MDTIC

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

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

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

"MANUAL PREVIO DE IMPLEMENTACIÓN Y COMPLEMENTACIÓN DE ESTANDARIZACIÓN DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES"

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

Presenta:

Miryam Eréndira López Rivera

Asesora:

Dra. Verónica Cortés Méndez

Ciudad de México, septiembre, 2022.

CONACYT

INFOTEC POSGRADOS

Autorización de impresión

INFOTEC
POSGRADOS

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

Maestría en Derecho de las Tecnologías de Información y Comunicación, MDTIC

Ciudad de México, 30 de agosto de 2022.

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

"Manual previo de implementación y complementación de estandarización de ciberseguridad para la protección de datos personales"

Desarrollado por la alumna: **Miryam Eréndira López Rivera** y bajo la asesoría de la Dra. Verónica Cortés Méndez cumple con el formato de Biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

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

Vo. Bo.

Lic. Juan Ramón Abarca Damián
Coordinador de Biblioteca

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

C.p.p.- Coordinación de Servicios Escolares

Agradecimientos

Dedico y agradezco a Dios y a todos mis maestros el apoyo para haber cursado a personas que siendo familia de sangre y por amor y cariño pertenecen a mi familia. Especialmente comparto y dedico este logro a la casta López Arredondo, hermanos de mi padre, Rogelio Antonio y a mis queridas tías Irma, Guillermina, Lourdes, Cleo y Maricela, que, pese a la distancia, me han demostrado un sincero cariño y apoyo en este sendero.

A mis hermanos de vida, Litzahajat Hernández, Roberto Rufino, Angélica Hernández y Sonia García, pues ustedes con sus ánimos, alegrías, enseñanzas y regaños evitaron el proceso emotivo de este proyecto de Maestría.

Asimismo, a los compañeros de sendero que por azares del destino y felizmente, continúan su camino de vida; Irma Rivera, y a los queridos hermanos Ramírez Vieyra, pues siempre han sido maestros de coraje, constancia y aspiración a ser la mejor versión de cada uno de nosotros mismos. Fuerza y coraje para avanzar y nunca detenerse pese a todo, eso es mi mejor obsequio.

A INFOTEC, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, por la creación de la Maestría en Derecho de las Tecnologías de Información y Comunicación, pues complementa mi carrera y define el sendero que había buscado, lo cual me permite crecer profesionalmente y con una nueva perspectiva de la realidad tecnológica inmersa en la que hoy en día vivimos.

Finalmente, agradezco a mis profesores que contribuyeron con sus conocimientos a mi crecimiento personal y profesional, y me han demostrado que cada paso es un avance y un paso más a la realización de mi proyecto profesional y de aspiración en el trayecto de vida.

Tabla de contenido

Índice de figuras

Índice de cuadros

Siglas y abreviaturas

CPEUM	Constitución Política de los Estados Unidos Mexicanos
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LGTAIP	Ley General de Transparencia y Acceso a la Información
LGPDPPSO	Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados
LFDA	Ley Federal de Derechos de Autor
LDI	Ley sobre delitos de imprenta
RLFPDPPP	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
PIDCP	Pacto Internacional de Derechos Civiles y Políticos
CADH	Convención Americana sobre Derechos Humanos “Pacto de San José de Costa Rica”
CPDHLF	Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales
EC-SPJ	Código de Ética de la Sociedad de Periodistas Profesionales de los Estados Unidos de América

Introducción

Actualmente, un sin número de aplicaciones y servicios que captan datos personales y que son concentrados en las bases de datos de las empresas, así como el uso de la segmentación de los usuarios en las plataformas para fines publicitarios pueden conllevar un alto riesgo de vulneración de la información, poniendo en riesgo la dignidad de las personas y sus derechos derivados.

Considerando que existe un veloz cambio en las plataformas tecnológicas y el ritmo de vida en razón a las condiciones actuales del país y la continua evolución mundial respecto a los bienes y servicios ofertados, la normativa aplicable, la autorregulación adoptada para el desarrollo óptimo de la tecnología y la actividad humana son formas de protección y respaldo de toda persona debe gozar como mínima protección.

Ante ello, las personas adoptan la tecnología como una forma de socialización humana y una herramienta de trabajo; en tanto las empresas incursionan a nuevas herramientas digitales, la automatización de los procesos y la explotación de nuevos mercados, así como la renovación de las formas de trabajo y modos de vida. A partir de esto, se considera necesario que toda entidad que realice un tratamiento de datos personales tenga un marco mínimo de ciberseguridad y con ello, sacar el mayor provecho de las Tecnologías con proporcionalidad al respeto de los derechos de los titulares.

Por esta razón, es necesario destacar que la ciberseguridad se divide en tres rubros principales: *seguridad digital* para computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos; *la seguridad de la información* registrada; y la *gestión de riesgos*[1].

Así, en el desarrollo del presente trabajo denotaremos las medidas mínimas y básicas para la infraestructura de las cuestiones técnicas, así como la estandarización nacional e internacional (tal como las ISO) como mejores

[1] Kaspersky Lab, *¿Qué es la ciberseguridad?*, publicación digital, [Consulta en agosto 2020]. Véase en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

prácticas del uso de la tecnología y gestión para el tratamiento de datos personales.

Como antecedente general, en los años 80 comenzaron a utilizarse “las buenas prácticas” y marcos de referencia de gestión de las tecnologías; sin embargo, fue hasta los años 90 en aras de respaldar la “calidad en el servicio” con la ISO-9000, y en consideración a la mejora continua, y con ello incursionar a las nuevas tecnologías que funcionan como plataformas de servicio.

Para el caso mexicano, en 2010 el gobierno emitió el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones (MAAGTIC); sin embargo, en 2014 se incorporó un apartado de “seguridad de la información”, renombrándolo como MAAGTIC-SI cuyo objetivo era coadyuvar en las mejores prácticas en gobernabilidad y gestión de TIC con aplicación a las entidades gubernamentales.

Considerando que las TIC son un punto de interconexión entre los usuarios con la información y a su vez, un punto de contacto con los proveedores de servicios, haciendo obligatorio el respeto a la normativa vigente; sin embargo, en la por lo cual las actividades deben estar respaldadas en la normativa mexicana y con la plusvalía del uso de mejores prácticas internacionales para la protección de los datos de los usuarios y la protección de las tecnologías que la gestionan.

Cabe señalar que las entidades privadas también pueden apegarse al MAAGTIC-SI, siendo una herramienta alterna, que les permitiría incrementar su valor institucional y tener un valor de plusvalía ante el mercado, en tanto observan la normativa de la materia y adopta los marcos de referencia para la gestión de las TIC.

Es conocido que la mayoría de las empresas son de índole mediana a pequeña, por lo que difícilmente tienen los medios abundantes y necesarios para implementar cursos o auditorías por un externo que les indique su nivel de riesgo y la forma de mitigación del mismo. Ante esta necesidad, se plantea

la siguiente hipótesis: “Con la adopción de recomendaciones internacionales y normalización mexicana, la ciberseguridad de los datos personales tratados por diversas entidades mediante Tecnologías de la Información, se podrá garantizar o ampliar el espectro del respeto a los derechos humanos”, lo cual podrá ser acogido con las medidas señaladas en el presente trabajo.

Así, los objetivos del desarrollo del presente son presentar y recomendar las herramientas básicas de salvaguarda de la información de los titulares, así como la creación de diagnóstico base bajo una óptica de Derechos Humanos, prevención de riesgos y salvaguarda de los derechos fundamentales ante gestión de datos personales por sistemas tecnológicos; utilización y análisis de las buenas prácticas internacionales sobre ciberseguridad y protección de la información personal a partir de la autorregulación nacional y en uso de herramientas de instrumentos de Instituciones internacionales en la materia.

Bajo dicha premisa, el resultado será que el interesado podrá identificar y generar un análisis básico de su estado de protección jurídica e implementar herramientas disponibles para la gestión de la información, respecto a los derechos humanos y seguridad de las tecnologías de la información.

Capítulo 1.
Antecedentes

Capítulo 1. Antecedentes

1.1 Origen de la normalización o estandarización

El origen de la normalización en el mundo surgió en los años del 1500 en Francia, pues por primera vez se implementaron etiquetas de certificación en el queso Roquefort y los vinos. Su objetivo fue la regulación y control de estos respecto al origen y pureza; sin embargo, fue hasta el siglo XX (1904) cuando la industria eléctrica utilizó la certificación francesa para garantizar la seguridad de los aparatos eléctricos y el equipo industrial.

1.2 Surgimiento de la Organización para la Estandarización Internacional (ISO)

La Organización para la Estandarización Internacional, ISO, fue creada por dos asociaciones dedicadas a la elaboración de estándares: la *International Federation of the National Standardizing Associations (ISA) y la United Nations Standards Coordinating Committee* (UNSCC, por sus siglas en inglés). La primera, fue una empresa norteamericana que desarrolló sus actividades en el sector electromagnético principalmente en Europa mediante un sistema métrico -regulada por la International Electrotechnical Commission (ICE)-; sin embargo, durante la Segunda Guerra Mundial ISA suspendió actividades al momento en que la comunicación a nivel internacional fue nula.

Al concluir la Segunda Guerra Mundial, a finales de 1944 resurgió en Londres el Comité de Coordinación de Estándares de las Naciones Unidas (UNSCC), la cual realizaba la gestión desde las oficinas del ICE con el secretario **Charles Le Maistre**[2] -mismo, que es considerado el padre de la normalización- quien propició la fundación del organismo de normalización hoy conocido como ISO.

---

[2] (Estandarización, 2015) Charles Le Maistre, (6 de enero de 1874 - 5 de julio de 1953) es considerado el padre de la estandarización internacional en el campo de la ingeniería eléctrica. Fue "… *secretario de la UNSCC fue la figura que después de la Segunda Guerra Mundial, propició la fundación del organismo de normalización que hoy conocemos como ISO. Rondaba el año 1945, durante el mes de octubre en Nueva York tuvo lugar una reunión entre los delegados provenientes de los diversos países que formaban parte de la UNSCC. En ella debatieron sobre el futuro de la normalización a nivel internacional y se acordó una aproximación con ISA, con la finalidad de constituir una organización que provisionalmente se llamaría `International Standards Coordinating Association´".*
Fue en julio de 194 en París cuando ISA y UNSCC decidieron realizar una nueva reunión con participación de 65 delegados de integrantes de ambas organizaciones provenientes de 25 países quienes acordaron la disolución de la ISA y convence a la UNSCC para que cesaran su actividad en beneficio de la nueva organización ISO. Así, el 26 de octubre de 1946 se crea la "International Organization for Standardization" como único organismo de normalización.

En el año 1945 en Nueva York se reunieron miembros de la UNSCC en la que debatieron sobre el *futuro de la normalización a nivel internacional y se acordó una aproximación con ISA, con la finalidad de constituir una organización que provisionalmente se llamaría "International Standards Coordinating Association" (sic.)*[3].

En 1946, ISA y UNSCC realizaron una reunión en Londres junto con el Instituto de Ingenieros Civiles en la que se acordó la disolución de ISA a razón de "...*ciertas irregularidades y por la inactividad que tuvo durante la Segunda Guerra Mundial..."*[4] e impulsar la actividad de la *International Standarization Organization (ISO)*.

El 27 de febrero del año 1947 comenzó oficialmente sus actividades con 67 comités de estandarización creados por ISA, con sede en Ginebra (Suiza). Actualmente, la Organización se considera como el principal editor de normas, de carácter no gubernamental con impacto internacional y conformado por la participación de 162 países y 3,368 organismos técnicos.

Cabe señalar que ha creado más de 19,500 normas ISO relacionadas a la fabricación y tecnología. Algunas de las más populares son la ISO 9001 para los Sistemas de Gestión de la Calidad; la ISO 14001 para los Sistemas de Gestión Ambiental, la ISO 27001 para los Sistemas de Gestión de Seguridad de la Información y la ISO 31000 para los Sistemas de Gestión de Riesgos.

Actualmente, el objetivo de la Organización Internacional de Estandarización es "... *simplificar la coordinación internacional y unificar los estándares industriales...*"[5], mejor conocidas como ISO.

1.3 Evolución de las normas de la Estandarización

En el giro comercial fue la empresa australiana Woolmark quién estableció una certificación para garantizar a los consumidores que sus productos (lana) de vestimenta, estaban confeccionados con lana pura completamente limpia.

Al ver el éxito de la certificación diversas empresas de múltiples sectores comenzaron a crear nuevos estándares de certificación con la

---

[33] (Unidas, s.f.) Comité de Coordinación de Estándares de las Naciones Unidas, El origen de las ISO, comunicado de Alema Adri, Calameo, [Versión digital] [Consulta en mayo 2020]. Véase en: https://es.calameo.com/read/00280480692ccd26e5b3e

[4] *Ibidem*. P. 1.

[5] *Idem*.

finalidad de garantizar la confiabilidad de los productos a los vendedores para los usuarios. Los ejemplos más representativos son los siguientes:

Figura 1. Estándares de certificación. Fuente: página web ISO.

Sin embargo, fue hasta 1987 que Europa emitió la nueva certificación denominada “Campaña de Bandera Azul”, ella destacó por la utilización de *estrellas* sobre bienes y servicios turísticos. Posteriormente, en 1988 Austria estableció la etiqueta “*Silberdistel*” para hospedajes y restaurantes en Kleinwalsertal.

En 1992 Brasil impulsó por primera vez la certificación ambiental con la “Cumbre de la Tierra” de las Naciones Unidas, con lo cual se creó la “Agenda 21” para la responsabilidad social y ambiental para todos los sectores de la sociedad mundial. Fue hasta 1996 que se creó la primera ISO 14001 para los sistemas de gestión ambiental universal.

Durante el año 2000 en Estados Unidos se crea la certificación “*American Automobile Association* (AAA), con el uso del sistema de “estrellas” sobre calidad de los hoteles en este país. Posteriormente Europa lo implementó para la regulación de la calidad de las llantas Michelin, extendiéndose al sector turístico, salud, higiene y seguridad. Paralelamente a ello, los representantes de los programas de certificación en turismo en Mohonk Mountain House, *crearon un lenguaje común y estándares mínimos comunes* para otorgar certificaciones de turismo sostenible y ecoturismo, lo cual permitió que en 2002 se celebrará el “Año Internacional del Ecoturismo”

con el que se impulsaron más de 60 programas de certificación de turismo ambiental (sociocultural y/o aspectos de turismo), la mayoría radicados en Europa.

No obstante, ante la proliferación controlada de los programas de certificación en 2007 de hasta 80 programas de certificación, los consumidores registraron confusión por la falta de reconocimiento de marcas y diversidad de estándares, por lo que en el 2008 se estableció un estudio de factibilidad llamado “Consejo de Acreditación de Turismo Sostenible” (STSC, siglas en inglés), el cual logró los estándares armonizados en Europa (estándar VISIT) y en las Américas (Red de Certificación en Turismo Sostenible de las Américas).

Finalmente, en 2009 los nuevos programas de certificación turística y los anteriores comenzaron a considerar temas de sostenibilidad: ambiental, social, cultural y económico llamado triple rentabilidad; de igual forma, se incorporaron criterios de calidad, administración, salud y seguridad.

1.4 Tipos de ISO

De acuerdo con los especialistas en certificación Patrick Mundler y Stéphane Bellon, existen diversas categorías generales de certificación[6]:

- **Contable.-** Sobre el proceso de verificación de cuentas de una organización.
- **Electrónica o digital.-** Refiere al proceso de atribución de certificado electrónico de forma unilateral o con apoyo de un tercero de confianza.
- **Medioambiental.-** Sobre el proceso para establecer y verificar la calidad del medio ambiente o su deterioro, como consecuencia de las actividades humanas.

[6] Mais on sait depuis longtemps que de nombreux offreurs misent sur une différenciation de leurs produits, que tous les produits ne se vendent pas dans les bourses mondiales et que sur la plupart des marchés, offreurs et demandeurs ne disposent pas du même niveau d’information.
G. Akerlof. << The market for “lemons”: quality uncertainty and…. Puisque les marchés ne peuvent assurer une bonne coordination entre offreurs et demandeurs, la mise en œuvre de dispositifs permettant d’améliorer l’information sur la qualité des produits est nécessaire. Ces dispositifs peuvent être variés: assurances, labels, marques, cahiers des charges..., ils ont tous vocation à permettre aux consommateurs d’améliorer leur niveau d’information sur les produits qu’ils achètent>>. Patrick Patrick Mundler, Stéphane Bellon, “Les Systèmes participatifs de garantie: une alternative à la certification par organismes tiers?”, EDITORA, PAIS (mayo 2011), 'Pour' #212, pp. 57-65. TRADUCIDO, TRADUCCIÓN PROPIA

- **Profesional.-** Es la atribución de un diploma, un título, o un certificado, que reconoce una competencia profesional.
- **Ventas discográficas.-** Es un reconocimiento a los artistas cuyas producciones alcanzaron altas cifras de ventas.
- **Diamond Award.-** Es un reconocimiento entregado por la 'Recording Industry Association of America' (RIAA), a los artistas que por un álbum y/o un disco sencillo, hayan logrado más de 10 millones de copias vendidas.
- **Disco de Diamante.-** Es un premio discográfico otorgado a un artista, por un sencillo, un video musical, un álbum o un single de álbum de estudio a razón de las altas ventas durante su carrera discográfica.
- **Forestal.-** Denota al consumidor si la madera o la leña que compra, ha salido o no de bosques gestionados de forma sostenible.

No obstante, también existe la “Certificación participativa o Sistemas participativos de garantía”, los cuales son gestionados y certificados por un grupo de productores y consumidores. Su base se refiere a la confianza, el intercambio de conocimientos y experiencias (Sistemas participativos de garantía).

A diferencia con la estandarización tradicional, estas verificaciones generalmente las realizan entes no gubernamentales y existe la posibilidad de incluir cuestiones macro como *criterios de calidad medioambiental, económico-financiera, y social;* además, permite o facilita el acceso a la certificación de pequeños empresarios. Algunos de los ejemplos de este tipo de reconocimiento es la Certificación Participativa sobre la agricultura biológica mediante la International Federation of Organic Agriculture Movements (IFOAM); en materia económica, se encarga Grupo Minga; en el sector de la construcción, la gestiona la Asociación Envirobat BDM'8 (Provenza-Alpes-Costa Azul) y la Asociación Ecobatp LR'9 (Centros de recursos en renovación sostenible, construcción y planificación en Occitania, Occitania) los cuales usan la etiqueta “Edificios sostenibles mediterráneos” (en francés: Bâtiments Durables Méditerranéens), por mencionar algunos.

