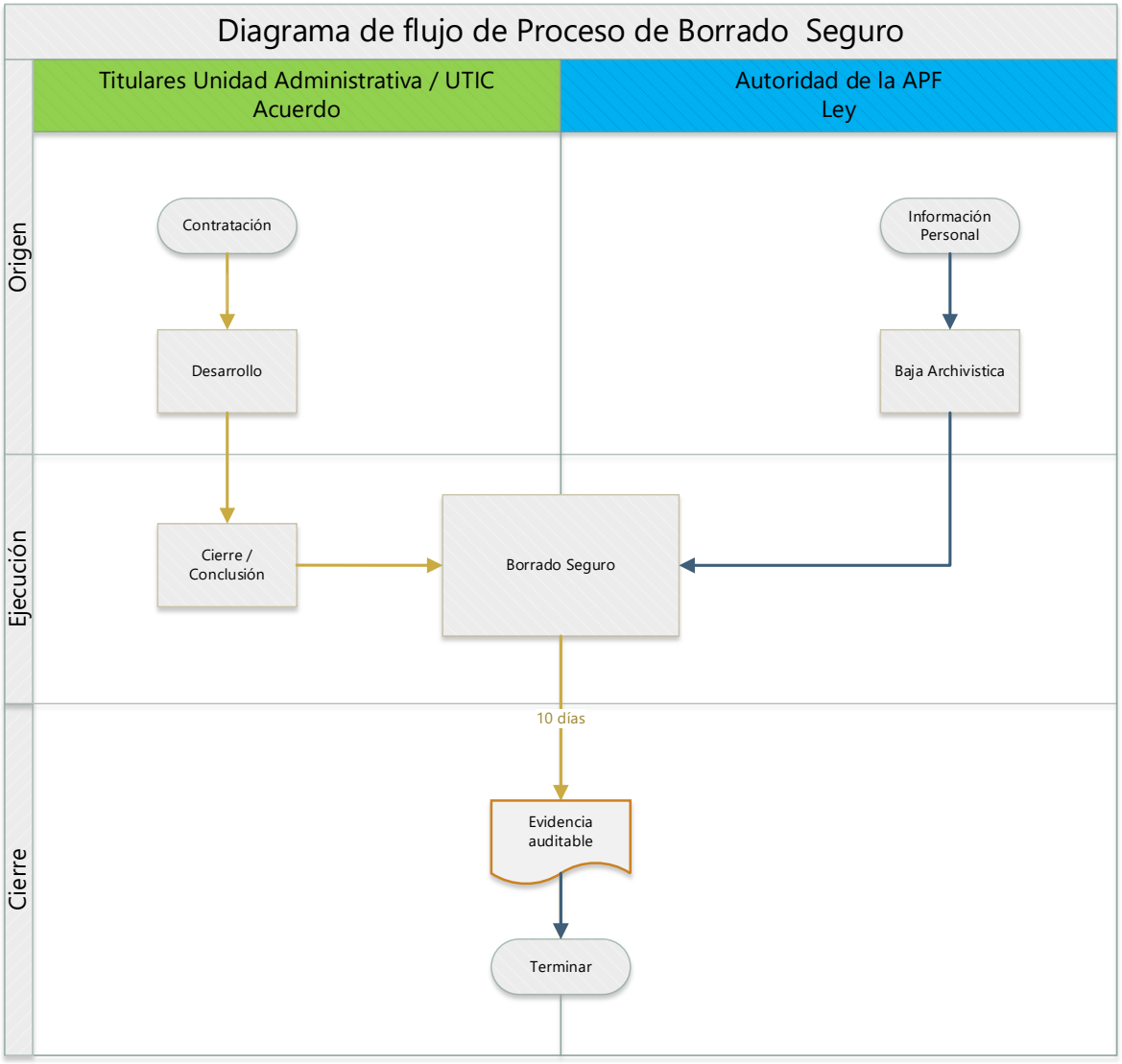
Capítulo 4. Propuesta de procesos básicos que permite el cumplimiento del MAAGTICSI y la Ley General.

4.1 Diagramas de flujo en el que convergen el MAAGTICSI y la Ley General.

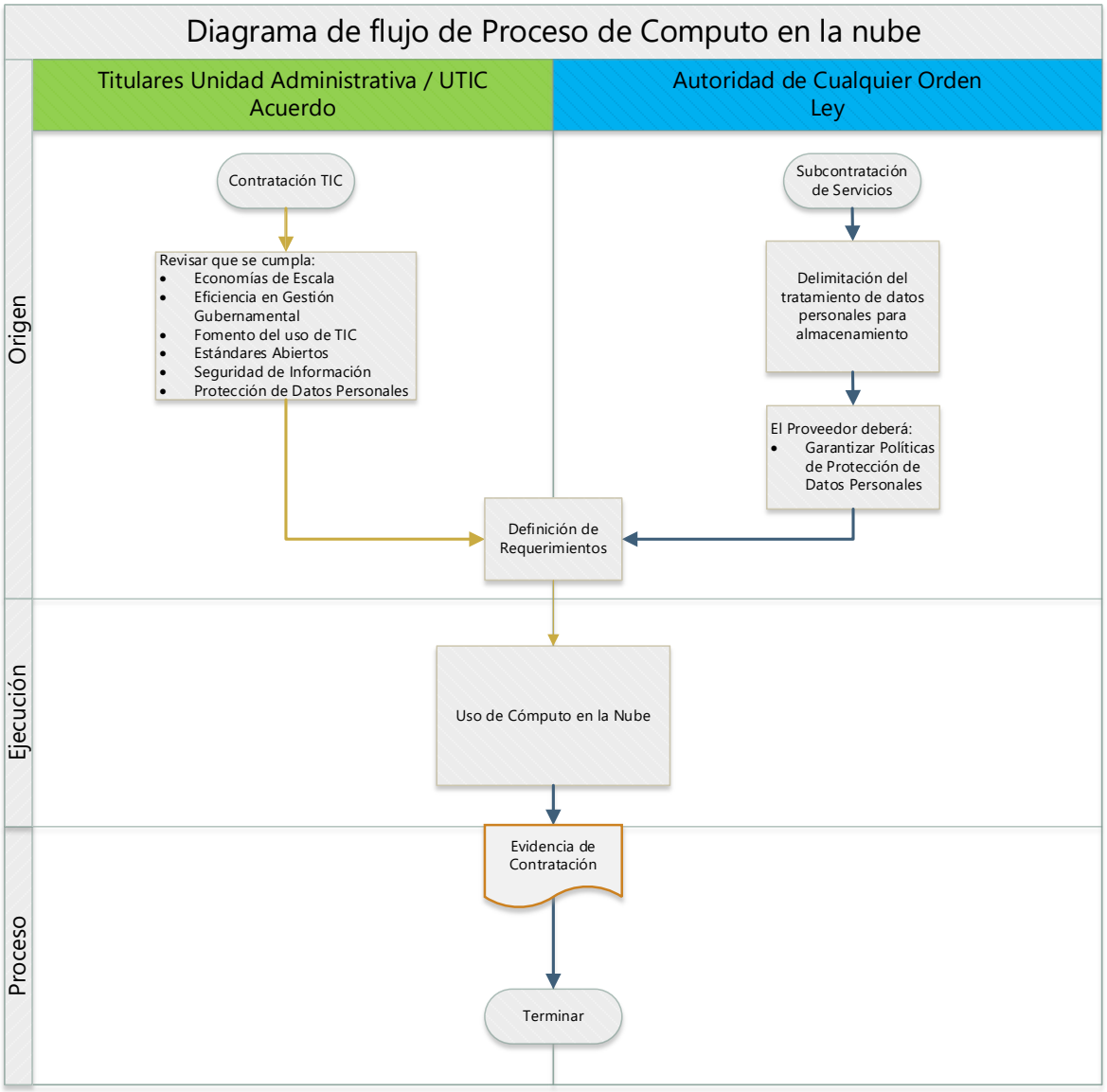
La presente propuesta tiene como finalidad, que los Servidores Públicos que conforman la APF, den cumplimiento a la normativa estipulada en el MAAGTICSI y la Ley General, logrando con ello una eficiencia, reducción y simplificación en los procesos establecidos en las normativas mencionadas, toda vez que del análisis elaborado en el capítulo anterior se detectó que existen actividades que conjuntando las similitudes entre ambas normativas se puede dar cumplimiento a las mismas.

Por lo anterior y con el propósito de que dicha propuesta sea más gráfica y de fácil seguimiento para los Servidores Públicos que conforman la APF, quisimos expresar mediante flujos diagramados en los cuales se expresara la diferencia de cada una de las normas y en qué momento en donde confluyen las similitudes del MAAGTICSI y la LEY GENERAL.