Adicionalmente, existen empresas como Great Place To Work (GPTW) las cuales se consolidan como una autoridad global en alta confianza y culturas de alto rendimiento en el lugar de trabajo. Particularmente en esta

empresa, y a manera de ejemplo, su actividad "...se *basa en investigaciones sobre la experiencia de los empleados* en las empresas que laboran *respecto al nivel de innovación, satisfacción del cliente y del paciente*, *compromiso de los empleados y agilidad organizacional*…"[7]. Ello le permite realizar una evaluación comparativa y mejores prácticas de empresas líderes a nivel mundial y la metodología de investigación probada en la industria[8] considerando la cultura laboral. Dicho análisis es publicado anualmente mediante la lista de las 100 mejores compañías para trabajar, y los mejores lugares de trabajo.

1.4.1 Características de las ISO

Existen diversos beneficios del uso de las normas estandarizadas, pero básicamente resaltaría el tema de la funcionalidad universal de los bienes y el tema de la competencia entre los productores o distribuidores; además de las repercusiones secundarias positivas en el uso de ello:

- *"Ofrece flexibilidad sobre la metodología basada en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar)".*
- *"Se elimina la obligatoriedad de la conservación de documentos diferentes a la "Declaración de aplicabilidad".*
- *"Se apuesta por un enfoque del análisis del riesgo en la fase de planificación y operación".*
- *"Se implementa el Software para ISO 27001 mediante la Plataforma de isotools, lo cual facilita la automatización de la ISO 27001".*

Un par de ejemplos de funcionamiento de las ISO son la IEC 30141 vs la ISO27001, pues su implementación conjunta permite implementar, automatizar y mantener los parámetros de los sistemas de gestión de seguridad bajo el ciclo PHVA para la mejora del Sistema, aplicación de las buenas prácticas y controles establecidos.

---

[7] (Work, 2019) Great Place To Work (Consulta en 2020). [Versión digital]. Véase en: https://greatplacetowork.com.mx/quienes-somos/

[8] Ibidem.: "…Décadas de investigación muestran que los lugares de trabajo con culturas de alta confianza obtienen mayores rendimientos en los resultados, niveles de innovación, satisfacción del cliente y del paciente, compromiso de los empleados y agilidad organizacional. Nuestros clientes se benefician de una serie inigualable de datos de evaluación comparativa y mejores prácticas de empresas líderes de todo el mundo junto con una metodología de investigación probada en la industria…"

Otro ejemplo más claro son los controles en calidad, pues la ISO 9001 -que trata de los sistemas de gestión de calidad-, la creación de la ISO 14001 -sobre la gestión ambiental- y la OHSAS 18001 -sobre los requisitos mínimos para la gestión de Seguridad y Salud en el Trabajo-.

Reflexión de utilidad sobre el uso de la normalización: ante la globalización y evolución social, cultural, tecnológica y económica de la humanidad se puede detectar que la universalidad se imprime en las personas y la evolución de la cultura y desempeño de las actividades humanas, por lo cual es necesario que la globalización denote actividad de normalización en las medidas de seguridad y gestión de la información.

1.4.1.1 Ventajas de la implementación de Sistemas de Gestión

Las ISO en cualquiera de los ámbitos de estandarización utiliza los Sistemas de Gestión que de manera general implican:

- *La simplificación de los requerimientos del sistema*
- *Optimización de recursos*
- *Reducción de costos*
- *Realización de auditorías integradas*
- *Reducción de los documentos*
- *Alineación de objetivos sobre los estándares y sistemas*
- *Creación de sinergias*
- *Reducción de duplicadores de políticas y procedimientos*
- *Incremento de la motivación de los trabajadores, y*
- *Mejora de la efectividad y eficiencia de la organización*

De forma general la implementación de un Sistema de Gestión implica la conformación de un equipo o comité para el establecimiento de las responsabilidades, el desglose de las herramientas a integrar en los departamentos de la empresa. Posteriormente, conforme a la implementación se desarrolla un plan de seguimiento en el cual se desglosan los avances, los ajustes realizados y la fase del proceso de integración.

Como en todo proceso al concluir la integración del Sistema se inicia la etapa de “mejora continua”, en la cual se innova y adaptan las nuevas herramientas que permiten incrementar eficiencia global sobre los resultados,

la mejora en la toma de decisiones bajo el nuevo modelo y la definición de los nuevos objetivos o prioridades de cada ente.

1.5 La normalización en México, normatividad interna

De acuerdo a la autoridad encargada del tema, la Secretaría de Economía, señala que la normalización es un procedimiento voluntario mediante el cual se evalúa, se somete a auditoría y se emite una garantía escrita, en el sentido de que una instalación, un producto, un proceso o un servicio, cumple con estándares específicos para su utilización y/o creación; es decir, "...*es el proceso de ajustar o adaptar ciertas características en un producto, servicio o procedimiento a fin de que éstos se asemejan a un tipo, modelo o norma en común*..."[9].

Este tipo de actividades, permiten la creación de los productos con características comunes, cuya funcionalidad es asequible en el país y en el mundo. Algunos de sus beneficios en temas de competencia económica es el acceso de las empresas en mercados transnacionales, reducción en los costos de producción e impulsa la innovación tecnológica. Un ejemplo de ello es la conexión de los audífonos, los semáforos viales y material y tamaño de las tarjetas bancarias.

Sin embargo, particularmente en México la normalización está a cargo de diversas dependencias del país; es decir, nuestro país emite **Normas Oficiales Mexicanas (NOM)** con carácter obligatorio; en tanto emite las **Normas Mexicanas (NMX)**, cuya diferencia con las NOM es la adecuación de forma voluntaria y su emisión depende de la Secretaría de Economía y del sector privado, mediante los Organismos Nacionales de Normalización.

---

[9] Secretaría de Economía, Qué es la Normalización o Estandarización, fecha de publicación del 26 de junio de 2018. [Versión digital] [Consulta en marzo 2019]. Véase en: *https://www.gob.mx/se/articulos/sabes-que-es-la-normalizacion-192107?idiom=es#:~:text=La%20normalizaci%C3%B3n%2C%20tambi%C3%A9n%20conocida%20como,o%20en%20cualquier%20otro%20pa%C3%ADs.*
(ibidem) "La Normalización, conocida también como Estandarización, permite la creación de normas o estándares que establecen las características comunes que deben cumplir los productos en diferentes partes del mundo. Esto significa que su manufactura o fabricación debe ser de la misma forma en México, Estados Unidos, China, o en cualquier otro país o parte del mundo.
Es, además, una actividad técnica especializada que ofrece muchos beneficios a nuestra sociedad: permite que las pequeñas y medianas empresas puedan acceder a mercados internacionales; contribuye a la reducción de costos de producción; y facilita el avance de las nuevas tecnologías".

1.5.1 Objeto y campo de aplicación

El objetivo de la revisión e implementación de estándares de seguridad mexicanos es complementarlos con las normas internacionales, con un énfasis de cumplimiento de las medidas de seguridad de las entidades sobre el tratamiento de los datos personales al marco jurídico mexicano y en atención a los tratados internacionales.

La creación de consideraciones previas a una implementación de sistemas de gestión y normalización para el tratamiento de datos personales permitirá a las organizaciones conocer la infraestructura tecnológica y metodológica para la adopción de un Sistema de Gestión de Seguridad de la Información (SGSI), cuyo objetivo es determinar los riesgos, amenazas y áreas de oportunidad para la planificación del Sistema con el fin de establecer los objetivos de Seguridad.

Con la aplicación de los controles de operación y la medición de los resultados mediante la auditoría interna y la revisión por la dirección del SGSI a fin de cerciorarse que los procesos funcionan conforme a lo planificado, en el entendido de la adopción de mejoras para la eficacia del Sistema.

1.5.2 Antecedentes de las Normas Oficiales Mexicanas

De acuerdo con la página de Internet gubernamental nom.mx[10] durante la época de Porfirio Díaz el país tuvo un incremento en la industrialización, por lo que surge la necesidad de crear controles sobre la producción desde su invención, la producción y el uso de patentes.

El primer sector que incursionó en el tema fue con la construcción del sistema ferroviario, pues la empresa originaria tenía los derechos totales sobre las vías, por lo que ninguna empresa podía realizar la misma actividad bajo los mismos parámetros de calidad, esto último conformó el principal origen de las Normas Oficiales Mexicanas (NOM).

Cabe señalar que México fue influenciado por Estados Unidos sobre la tarea del cuidado de los consumidores y el cumplimiento de parámetros en

[10] Normas Oficiales Mexicanas, Cómo surgieron las NOM en México, 2015. [Versión digital] [Consulta en enero 2020]. Véase en: http://nom-mx.com.mx/articulo/como-surgieron-las-nom-en-mexico

productos y servicios para su intercambio internacional, por lo que los primeros pasos fueron la emisión de leyes y reglamentos.

En 1986, cuando México se suscribe al Acuerdo General sobre Aranceles y Comercio (GATT, por sus siglas en inglés), ISO fungió como mediador de calidad de productos nacionales. Ante ello, el país creó la Ley Federal sobre Metrología y Normalización[11] (LFMN) publicada en el Diario Oficial de la Federación el 1° de julio de 1992, en la cual se crean documentos llamados Normas Oficiales Mexicanas (NOM), los cuales **determinan estándares técnicos de cumplimiento en bienes y servicios fabricados y/o comercializados en el territorio mexicano**.

Asimismo, se creó el Centro Nacional de Metrología (CENAM) y la Dirección General de Normalización (DGN), la función del primero era la verificación y el establecimiento de datos duros, y el segundo desempeñó funciones administrativas.

Actualmente, estas normativas velan por la salud y el patrimonio de los ciudadanos, a través de la definición de requisitos, especificaciones, procedimientos y metodologías establecidas por distintas dependencias gubernamentales con la finalidad de evaluar parámetros de riesgos y evitarlos.

Cabe señalar que las NOM se distinguen por ser obligatorias en el territorio nacional, regular procesos de producción y minimizar riesgos para las personas, animales o medio ambiente.

En ese sentido, conforme la importancia y reclamo del respeto de los Derechos Humanos se comenzó a detonar la importancia de los datos personales y la necesidad de minimizar de riesgos; por lo que el excomisionado del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México, Gustavo Parra Noriega, reconoció que los ciudadanos dudaban sobre su información personal y que consideraban “confidenciales”, por lo que no había certeza de su uso y de la responsabilidad de los gestores[12].

---

[11] Ley Federal sobre Metrología y Normalización (LFMN), publicación en el Diario Oficial de la Federación, del 1° de julio de 1992. [Consultada en junio de 2019]. https://www.gob.mx/cms/uploads/attachment/file/107522/LEYFEDERALSOBREMETROLOGIAYNORMALIZACION.pdf

[12] “Sector salud tiene el deber de brindar un aviso de privacidad a pacientes, Testigos Sociales”, publicación de mayo 2021. [Versión digital] [Consultada en junio 2021]. Véase en: http://www.testigossociales.org.mx/es/contenido/noticias/sector-salud-tiene-el-deber-de-brindar-un-aviso-de-privacidad-pacientes

Así, fue hasta 2009 cuando la autoridad reconoció la autonomía y la naturaleza jurídica, con lo cual se elevó a Derecho humano, por lo que en 2010 en México se expidió la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[13] (LFPDPPP) y en 2017 se aprobó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[14] (LFPDPPSO) o sector público.

Con el nuevo marco jurídico, en 2018 México logró emitir las leyes normativas secundarias por el INAI y el Sistema Nacional de Transparencia Protección de Datos (conformado por autoridades locales y nacionales, la Auditoría Superior de la Federación, el Archivo General, el INEGI y la Secretaría de la Función Pública) con la misión de vigilar e emitir la evaluación de impacto y medidas preventivas.

Pese a dicho esfuerzo, la continua evolución de la tecnología y las nuevas tendencias sociales, se evidencia la necesidad de proteger los datos personales dentro de los sistemas informáticos en tanto se realizan acciones de concientización de la población sobre la importancia del uso y protección de su información debido a la recopilación de estos mediante dispositivos electrónicos, y el apego a la normativa nacional y uso de instrumentos internacionales, en pro de la dignidad humana.

1.5.2.1 Objeto y campo de aplicación

Su objeto de regulación son los productos y procesos que conlleven riesgos para la seguridad de la salud o integridad de las personas, animales, vegetales, medio ambiente o afectación a los recursos naturales. Son de carácter obligatorio en el territorio mexicano.

---

[13] Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicación en el Diario Oficial de la Federación, el de julio de 5 de julio de 2010. [Versión digital] [Consultada en junio 2019]. Véase en: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

[14] Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicación en el Diario Oficial de la Federación el 26 de enero de 2017. [Versión digital] [Consultada en junio 2019]. Véase en: https://dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

Su marco jurídico es la Ley Federal sobre Metrología y Normalización[15] publicada en el Diario Oficial de la Federación el 1° de julio de 1992. Las NOM son de observancia obligatoria.

1.5.2.2 Particularidades de las NOM

A diferencia de las ISO, las Normas son una denominación dada en clave que identifica el producto o servicio; el método; su proceso; su instalación u objetos de la NOM conforme a su fin. Seguido de ello, se mencionan las especificaciones o características correspondientes al bien, los métodos de prueba aplicables respecto a la Norma y la muestra; es decir, las características de la información a contener los productos, por ejemplo, las especificaciones diseño y la forma de uso.

Ante ello, conviene exponer una categorización de los tipos de Normas reconocidas en nuestro país:

- ***Internacionales.****-Con el interés internacional en temas de estandarización y calidad, muchos países utilizan las ISO como de aplicación obligatoria o establecen requisitos mínimos para el ingreso de bienes y servicios a su población.*
- ***Regionales.-*** *Estas son generadas y adoptadas por un grupo de países, que por sus relaciones convienen beneficios mutuos. Un ejemplo de ello, es la Comisión Panamericana de Normas Técnicas (COPAN) y la Comisión Europea de Normalización (CEN).*
- ***Nacionales.-*** *A diferencia de las anteriores, este tipo de normas son emitidas por algún Organismo Nacional de Normalización. En el caso de México, el encargado es la Dirección General de Normas (DGN), la cual pertenece a la Secretaría de Economía.*
- ***Normas Mexicanas o NMX.-*** *En el caso de México, son las elaboradas por la Secretaría de Economía, el CENAM, la DGN o cualquier otro organismo de normalización que pretenda la normalización enfocadas en reglas, especificaciones, métodos de prueba, directrices, características o prescripciones*

[15] Ley Federal sobre Metrología y Normalización, publicación en el Diario Oficial de la Federación el 1° de julio de 1992. [Versión digital] [Consultada en junio 2019]. Véase en: https://docs.mexico.justia.com/federales/ley_federal_sobre_metrologia_y_normalizacion.pdf

aplicables a productos, procesos, instalaciones, sistemas, actividades, servicios, producción u operación, las relativas a la terminología, simbología, embalaje, marcado o etiquetado.

A diferencia con las NOM, estas no son de cumplimiento obligatorio; sin embargo, entablan directrices de calidad.

- ***Asociación.-*** *Son generadas por grupos de fabricantes del mismo giro o producto, cámaras industriales y/o asociaciones de consumidores. Su finalidad es que los bienes que contengan los mínimos parámetros de calidad, intercambiabilidad y evitar la competencia desleal.*
- ***Empresariales.-*** *Son normas emitidas por grupos de empresas que pretenden guiar las compras, la producción, ventas y otras operaciones. Es importante destacar que esta práctica busca la orientación en el proceso de producción y venta, por lo que no implican el acuerdo de precios en el mercado, pues de lo contrario se incurriría en una práctica desleal.*

  Además, la Procuraduría Federal del Consumidor (Profeco) tiene la facultad de expedir NOM´s, emitir criterios de observancia, vigilar su cumplimiento y sancionar su omisión (artículo 3)[16]*.*

  En ese sentido se puede resaltar que las tendencias de la normalización en algunos países en el tema de proteccionismo; sin embargo, la mayoría de las naciones realizan actividades de globalización y comercio internacional, por lo que es de interés mantener parámetros de calidad y sanidad -principalmente-.

  Cabe señalar que las ISO son las principales referencias sobre la normalización voluntaria[17]*, las cuales pueden ser adoptadas por cualquier tipo de organización, industria o sector con la*

[16] Ley Federal de Protección al Consumidor, [Versión digital], [Consulta agosto 2020]. Véase en: https://www.profeco.gob.mx/juridico/pdf/l_lfpc_ultimo_CamDip.pdf

[17] Organización Internacional de Estandarización y Organización de las Naciones Unidas para el Desarrollo Industrial (ONUDI), *Organismos Nacionales de Normalización en Países en Desarrollo*, [Versión digital] [Consulta en agosto 2020], página 1. Véase en: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/fast_forward-es.pdf

finalidad de prevenir, disminuir y formas de mitigación de los riesgos.

Bajo este panorama, se considera necesario la aplicación de la normalización en medidas de seguridad para salvaguarda de la información personal, con apego a la normativa nacional y regulación de los efectos y resultados del uso de las tecnologías. Ante ello, el uso de la normalización de la ISO permite adoptar acciones de detección de riesgos y oportunidades, estructura de objetivos de calidad, procesos de planificación de cambios en temas de: infraestructura o ambiente de trabajo, seguridad en dispositivos IoT, documentación, conocimientos, controles, competencias, conciencia y comunicación; en tanto permite aplicar esquemas de evaluación y de acciones correctivas conforme a las necesidades del ente.

1.6 Origen y justificación de los datos personales

1.6.1 Concepto

El Convenio 108 del Consejo de Europa[18] (28 de Enero de 1981) para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, en adelante el Convenio 108, indica que este instrumento internacional pretende garantizar el derecho humano (únicamente para las personas) sobre la vida privada, independientemente de la nacionalidad o lugar de residencia respecto al tratamiento automatizado de los datos personales, partiendo de la finalidad *"...garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona*…"[19] (Artículo 1).