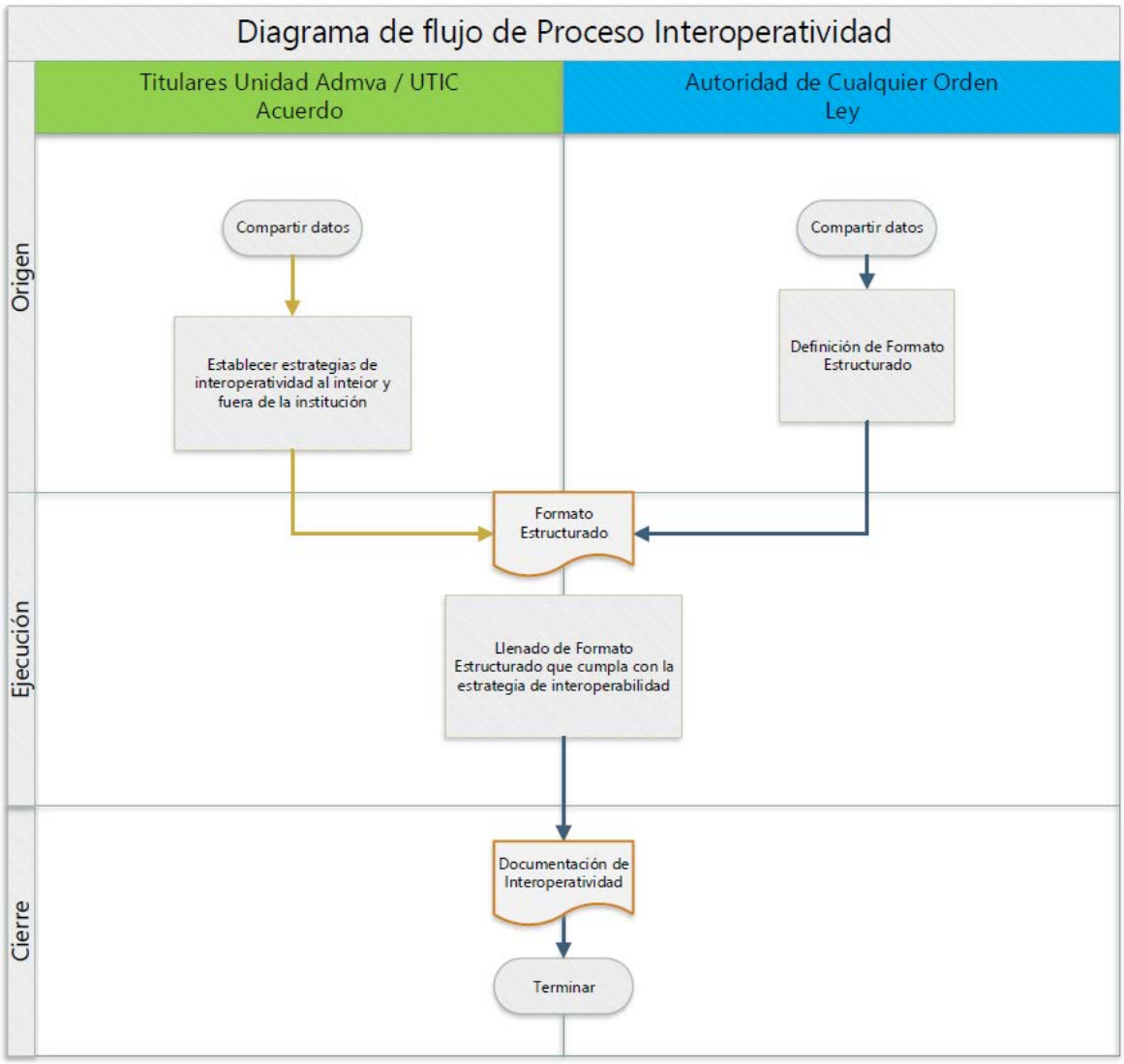
1. Diagrama de flujo de Proceso de Borrado Seguro



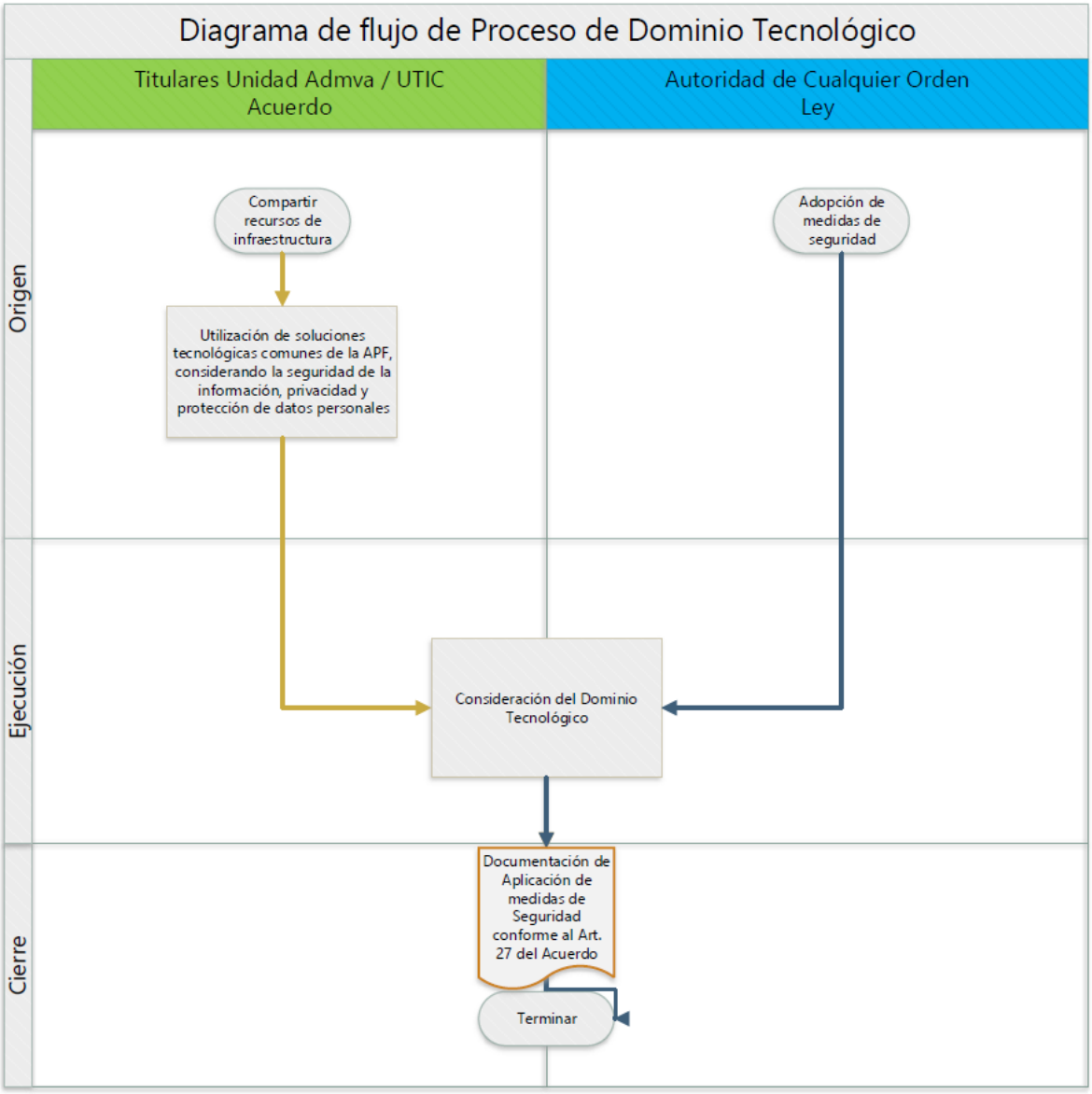
2. Diagrama de flujo de Proceso de Computo en la Nube



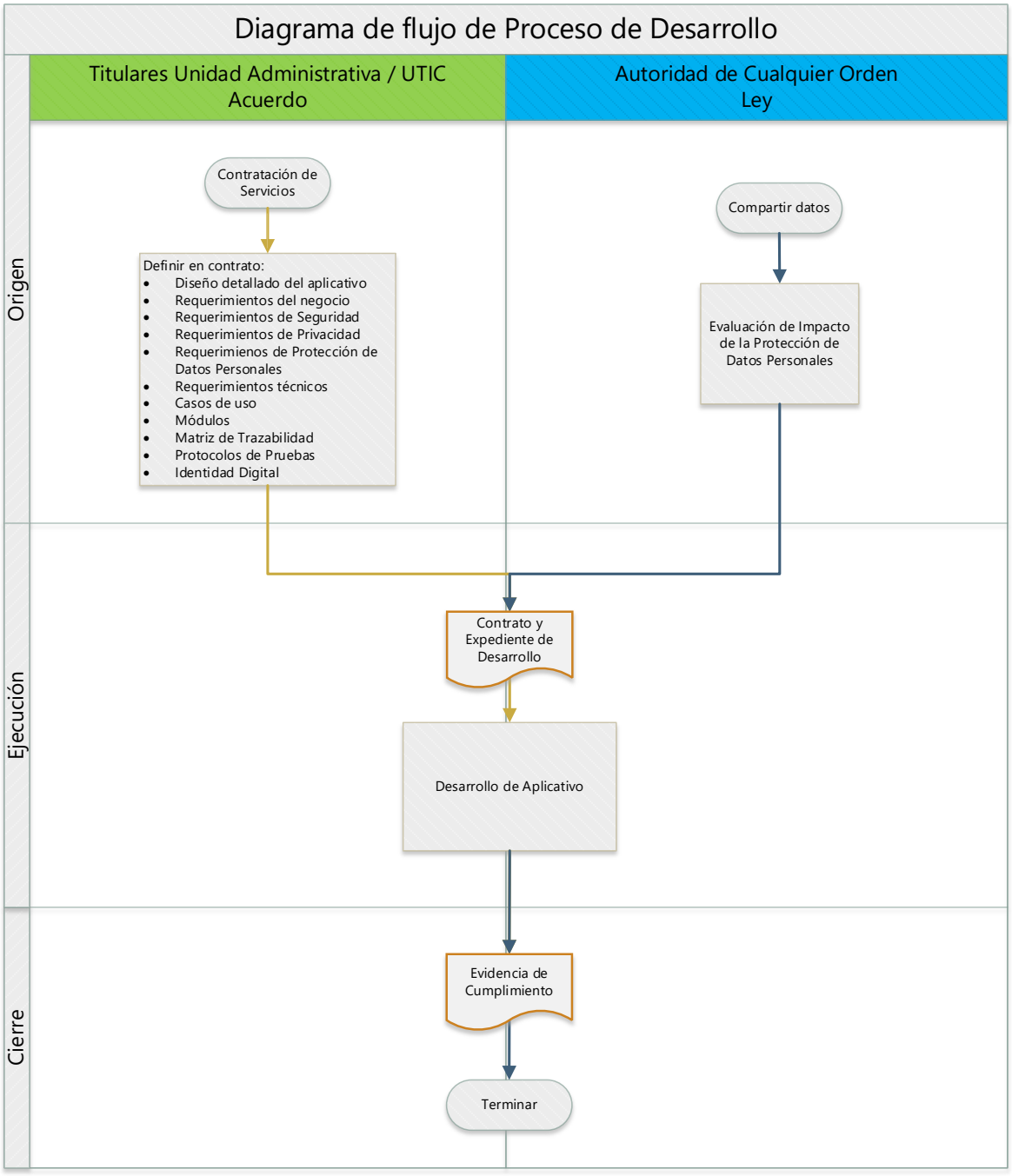
3. Diagrama de flujo de Proceso de Interoperabilidad



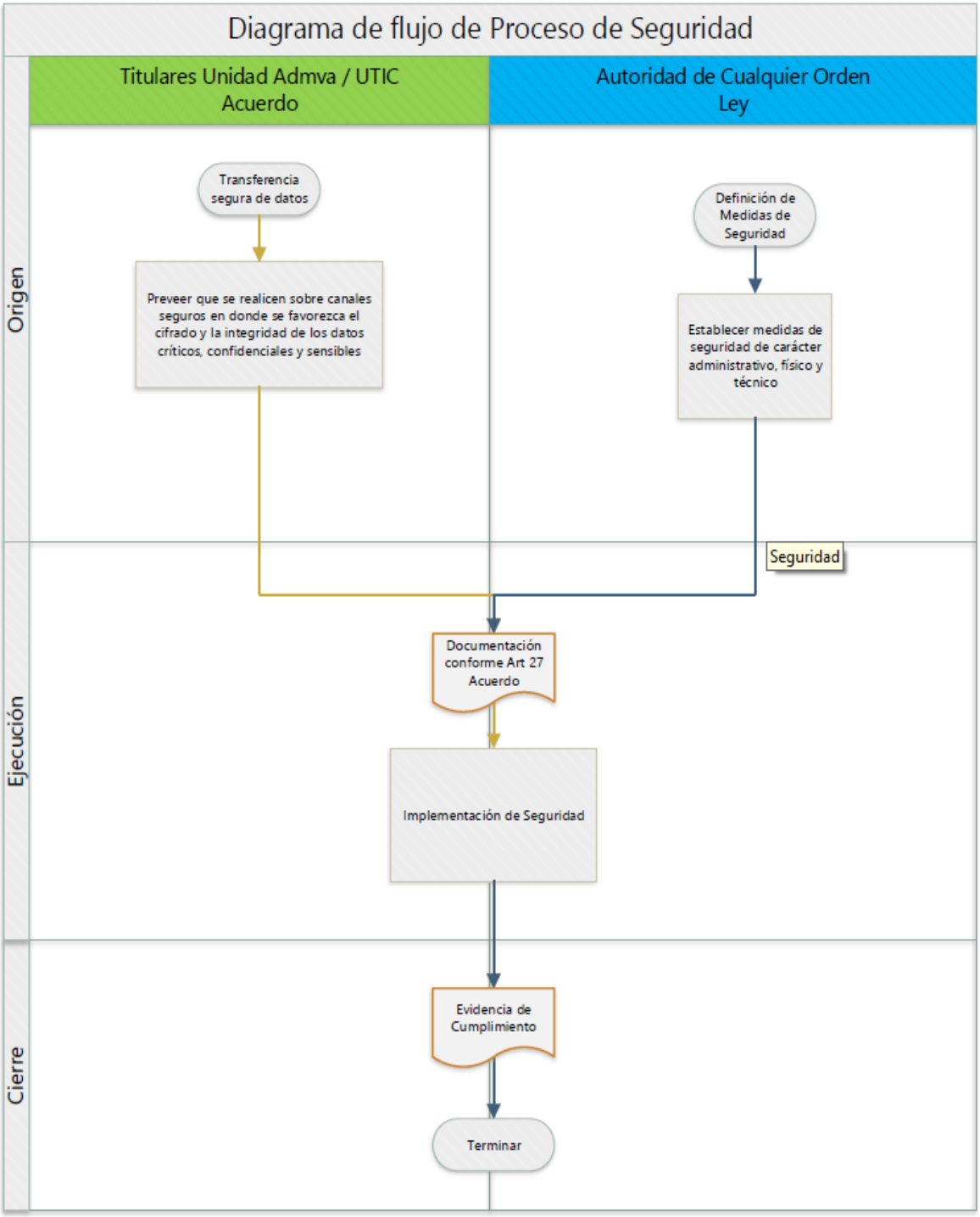
4. Diagrama de flujo de Proceso de Dominio Tecnológico