[18] Convenio N° 108 del Consejo de Europa para la Protección de las personas con respecto al Tratamiento automatizado de datos de carácter personal y protocolo adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento automatizado de datos de carácter personal,. A las autoridades de control y a los flujos Trasfronterizos de Datos, Publicación del Consejo de Europa el 28 de enero de 1981. [Versión digital] [Consultado en mayo 2019. Véase en: https://archivos.juridicas.unam.mx/www/bjv/libros/12/5669/15.pdf

[19] Ibidem. Artículo 1 (p. 1).

Asimismo, el Reglamento General de Protección de Datos (RGPD) señala que el concepto un dato de carácter personal es *"cualquier información concerniente a personas físicas identificadas e identificables*"[20] (artículo 4).

Así, el derecho humano origen de la protección de datos es la dignidad, de acuerdo a la Real Academia Española, pues la "…*dignidad de la persona es una cualidad propia de la condición humana de la que emanan los derechos fundamentales, junto al libre desarrollo de la personalidad, que precisamente por ese fundamento son inviolables e inalienables. Asimismo, es el valor del hombre y fin supremo de todos los derechos y acción del Estado…"*[21] (ibídem).

Para el caso de la legislación mexicana, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), señala que *"...los datos personales son toda aquella información que se relaciona con nuestra persona y que nos identifica o nos hace identificables. Nos dan identidad, nos describen y precisa*..."[22] siendo subdivididos en dos categorías: *generales y sensibles.*

La diferencia de la categoría radica en la naturaleza de la información; es decir, los datos que pudieran ser conocidos públicamente y derivaran en afectación de la esfera jurídica del individuo, tal como es la discriminación –sea por origen étnico, preferencia sexual e ideología política, por mencionar algunos-; así, este tipo de información pertenece al segmento de *datos personales de carácter sensible*. A diferencia con la información que es

---

[20] Reglamento General de Protección de Datos, Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos. [Versión digital] [Consulta en mayo 2019]. Véase en: *https://www.boe.es/doue/2016/119/L00001-00088.pdf*
Ibidem. Artículo 4. "«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona". [Versión digital]. [Consulta agosto 2020].

[21] Real Academia Española, diccionario del español jurídico definición de dignidad de la persona. [Versión digital] [Consulta abril 2020]. Véase en: https://dej.rae.es/lema/dignidad-de-la-persona

[22] El abc de los datos personales, Conferencia Mexicana para el Acceso a la Información Pública, publicación. Publicación del El Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (Infoem). [Versión digital] [Consulta en julio 2020]. Véase en: https://www.infoem.org.mx/doc/publicaciones/ABC_Datos.pdf

recabada por un tercero para la realización de un servicio o servicio y no genere perjuicio a la esfera jurídica, quedando en el segmento de *datos personales de carácter general.*

Es de resaltar que cada persona tiene la propiedad de sus datos personales, pese a que estos sean utilizados o recabados por terceros que, en cuyo caso, contrae obligaciones de protección y resguardo de la información solo por ser poseedor de tal información. Y aunado a la determinación de ser un derecho fundamental, es permisible la exigencia de un tratamiento y resguardo adecuado y digno.

Actualmente, las generaciones utilizan las Tecnologías de la Información en el que solo por el hecho de utilizar Internet, plataformas y sistemas dejan su registro o huella personal que ante un uso puede resultar en la generación de perfiles de usuarios sobre sus actividades e intereses utilizados por bases de datos que no denotan su política de uso y tratamiento de información generada.

Ante ello, es necesario explicar la conceptualización de "*dato*" y todas las actividades derivados de ello, con la finalidad de reconocer el riesgo ante una vulneración y posibles repercusiones jurídicas.

El artículo 2 del Convenio 108[23] define lo siguiente:

A. *«Datos de carácter personal»* cualquier información relativa a una persona física identificada o que la hace identificable;

B. *«Fichero automa*tizado» cualquier conjunto de datos bajo tratamiento automatizado;

C. «Tratamiento automatizado» son las operaciones realizadas en forma parcial o total con procedimientos automáticos: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión;

[23] Convenio 108… Ibidem. Artículo 2 (p. ").

D. Autoridad «controladora del fichero» es la persona física o jurídica, autoridad o cualquier otro organismo competente para determinar la finalidad del fichero, categorías y operaciones aplicables

Con este esquema, se puede observar que el campo de aplicación no diferencia entre el sector público y privado, en cualquiera de sus modalidades -agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo compuesto directa o indirectamente de personas físicas, tengan o no personalidad jurídica- (art.3 del Convenio 108); no obstante, existen algunas categorías de ficheros automáticos sometidas a disposiciones de protección de datos, lo cual exige una modificación en las categorías suplementarias de los ficheros.

De acuerdo al Convenio, en el caso de que los países hubieran realizado ampliaciones, solamente se aplicarán a determinadas categorías de ficheros de carácter personal cuya lista quedará depositada. Por otro lado, si existieron exclusiones de categorías anteriores, no se podrá solicitar su aplicación al presente convenio; de igual forma, cuando un estado no haya procedido a una u otra de las ampliaciones previstas (...) no podrá pretender que se aplique el presente Convenio en esos puntos con respecto a una parte que haya procedido a dichas aplicaciones.

Con estas precisiones, se observa que cualquier país puede adherirse al Convenio 108 y con ello adoptar y/o complementar la normativa nacional respecto a las categorías ya establecidas; sin embargo, en algunas no contempladas en el Convenio no podrán ser exigidas ante una controversia jurídica. Dicha precisión denota que tanto instituciones como países deben de tener conocimiento del alcance e impacto que puede tener la información en las Tecnologías, y por ende, generar respaldo jurídico y normativo que permita defender a los cibernautas ante alguna vulneración a sus derechos.

1.6.2 Tipos de datos personales

Ante la era tecnológica, el Reglamento General de Datos Personales de Europa (RGDP) señala que un dato personal es "…*cualquier información*

concerniente a personas físicas identificadas e identificable[24]*…",* pues ello las hace únicas y estos se dividen en las siguientes categorías:

- *Identificativos*: nombre, apellidos, identificaciones, número de seguridad social, domicilio, teléfono, correo electrónico, fotografías o audios de voz, fecha y lugar de nacimiento, edad, estado civil, datos familiares.

- *Social y propiedad:* propiedades, aficiones y formas de vida, inscripciones en foros, clubes o asociaciones.

No obstante, algunas organizaciones como el INAI señalan que existen otras subdivisiones en datos: *Académicos* (formación, expedientes), *Profesionales* (experiencia y expediente profesional), *Sindical o de agrupación*, *Económico-financieros* (datos bancarios, ingresos), *Médicos* (historial clínico), *Judiciales* (procedimientos judiciales, sanciones) y *Sociales* (ayuda o subvención, prestaciones sociales, subsidios, pensiones), entre otros.

Cabe señalar que algunos de estos datos están especialmente protegidos debido a que puede afectar el desarrollo de las personas de forma negativa simplemente por hecho de ser conocidos: ideología, orientación sexual, afiliación sindical, salud, religión u origen racial o étnico de una persona, ello implica un aumento en el nivel de seguridad es superior a los demás. Es por ello, que ante la intención de recabar esta información los responsables deben recabar expresamente y por escrito el consentimiento de la recopilación y tratamiento de la información, con el objetivo de resguardar el derecho fundamental de la persona.

En el caso de la información biológica o biométrica, el Reglamento apunta que *"...los datos biométricos son aquellos datos personales referidos a las características físicas, fisiológicas o conductuales de una persona que posibiliten o aseguren su identificación única..."*[25]*,* tal como lo es la huella

[24] Ley de Protección de Datos Personales para el Distrito Federal, Publicación en la Gaceta Oficial del Distrito Federal del 3 de octubre de 2008. [Versión digital] [Consulta en junio 2019]. Véase en: http://www.infodf.org.mx/aviso/doctos/Ley%20de%20Proteccion%20de%20Datos%20Personales.html

[25] (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 26 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre

digital y el iris. De ahí la razón del conocimiento del tratamiento de los datos personales de los titulares y la inversión para el resguardo de la información en los sistemas electrónicos de los particulares y gubernamentales, pues un riesgo tendría impacto en las esferas jurídicas de los interesados.

Ante ello, resulta útil conocer una herramienta para la protección de las personas: uso de los "Datos seudonimizados o información de identificación no directa". Ello permite que la información no apunte a la identificación directa de los usuarios sin interferir con la creación de perfiles con base en el comportamiento; tal como sucede en el marketing digital, pues con el registro de los intereses, las empresas realizan una segmentación publicitaria que consumara en la presentación de un anuncio en un momento concreto.

Bajo esta tesitura, el RGPD establece una clara distinción entre la información de identificación directa y los datos seudonimizados: *"...el uso de seudonimización en datos personales puede reducir el riesgo asociado a la gestión de datos y ayudar a los responsables y encargados del tratamiento a cumplir con sus obligaciones de protección de datos..."*[26].

Ello se complementa con el considerando 29 del Reglamento, pues explica que la seudonimización no implica la anonimización de los datos o disociación completa sin retorno o imposibilidad de reversión de los mismos; ya que al obtener información adicional, el sujeto puede ser identificable. Es por ello, que nuevamente se visualiza la necesidad del uso de medidas de seguridad de los datos con el fin de evitar la identificación plena del usuario.

En el caso de México, el Instituto Nacional de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de

---

circulación de estos datos (Deroga Directiva 95/46CE), 2016) (Reglamento General de Protección de Datos, RGPD), *Ibidem*. Artículo 4, apartado 14. [Versión digital] [Consulta en marzo 2019]. Véase en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[26] Ibidem. Considerando 28 del Reglamento General de Datos Personales, [Versión digital] [Consulta en agosto 2020]. "La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos...".

Cuentas de la Ciudad de México[27] (INFO CDMX) categoriza la información personal de la siguiente forma:

- Datos identificativos (nombre, domicilio, edad, firma, RFC, etc.)
- Datos electrónicos (correo electrónico)
- Datos laborales (puesto, domicilio oficial, correo oficial, etc.)
- Datos patrimoniales (cuentas bancarias, información crediticia, etc.)
- Datos sobre procedimientos administrativos y/o jurisdiccionales
- Datos académicos (trayectoria educativa, título, número de cédula profesional, etc.)
- Datos de tránsito y movimientos migratorios (cédula migratoria)
- Datos sobre la salud (estado de salud, enfermedades contraídas o en curso, etc.)
- Datos biométricos (huella digital)
- Datos sensibles, especialmente protegidos (vida sexual, religión, origen étnico, etc.)
- Datos personales de naturaleza pública (firma de servidores públicos, fotografía de servidores públicos, etc.)

Cabe señalar que al ser información inherente a las personas, ello la vuelve identificable y su identidad podría determinarse ante un cruce de

[27] (Instituto Nacional de Transparencia, s.f.) Instituto Nacional de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, Protege tus datos personales. [Versión digital], [Consulta en agosto 2020]. Véase en: http://www.infodf.org.mx/index.php/protege-tus-datos-personales/preguntas-frecuentes.html

información en relación a su identificación, fisonomía o aspectos económicos[28].

1.6.2.1 Diferencia entre "transmisión" y "transferencia" de datos

En atención a la relevancia del desglose del tipo de información generada por un individuo, resulta necesario diferenciar el concepto de "transmisión" y "transferencia" de datos personales, pues jurídicamente ambos conceptos son completamente diferentes:

- la Federación Nacional de Comerciantes de Colombia indica que: *"...la transmisión de datos es aquella que involucra la comunicación de datos personales fuera o dentro del territorio nacional entre un Responsable del Tratamiento y un Encargado, para que este último realice el tratamiento de esos datos por cuenta del primero."*[29]
- el Artículo 5.1.s del Reglamento de la Ley Orgánica de Protección de Datos (RLOPD) Española define la transferencia como *"...una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable..."*[30] y se perfecciona cuando el responsable se ubique en un país y envíe los datos a otro fuera del país; lo cual quedará a reserva de los países el tratamiento de los datos en función a los acuerdos internacionales y su legislación.

Bajo esta tesitura, se denota que la diferencia radica en la ubicación o destino de la información (encargado), respecto al responsable; razón por lo cual parte de una nueva responsabilidad o proceso a asumir por parte del responsable: la creación de un nuevo *Contrato de Transmisión o Transferencia de Datos Personales,* que debe de contener de forma mínima lo siguiente:

- Las medidas de seguridad tecnológicas o físicas sobre los canales de transmisión
- Las finalidades de uso autorizado por el titular

---

[28] ...la identidad podría determinarse directa o indirectamente a través de cualquier información como puede ser nombre, número de identificación, datos de localización, identificador en línea o uno o varios elementos de la identidad física, fisiológica, genética, psíquica, patrimonial, económica, cultural o social de la persona… (Idem.)

[29] ((FENALCO), 2018) Federación Nacional de Comerciantes de Colombia (FENALCO), Superindustria se pronuncia sobre los elementos esenciales del contrato de transmisión de datos personales, [publicación web], [Consulta agosto 2020]. Véase en: http://www.fenalco.com.co/gesti%C3%B3n-jur%C3%ADdica/superindustria-se-pronuncia-sobre-los-elementos-esenciales-del-contrato-de

[30] ((LOPD), 2018) Ley Orgánica de Protección de Datos (LOPD). [Versión digital] [Consulta en enero 2020]. Véase: *https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf*

- Las medidas de seguridad a implementar por el encargado para evitar la alteración, sustracción y / o destrucción no autorizados
- Los canales para ejercer los derechos del titular
- El uso de la información al término del contrato
- La responsabilidad jurídica por el incumplimiento del contrato ante el Tratamiento de los datos, ante fugas, alteraciones y / o acceso no autorizado
- Duración de la conservación de la información
- Permisos de transmisión y/o transferencia de datos
- Desglose del ente jurídico responsable.

De esta manera, se pretende brindar un amplio espectro de protección jurídica contractual que celebren las partes ante una vulneración; sin embargo, ello no exime de la responsabilidad del Responsable ante el titular en caso de una vulneración o uso no acordado de parte del Encargado, por lo que de celebrar el Contrato adecuadamente todas las partes quedan sujetas a lo estipulado y con protección de la legislación vigente, con lo cual se minimiza el desentendimiento o deslinde de responsabilidad por cualquiera de las partes.

Aunado a ello, es necesario conocer el ciclo del uso de los datos personales para entender el impacto y alcance de este tipo de Contrato.

1.6.2.2 Ciclo de uso de los datos personales

De acuerdo con la Agencia Española, existe un *ciclo de vida de los datos personales* dividido en dos etapas:

- Primera: "*Captura de datos para su tratamiento* (formularios web o físicos, grabaciones de audio y video, redes sociales, sensores*), clasificación o almacenamiento interno, tratamiento* (operaciones realizadas de forma automatizados o manuales), y *la cesión o transferencia* a un tercero (traspaso o comunicación en cualquiera de sus formas)".
- Segunda: "*Destrucción o eliminación* de los datos almacenados a fin de que estos no puedan ser recuperados de los soportes de almacenamiento".

Con ello en consideración, para la elaboración de un Contrato de Transmisión o Transferencia de Datos Personales será necesario que ambas

partes ubiquen la etapa en la que se encuentran, y con ello desarrollar –conforme a sus actividades y finalidades- la creación del Contrato con las premisas de la primera etapa y sumar la segunda, respecto al tiempo para la eliminación o destrucción definitiva de los datos en los sistemas de gestión.

1.6.2.3 Justificación de la implementación de estándares normalizados para el tratamiento de datos personales en sistemas digitales

Considerando que los datos personales son toda aquella información que identifica a una persona, es necesario que tanto los responsables como los encargados de tratamiento implementen sistemas o funciones estandarizadas en la seguridad de la información. Pues además de cumplir con marcos normativos internos y por mandato de su normativa, la implementación de *buenas* prácticas.

En el caso de México, debe de recordarse que el 12 de junio de 2018 se publicó en el Diario Oficial de la Federación el decreto por el cual se aprueba la adherencia al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del 28 de enero de 1981 (Convenio 108), y su Protocolo Adicional del 8 de noviembre de 2001, relativo a las autoridades de control y a los flujos transfronterizos de datos; por lo que las entidades en el país deben atender a los *Principios básicos para la protección de datos* (artículo 4o y 5o); todos los países adheridos al Instrumento tienen el compromiso de adoptar las medidas necesarias para "...h*acer efectivo lo establecido en el documento desde el momento de su vigencia..."* (Art. 4o) basados en el principio de Calidad de los datos para el tratamiento automatizado (art. 5). Lo cual permitiría lograr un equilibrio entre la protección de los datos personales y el libre flujo de información personal entre países, con el fin de coadyuvar al flujo del comercio internacional.

De esta forma y a manera de explicación, el Convenio 108[31] exige que toda información de las personas deberá de:

- Ser obtenida y tratada de forma leal y legítima

[31] Convenio 108. Ibidem. Artículos 4o y 5o (p. 3).

- Registrar las finalidades determinadas y legítimas, y no se utilizaran de una forma incompatible con dichas finalidades

- Ser adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado

- Ser exactos y si fuera necesario puestos al día, y

- Se conservarán bajo una forma que permita la identificación de las personas concernidas durante un periodo de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado

Ello remonta a que actualmente, en México ya se tiene la legislación aplicable y los medios de jurisdicción en caso de una vulneración; por lo que, con atención a la globalización y a la intención del Convenio 108 sobre no obstrucción del comercio internacional por la información, vale la pena que las entidades jurídicas, independientemente que sean gubernamentales o privadas, incluyan mejores prácticas y recomendaciones emitidas por organizaciones especializadas en la materia, pues el objetivo en sí es la protección de los derechos del individuo y un derecho humano; y no la salvaguarda de los Responsables sin atención al individuo.

1.6.3 Uso de los datos personales en México

De acuerdo con el Instituto Nacional de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, toda persona tiene el derecho fundamental de la *Autodeterminación informativa,* es decir; la facultad de las personas de aplicar control a sus datos personales en posesión de terceros, conocer la finalidad de captación, uso, vigencia de uso y responsable del tratamiento con la finalidad de "*proteger su dignidad e intimidad" y con ello, evitar el uso ilícito e indiscriminado*[32]*,* lo cual se denomina tratamiento de datos.

[32] Instituto Nacional de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, Conceptos, [Versión digital], [Consulta julio 2020]. Véase en: http://www.infodf.org.mx/index.php/protege-tus-datos-personales/preguntas-frecuentes.html
Ibidem. "Autodeterminación informativa: Es un derecho fundamental del individuo, a través del cual éste puede ejercer un conjunto de controles sobre sus datos personales cuando éstos se encuentran en posesión de otras instancias (públicas y privadas). Este derecho le permite al titular de los datos conocer y controlar qué datos de su persona han sido recabados, para qué finalidad o motivo, cuál será el uso

Es decir, cada ente jurídico determinará (*principio de responsabilidad proactiva*[33], RGPD) el nivel de agregación o segregación de datos sobre el registro de actividades de tratamiento a razón de su finalidad y las bases jurídicas aplicables

Así, se puede identificar a las figuras jurídicas del tratamiento de datos personales en México:

1.6.4 Figuras del tratamiento de datos personales

Ambas leyes en la materia mexicana, la Ley Federal de Protección de Datos Personales en Posesión de Particulares[34] (LFPDPPP) y la Ley General Protección de Datos Personales en Posesión de Sujetos Obligados[35] (LGPDPPSO), en vista a la responsabilidad jurídica de las personas físicas o morales que realicen tratamiento de datos personales, la legislación nacional y los instrumentos internacionales, se configuran las siguientes figuras para la determinación de responsabilidad[36], de acuerdo al Info CDMX el:

- ***Titular**: es la persona física titular de los datos;*
- ***Responsable**: es cualquier persona física o moral, autoridad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos, que*

---

específico que se les dará, cuál será la vigencia de su uso y quién es responsable de su tratamiento (recolección, integración, resguardo). Todo ello con el objetivo de poder proteger su dignidad e intimidad evitando el uso ilícito e indiscriminado de su información personal, y tener la posibilidad de otorgar su consentimiento expreso, si así lo considera pertinente, para la cesión y transferencia de dichos datos a tercero"

[33] Idem. Principio de responsabilidad proactiva, "...un principio ya introducido en 1980 por la OCDE en el Código de Conducta o Guías de Protección de la Privacidad y flujo transfronterizo de datos personales o Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales y en el año 2010 por el Grupo de Trabajo del artículo 29 a través de la opinión 3/2010 sobre el principio de la Responsabilidad Proactiva o "Principio de Accountability". En este informe el GT 29 presentó una propuesta concreta para introducir el principio de "Responsabilidad Proactiva" en la normativa de protección de datos, de tal forma que los responsables del tratamiento pongan en marcha procedimientos y medidas eficaces para garantizar el cumplimiento de los principios y obligaciones establecidos en la Directiva, y poder así demostrar ante las autoridades el cumplimiento de la misma. Véase en https://www.oecd.org/sti/ieconomy/15590267.pdf y https://ec.europa.eu/newsroom/article29/news-overview.cfm?searchfield=3%2F2010#

[34] Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicación en el Diario Oficial de la Federación, el de julio de 5 de julio de 2010. [Versión digital] [Consultada en junio 2019]. Véase en: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

[35] Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicación en el Diario Oficial de la Federación el 26 de enero de 2017. [Versión digital] [Consultada en junio 2019]. Véase en: https://dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

[36] Instituto Nacional de Transparencia… (Idem).

decida y determine finalidad, fines, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de datos personales;

- ***Usuario**: es el autorizado por el responsable y parte de la organización del sujeto obligado, que dé tratamiento y/o acceda a los datos y/o a los sistemas de datos personales;*
- ***Encargado**: es la persona física o jurídica, pública o privada, ajeno al responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable; y*
- ***Oficial de Datos Personales**: es el especialista en materia de Protección de Datos Personales, quien tiene, entre otras atribuciones, auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales; asesorar a las áreas del sujeto obligado en materia de protección de datos personales; registrar ante el Instituto los sistemas de datos personales, así como su modificación y supresión; y hacer las gestiones necesarias para el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales en posesión del responsable*[37].

De esta forma, se puede visualizar que el país al adherirse al Convenio, adoptó los principios, estructura e intenciones para el uso mexicano; por ello, se denota cierta similitud entre el documento internacional y la legislación del país. Planteado el origen de la base normativa, se deben de comprender los principios del tratamiento con la finalidad de comprender el uso, impacto y alcance de un tratamiento “no adecuado”.

1.6.5 Principios del tratamiento de datos personales

Conforme al Convenio 108, los países deben velar por el cumplimiento del instrumento desde el momento de su vigencia (art. 4o) basados en:

1. Principio de *Calidad* (art. 5): todos los datos se obtendrán y tratarán leal y legítima; se registraran para finalidades determinadas y legítimas, y no se utilizaran de una forma incompatible con dichas finalidades; serán adecuados, pertinentes y no excesivos en relación con las finalidades

[37] (Instituto Nacional de Transparencia, s.f.) Instituto Nacional de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, Conceptos, protege tus datos. [Versión digital] [Consulta marzo 2020] Véase en: http://www.infodf.org.mx/index.php/protege-tus-datos-personales/preguntas-frecuentes.html

(proporcionalidad); serán exactos y si fuera necesario puestos al día; y se conservarán bajo una forma que permita la identificación de las personas durante el periodo necesario para las finalidades registradas.

2. *Categorías particulares de datos* (art 6): la información que revele el origen racial, la opinión política, la convicción religiosa, condenas penales, datos de salud y/o vida sexual "...*no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas...*".
3. *Seguridad de los datos* (art 7): Las entidades deberán implementar medidas de seguridad para la protección de datos personales registrados en ficheros automatizados contra la destrucción y/o pérdida accidental o no autorizada, así como para el acceso, modificación o difusión no autorizada.
4. *Garantías complementarias para la persona concernida* (art 8): Todo titular de datos deberá tener la posibilidad de:
    a. conocer la existencia de un fichero automatizado de datos personales, su finalidad, la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;
    b. obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos que le concierne, así como la comunicación de los datos en forma comprensible;
    c. obtener la rectificación o el borrado al momento de una infracción por un incorrecto tratamiento automatizado de la información respecto a los artículos 5o y 6o
    d. disponer de recursos ante una omisión de una petición de confirmación o, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo.
5. *Excepción y restricciones* (art 9): De acuerdo al Convenio, *no se admitirá excepción alguna en las disposiciones de los artículo 5, 6 y 8*, los que se encuentren en el artículo 2 y si hay una previsión en la Ley del país parte salvo que *constituya una medida necesaria en una sociedad democrática*: la protección de la seguridad del Estado, la seguridad pública, sobre los intereses monetarios del Estado o la

represión de infracciones penales; protección de la persona interesada y los derechos y libertades de otras personas.

Asimismo, sobre los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de los involucrados.

Finalmente, el Convenio en el artículo 10 estipula las sanciones y recursos convenientes *contra las infracciones de las disposiciones de derecho íntimo que hagan efectivos los principios básicos para la protección de datos;* haciendo hincapié en que *ninguna de las disposiciones del presente capítulo se interpretará en el sentido de que limite la facultad, o afecte de alguna otra forma a la facultad de cada Parte, de conceder a las personas concernidas una* ***protección más amplia*** que la prevista en el Convenio (Art 11).

En ese tenor, México estipula en la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) sobre la obtención del "...e*l consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca...*[38]" (Artículo 9). Asimismo, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados lo contempla en el artículo 3 fracción VIII, indicando el acto como la *"...manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos…*".

En ese sentido, el RGPD enumera una serie de obligaciones sobre el tratamiento de datos que la normatividad mexicana (LFPDPPP) estipula como bases de tratamiento[39]:

- Los avisos de privacidad deben ser de forma escrita, con lenguaje simple y de fácil acceso sobre el tratamiento de la información de los interesados (art 8 y 9). Ello aplica también para las transferencias internacionales de los datos (art 37)

[38] Ley Federal de Protección de Datos Personales en Posesión de Particulares, artículo 9. [Versión digital] [Consulta marzo 2020] Ibidem, p. Véase en: http://www.precisiontools.com.mx/LFPDPPP.pdf

[39] Ley Federal de Protección de Datos Personales en Posesión de Particulares Artículos 8,9, 19, 37, 20, 39 de y el Reglamento el artículo 45. [Versión digital] [Consulta marzo 2020]. Véase en: http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

- Designar un Delegado de Protección de Datos, también llamado responsable, quién decide sobre el tratamiento (art 3, fr XIV)
- Los responsables deberán registrar las actividades u operaciones de tratamiento -no contemplado expresamente en la LFPDPPP-
- Realizar análisis de riesgo del tratamiento realizado a fin de establecer medidas de prevención, planes de emergencia ante eventualidades y sus procedimientos (art 19)
- Notificar violaciones y vulneraciones de seguridad a los afectados y autoridades de forma inmediata (art 20)
- Evaluar impacto de los riesgos consumados sobre los productos y/o servicios que puedan superponer en riesgo la protección de datos de los afectados y con ello, adoptar acciones para la erradicación o minimización de estos; en el caso de México, este párrafo refiere a la prevención de riesgo respecto nuevas prácticas (art 39, fr X)
- Creación y diseño de bienes y servicios enfocados a la Privacidad e instaurar medidas de seguridad que garanticen la protección de la información bajo el principio de proporcionalidad (art 45 del Reglamento de la LFPDPPP) respecto a la necesidad de captación, su relevancia en relación a las finalidades.
-

De esta forma, se denota que la legislación mexicana pretende respaldar los derechos de los individuos, en especial a su dignidad; haciendo hincapié en los Derechos ARCO, respecto de los principios de tratamiento de datos personales; sin embargo, es posible que la sociedad actualmente no esté del todo consciente sobre la importancia y posible perjuicio que tendrían ante una vulneración o tratamiento no adecuado. Pues, la información entregada o generada a las plataformas y sistemas, en muchas ocasiones no es del todo clara respecto a su uso.

Capítulo 2.
Aplicación de la estandarización en el marco internacional

Capítulo 2. Aplicación de la estandarización en el marco internacional

De acuerdo a la Organización Internacional de Estandarización (ISO), el uso de la normalización permite a las empresas, gobierno y sociedad para el desarrollo sostenible en diferentes ámbitos: económico, ambiental y social y "*...las normas ISO hacen una contribución positiva al mundo en que vivimos, facilitan el comercio, diseminan el conocimiento, difunden los avances innovadores en tecnología, y comparten buenas prácticas de gestión y de evaluación de la conformidad...*"[40].

A nivel internacional, ISO ha realizado modelos de aplicación de las normas[41] en diferentes países; no obstante, para la comparativa del presente análisis se analizará el caso de Europa y Estados Unidos, desde la perspectiva jurídica y de normalización, con el objetivo de conocer y comparar la normativa mexicana; y de ser posible, buscar un punto de retroalimentación a los modelos normativos en relación a la protección de datos a nivel internacional.

2.1.1 Europa

Este continente se basa en los principios de: *utilización voluntaria de las normas, integración con normas internacionales, apertura y transparencia, participación de las partes y aseguramiento del consenso en el proceso de decisión*. Adicionalmente, la estandarización permite la eliminación de los obstáculos comerciales, sociales, ambientales y técnicos o tecnológicos, lo cual incrementa la competitividad de las empresas. Como resultado, en 2004 la Comisión Europea declaró que:

> "*...La Comisión, en colaboración con los organismos de normalización europeos, continuará fomentando el desarrollo de normas internacionales por los organismos internacionales de normalización apropiados y promoviendo su utilización. Cuando*

[40] (Normalización O. I., Guía para los organismos nacionales de normalización de ISO, 2010) Organización Internacional de Normalización, Guía para los organismos nacionales de normalización de ISO Involucrando a las partes interesadas y creando consenso, Publicación de diciembre 2010/3. [Versión digital] [Consulta marzo 2020]. Véase en: https://www.iso.org/files/live/sites/isoorg/files/store/sp/PUB100269_sp.pdf

[41] (Normalización O. I., Uso y referencia a normas ISO e IEC en reglamentación técnica, 2007) Organización Internacional de Normalización, Uso y referencia a normas ISO e IEC en la reglamentación técnica, publicación de 2007. [Versión digital] [Consulta marzo 2020]. Véase en: https://www.une.org/normalizacion_documentos/referencia_normas_iso_iec_reg_tecnica.pdf

existan normas internacionales, deberán, siempre que sea posible, transponerse de manera uniforme por las organizaciones de normalización europeas y utilizarse como base de la reglamentación comunitaria..."[42].

La política Europea[43] a nivel social destaca por promover la cooperación entre los países miembro, la coordinación y la aproximación de las políticas nacionales, participación de las autoridades locales, los sindicatos y las organizaciones patronales, por lo cual con la Proclamación del Pilar Europeo de Derechos Sociales en Gotemburgo (noviembre de 2017), la Agenda Europea situó como epicentro de su política social a los ciudadanos, conocido como *citizens first*.

En ese contexto, la Unión Europea presentó tres iniciativas versadas en los Derechos Sociales de Gotemburgo, las cuales destacan en:

- la legislación armonizada en materia de protección de los Consumidores y el Reconocimiento Mutuo de normativas nacionales de productos no armonizados, denominada "*Lex Goods"*
- actualización de normas comunitarias para protección de los consumidores (Acciones Representativas para la Defensa de Intereses Colectivos de los Consumidores", denominado "Paquete `A New Deal for Consumers´", y
- la propuesta de contratos de compraventa de bienes y servicios vía electrónica y tradicional, así como de los Contratos de Contenidos Digitales llamado "*Paquete Legislación de Contratos"* o *"Contract Law"*

Dicha normativa es destacable debido a que además de innovar la auto regulación jurídica sobre la protección de datos personales en relación la normativa vigente; sin embargo, las instituciones y organizaciones que han logrado la combinación del *soft-law*[44]*,* con la finalidad de respetar los derechos

[42] Ibidem.

[43] (Ministerio de Asuntos Exteriores, 2018) Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, Políticas Comunes de la Unión Europea, [Versión digital] [Consulta marzo 2020]. Véase en http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/UnionEuropea/Paginas/Pol%C3%ADticas-comunes-de-la-Uni%C3%B3n-Europea.aspx

[44] (Española, 2020) Real Academia Española (RAE), [Versión digital] [Consulta en marzo 2020]. Véase: https://dpej.rae.es/lema/soft-law#:~:text=Conjunto%20de%20normas%20o%20reglamentaciones,de%20conducta%2C%20principios%2C%20etc. Ibidem. Definición de Soft Law: "*Int, Priv. Conjunto de normas o reglamentaciones no vigentes que pueden ser consideradas por los operadores jurídicos en materias de carácter preferentemente dispositivo y que incluye recomendaciones, dictámenes, códigos de conducta, principios, etc. Influyen asimismo en el desarrollo legislativo y pueden ser utilizadas como referentes específicos en la actuación judicial y arbitral.*

humanos y el uso de la normalización como estrategia jurídica y comercial en el bloque económico ya sea nacional o internacional.

Asimismo, la Asociación Española de Normalización y Certificación[45] (AENOR), este continente se distingue por la aplicación de los *"requisitos esenciales" para los productos y servicios*[46] *(*en cumplimiento al artículo 5 de la Directiva 1999/5/CE sobre equipos radioeléctricos y equipos terminales de telecomunicación) sobre la protección a la salud y la seguridad debido a que *los procedimientos e infraestructura que apoyan estas directivas ya están muy desarrollados y garantizan un funcionamiento eficaz en los diferentes sectores,* lo cual es denominado "legislación Nuevo Enfoque", la cual se rige con los siguientes principios:

- Formatos y redacción que permite la aplicación voluntaria de normas "*como medio"* de cumplimiento de las obligaciones legales en razón del producto y sus riesgos. Puede o no, contener requisitos de cumplimiento,
- *"...Una vez que las directivas se redactan y aprueban por el proceso legislativo europeo, comienza un diálogo con los organismos de normalización europeos..."*
- El proceso es el siguiente: la Comisión redacta una solicitud formal -de lo que los organismos de normalización- de lo consideradas como "*necesarias y apropiadas"* y denominada *"Mandato de Normalización"*. Dicho documento es creado por comités (representantes gubernamentales europeos) de expertos del campo a regular y por los comités de política de normalización amplia. Una vez que es aprobada la solicitud, los organismos de normalización organizará el trabajo para la aplicación a los países miembro. Las normas utilizadas como apoyo serán utilizadas por consultores independientes y verificar si cumplen con lo reglamentario. Finalmente, la Comisión Europea emite una documentación oficial y se publica en su portal de Internet.

Int. Púb. Actos jurídicos que sin fuerza vinculante obligatoria contienen las pautas inspiradoras de una futura regulación de una materia, abriendo paso a un posterior proceso de formación normativa".

[45] Asociación Española de Normalización y Certificación, Uso y referencia a normas ISO e IEC en la reglamentación técnica, Publicación de 2007. [Versión digital] [Consulta agosto 2020]. Véase en: https://www.une.org/normalizacion_documentos/referencia_normas_iso_iec_reg_tecnica.pdf

[46] Ibidem. P.20.

- Al existir una normativa, los fabricantes pueden elegir la utilización de las normas voluntarias y con ello, garantizar la observación legal

Cabe señalar, que el uso de las normas confieren la *"presunción de conformidad"* sobre el cumplimiento legal y reglamentario. La clave del Nuevo Enfoque es que "...*es un modelo específico de legislación de probada eficacia que combina de manera adecuada el interés público (es decir, la protección de la salud y la seguridad de las personas, la protección de los consumidores y la protección del medio ambiente) y el interés de las organizaciones privadas que producen las normas (de productos y servicios) de acuerdo con el estado del arte...*[47]*"*. Con ello, se crean "...*formas de legislar más flexibles y menos estrictas...*"[48] acordes a las necesidades reales con un marco reglamentario.

En ese sentido, el modelo de la *autodeterminación* en Europa ha brindado beneficios en los campos, que por su naturaleza, requiere de expertos y el cumplimiento de las normativas jurídicas, siendo así el campo de aplicación el de las Tecnologías de la Información y Comunicación, medio ambiente y la protección de los consumidores. La Comisión Europea prevé la expansión de este modelo de gobernanza al sector de servicios.