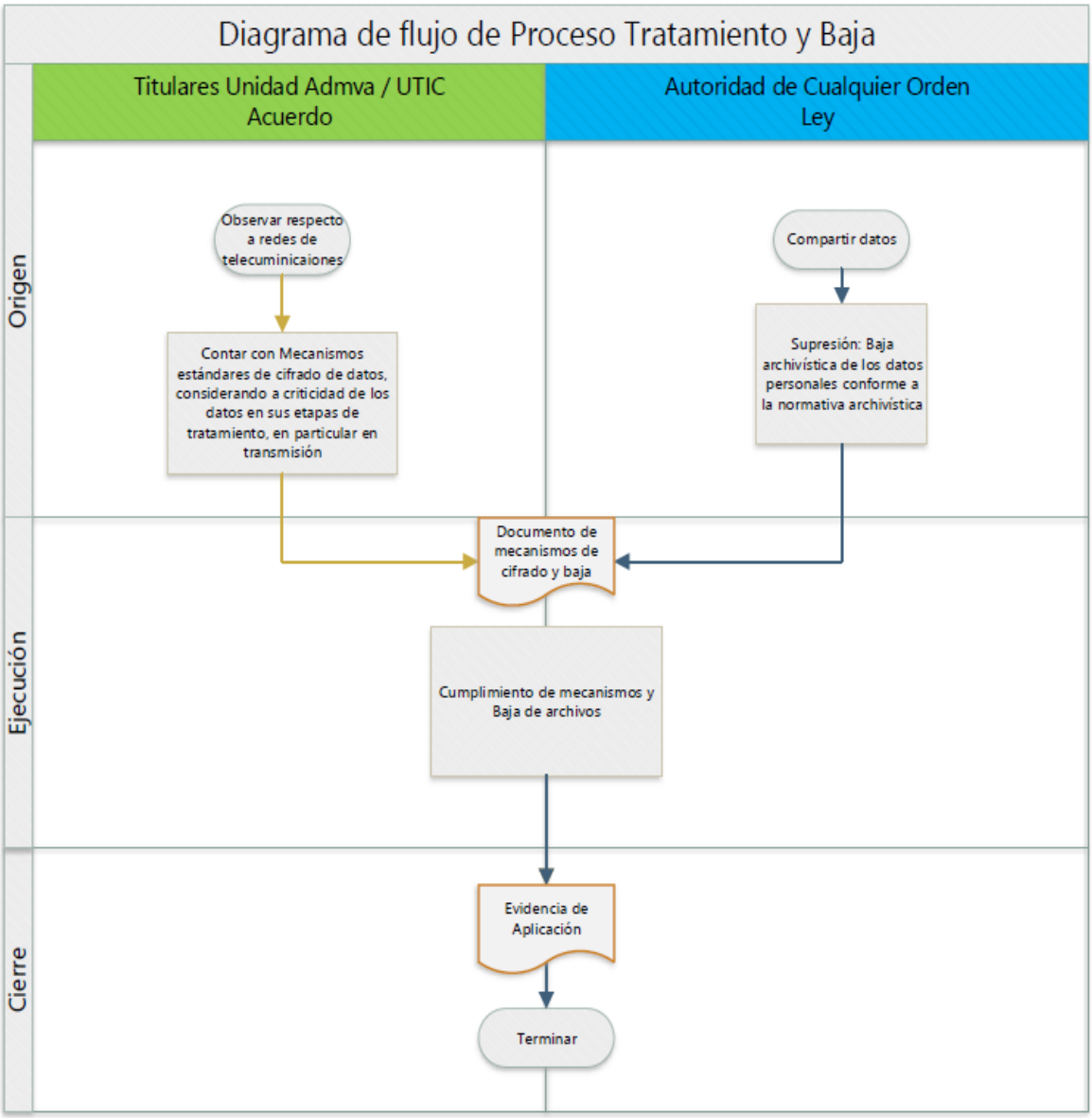
5. Diagrama de flujo de Proceso de Desarrollo



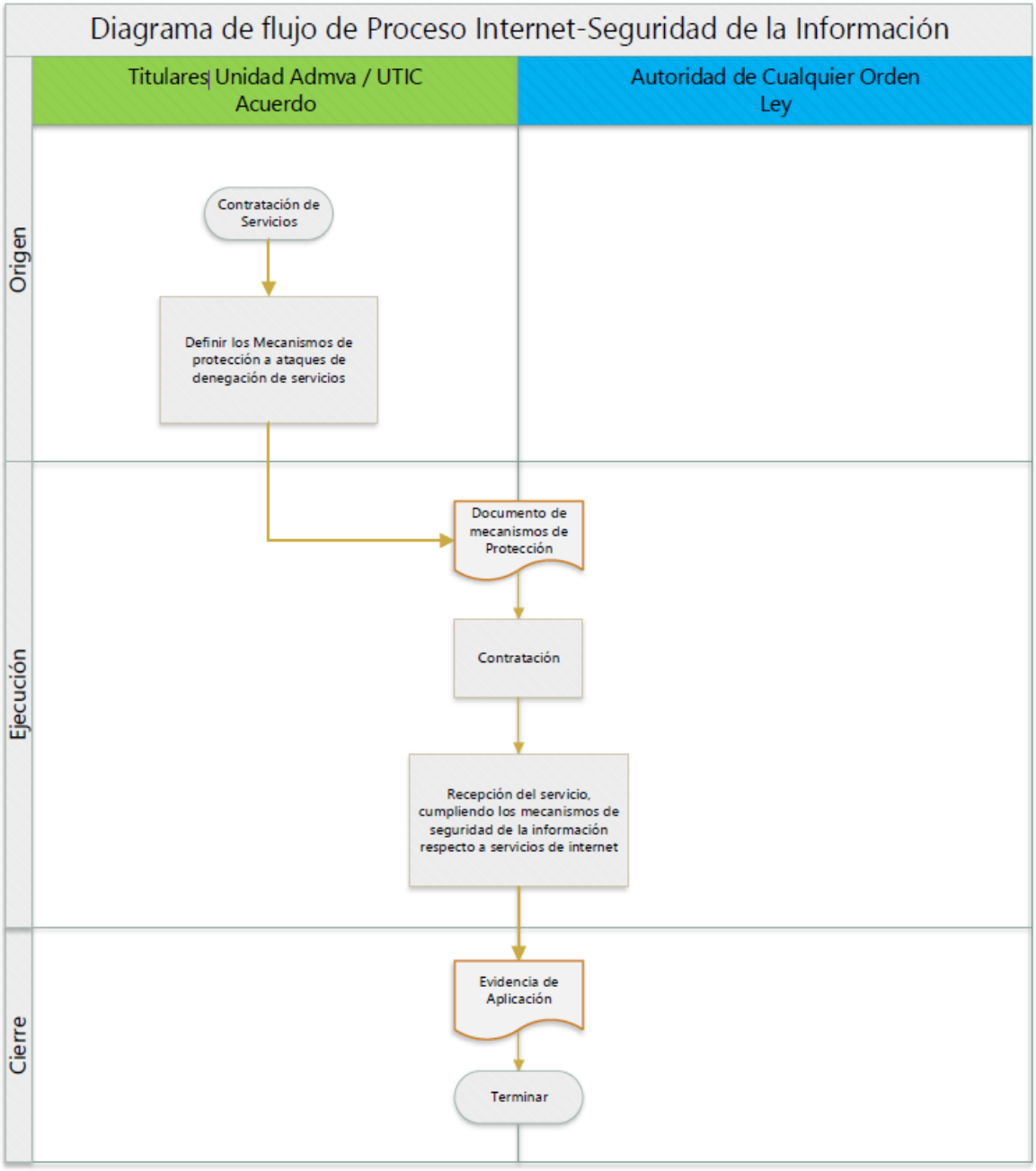
6. Diagrama de flujo de Proceso de Seguridad



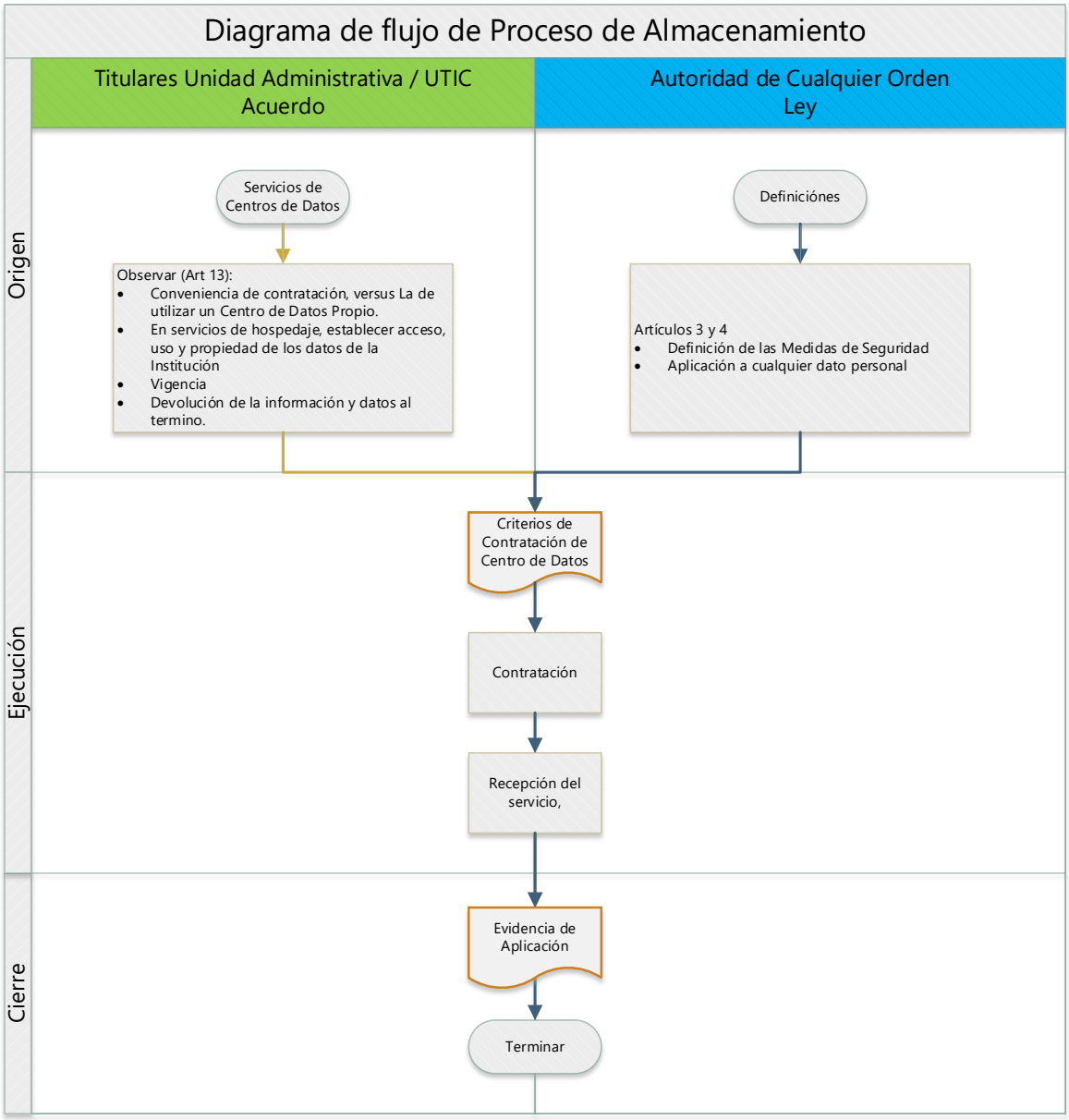
7. Diagrama de flujo de Proceso Tratamiento y Baja