2.1.2 Estados Unidos

A raíz de los ataques terroristas del 11 de septiembre de 2001, con la aprobación de la Ley Patriota, el país permite el intercambio de los datos personales de todo individuo que sea sospechoso de participación en actividades de blanqueo de dinero o terrorismo; lo cual amplió la posibilidad de acceder y compartir información personal. No obstante, el Tribunal Supremo de Estados Unidos reconoció el derecho a la intimidad con arreglo a su Constitución, pese a que su Carta Magna no lo contenga de forma explícita muchos estados establecen medidas de protección de la privacidad en sus propias constituciones. Sin embargo, solo California extendió la protección de datos de una interferencia del gobierno a una obligación del sector privado.

Por otro lado, al ser miembro de la Organización Mundial del Comercio (OMC), este país es responsable de verificar que las actividades de normalización sean totalmente conformes con el Acuerdo de la OMC sobre

[47] Idem, p. 20.
[48] Idem, p. 20.

Obstáculos Técnicos al Comercio (OMC/OTC), mismo que funge como un estándar de uso de las normas, generalmente utilizados como normativa internacional o base de reglamentación técnica.

Es pertinente señalar que esta nación es el principal redactor y usuario de las especificaciones y normas, su estimación se eleva a más de 44,000 leyes, reglamentos técnicos y especificaciones diferentes; en tanto que las normas emitidas por el sector privado del continente se estima a 50,000 normas. No obstante, de acuerdo a la Organización Internacional de Estandarización, su base de estandarización parte del consenso y adscripción voluntaria de los organismos.

Es de mencionar que aproximadamente 200 normativas están acreditadas por el Instituto Nacional Estadounidense de Estándares (ANSI) para desarrollar Normas Nacionales Americanas (ANS); adicionalmente, los catálogos de las ISO e IEC son consideradas "...*potencialmente utilizables en la reglamentación por las agencias del gobierno federal estadounidense o se pueden referenciar si se considera apropiado...*"[49].

Algunos de los usos de las normativas son: *adopción* voluntaria parcial o total en la reglamentación interna; *firme adhesión* a la norma específica en el programa reglamentario salvo prueba de uso innecesario; *base reglamentaria,* asequible a cambios considerados apropiados para posteriormente ser publicada en el Registro Federal como proyecto de reglamento; *guías reglamentarias,* no son obligatorias pero considerado un "medio aceptable"; *directrices* para el respeto de la normativa general y de consulta, aunque ello no exime de errores u omisiones a la reglamentación general; y *adhesión* en caso de que se determine innecesario el uso de un reglamento obligatorio y existe la voluntad de adhesión.

A diferencia del modelo europeo, la normativa estadounidense deben ser "...*rentables, coherentes, razonables y comprensibles y que el proceso reglamentario debe ser abierto, transparente y justo para todas las partes interesadas...*"[50] *y aceptables en el sector de salud, seguridad de los productos, seguridad de los usuarios u operadores, medio ambiente,*

[49] Idem, p.
[50] Idem, p..

protección de los consumidores, y características de los productos, así como otros aspectos de interés público.

Adicionalmente, la política federal sobre el uso de la normalización debe estar armonizada con la Ley Nacional de Fomento y Transferencia de Tecnología (NTTAA, Ley pública 104-113), cuyo objetivo es el uso voluntario para el cumplimiento de los objetivos de las entidades, salvo sean ineficaces o contraria a la legislación aplicable.

Con esta precisión, se denota nuevamente el uso de las estandarización bajo el principio de la voluntad, consenso y colaboración de los organismos interesados; además de resaltar la confianza del gobierno federal a la normativa del sector privado. La circular A-119 de la Oficina de Gestión y Presupuesto (OMB) es la responsable de la participación federal en el desarrollo de estas normas en atención a los requisitos de la NTTAA.

2.1.2.1 Aplicación del "Escudo de Privacidad" de Estados Unidos

Con la emisión del Convenio 108 del Consejo de Europa, el 28 de enero de 1981; la Directiva 95/46/CE del Parlamento Europeo y del Consejo, el 24 de octubre de 1995, se configuraron como referentes internacionales sobre el tratamiento de datos personales. Sin embargo, el 12 de julio de 2016 se publicó en el Diario Oficial de la Unión Europea la "Decisión de Ejecución (UE) 2016/1250 de la Comisión con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU"[51] también conocido como "Escudo de Privacidad UE-EEUU".

Las bases y principios de este documento son las siguientes:

- *La Directiva 95/46/CE establece las normas que regulan las transferencias de datos personales desde los Estados miembros a terceros países en la medida en que tales transferencias se encuentren comprendidas en el ámbito de aplicación de dicho instrumento.*

[51] Decisión de Ejecución (UE) 2016/1250 De La Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU, Diario Oficial de la Unión Europea, publicación del 12 de julio de 2016. [Versión digital] [Consulta en abril 2020]. Véase en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D1250&from=DE

El artículo 1 y los considerandos 2 y 10 de la Directiva velan por el respeto de los derechos fundamentales, en especial del *respeto a la vida privada.*

- Conforme al artículo 25 apartado 1 de la Directiva, las naciones miembro autorizarán la transferencia de datos cuando garantice un nivel de protección adecuado y se cumplan con anterioridad las disposiciones de la Directiva. Será la Comisión la que garantice la aplicación de la Directiva en razón a la legislación interna y adscripciones internacionales en la materia. Es de señalar, que esta es una mínima aplicable y no se requiere alguna garantía adicional.

  Adicionalmente, el apartado 2 menciona que la evaluación legislativa del tercer país atenderá a las circunstancias, categoría de datos, normativa de derecho general y sectorial vigente.

  Para el cumplimiento de la Directiva en relación a Estados Unidos determina que los *«principios de puerto seguro para la protección de la vida privada»* serán aplicados conforme a la normativa del Departamento de Comercio de Americano*,* ya que *se considera que garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a organizaciones establecidas en Estados Unidos*[52]*.*

  En relación al puerto seguro, respecto a las Comunicaciones COM(2013) 846 y COM(2013) 847 final de 27 de noviembre de 2013, la Comisión consideró que su fundamento debía revisarse y reforzarse al marco de una serie de factores: *aumento exponencial de los flujos de datos y su importancia fundamental para la economía transatlántica, el rápido crecimiento del número de empresas estadounidenses que se adhieren al régimen de puerto seguro y la nueva información sobre la escala y el alcance de determinados programas de inteligencia de EE. UU. que suscitan dudas en cuanto al nivel de protección que se puede garantizar.*

  Adicionalmente, la Comisión identificó insuficiencias y deficiencias de puerto seguro de los trabajos del Grupo de Contacto de Estados Unidos por lo que emitió 13 recomendaciones con la finalidad de *fortalecer los*

[52] Ibidem. Artículo 25, apartado 2 de la Decisión 2000/520/CE

principios sustantivos de privacidad e incrementar la transparencia de las políticas de privacidad de las empresas auto certificadas de los EE. UU.; mejorar y hacer más eficaz el control por parte de las autoridades estadounidenses del cumplimiento de los principios por las empresas; facilitar mecanismos de resolución de conflictos para las reclamaciones de los ciudadanos; y garantizar que el recurso a la excepción en ámbitos de seguridad nacional, contemplada en la Decisión 2000/520/CE se limita a lo estrictamente necesario y proporcionado.

- En la sentencia del asunto C-362/14, Maximillian Schrems/Data Protection Commissioner del 6 de octubre de 2015, el Tribunal de Justicia de la Unión Europea *declaró inválida la Decisión 2000/520/CE* sin examinar el contenido de los *principios de puerto seguro para la protección de la vida privada;* pues *el Tribunal observó que la Comisión no había manifestado en dicha Decisión que los Estados Unidos «garantizarán» efectivamente un nivel de protección adecuado en razón de su legislación interna o de sus compromisos internacionales.* Ante ello, el Tribunal explicó que:

  > *Si bien la expresión «nivel de protección adecuado» que figura en el artículo 25, apartado 6, de la Directiva 95/46/CE no significa un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la UE, debe entenderse en el sentido de que exige que el tercer país interesado garantice efectivamente un nivel de protección de las libertades y derechos fundamentales «sustancialmente equivalente» al garantizado en la Unión por la Directiva 95/46/CE, entendida a la luz de la Carta de los Derechos Fundamentales. Aunque los medios de los que se sirva ese tercer país para garantizar dicho nivel de protección pueden ser diferentes de los aplicados en la Unión, deben ser eficaces en la práctica.*

Adicionalmente, el Tribunal de Justicia criticó que la Decisión 2000/520/CE *no contuviera constataciones suficientes sobre la existencia en Estados Unidos de normas estatales destinadas a limitar las posibles injerencias en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a Estados Unidos, injerencias que estuvieran*

autorizadas a llevar a cabo las entidades públicas de ese país cuando persigan fines legítimos, como la seguridad nacional, y sobre la existencia de una tutela judicial efectiva contra injerencias de esa naturaleza.

En ese sentido, la Comisión en 2014 inició conversaciones con las autoridades de Estados Unidos en relación al tema de puerto seguro y las recomendaciones emitidas mediante la COM (2013) final y consideraciones de la sentencia C-362/14 de Schrems dando como resultado el cumplimiento del artículo 25 de la Directiva 95/46/CE, mismas que fueron publicadas en el Registro Federal de Estados Unidos y resumidas en lo siguiente: observancia de los principios de privacidad (anexo II)*, así como los compromisos y declaraciones oficiales de diversas autoridades estadounidenses recogidos en los documentos de los anexos I y III a VII, constituyen el denominado «Escudo de la privacidad UE-EE. UU.»* Con lo cual, la Comisión determinó que con base a los considerandos 136 a 140 *los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU. desde la Unión a entidades auto-certificadas establecidas en los Estados Unidos*[53]*.*

Es menester mencionar los principios del "Escudo de la Privacidad": basado en un *sistema de autocertificación por el que las entidades estadounidenses se comprometen a cumplir una serie de principios de protección de la vida privada* aplicable a los responsables, encargados *obligados contractualmente a actuar únicamente siguiendo instrucciones del responsable del tratamiento de la UE y asistir a este último a responder a las personas físicas que ejerzan sus derechos con arreglo a los principios.* Ello, no tendrá perjuicio de la aplicación de la Directiva 95/46/CE y permite que se *autoricen las transferencias de un responsable o encargado del tratamiento en la Unión a organizaciones de los Estados Unidos que hayan autocertificado su adhesión a los principios con el Departamento de Comercio y se hayan comprometido a atenerse a ellos;* sin embargo, precisa que los principios aplican al tratamiento de datos realizados por entidades estadounidenses *siempre que el tratamiento no entre en el ámbito de aplicación de la legislación de la Unión.*

---

[53] Idem.

Cabe señalar que los *principios se aplicarán inmediatamente después de la certificación* salvo -en relación con el principio responsabilidad ulterior- cuando existan relaciones comerciales preexistentes con terceros y la entidad decida autocertificarse, por lo que *la organización estará obligada a hacerlo lo antes posible, y en cualquier caso en un plazo máximo de nueve meses a partir de la autocertificación, siempre que ello tenga lugar en los dos primeros meses siguientes a la fecha en que se haga efectiva la cobertura de del Escudo de la privacidad.* Durante este plazo, la entidad deberá aplicar *el principio de notificación y opción (que permite al interesado de la UE la exclusión voluntaria) y, cuando se transfieran datos personales a un tercero que actúe como agente, deberá comprobar que este ofrece al menos el mismo nivel de protección que exigen los principios.*

- El **principio de notificación** refiere a informar a los interesados el tratamiento de sus datos, la publicación de las políticas de privacidad, enunciar *enlaces al sitio web del Departamento de Comercio (con información más detallada sobre la autocertificación, los derechos de los interesados y los mecanismos de recurso existentes) y un proveedor de modalidades alternativas de solución de conflictos.*
- El **principio de integridad de los datos y de limitación de la finalidad**, estos *deberán limitarse a lo pertinente para la finalidad del tratamiento, tener fiabilidad para el uso previsto y ser exactos, completos y actuales.* Además, no se podrá realizar un tratamiento de datos con fines incompatibles que motivaron su recolección o la autorización de su uso del interesado de forma posterior.
- El **principio de seguridad** refiere a que las entidades *que creen, mantengan, utilicen o difundan datos personales deberán tomar medidas de seguridad «razonables y adecuadas», habida cuenta de los riesgos asociados al tratamiento de los datos y la naturaleza de estos.* En el caso de subtratamiento, se deberá celebrar previamente un contrato que *garantice el mismo nivel de protección que el proporcionado por los principios de privacidad, y tomar medidas para asegurar su debida aplicación.*
- *El* **principio de acceso** *reconoce el derecho de los interesados a que, sin necesidad de una justificación ni tener que abonar una tasa*

excesiva, una entidad les confirme si trata datos personales relacionados con ellos y les comunique los datos en cuestión en un plazo razonable; ello, únicamente podrá *restringirse en circunstancias excepcionales* y ser debidamente justificada y demostrativa sobre las mismas.

Adicionalmente, los interesados podrán *corregir, modificar o suprimir información personal cuando sea inexacta o se hayan incumplido los principios de privacidad en su tratamiento.* En el caso de entidades con tratamiento automatizado, se podrán *adoptar decisiones que afectan al individuo (por ejemplo, concesión de créditos, ofertas hipotecarias, empleo),* pues la legislación de E.U. tiene *protección específica contra las decisiones negativas.*

- *El **principio de recurso, aplicación y responsabilidad** refiere que las entidades deberán contar con mecanismos sólidos a fin de garantizar la observancia de los demás principios de privacidad y una vía de recurso para los interesados de la UE cuyos datos personales hayan sido tratados de manera irregular, incluida una tutela judicial efectiva. Es decir, cuando una entidad se haya autocertificado, adquiere la obligación de cumplir cabalmente los principios del Escudo de Privacidad y deberá de renovar anualmente su certificado y adoptar medidas que verifiquen sus políticas publicadas son aplicadas.*
- *Con base al **principio de responsabilidad de la transferencia ulterior**, "...sólo se podrán transferir datos: i) con fines limitados y específicos, ii) en virtud de un contrato (o de un acuerdo similar dentro de un grupo de empresas), y iii) únicamente si dicho contrato ofrece el mismo nivel de protección que el garantizado por los principios, lo que incluye el requisito de que la aplicación de los principios se limite únicamente a la medida necesaria a efectos de la seguridad nacional, la actuación policial y otros fines de interés público...". Ello va de la mano con el principio de notificación y el principio de opción, en caso de transferencia ulterior de datos "...especialmente protegidos", los titulares deberán dar su consentimiento expreso atendiendo al principio de integridad y de limitación de la finalidad; adicionalmente, deberán de tener el mismo nivel de protección y el tercero solo podrá*

tratar los datos personales que se le transfieran de manera que no sea incompatible con los fines que motivaron en un principio su recogida o que el interesado haya aprobado posteriormente.

Con la exposición de los principios del "Escudo de Privacidad", es notorio el respeto a los derechos determinados en el Convenio 108 y a la Directiva 95/46/CE, siendo así que las Autoridades de Protección de Datos (APD) en Estados Unidos es el Departamento de Comercio, quien publica anualmente una lista de las entidades con auto-certificación vigente y un listado de las que hayan sido eliminadas de la lista y su razón de eliminación (expiración del certificado o baja voluntaria). Ello denota un nuevo modelo de regulación jurídica apegada a los principios y estructura de regulación, y considerando que Estados Unidos es una de las potencias mundiales, se denota la intención de respeto de los Derechos Humanos y una entidad que regula y vigila el apego a la legislación eje –internacional- que impacta a terceras naciones.

En ambos casos, el Departamento de Comercio verificará que estas entidades "...*van a devolver, borrar o conservar los datos personales recibidos anteriormente en virtud del marco. Si conservan estos datos, las entidades están obligadas a seguirles aplicando los principios*. *En los casos en que el Departamento de Comercio haya eliminado del marco a entidades debido a un persistente incumplimiento de los principios, se asegurará de que estas entidades devuelvan o supriman los datos personales recibidos..."*[54].

Adicionalmente, el Departamento de Comercio realizará revisiones permanentes del cumplimiento de las entidades auto certificadas, aplicará revisiones ante denuncias específicas (no frívola) por la omisión de respuesta de alguna solicitud de información de una entidad o cuando existan pruebas creíbles que sugieran el no cumplimiento de los principios.

De esta forma, es necesario reconocer y reflexionar que la sociedad de la información contrae la habilitación de los Derechos Humanos y replantea el alcance sistémico de los riesgos delictivos tradicionales y adiciona un encuadre a lo delictivo en el mundo digital, por lo que se requiere de una

[54] *Idem.*

gobernanza en la Internet adecuada o el apego al *soft law* en vista del avance tecnológico.

2.1.3 México

De forma comparativa, en México la normalización está regida por la voluntad y el cumplimiento obligatorio. Actualmente, es la Secretaría de Economía, mediante la Dirección General de Normas, al marco del artículo 39 para integrar el Programa Nacional de Normalización y numeral 54 de la Ley Federal de Metrología y Normalización (LFMN) está dirigido al uso común y repetido de la estandarización aplicable a *todos los productos, procesos, métodos, instalaciones, servicios o actividades deberán cumplir con las normas oficiales mexicanas*[55]*;* sin embargo, ante la naturaleza del derecho mexicano, existen tres tipos:

- las Normas Oficiales Mexicanas (Abreviada como: NOM, PROY-NOM o NOM-EM) son de observancia obligatoria, pues establecen l*as características y/o especificaciones que deban reunir los productos y procesos cuando éstos puedan constituir un riesgo para la seguridad de las personas o dañar la salud humana, animal, vegetal, el medio ambiente general y laboral, o para la preservación de recursos naturales … medir, los patrones de medida y sus métodos de medición, verificación, calibración y trazabilidad … especificaciones y/o procedimientos de envase y embalaje de los productos (*art. 40)
- las Normas Mexicanas (Abreviada como: NMX o PROY-NMX) regidas en el artículo 54 de la LFMN, cuyo uso es de "...*referencia para determinar la calidad de los productos y servicios de que se trate, particularmente para la protección y orientación de los consumidores...*[56]*";* no obstante, estas no pueden tener especificaciones inferiores a las Normas Oficiales. Dicha reglamentación es de adhesión voluntaria, y
- las Normas de Referencia, contenidas en el artículo 67 de la LFMN, son emitidas por la administración federal cuyo objetivo es *"...constituir*

[55] (Normalización L. F., 1992) Ley Federal de Metrología y Normalización, publicación del 1º de julio de 1992. [Versión digital], [Consulta en agosto 2020]. Véase en: https://www.gob.mx/cms/uploads/attachment/file/107522/LEYFEDERALSOBREMETROLOGIAYNORMALIZACION.pdf

[56] Ibidem. Artículo 38, apartado V.

comités de normalización para la elaboración de las normas de referencia conforme a las cuales adquieran, arrienden o contraten bienes o servicios..." estas serán utilizadas cuando las NOM o las normas internacionales no cubran los requerimientos de las mismas o las especificaciones de estas se consideren inaplicables u obsoletas

De acuerdo a la Secretaría de Economía, para el uso de la metrología en México se estableció el Sistema General de Unidades de Medida, el Sistema Nacional de Calibración y el Centro Nacional de Metrología, cuyo objetivo es establecer los requisitos para la fabricación, importación, reparación, venta, verificación y uso de los instrumentos para medir y los patrones de medida; así como establecer la obligatoriedad de la medición en transacciones comerciales e indicar el contenido neto en los productos envasados.

En ese sentido, México realiza también la estandarización mediante los Organismos Nacionales de Normalización[57] (ONN) cuyo objetivo es la elaboración y expedición de normas en las materias inscritas en la Dirección General de Normas en observación al numeral 72 de la Ley de la materia. Dicha colaboración se realiza en colaboración con sectores interesados en comités, dependencias gubernamentales y la administración federal.

Actualmente, existen solo 10 ONN[58] en México:

- Sociedad Mexicana de Normalización (NORMEX)
- Instituto Mexicano de Normalización y Certificación (IMNC)
- Asociación de Normalización y Certificación (ANCE)
- Instituto Nacional de Normalización Textil (INNTEX)
- Organismo Nacional de Normalización y Certificación de la Construcción y Edificación (ONNCCE)
- Normalización y Certificación Electrónica (NYCE)

[57] (Economía, 2010) Secretaría de Economía, *Organismos Nacionales de Normalización*, [Versión digital], [Consulta en agosto 2020]. Véase en: http://www.2006-2012.economia.gob.mx/comunidad-negocios/normalizacion/nacional/procesos-de-normalizacion/organismo-nacionales

[58] (Normas, 2012) Dirección General de Normas, *Organismos Nacionales de Normalización*, publicación del 31 de julio de 2012. [Versión digital], [septiembre 2020]. Véase en: http://www.2006-2012.economia.gob.mx/files/comunidad_negocios/normalizacion/2012_07_31_ONN.pdf

- Consejo para el Fomento de la Calidad de la Leche y sus derivados (COFOCALEC)
- Centro de Normalización y Certificación de Productos (CNCP)
- Cámara Nacional de la Industria del Hierro y del Acero (CANACERO)
- Organismo Nacional de Normalización de Productos Lácteos, A.C. (ONNPROLAC)

Con el sistema mexicano, es posible ver una estructura de normalización similar a la estadounidense; sin embargo, es notoria la atención a la guía y apego de las reglas internacionales para la estandarización, con la distinción de la creación de normalización en entidades gubernamentales, ya que estas ejercen propiamente la autodeterminación interna; en tanto que los organismos externos, se apegan a las normas emitidas por la Secretaría de Economía y las emitidas por los ONN.

2.1.3.1 Consideraciones para la autorregulación en México para la Protección de Datos

La Secretaría de Economía y la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) crearon un estudio[59] en el que se analizó la autorregulación para la privacidad de los datos personales en las tecnologías de Comunicación en la que se destaca que la legislación mexicana si permite la autorregulación en sentido de minimización el sentido sancionatorio en caso de algún incumplimiento (art. 81 del Reglamento de la LFPDPPP).

Cabe señalar que la autorregulación en México en materia de Datos Personales se contempla del artículo 79 al 86 del Reglamento, cuyo uso de es de complementación a la legislación (art. 79), por lo que es necesario resaltar los siguientes puntos:

[59] Secretaría de Economía y la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI), *Estudio de la Autorregulación en Materia de Privacidad y Protección de Datos Personales en el Ámbito de las TI*, [Versión digital], [Consulta en septiembre 2020]. Véase en: https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_04.pdf

- La autorregulación funciona como incentivo reputacional *de buena calidad*[60] y confianza en el mercado; adicionalmente, en el artículo 105 del Reglamento de la Ley Federal de Metrología y Normalización promueve el "Premio Nacional de Calidad" como incentivo empresarial de modernización y competitividad[61]
- Los códigos para la autorregulación en México, también considerados códigos deontológicos, tienen la estructura de los Principios Nacionales de Privacidad[62] de Australia (npps por sus siglas en inglés) en modalidad de arbitraje
- En México, la representatividad no es un requisito obligatorio del sector, pues se ve como un acuerdo voluntario entre organizaciones (art. 79 RLFPDPPP); además, es considerado un facilitador de la aplicación legislativa (art. 86 RLFPDPPP)
- Existen diversos países -Alemania, Australia, España, Italia y Uruguay- que exigen la publicidad y registro de los códigos, para México deben ser registrados en términos del último párrafo del artículo 44 de la LFPDPPP (art. 86 del RLFPDPPP) ante el -hoy extinto- Instituto Federal de Acceso a la Información y Protección de Datos (IFAIPD)
- La revisión de los códigos no se encuentran estipulados en la legislación mexicana, pues no se indican fechas de término o vigencia de los códigos
- De acuerdo a la Secretaría de Economía, los códigos prevén fórmulas para evaluar periódicamente la eficacia de los instrumentos de autorregulación y miden "...*el grado de satisfacción de los afectados (...) Y actualizando el contenido para adaptarlo a la normativa general o*

---

[60] (Núñez E., s.f.) Núñez E., Javier y Lima, José Luis, *Incentivos Reputacionales para la Autorregulación: Un Análisis Experimental*, [Versión digital] [Consulta en septiembre 2020]. Véase en: http://www.econ.uchile.cl/uploads/publicacion/61f57e85-5657-4551-b53b-59a24c79baed.pdf

[61] (Normalización R. d., 1999) Reglamento de la Ley Federal de Metrología y Normalización. [Versión digital], [Consulta en septiembre 2020]. Véase en: http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo88524.pdf
Ibidem. Título sexto, artículo 105. *"…El Premio Nacional de Calidad será un instrumento para promover, desarrollar y difundir la calidad de los procesos industriales, comerciales, de servicios y sus productos, con el fin de apoyar la modernización y competitividad de las empresas establecidas en el país…"*

[62] (Australia, 2020) Privacy Act, Anexo 3, sobre las obligaciones de: 1) obtención 2) uso y revelación 3) calidad de la información 4) seguridad de la información 5) transparencia 6) acceso y corrección 7) identificador 8) anonimidad 9) Flujo transfronterizo 10) Información sensible. Ley publicada en 1988. [Versión digital], [Consulta en septiembre 2020]. Véase en: https://www.legislation.gov.au/Details/C2020C00168

sectorial...", México, aplica como tal la literalidad de la Ley y considera los códigos en caso de existir

- La legislación austriaca señala códigos *temporales o con alcance limitado,* la diferencia es que el primero tiene vigencia establecida y el segundo, permite cumplir operaciones de las entidades. En México no existe ningún precepto relativo a la videncia de los códigos

En comparativa, la Unión Europea (UE) con la Directiva de Protección de Datos Personales[63] al ser normas aprobada por las instituciones de la Unión, su naturaleza es de carácter obligatorio mediante el "Código de Conducta Europeo de la FEDMA, (Federation of European Direct and Interactive Marketing) sobre la utilización de datos personales en la comercialización directa" y se dirige a las actividades transnacionales de la sociedad de la información que promueve la UE. Sin embargo, para México, los códigos deben considerar los siguientes preceptos del Reglamento:

- *...las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos personales, que complementen lo dispuesto por la Ley, el presente Reglamento... (*art. 79); es decir, de carácter vinculante y voluntario
- La autorregulación se traduce *en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos y tendrán los siguientes objetivos*[64] (art. 80)*:*
    - Coadyuvar al cumplimiento del principio de responsabilidad
    - Establecer procesos y prácticas cualitativas para la protección de datos

[63] (Directiva 95/46/CE de Protección de Datos Personales del Parlamento Europeo y del Consejo, 1995) Directiva 95/46/CE de Protección de Datos Personales del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. [Versión digital], [Consulta en agosto 2020]. Véase en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

[64] (Particulares R. d., 2011) Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicación del 5 de julio de 2010, Capítulo VI De la Autorregulación Vinculante. [Versión digital], [Consulta en septiembre 2020]. Véase en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

    - Fomentar que los responsables establezcan políticas, procesos y buenas prácticas para el cumplimiento de los principios
    - Promover que los responsables voluntariamente cuenten con constancias o certificaciones de observancia legislativa
    - Identificar a los responsables con políticas de privacidad alineadas al cumplimiento de los principios y derechos previstos, así como de competencia laboral
    - Facilitar la coordinación entre los esquemas de autorregulación reconocidos internacionalmente
    - Facilitar las transferencias de datos entre responsables con autorregulación
    - Promover el compromiso de los responsables con la rendición de cuentas y adopción de políticas internas consistentes con criterios externos, así como auspiciar mecanismos para implementar políticas de privacidad (herramientas, transparencia, supervisión interna continua, evaluaciones de riesgo, verificaciones externas y sistemas de remediación)
    - E*ncauzar mecanismos de solución alternativa de controversias entre responsables, titulares y terceras personas, como son los de conciliación y mediación.*
- La adhesión a estos esquemas será considerada para la atenuación de la sanción en caso de algún incumplimiento
- Los esquemas de autorregulación deben considerar (art. 82):
    - El ámbito de aplicación
    - Procedimientos o mecanismos para la aplicación eficaz y la medición de la eficacia
    - Sistemas de supervisión y vigilancia interna y externa
    - Programas de capacitación para quienes traten los datos personales
    - Mecanismos para facilitar el ejercicio de derechos de los titulares
    - Identificación de las personas físicas o morales adheridas, que posibilite reconocer a los responsables que satisfacen los requisitos de la autorregulación, y
    - Las medidas correctivas eficaces en caso de incumplimiento

- La certificación deberá ser otorgada alguna certificadora conforme a los parámetros del artículo 43, fracción V de la Ley, y
- Los esquemas de autorregulación notificados en términos del último párrafo del artículo 44 de la Ley formarán parte de un registro, que será administrado por el Instituto y se incluirán los que con los requisitos del artículo 43, fracción V de la Ley

Respecto a las mejores prácticas para la Protección de Datos, la Secretaría de Economía en México refiere que en el Reino Unido coexisten dos tipos de códigos deontológicos: los emitidos por la autoridad encargada de aplicar la Ley de la materia (*Data Protection Act* 1998, LPD1998), y la proveniente de asociaciones de comercio previa presentación, consideración y opinión del Comisionado de la *Information Commissioner's Office* (ICO).

La dependencia mexicana resalta que el *Personal information online code of practice*[65] o Código de Buenas Prácticas sobre Datos Personales *"...es uno de los códigos más completos, concisos e ilustrativos de aquellos que fueron analizados en la región de la UE, tomando en consideración además que incorpora recomendaciones sobre comercio electrónico..."*[66].

Dicho documento contiene información sobre: la recopilación de datos personales a través de formularios en línea; uso de cookies o direcciones IP para dirigir contenidos (segmentación); uso de datos personales para comercializar productos o prestar servicios; y uso de instalaciones de *cloud computing*[67] para tratar datos personales.

El *Código de Buenas Prácticas para el Intercambio de Datos*[68] en el que se enfoca en la transferencia de datos y legislación aplicable; licitud y transparencia; Seguridad Normativa interna (Governance); Derechos de los titulares; Facultades de la autoridad y sanciones Notificaciones a la ICO ante intercambios; Acceso a la información; y Convenios de intercambio. Ello

---

[65] ((ICO), 2011)), Personal information online code of practice, emitido el 26 de mayo de 2011. [Versión digital] [Consulta en agosto 2020] Véase en: https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf

[66] (Sic.)

[67] (Oracle, s.f.) Definición*, ¿Qué es el cómputo en la nube?,* [publicación web] [Versión digital], [Consulta en septiembre 2020]. Véase en: https://www.oracle.com/mx/cloud/what-is-cloud-computing/
Ibidem. "*Cuando una empresa elige `moverse a la nube´, significa que su infraestructura de TI se almacena fuera de sus instalaciones, en un centro de datos mantenido por el proveedor de cómputo en la nube (como Oracle). El proveedor de la nube tiene la responsabilidad de administrar la infraestructura de TI del cliente, integrar aplicaciones y desarrollar nuevas capacidades y funcionalidades para adecuarlas al ritmo de las demandas del mercado..."*

[68] Ibidem.

permite evitar la "...transferencia incontrolada de datos..." pues *"...es una de las prácticas que genera mayores riesgos contra la seguridad de los datos personales..."*, afirma la Secretaría de Economía.

La autoridad mexicana señala que la aplicación de los códigos ICO o sus recomendaciones "… no garantiza el cumplimiento del resto de principios y obligaciones sobre la materia. (...) Los códigos ingleses funcionan para resolver dudas sobre cuestiones particulares, pero de ninguna forma proporcionan el tipo de información que garantice un cumplimiento integral de la legislación vigente sobre la materia, que en todo caso debe someterse a un análisis jurídico y técnico[69]…"

Finalmente, es de mencionar que el Código Tipo de Confianza Online de España cubre tres aspectos para los prestadores de servicios de la sociedad de la información: Protección del consumidor, Cumplimiento de las disposiciones de la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico y Protección de datos personales. Su objetivo es promover la adhesión con la creación de un sello distintivo en las páginas web, como garantía de seguridad en sus operaciones *a nivel de consumidor como en relación con el tratamiento y seguridad de los datos personales[70].*

En ese sentido, cabe señalar que la Unión Internacional de Telecomunicaciones emitió un artículo[71] el cual sustenta que "… todo individuo puede optar por la cesión o la comercialización de sus datos personales en la nube, no obstante, esta debe ser una decisión fundada..."[72], toda vez que es necesario la existencia de un punto de equilibrio entre la protección de datos de los consumidores y sus datos al utilizar servicios en la nube. Con la consideración que los prestadores de servicios electrónicos son entes privados, en el informe de Tendencias en las Reformas de Telecomunicaciones de 2013[73] la escritora y consejera principal en Londres de

[69] (Sic.)
[70] (Sic.)
[71] Unión Internacional de Telecomunicaciones, *Protección de datos y privacidad en la nube ¿Quién es el propietario de la nube?*, publicación de septiembre 2015. [Versión digital] [Traducción propia] [Consulta en octubre 2019]. Véase en: https://historicjournals.itu.int/viewer/720/?return=1&css-name=include#page=1&viewer=picture&o=&n=0&q=
[72] Ibidem.
[73] Unión Internacional de Telecomunicaciones, *Informe de Tendencias en las Reformas de Telecomunicaciones de 2013*, publicación de 2013. [Versión digital] [Consulta en octubre 2019]. Véase en: https://www.itu.int/es/publications/ITU-D/pages/publications.aspx?parent=D-PREF-TTR.14-2013&media=electronic

Charles Russell LLP, Stephanie Liston, recomienda la elaboración de un modelo de reglamentación adaptado que establezca un equilibrio entre las necesidades y oportunidades comerciales, la realidad tecnológica y la expectativa razonable de todo ciudadano de tener derecho a la intimidad en un ecosistema digital internacional.

> *Es preciso sopesar los beneficios financieros que ofrecen servicios en la nube a gobiernos, empresas, ciudadanos y consumidores junto con los riesgos que dichos servicios pueden entrañar para la vida privada o los datos personales de todo individuo. No obstante, existe una creciente confusión en torno a quién corresponde la obligación de proteger dichos datos.*

Con la actual libertad de expresión de los individuos y su autodeterminación, en muchos de los casos estos desconocen o infravaloran los riesgos de la seguridad de la información, su valor intrínseco "…considerados como `el nuevo petróleo´"[74] desde el punto de vista comercial y con ello, la creación de un nuevo derecho económico de los titulares.

De esta forma, de acuerdo a un estudio del Eurobarómetro Especial sobre actitudes individuales con relación a la privacidad de 2011[75], el 74% de los encuestados considera la divulgación de información en línea como un aspecto cada vez más frecuente del día a día con especial énfasis en el registro de actividades en teléfonos móviles, tarjetas de pago e Internet móvil. Sin embargo, el 58% considera alguna alternativa para evitar la divulgación de información personal si querían obtener productos y servicios.

Ante ello, Liston apuntó que la Directiva de 1995 sobre protección de datos de la Unión Europea señala que "… *las obligaciones relativas a la protección de datos se imponen por lo general a los responsables del control de datos, mientras que los encargados de procesarlos sólo están sujetos a requisitos de seguridad específicos. Sin embargo, las diferentes definiciones utilizadas en los distintos países europeos, junto con la imprecisión a la hora*

---

[74] Ibidem.

[75] Eurobarómetro Sondeos de opinión del Parlamento Europeo, estudio de 2011. [Versión digital] [Consulta en mayo 2020]. Véase en: https://www.europarl.europa.eu/at-your-service/es/be-heard/eurobarometer/the-european-ombudsman-and-citizens-rights

de clasificar a un proveedor de servicios en nube como un controlador o un procesador, dan lugar a ambigüedades"[76]. Cuyas consecuencias recae en el cliente, quién "*controla las acciones del proveedor o el movimiento de los datos"* no obstante, "*los clientes de los servicios en nube están obligados a actuar con la debida diligencia a la hora de elegir un proveedor que ofrezca las garantías suficientes de fiabilidad, competencia y seguridad exigidas por las leyes"*[77].