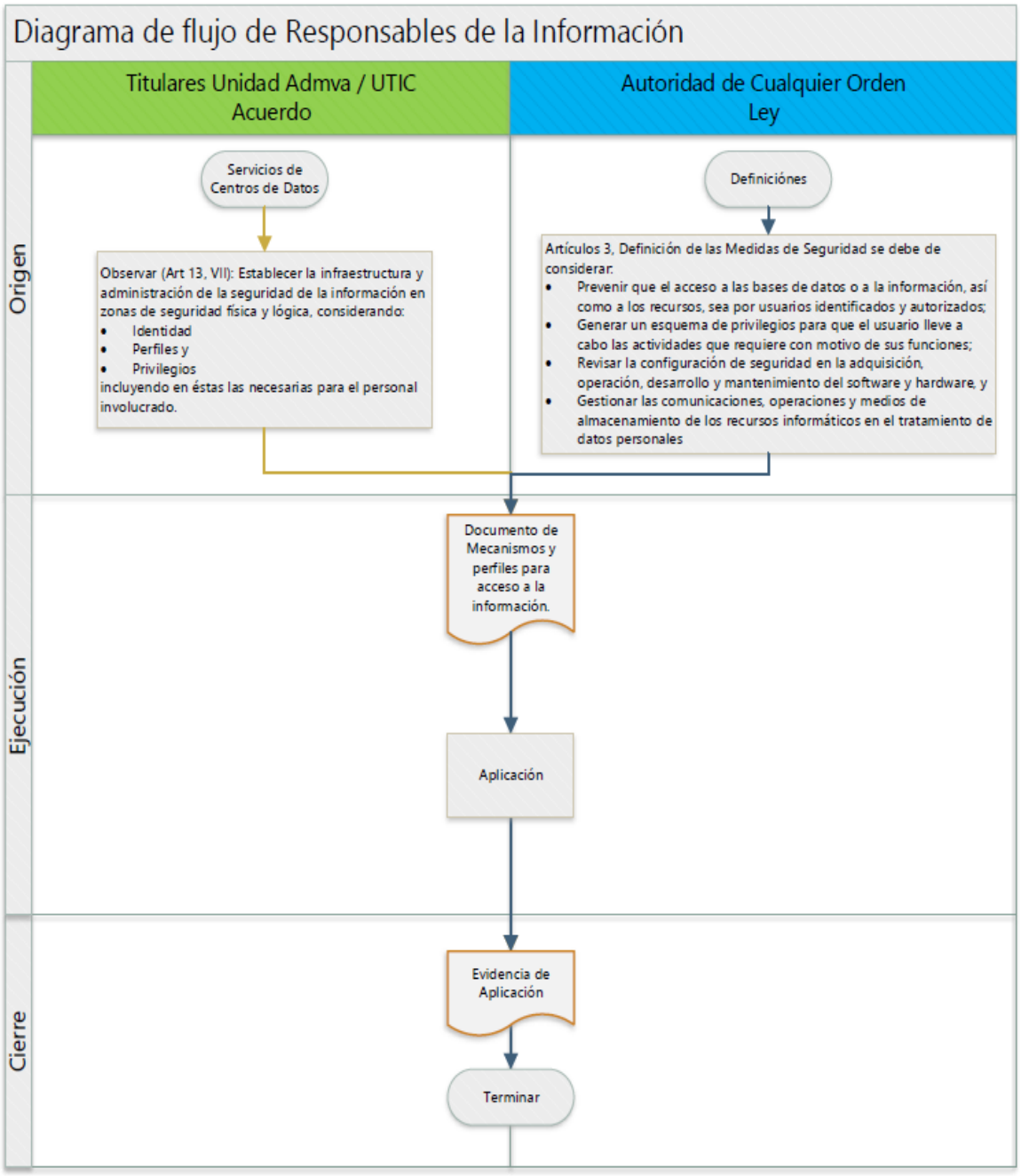
8. Diagrama de flujo de Proceso Internet-Seguridad de la Información



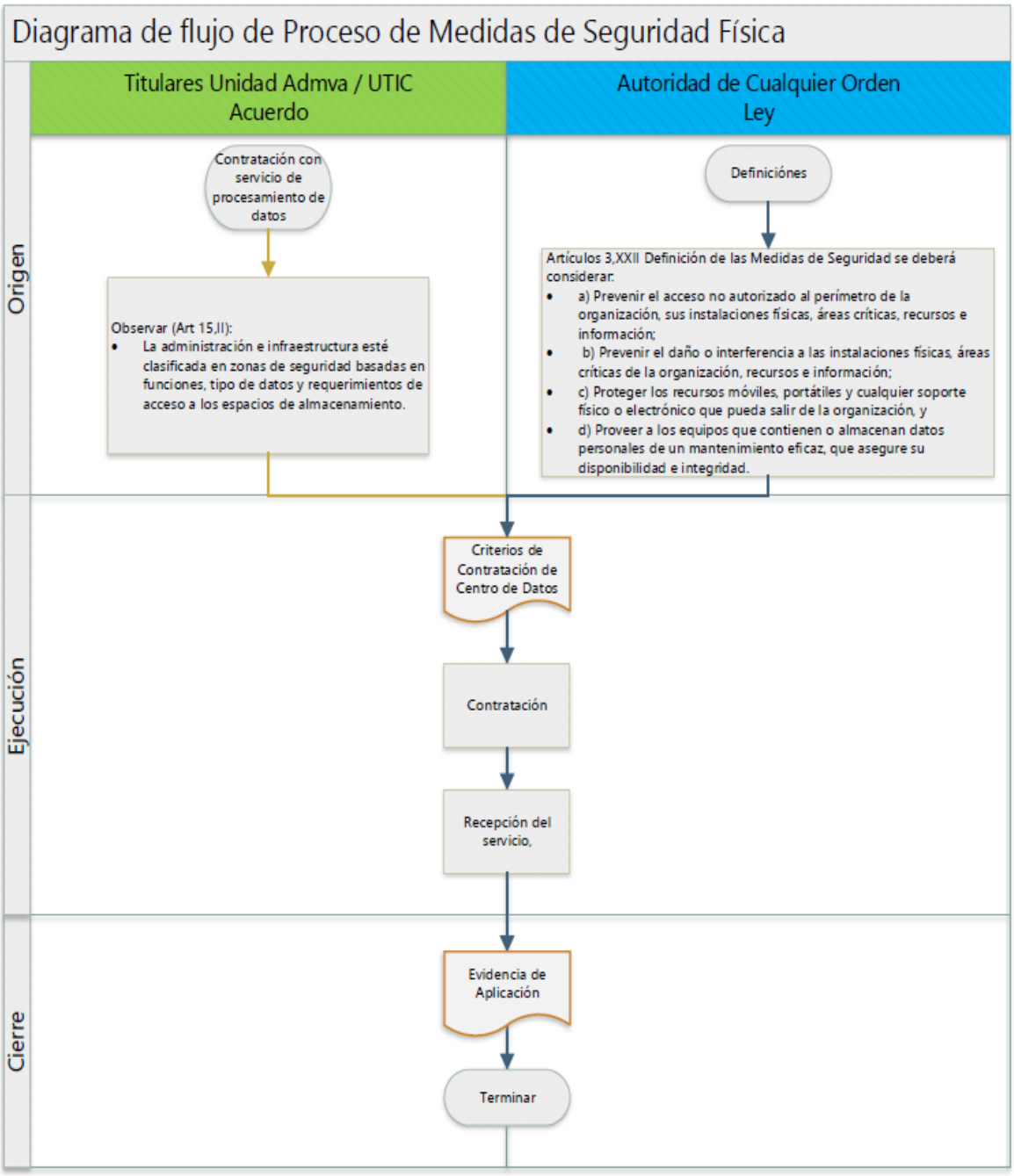
9. Diagrama de flujo de Proceso de almacenamiento



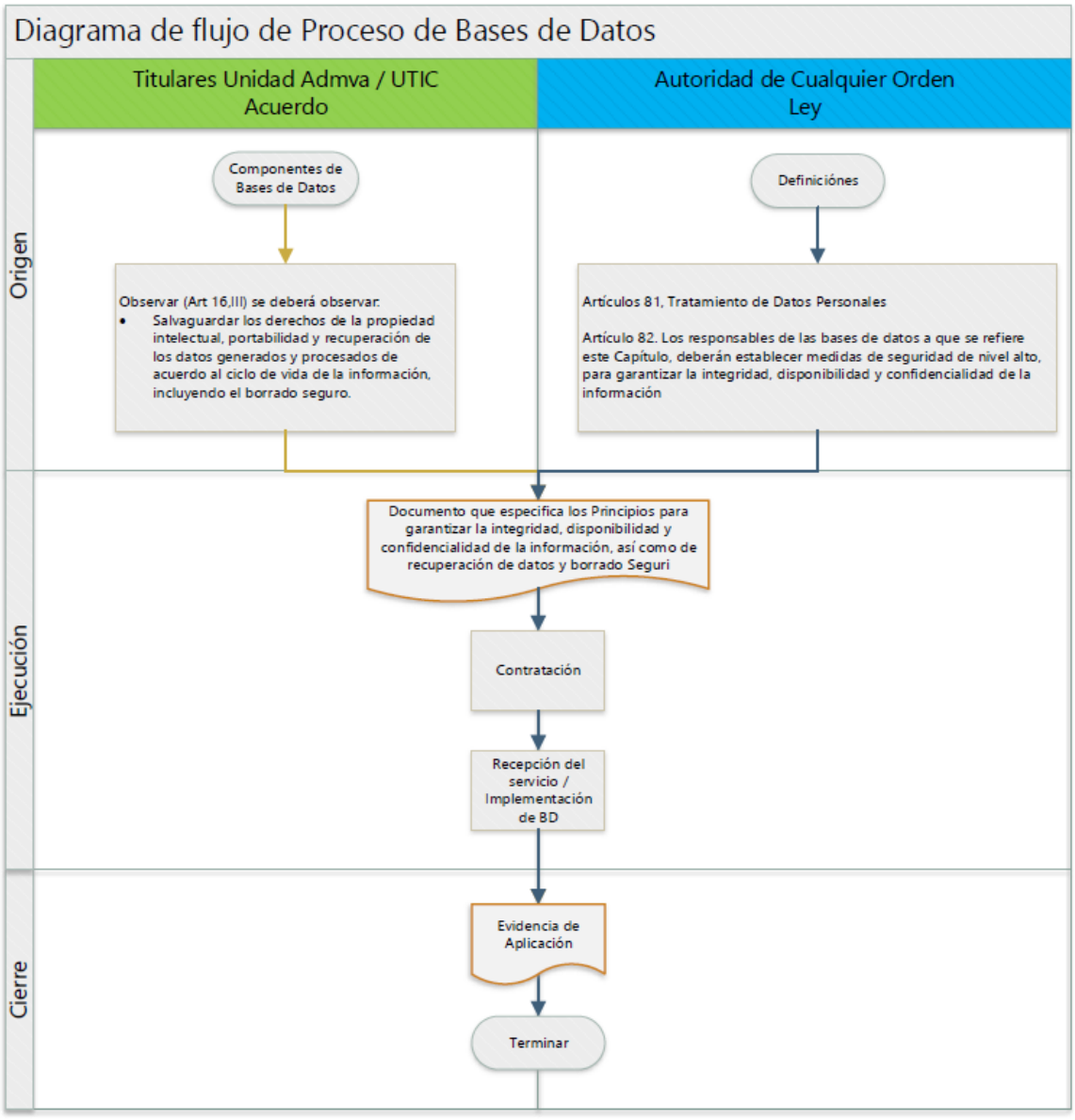
10. Diagrama de flujo de responsables de la información



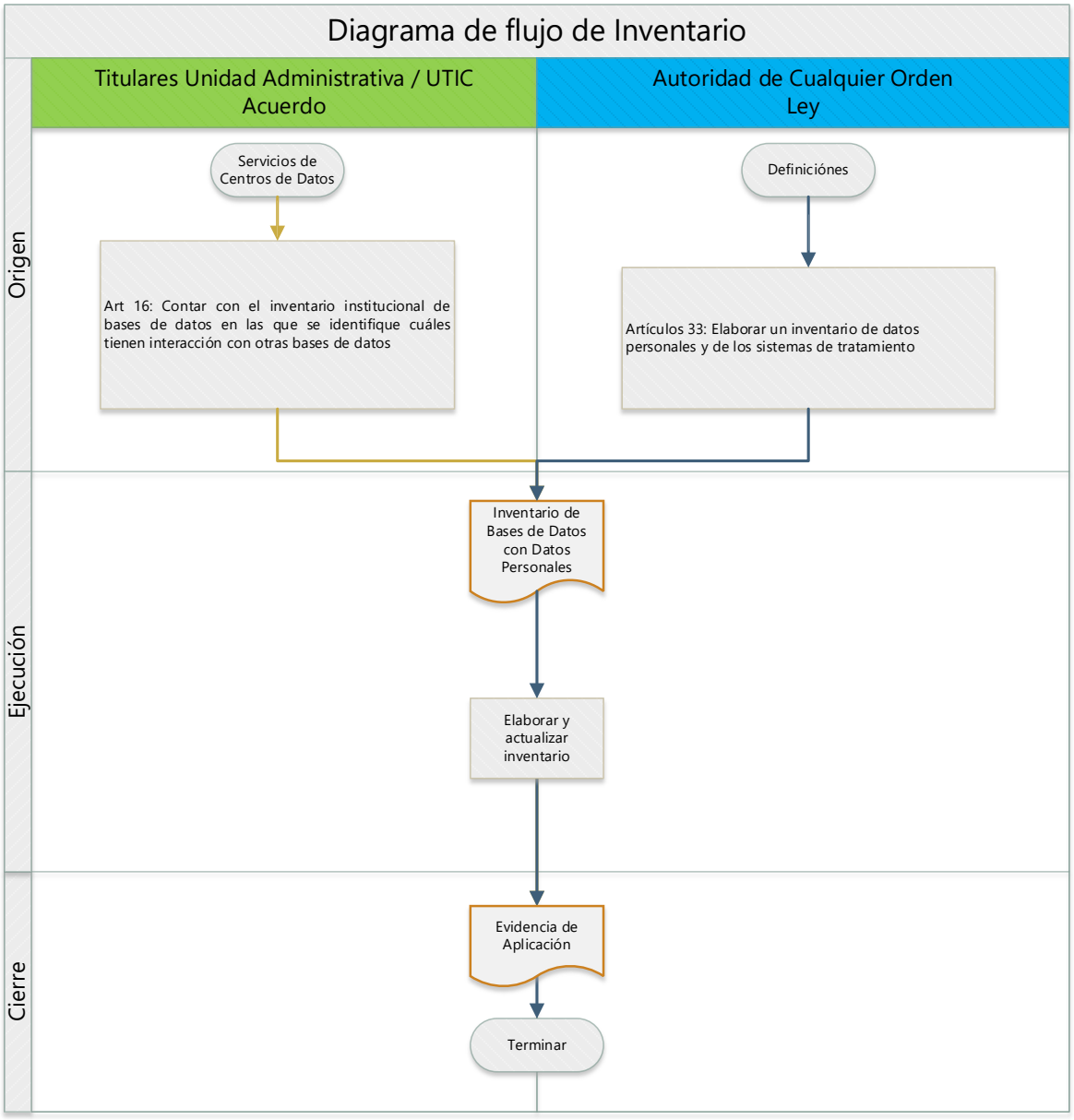
11. Diagrama de flujo de Proceso de Medidas de seguridad física