Con respecto a los flujos transfronterizos de datos, Liston recuerda que la Directiva Europea determina que esta información no debe transferirse a países fuera del Espacio Económico Europeo y cualquier otro que no tenga un andamiaje jurídico y de protección. Por lo que un ejemplo de cumplimiento es la transnacional Amazon, pues diseñó una nube europea que garantiza la estadía de los datos personales dentro de las fronteras de la Directiva.

Otro punto a considerar es el consumo de la computación en la nube, pues carece de ubicación fija y los "proveedores tienden" *a ser reacios a establecerse únicamente en los países especificados. Por tanto, el cliente puede verse incapaz de determinar en tiempo real la localización de los datos que están siendo procesados o almacenados*"[78]. Lo cual denota una debilidad en la garantía del derecho del individuo ante transferencias a países que carezcan de leyes en la materia; por lo que, surge la necesidad de establecer cláusulas contractuales sobre la transferencia y seguridad conforme a la Directiva Europea. Otra opción es la adopción de normas corporativas vinculantes a la transferencia regular de datos mediante su red corporativa.

Con respecto al punto jurídico, Stephanie Liston, aseveró que "*no existe una legislación sobre privacidad universalmente vinculante que abarque a todos los países del mundo*[79]". Pues las naciones que crearon leyes de privacidad o protección de datos "*se sirven de la regulación de los flujos de datos internacionales como mecanismo para proteger la privacidad individual y ejecutar las políticas nacionales*[80]*".*

---

[76] Unión Internacional de Telecomunicaciones, *Protección de datos …, op. cit.,* datos de sitio.
[77] *Idem.*
[78] *Idem.*
[79] *Idem.*
[80] *Idem.*

2.3.4 Referencias Internacionales de marco normativo en Protección de Datos Personales en comparativa con la Unión Europea

2.3.4.1 Reino Unido

Los tribunales restringieron la definición del concepto de datos personales indicando que dichos datos deben ser fundamentalmente de carácter biográfico y han de centrarse en el individuo en cuestión en lugar de en otra persona, transacción o evento.

2.3.4.2 Francia

La Comisión Nacional de Informática y Libertades controla la aplicación de la Ley relativa a la informática, los ficheros y las libertades de Francia, la cual publicó una Guía sobre el tratamiento legal de los datos personales, e impone una serie de requisitos de notificación y cooperación a los responsables del tratamiento de datos y determinó que condiciones para mantener la seguridad de los datos personales y, en determinadas circunstancias, obtener la aprobación de la Comisión antes de su tratamiento.

2.3.4.3 Alemania

En este país, los datos personales deben ser obtenidos directamente del interesado excepto que la ley los requiera con fines comerciales genuinos o se precise un esfuerzo desproporcionado y no haya indicios de que los intereses del titular puedan verse afectados. Asimismo, la Ley Federal de Protección de Datos enfatiza en el diseño de sistemas de protección de datos que procesen la menor cantidad posible de datos personales, detonando el uso de la anonimidad y uso de seudónimos.

2.3.4.4 Canadá

La Carta Canadiense de Derechos y Libertades protege a todo individuo contra “registros, confiscaciones o investigaciones abusivas”, lo cual es un derecho extendido a la “expectativa razonable de privacidad”. La jurisprudencia del Tribunal de Apelación de Ontario introdujo en el Derecho Común (Common Law) la responsabilidad civil por invasión de la intimidad (“intrusión en la intimidad”). Sin embargo, esta normativa no restringe a las transferencias internacionales de datos personales, pero determina que estas son responsabilidad del que divulga la información.

2.3.4.5 Brasil

En consideración de la ITU, aún tiene que ejecutar una legislación específica de protección de datos; pues a pesar de que la Constitución reconoce los derechos fundamentales a la intimidad y la confidencialidad de la correspondencia. Además, el Código Civil establece que toda persona puede solicitar protección contra cualquier amenaza a los derechos de la personalidad y que la vida privada de todo individuo es inviolable. Del mismo modo, el Código de Protección del Consumidor contiene amplias protecciones que incluyen los derechos a acceder y modificar los datos personales registrados.

2.3.4.6 República Sudafricana

Al igual que Brasil, es un país carente de legislación específica de protección de datos pero acoge el derecho a la intimidad en su Constitución. Además, tiene la Ley de protección al consumidor de 2008 y Ley de comunicaciones y transacciones electrónicas de 2002; la primera, contiene disposiciones relativas a la información de carácter personal; pero, la segunda es de carácter facultativo y cualquier adhesión debe convenirse en un acuerdo con el interesado.

2.3.4.7 Arabia Saudita

Esta nación no posee una legislación específica de protección de datos; sin embargo, varias de sus leyes recogen el derecho a la intimidad. Cabe señalar que la Ley fundamental de gobierno de Arabia Saudita estipula, como un principio fundamental, que toda la correspondencia y las comunicaciones entre distintas partes deben mantenerse en una estricta confidencialidad y no ser divulgadas. Sin embargo, si existe alguna ausencia legislativa, los tribunales recurren a la Sharia (Ley islámica).

Dicha Ley, reconoce el derecho a reclamar una indemnización por daños y perjuicios por divulgación indebida de datos personales cuando la información revelada entrañe pérdida o daño a la persona en cuestión.

2.3.4.8 Emiratos Árabes Unidos

Los Emiratos Árabes Unidos no tienen legislación específica de protección de datos; sin embargo, acogen el derecho a la intimidad en su Constitución y en diversas leyes.

La Carta Magna señala que toda persona goza de libertad de comunicación por correo, telégrafo u otros medios de comunicación, y la confidencialidad de la misma se garantiza con arreglo a la ley. Además, el Código Penal contiene ciertos derechos relativos a la privacidad y la protección de datos personales datos.

2.3.4.9 India

Al contrario de los Emiratos Árabes, el gobierno hindú no contempla un derecho constitucional relativo a la privacidad, pese a que su Tribunal Supremo determinó que la privacidad se acoge al derecho a la vida y la libertad personal.

De esta forma, la Ley de tecnología de la información de 2000, determinó que las empresas deben mantener prácticas de seguridad razonables a la hora de gestionar datos personales y que, si se obtienen en virtud de un contrato, dichos datos no deben divulgarse más allá de los límites del mismo sin el consentimiento del interesado.

2.3.4.10 Japón

Como miembro de la Cooperación Económica Asia-Pacífico (APEC), Japón comparte el concepto de privacidad de la APEC, por lo que creó la Ley de protección de datos personales, la cual regula la obtención y uso de datos personales dentro del país e incluye todos los supuestos de utilización de datos; sin embargo, sólo se aplica a situaciones que impliquen información personal de 5,000 individuos o más.

Asimismo, impone obligaciones comunes relativas al consentimiento, la seguridad y la provisión de la información, junto con requisitos adicionales para supervisar a empleados y terceros encargados de manipular datos personales.

En conclusión del presente capítulo, se denota que diversos países reconocen el derecho de la privacidad de forma independiente o en correlacionado a la intimidad a nivel constitucional; sin embargo, carecen de leyes propias de la materia, con lo cual se denota una debilidad jurídica para la garantía de la salvaguarda y respeto de los derechos de los individuos.

No obstante, los gobiernos adoptan y adaptan las legislaciones de la Unión Europea para su aplicación interna, ello debido a que las instituciones

privadas aprovechan las omisiones y carencias jurídicas para hacer del tratamiento de datos personales conforme sus intereses. Por otro lado, la existencia del *soft law* ha permitido que algunas instituciones adopten medidas de autorregulación en la materia conforme a las TIC, haciendo evidente la creatividad e intención al apego al modelo europeo o la creación de modelos alternos, como el americano, para el respeto al derecho de los individuos demostrando que no existe justificante para la omisión de la normativa.

Capítulo 3.
Riesgos para la transmisión de los datos personales

Capítulo 3. Riesgos para la transmisión de los datos personales

La Agencia Española de Protección de Datos[81] emitió un documento basado en estándares internacionales ISO (ISO/IEC 27005:2008 Tecnologías de la Información – Técnicas de Seguridad – Gestión de riesgos de seguridad de la Información; ISO 31010 de Gestión y Evaluación de Riesgos ISO 29134 Tecnologías de la información – Guías para las Evaluaciones de Impacto en la Protección de los Datos; y la Guía sobre las Evaluaciones de Impacto en Protección de datos (WP248) – Grupo Europeo Artículo 29) en la que señala que *el diseño adecuado de las actividades de tratamiento es un aspecto clave para poder garantizar los derechos y libertades de los interesados*[82] (...) *y es el momento idóneo para definir las medidas de control y seguridad*[83] (ibídem, página 8).

Primeramente, define la gestión de riesgos como *el conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como, las medidas para su reducción o mitigación*[84] ya que en caso de que esta se materializa, presentaría un impacto aunado de consecuencias negativas. Ante ello, identificar los riesgos implica considerar la amenaza de origen basada en tres etapas:

- *identificación de amenazas*, sobre la determinación de escenarios de riesgo desde la perspectiva de privacidad ante posibles daños o perjuicios de los interesados. Ellos se subdividen en lo siguiente:
    - *Acceso ilegítimo a los datos*, lo cual vulneraría o menoscabaría la confidencialidad
    - *Modificación no autorizada de los datos*, vulnerando la integridad de los mismos
    - *Eliminación de los datos*, perpetrando así la disponibilidad
- *evaluación*, lo cual *consiste en valorar el impacto de la exposición a la amenaza, junto a la probabilidad de que esta se materialice;* es decir, la

[81] Agencia Española de Protección de Datos, *Guía Práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD,* [Versión digital], [Consulta mayo 2020]. Véase en https://d3t4nwcgmfrp9x.cloudfront.net/upload/AnalisisDeRiesgosRGPD.pdf
[82] *Ibidem, p.*
[83] *Ibidem, p.*
[84] *Ibidem, p.*

consideración de todos los posibles escenarios de vulnerabilidad, determinación de los posibles daños al interesado ante la materialización de la amenaza -impacto- respecto a la posibilidad de presentarse

- *tratamiento de los riesgos*, cuyo *objetivo de tratar los riesgos es disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen;* es decir, consideración, determinación y aplicaciones de las medidas necesarias que reduzcan o mitiguen el riesgo

En ese sentido, el Reglamento pretende la mitigación y evaluación de riesgos con un enfoque implicaciones que los tratamientos de datos de carácter personal tienen sobre los interesados por lo que *implica estimar el daño y la tipología de daño que se puede producir sobre los interesados.*

Para ello, se considera los siguientes apartados del RGDP[85]:

Artículo 25, apartado 1: "Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, ***el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización****, concebidas* ***para aplicar de forma efectiva los principios de protección de datos****, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados".*

Artículo 25, apartado 2: "El responsable del tratamiento aplicará las ***medidas técnicas y organizativas*** *apropiadas con miras a garantizar que,* ***por defecto, solo sean objeto de tratamiento***

[85] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 26 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos dato (Deroga Directiva 95/46 CE). Publicación del 27 de abril de 2016. [Versión digital], [Consulta en agosto 2020]. Véase en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

los datos personales que sean necesarios *para cada uno de los fines específicos del tratamiento".*

Artículo 32: "Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, ***el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo****, que en su caso incluya, entre otros:*

- *La seudonimización y el cifrado de datos personales;*
- *La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
- *La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
- *Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

Con lo anterior, se denota la necesidad de determinar la necesidad de establecer medidas de control y seguridad para el tratamiento de datos respecto a la determinación del nivel de riesgo de *destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*.

En el país, las instituciones privadas y gubernamentales deben de conocer los beneficios de la adopción de recomendaciones y prácticas internacionales que favorecen la seguridad, control y mecanismos de evaluación constante y con ello, crear continua innovación de estos mecanismos en pro de las personas.

3.1 Aplicación de una Evaluación de Impacto sobre la Protección de Datos

Como cualquier procedimiento precautorio, como las auditorías internas, el objetivo de una *Evaluación de Impacto sobre la Protección de Datos*[86] (EIPD) es medir el grado de riesgo que se encuentra alguna entidad de la actividad que realiza respecto al tratamiento de la información.

Cabe señalar que la Agencia Española de Protección de Datos (AEPD) señala que la *EIPD es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas (...) con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable*. Sin embargo, pese a que el Reglamento señala que estas Evaluaciones se realicen *previas* al tratamiento, éste no señala las operaciones del tratamiento inicial.

En ese sentido, con este tipo de acciones de los responsables podemos visualizar la *responsabilidad proactiva* del responsable, pues al evaluar la aplicación de una Evaluación ante el riesgo de la actividad o determinar la realización de la misma, debe ser debidamente documentada y expresar los motivos de la conclusión.

3.2 Impacto de los datos personales y su resguardo en sistemas tecnológicos

Considerando que la protección de datos personales parte de un Derecho Fundamental, el uso y tratamiento que le den los responsables a la información de los titulares, es de suma importancia conocer el alcance e impacto de un mal tratamiento de los mismos, por ende, el artículo 35.3 del RGPD atañe una categorización de riesgo elevado:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado (perfilaje) y que produzcan efectos jurídicos de las personas

[86] Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD. Publicación de septiembre 2019. [Versión digital], [Consulta en marzo de 2020]. Véase en: https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

- Tratamiento a gran escala de las categorías especiales de datos personales, o datos sobre condenas e infracciones penales o medidas de seguridad conexas.
- Observación sistemática a gran escala de una zona de acceso público.

Adicionalmente, con el objetivo de poder determinar qué tipo de tratamientos pueden considerarse de alto riesgo, el GT29 en el documento WP248 Directrices sobre las Evaluaciones de Impacto en la Protección de Datos introduce criterios que pueden evidenciar un elevado riesgo inherente a las actividades de tratamiento y con ello, determinar la realización de una Evaluación.

Al determinar la naturaleza, alcance, contexto y finalidades del tratamiento de datos (35.1 del RGPD) deben de considerarse las siguientes premisas, según la Agencia Española:

- *Naturaleza del tratamiento*, es decir, determinar si se implica un alto riesgo ante las categorías de datos
- Valorar las *circunstancias* por las que se realiza el tratamiento, por ejemplo, cruce de fuentes de información
- *Valorar los efectos o consecuencias del tratamiento*, estas pueden ser jurídicas, económicas y exclusión de beneficios sociales o fiscales. Su objetivo es verificar si suponen un alto riesgo sobre la invasión de la privacidad por el uso de tic, posibles responsables, uso de las transferencias internacionales o cesión de tratamiento.

Un ejemplo de la Agencia es: *si la finalidad incluye: Toma de decisiones Elaboración de perfiles Análisis predictivo Prestación de servicios relacionados con la salud Seguimiento, control y observación de personas (monitorización).*

La forma de elegir entre una Evaluación y un Análisis es determinar si se requiere un mapeo de riesgos globales del tratamiento de los datos en procesos similares y determinar medidas de seguridad (Análisis) *vs* la necesidad de determinar un riesgo específico en una operación cerrada y con ello, asumir medidas precautorias y de respuesta ante una vulnerabilidad (Evaluación).

Capítulo 4.
Manual básico para la implementación de la ciberseguridad

Capítulo 4. Manual básico para la implementación de la ciberseguridad

4.1 Diagnóstico inicial

Para la implementación de un sistema de gestión normalizado basado en la Norma Mexicana NMX-I-27032-NYCE-2018[87] primeramente se deben tener la siguiente precisión: su objetivo es "...proveer una guía para mejorar el estado de la ciberseguridad…", con el objeto de atención en: seguridad de la información, seguridad en redes, seguridad en Internet, y protección de la infraestructura de información crítica (PIIC).

Bajo esta tesitura, el proyecto de investigación presente se considera pertinente el uso del procedimiento del método clínico[88] para el desarrollo de la presente propuesta debido a que esta se traduce en la aplicación del método científico aplicado a pacientes en el sector salud; es decir, "...se define como una forma de utilizar el método científico a escala observacional y experimental pues toda observación bien hecha es una investigación y toda terapéutica bien diseñada un experimento..."[89] por lo que conlleva una dinámica del proceso y la ejecución de la lógica para alcanzar un objetivo.

Con observancia del párrafo anterior y en referencia a la Norma NMX-I-27032-NYCE-2018 "Tecnologías de la Información-Técnicas de Seguridad-Lineamientos para la Ciberseguridad" y la ISO IEC 62443 se enuncian parámetros obligatorios tanto para el diseño de los sistemas o los requisitos específicos para fabricantes; en atención a las respectivas Leyes Federales de Protección de Datos Personales en aras de la protección de la información, basado en lo siguiente:

- análisis de riesgos de seguridad Informática
- control de acceso físico y lógico a los sistemas

---

[87] Declaratoria de vigencia de la Norma Mexicana NMX-I-27032-NYCE-2018, publicación del 26 de junio de 2018, [Versión digital], [Consultada en agosto 2020]. Véase en: https://dof.gob.mx/nota_detalle.php?codigo=5529046&fecha=26/06/2018

[88] "... el método clínico es el método científico de la ciencia clínica, la que tiene como objetivo de estudio el proceso salud enfermedad. Toda práctica médica que no se base en el método clínico será ajena a la ciencia clínica y, en gran parte, responsable de la `mala práctica médica´". Cruz Hernández Jeddú, Hernández García Pilar, Abraham Marcel Enrique, Dueñas Gobel N, Salvato Dueñas A. Importancia del Método Clínico. Rev Cubana Salud Pública. Publicación en Internet el 2012 Septiembre, pp. 29. [Consulta en agosto 2020]. Véase en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-34662012000300009&lng=es

[89] Arteaga Herrera J, Fernández Sacasas J. El método clínico y el método científico. Medisur Publicación en Internet de 2010, pp. 8. [Versión digital], [Consulta en agosto 2020]. Véase en: http://medisur.sld.cu/index.php/medisur/article/view/1312

- garantía de la tríada de la información (*Confidencialidad, Integridad y Disponibilidad*, CIA, por sus siglas en inglés)
- procesamiento de los datos para la crear perfiles específicos para el valor de la empresa y las responsabilidades de la industria: proceso automatizado
- la industria 4.0 y su impacto en el mercado laboral
- la nube, la virtualización de equipos o sistemas
- soluciones para el teletrabajo[90], como *Bring Your Own Device* (BYOD) o *Choose Your Own Device* (CYOD) con plataformas *Mobile Equipment Management* (MEM's) o *Mobile Device Management MDM´s*
- ingeniería social
- convergencia tecnológica.