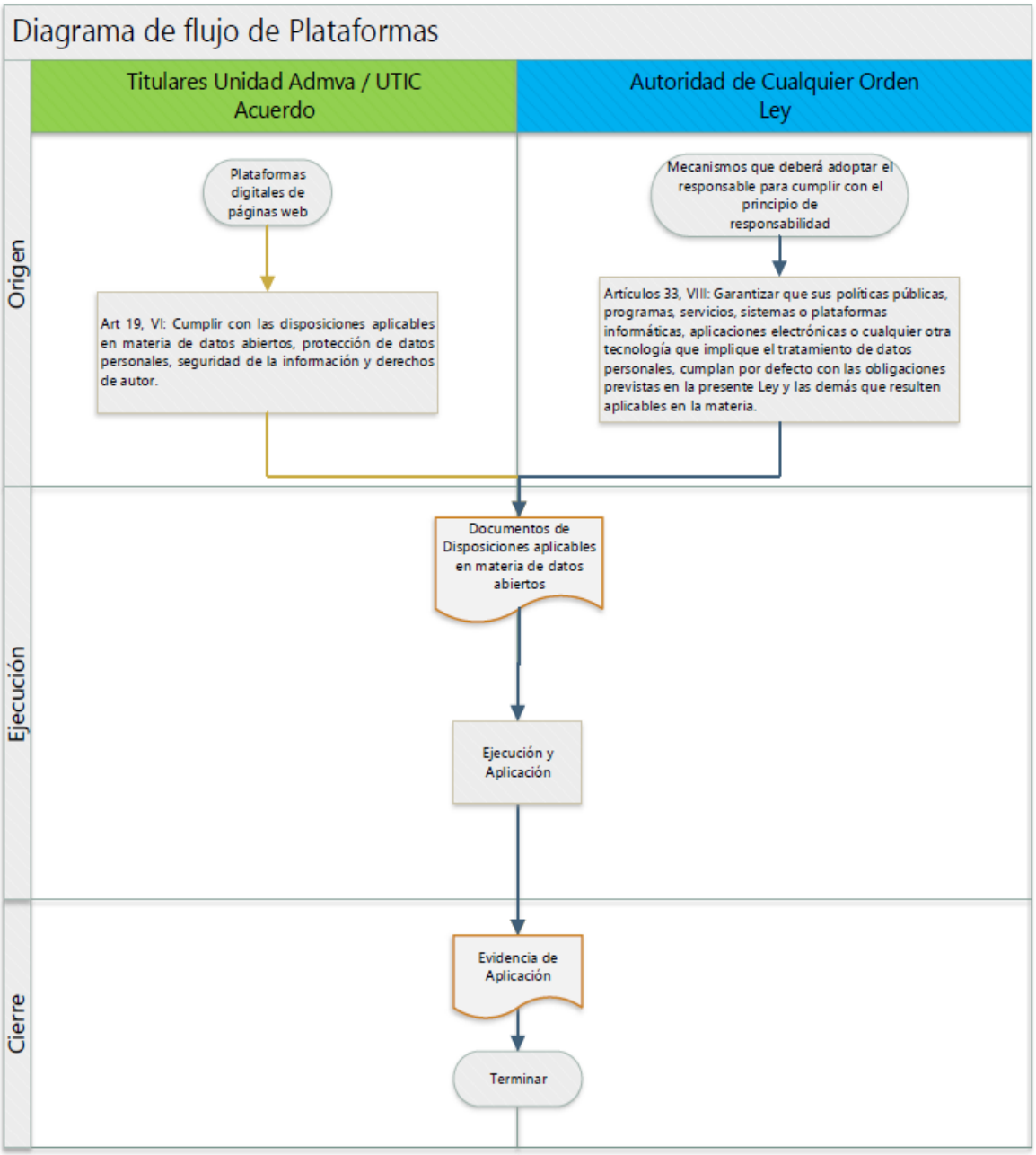
12. Diagrama de flujo de Proceso de Bases de Datos



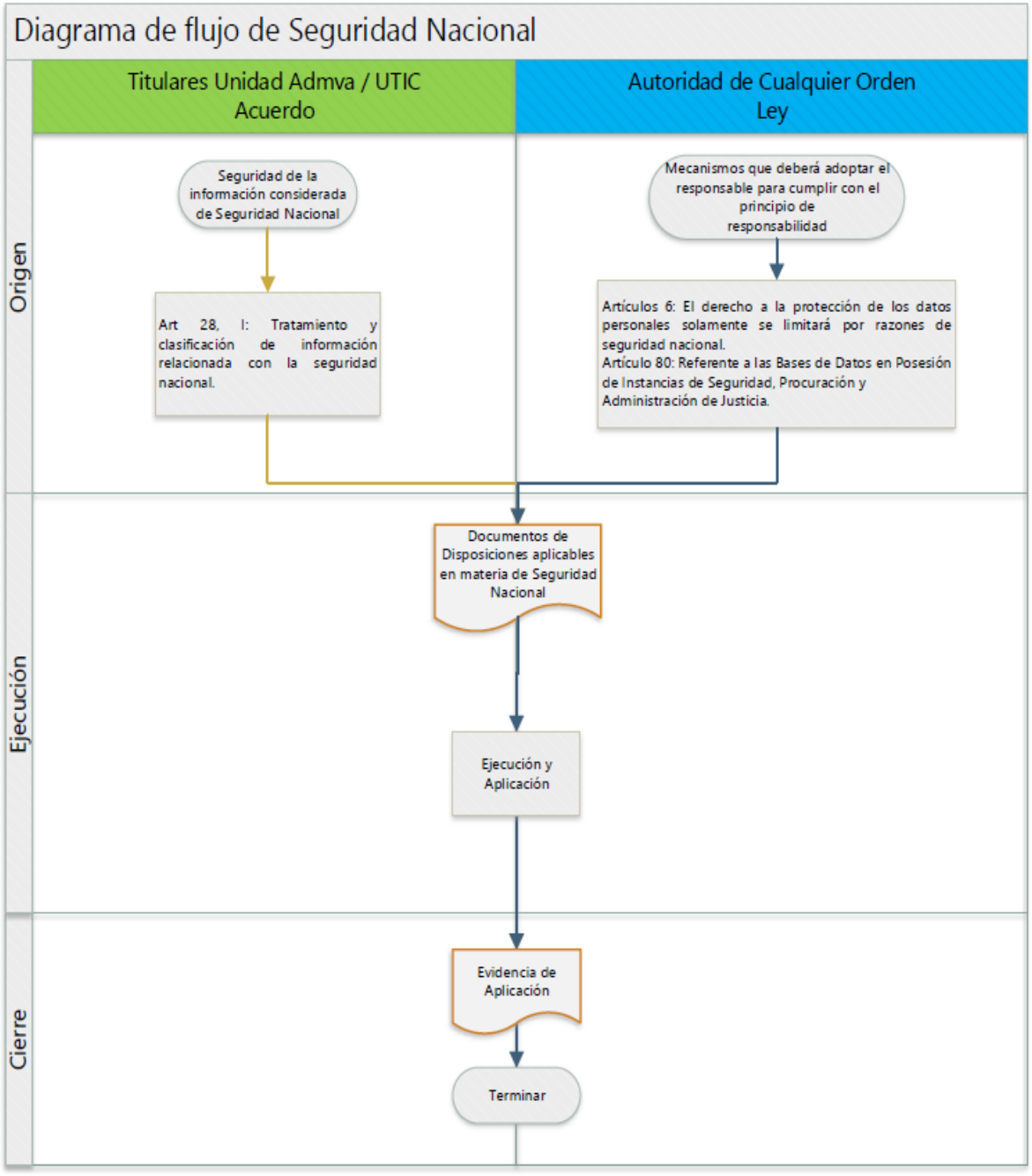
13. Diagrama de Flujo de Inventario



14. Diagrama de flujo de plataformas



15. Diagrama de flujo de seguridad nacional



Conclusiones

A lo largo del trabajo de investigación hemos expuesto la importancia de los datos personales en la gestión de la APF, al mismo tiempo que resaltamos la importancia de contar con un marco normativo que busque asegurar los datos personales que son uno de los activos más importantes, la finalidad de alinear los procesos de ASI de MAAGTICSI con los deberes de la Ley es que con los mismos procesos operativos se dé cumplimiento a estos dos instrumentos vinculantes.

En los tiempos actuales donde la constante evolución tecnológica es un parámetro que nos marca la pauta, es importante seguir adecuando los marcos jurídicos que por un lado busquen dar certeza y garantizar derechos a los ciudadanos a la protección de sus datos personales, pero al mismo tiempo sean lo suficientemente flexibles para adecuarse y no bloquear la innovación tecnológica e incentivar la economía.

Por otro lado, consideramos que uno de los grandes problemas en cualquier gestión de la administración pública es la falta de presupuesto para el cumplimiento de diversas normativas, por ello con este trabajo identificamos y proponemos una solución para economizar los recursos presupuestales, humanos y operacionales, a fin de cumplir con lo establecido en estos dos ordenamientos legales.

De acuerdo con la similitud que presentan ambas normas señaladas y contrastadas en los Capítulo 3 y 4, si bien una está a nivel de Ley y otra es un Manual, lo que jurídicamente y jerárquicamente es indiscutible que se debe dar cumplimiento a la primera, es de importancia resaltar que el MAAGTICSI, se viene implementando en la APF, desde el año 2010, que fue donde se dio la llamada tala regulatoria, incluida en un Acuerdo publicado en el DOF el 10 de agosto de 2010, el cual señalaba que las dependencias y entidades, se deberían abstener de emitir regulación adicional a las disposiciones, políticas o estrategias, acciones o criterios y procedimientos expedidos por la SFP.

Dentro de la presente investigación se evidenciaron las similitudes y puntos de coincidencia entre ambas normatividades, por tal motivo se establecieron los

diagramas mostrados en el capítulo cuarto, en los cuales se exhibe de manera gráfica como serían los procesos más eficientes para dar cumplimiento a dichos ordenamientos legales, simplificando su aplicación en la APF, ayudando con ello a que los Servidores Públicos, encargados de estas labores.

Asimismo, en los capítulos anteriores, se evidenció que al simplificar procesos se realiza un resguardo conveniente de los datos personales que se utilizan en la APF.

Como se abordó en el capítulo segundo, con el paso de los años el Gobierno Mexicano ha utilizado la tecnología a fin de tener almacenada información de cada ciudadano, es decir, desde que se nace se lleva un control del registro de cada integrante de la sociedad, información de salud a través del expediente clínico (el cual no se encuentra funcionando actualmente pero es la tendencia[44]) , información de nivel de educación por medio de la cedula profesional, entre otros, sin embargo, el tratamiento de esta información no había sido regulada. Con la promulgación de la Ley General se han normado los procesos a fin de asegurar la información en posesión de sujetos obligados.

El MAAGTICSI, prevé el cuidado de las Instituciones de la APF y las medidas que debe tomar estas para resguardar las infraestructuras, lo cual, en combinación con la Ley, permitirá darle certeza a los Servidores Públicos y a los ciudadanos de que su información está siendo protegida y resguardada, bajo mecanismos que garantizan su confidencialidad, integridad y disponibilidad.

Asimismo, la Ley en su artículo 70, prevé que exista interoperabilidad[45] entre los sistemas informáticos y bases de datos, entre las dependencias y entidades, pretendiendo con ello facilitar los trámites que los ciudadanos realicen con el gobierno; comunicarse las diversas instituciones hacia adentro, compartiendo información que ya fue solicitada previamente al ciudadano o con la que ya cuenta

[44]Manual del Expediente clínico electrónico. Consultado en http://www.who.int/goe/policies/countries/mex_ehealth.pdf el 09 de abril de 2018

[45] Consultado en https://www.gob.mx/interoperabilidad el día 10 de marzo de 2018

el gobierno, con la intención que a través del aprovechamiento de las tecnologías de información y comunicaciones, esto se pueda realizar, y a través del MAAGTICSI, que estos se den a través de canales seguros, con esto se pretende hacer más fácil la vida de los ciudadanos y no estar pidiendo como gobierno información que en realidad ya cuenta con ella. Por lo anteriormente expuesto, se concluye que la propuesta presentada se enfoca principalmente en el ámbito tecnológico y legal, toda vez que los procesos evidenciados están enfocados a la seguridad de la información dentro de la infraestructura tecnológica en las dependencias y entidades de la APF, lo cual permite cumplir, a su vez, con los elementos normativos que estipula la Ley.

Fuentes consultadas

Páginas Web

- ✓ Página Definición,DE consultado en https://definicion.de/modelo-de-gestion/ el 10 de diciembre de 2017.

- ✓ Tala regulatoria, Página de la Secretaría de la Función Pública consultada en http://2006-2012.funcionpublica.gob.mx/index.php/unidades-administrativas/ssfp/mejor-gobierno/tala.html el 11 de diciembre de 2017.

- ✓ Plan Nacional de Desarrollo. Estado de Derecho y Seguridad. Confianza en las Instituciones Públicas. Estrategia 10.3 Reducir los trámites burocráticos con la finalidad de abatir la discrecionalidad. Consultado en http://pnd.calderon.presidencia.gob.mx/index.php?page=confianza-en-las-instituciones-publicas el 11 de diciembre de 2017.

- ✓ Programa Especial de Mejora de la Gestión en la Administración Pública Federal 2008-2012, consultado en dof.gob.mx/nota_to_doc.php?codnota=5059570 el 12 de diciembre de 2017.

- ✓ Diario Oficial de la Federación. 13 de julio de 2010. Consultado en http://dof.gob.mx/nota_detalle.php?codigo=5151475&fecha=13/07/2010 el 12 de diciembre de 2017.

- ✓ Diario Oficial de la Federación. Consultado en http://dof.gob.mx/nota_detalle_popup.php?codigo=5106082 el 13 de diciembre de 2017.

- ✓ Diario Oficial de la Federación consultado en http://dof.gob.mx/nota_detalle.php?codigo=5151475&fecha=13/07/2010 el 10 de diciembre de 2017

- ✓ Plan Nacional de Desarrollo 2013-2018. Consultado en http://pnd.gob.mx/ el 14 de diciembre de 2017.

- ✓ Diario Oficial de la Federación. Consultado en http://www.dof.gob.mx/nota_detalle.php?codigo=5312420&fecha=30/08/2013 el 14 de diciembre de 2017.

- ✓ Decreto que establece las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal. Consultado en https://www.gob.mx/cms/uploads/attachment/file/143509/DECRETO_que_establece_las_medidas_para_el_uso_eficiente.pdf el 14 de diciembre de 2017.

- ✓ Diario Oficial de la Federación. Consultado en http://www.dof.gob.mx/nota_detalle.php?codigo=5343881&fecha=08/05/2014 el 14 de diciembre de 2017.

- ✓ Diario Oficial de la Federación. Consultado en http://dof.gob.mx/nota_detalle.php?codigo=5424367&fecha=04/02/2016 el 18 de diciembre de 2017.

- ✓ Interopera MX consultado enhttps://www.gob.mx/interoperabilidad el día 10 de marzo de 2018

- ✓ Declaración Universal de los Derechos Humanos, consultado en http://www.un.org/es/documents/udhr/history.shtml

- ✓ Carta de los Derechos Fundamentales de la Unión Europea, consultado en http://www.europarl.europa.eu/charter/pdf/text_es.pdf

Libros

- ✓ TENORIO Cueto, Guillermo A, Los datos personales en México, Perspectivas y retos de su manejo en posesión de particulares, 1ª ed., México, Porrúa-UP, 2012

- ✓ TÉLLEZ Carbajal, Evelyn, et al., Derecho y TIC Vertientes Actuales, Instituto de Investigaciones Jurídicas, 2016

- ✓ ORNELAS Lina, "La recepción del derecho a la protección de datos en México: breve descripción de su origen y estatus legislativo", Protección de Datos Personales, 2013.

- ✓ PIÑAR Mañas José L., et al., La protección de Datos Personales en México, 1ª ed., Tirant lo Blanch México, México, 2013

- ✓ PESCHARD Mariscal Jacqueline, 2013, "El Derecho Fundamental a la Protección de Datos Personales en México", Tirant Lo Blanch eds, La Protección de Datos Personales en México.

- ✓ GIL Elena, "Big Data, privacidad y protección de datos", 1ª ed., Agencia Española de Protección de Datos, 2016, España.

- ✓ GERALDES Da Cunha Lopes Teresa M., Las recientes reformas en materia de protección de datos personales en México. Centro de Investigaciones Jurídicas y Sociales Universidad Michoacana de San Nicolás de Hidalgo.

Morelia, México.

- ✓ Compendio de Lectura y Legislación, Protección de Datos Personales, Tiro Corto Editores, México 2010

Normatividad

- ✓ Constitución Política de los Estados Unidos Mexicanos
- ✓ Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 2014, México
- ✓ Lineamientos de Protección de Datos Personales, 2005, México, IFAI
- ✓ Diario Oficial de la Federación (DOF)
- ✓ Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2010, México, Cámara de Diputados del H. Congreso de la Unión
- ✓ Reforma al artículo 6 constitucional que establece el acceso a la información pública como un derecho fundamental de los mexicanos, IFAI, 2007
- ✓ Ley de Protección de Datos Personales en Posesión de Particulares.
- ✓ Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017, México.
- ✓ Anuario Jurídico y Económico Escurialense, XLIV (2011) 317-334 / ISSN: 1133-3677
- ✓ Implicaciones de una Ley general en materia de protección de datos personales publicada en el Diario Oficial de la Federación (DOF) el 5 de julio de 2010. Para mayor información consultado en http://dof.gob.mx/nota_detalle.php?codigo=5150631&fe cha=05/07/2010 el 2 de diciembre de 2017.
- ✓ Recomendaciones en materia de seguridad de protección de datos personales
- ✓ Estándares Internacionales sobre Protección de Datos Personales y Privacidad – Resolución de Madrid
- ✓ R3D (México), Análisis Normativo Protección de Datos Personales en México

- ✓ Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información: Hacia una Cultura de Seguridad

- ✓ Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones de Seguridad de la Información