En ese sentido, el primero paso será la determinación de la naturaleza de los datos personales tratados por parte del responsable, por lo cual se recomienda la aplicación de la Guía de Análisis de riesgos de Protección de Datos Personales de la Agencia Española y el siguiente diagnóstico inicial:

Planteamiento	**Nivel de riesgo**			
Existe tratamiento de datos personales	SI 10		NO 0	
Existe un encargado del tratamiento de datos	SI 0		NO 10	
Tipos de datos personales utilizados	generales	sensibles	biométricos	financieros
	Básico 1	Medio 2	Fuerte 3	Crítico 5
Finalidades de uso claro y legal	SI 0		NO 10	
Existe la transferencia de datos a terceros nacionales	SI 10		NO 0	
Existe la transferencia de datos a terceros internacionales	SI 10		NO 0	
Existe tiempo específico de tratamiento	SI 0		NO 10	

[90] Thibault Aranda, X. "Aspectos jurídicos del teletrabajo". Revista Ministerio de Trabajo y Asuntos Sociales. Madrid. 1998. nº.11. [Versión digital] [Consulta en agosto 2020]. Véase en: https://expinterweb.empleo.gob.es/libreriavirtual/descargas.action?f_codigo=W0149811&codigoOpcion=3
"…El teletrabajo puede definirse como una forma de organización y/o ejecución del trabajo realizado a distancia, en gran parte o principalmente, mediante el uso intensivo de las técnicas informáticas y/o de telecomunicación…"

Se realizarán cruces de información para la creación de perfiles o segmentación social	SI 10	NO 0
Se aplica la anonimato o de seudónimos	SI 0	NO 10
Se usa tecnología vanguardista y actualizada	SI 0	NO 10
Existen filtros y/o control de acceso a la información	SI 0	NO 10

Cuadro 1. Cuestionario diagnóstico del nivel de riesgo para la protección de datos personales. Fuente: Elaboración propia

La función de este cuadro diagnóstico es de 90 puntos o más, se interpreta un nivel crítico en el tratamiento de datos, por lo que deben aplicarse medidas robustas y necesarias para su seguridad; si el parámetro es de 40 a 60 puntos, el nivel de riesgo a implementar es de medio a fuerte; en tanto que menos de 40 puntos se traducen en un nivel de riesgo base.

En una segunda fase, la aplicación de la Guía Española en relación al ciclo de vida recomienda la aplicación gráfica del tratamiento de datos personales.

		CICLO DE VIDA DE LOS DATOS EN LAS OPERACIONES DEL TRATAMIENTO				
		Captura de datos	*Clasificación / Almacenamiento*	*Uso / Tratamiento*	*Cesión o transferencia de los datos a un tercero para su tratamiento*	*Destrucción*
ELEMENTOS QUE INTERVIENEN EN LAS OPERACIONES DE TRATAMIENTO	*Actividades del proceso*					
	Datos tratados					
	Intervinientes involucrados					
	Tecnologías intervinientes					

Cuadro 2. Ciclo de vida de los datos en las operaciones del tratamiento. Fuente: Agencia Española de Protección de Datos

4.1.1 Implementación de medidas de seguridad

Una vez que se ha detectado el problema o área de oportunidad en el tratamiento de datos personales ejercido por alguna entidad, se deben aplicar medidas correctivas tanto jurídicas como tecnológicas, conforme al nivel de riesgo, tal como:

De acuerdo con la Unión Internacional de Telecomunicaciones, *"la seguridad de las informaciones sólo tiene sentido cuando se aplica a datos y procesos de cuya exactitud no se tiene certeza absoluta (concepto de calidad de datos y de procesos) con objeto de que sean perdurables en el tiempo (concepto de perdurabilidad de los datos y de continuidad de los servicios)*[91]*..."* por lo que la infraestructura física-tecnológica debe permitir la implementación de una o varias medidas de seguridad por encriptación, aislamiento de entornos, redundancia de recursos, procedimientos de vigilancia, de control, de gestión de incidentes, de mantenimiento, de control de acceso y de gestión de sistemas.

4.1.2 Encriptación de los datos

Esta permite la confidencialidad de los datos, verificar su integridad y autentificar las entidades, ello se basa en dos técnicas: *encriptación simétrica o llave secreta y la encriptación asimétrica o llave pública.* El nivel de seguridad puede aplicarse a las categorías de datos personales por algoritmo.

Es decir, para el descifrado simétrico ocurre cuando la clave es la misma para encriptar o descifrar la información; los principales algoritmos de este tipo de encriptación son DES, RC2, RC4, RC5, IDEA y AES. Sin embargo, ello deja una brecha de seguridad, pues al ser la misma cualquiera con acceso a las claves podría manipular y/o acceder a la información contenida.

Sin embargo, en el caso de la encriptación asimétrica esta es basada en el uso de un par único de claves, una pública y una privada; a diferencia con el encriptado anterior, la clave pública puede estar al alcance de terceros; en tanto que la llave privada es de uso y conocimiento privado.

Es decir, al momento de encriptar una información con clave pública el destinatario podrá acceder al contenido con la clave privada. Cabe mencionar que los principales formatos son RSA (por R. Rivest, A. Shamir y L. Adelman), Diffie-Hellman y El Gamal.

Cabe mencionar que el éxito de este método de seguridad está basado en la confidencialidad y el grado de seguridad de los algoritmos; así como la infraestructura física y tecnológica de las plataformas.

---

[91] Unión Internacional de Telecomunicaciones, *Guía de ciberseguridad para los países en desarrollo*, edición 2007. [Versión digital], [Consulta en agosto 2020]. Véase en: https://www.itu.int/dms_pub/itu-d/opb/str/d-str-secu-2007-msw-s.doc

4.1.3 Certificado digital

Este es certificado de la identidad de una persona basado en la identidad de su propietario y clave de identificación. Para ello se utiliza la norma X.509 «*Directory authentification framework*» pues contiene una propuesta de arquitectura en el uso de certificados digitales. Sin embargo, este se reduce a la certeza plena de quien accede y/o manipula la información; por lo cual considero este tipo de certificación debe aplicarse a todo aquel que por razones de su actividad -con previo contrato y aviso de confidencialidad- debe tener acceso a la información de los titulares.

Cabe señalar que este tipo de certificados permite la conexión de un número importante de usuarios a un servidor determinado; sin embargo, si estos son traspasados o falsificados se podrá corromper el sistema. De ahí que debe revocarse al momento de una vulneración o ante la salida de un encargado de tratamiento de los datos.

El nivel de seguridad de estas infraestructuras se basan en: la complejidad de la infraestructura; el nivel de seguridad; y la validez y/o restricción de certificados.

4.1.4 Integridad de los datos

Cabe señalar que la integridad de la información por encriptación simétrica o asimétrica es total, pues al ser encriptada se genera un tipo de “huella digital” en bits, por lo que al ser descifrado se hace una comparativa entre el mensaje recibido y el emitido original, si existe similitud se da por veraz la información contenida.

4.1.5 El protocolo IPSec

Esta herramienta permite la confidencialidad para el transporte de información y autenticación ante una transferencia al protocolo IP con el uso de la extensión de la autenticación (*Authentication Header* [AH], encabezamiento de autenticación) o del encabezamiento de confidencialidad – autenticación (*Encapsulating Security Payload Header* [ESP], encabezamiento de encapsulamiento de la parte útil de seguridad), pues funciona por punto a punto entre el emisor y el receptor; por lo que imposibilita la modificación de los datos transmitidos y la autenticidad de la dirección de origen que figura en el paquete.

Asimismo, el protocolo IPSec permite crear redes privadas virtuales entre el canal de comunicación en una infraestructura de red no fiable. Un ejemplo de ello se encuentra en el uso del software SSL (*Secure Sockets Layer*, capa de zócalos segura) para las transacciones comerciales por Internet.

Cabe mencionar, el nivel de riesgo en este tipo de intercambio de información es la seguridad de la mensajería electrónica y de los servidores de nombres, por lo que también deben ser factores a considerar al momento de diseñar un sistema de ciberseguridad.

Los riesgos de seguridad afrontados, en relación con el uso de un sistema de mensajería, se relacionan con: la pérdida, interceptación, alteración o destrucción de los mensajes; la infección de sistemas con mensajes con virus, gusanos o troyanos; envío de mensajes indeseados; usurpación de identidad; entre otros.

Asimismo, el uso del protocolo SMTP (*Simple Mail Transfer Protocol*, protocolo sencillo de transferencia de correo) permite el envío de mensajes por Internet con mecanismos de seguridad. Algunos de ellos son los protocolo es el *Secure Multipurpose Internet Mail Extensions* (extensiones de correo Internet polivalente seguro) o *Secure MIME* (S/MIME), el *Privacy Enhanced Mail* (PEM, correo de privacidad mejorada) y el *Pretty Good Privacy* (PGP, privacidad bastante buena).

Uso de los cortafuegos o *firewalls* para la detección de intrusiones, incidentes y anomalías que pretenden identificar los riesgos en los sistemas y su protección. Ello es una de las herramientas básicas de cualquier sistema que debe de tener cualquier persona, sistema y plataforma.

La implantación y configuración de estas herramientas permite la creación de un sector de la seguridad de la red y de conexión en el sistema; sin embargo, es necesario complementarlo con otras herramientas, medidas del sistema y procedimientos implementados.

4.1.6 Control de acceso

Una de las herramientas de seguridad es la instalación de mecanismos de control de acceso a los sistemas para la identificación del personal, sistemas de autentificación por clave, biométricos y mecanismos de doble autenticación en

aras de la salvaguarda de la calidad, integridad y seguridad de la información personal de los titulares.

En este sentido, la configuración para perfiles de los usuarios es necesaria para la manipulación de la información; por lo que se recomienda la aplicación de mecanismos de control de tratamiento de la información similar a la criptología *hash*[92]; pues con este mecanismo en el que las contraseñas o información no es almacenada texto plano y con ello evitar la divulgación de la información, así como para asegurar que los archivos no fueron alterados. Ello se logra con la comparativa de los hash creados antes y después de la transmisión de los datos.

Las funciones más comunes del hash son mediante el hash SHA-1, MD 5 y SHA-2 por lo que con un generador de hash creará un total de 40 caracteres independientemente de los caracteres de la información. De forma ejemplificativa, realice una prueba de campo con el generador de hash online[93] con mi nombre completo, dando el siguiente resultado:

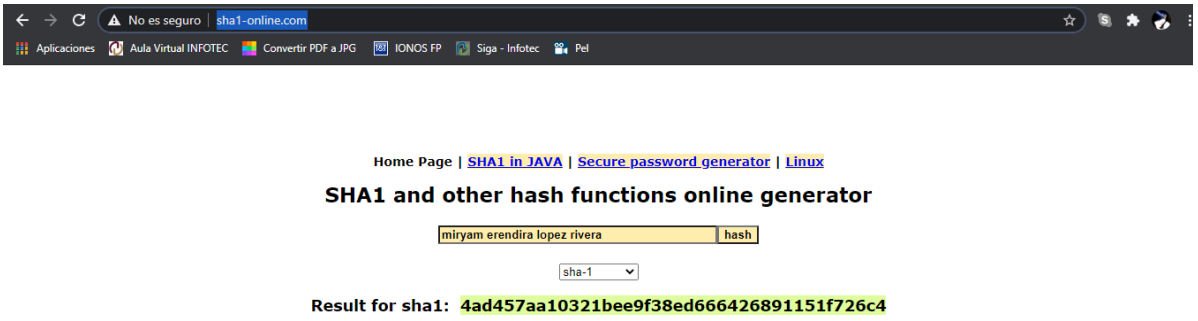

Figura 2. Generación de hash con nombre propio.

Fuente: Sha online

Para mi nombre completo, el hash SHA 1 es: 4ad457aa10321bee9f38ed666426891151f726c4 por lo que si invierto los nombres tendremos un hash totalmente diferente: fe7629cbb9d854f452edc6393e906ef891504cba.

---

[92] Donohue Brian, ¿Qué es un hash y cómo funciona?, publicación digital de KasperskyLab, abril de 2020. [Consulta en agosto 2020] Véase en: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/#:~:text=10%20Abr%202014-,Una%20funci%C3%B3n%20criptogr%C3%A1fica%20hash%2D%20usualmente%20conocida%20como%20%E2%80%9Chash%E2%80%9D%2D,tendr%C3%A1%20siempre%20la%20misma%20longitud
"Una función criptográfica hash- usualmente conocida como "hash"- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud".

[93] SHA 1 online. Véase en: http://www.sha1-online.com/

Figura 3. Generación de hash con nombre propio modificado.

Fuente: Sha online

Ello prueba que no existen dos entradas que produzcan el mismo hash de salida[94]. Asimismo, al utilizar un conversor de hash SHA 1 online[95] para intentar descifrar los hash generados en por mi nombre la aplicación simplemente no pudo identificar el formato del hash y mucho menos descifrar la información:

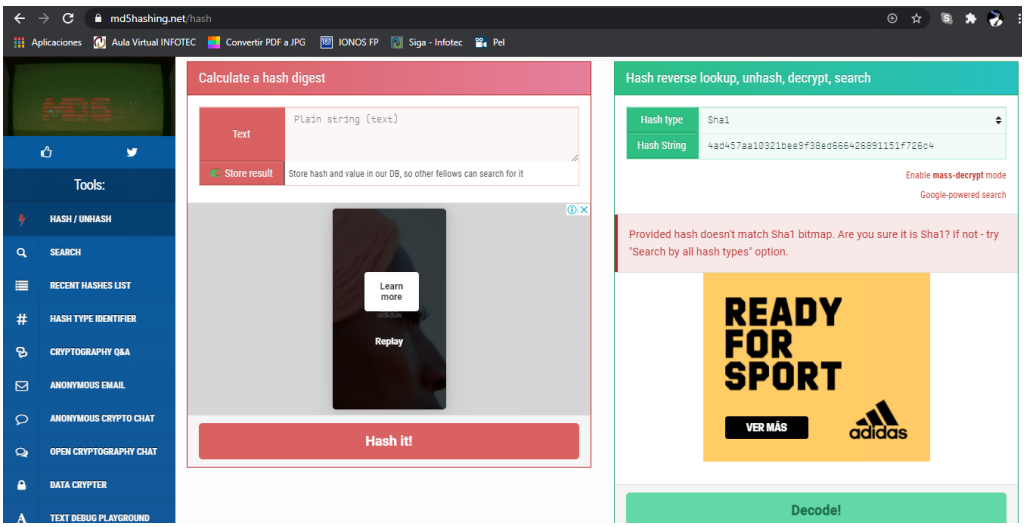

Figura 4. Búsqueda para descifrar hash generado con nombre propio.

Fuente: Sha online

Así, con estas herramientas de identificación y mecanismos de integridad de la información, lo único que resta es la correcta gestión de las autorizaciones por perfil de usuario, permisos de acceso a los sistemas y redes. En ese sentido, se recomienda aplicar una doble autenticación en caso de que el sistema hubiera sufrido una alteración o una falla mecánica-tecnológica.

Para ello, se pueden hacer diferentes combinaciones de tipos de autentificación y control de acceso por su origen: contraseña o número de identificación personal (PIN-*Personal Identification Number*); instrumento como

[94] (Brian, 2020), (ibídem).
[95] MD5Hashing, Portal web. [Consulta en septiembre]. Véase en: https://md5hashing.net/hash

tarjeta o ficha de acceso; y biométricos (huella digital, vocal, retina). Por ejemplo, implementación de un número de identificación personal más clave por tarjeta de acceso o uso de clave personal más identificación por clave de voz. Pues el nivel de confiabilidad dependerá del grado de seguridad en su configuración y los mecanismos físicos utilizados, así como el grado de confiabilidad contractual y moral del personal.

> *Los servidores de autenticación no deben ser falibles ni vulnerables puesto que de su robustez depende el nivel de seguridad global de la infraestructura informática y de las telecomunicaciones*[96]*.*

Cabe señalar que el uso de la biometría se basa en un tratamiento estadístico y probabilístico del dato; con ello, el uso de los biométricos conlleva la confidencialidad y tratamiento de información sensible de los titulares y su uso inadecuado vulneraría la integridad de persona.

4.1.7 Protección de la comunicación

Para la infraestructura física debe de contemplarse que existe una matriz central de comunicación o punto de origen en el que se concentra la información, por lo que el flujo de datos por parte de los usuarios debe ser ininterrumpida; por lo que se requiere de un aislamiento capaz que protegerlo de las condiciones externas como el clima, así como el uso de las Jaulas de Faraday[97] cuya finalidad es proteger las transmisiones de captadores de radiaciones electromagnéticas.

Así, la Guía de ciberseguridad para los países en desarrollo de la Unión Internacional de Telecomunicaciones (UIT) asevera que *"...la infraestructura de transmisión se debe proteger contra la radiación eventual, que podría poner en peligro la transmisión de datos, y contra los ataques pasivos (escucha de datos) y*

---

[96] (Brian, 2020), (ibídem).

[97] (Hidalgo, 2020) Universidad Autónoma del Estado de Hidalgo, [publicación digital] [Consulta agosto 2020]. Véase en: https://www.uaeh.edu.mx/scige/boletin/prepa4/n10/r3.html
Definición: (sic.) Jaula de Faraday: Es una caja metálica cuya finalidad es el de proteger los campos eléctricos estáticos, ya que en su interior el campo es nulo y se utiliza para proteger de descargas eléctricas. Su funcionamiento se basa en las propiedades de un conductor en equilibrio electrostático; la caja metálica se coloca en presencia de un campo eléctrico externo, donde las cargas positivas se quedan en las posiciones de la red, los electrones son libres y comienzan a moverse actuando una fuerza sobre ellos: F=eE_ext, (e) es la carga del electrón (con movimiento en sentido contrario al campo eléctrico), E_ext es la intensidad del campo eléctrico externo.
Cuando las cargas en el interior comienzan a desplazarse, crean un campo eléctrico de sentido contrario al campo externo de la caja; en consecuencia el campo eléctrico resultante en el interior del conductor es nulo, por lo que ninguna carga puede atravesarla. A este fenómeno se le denomina apantallamiento eléctrico y se utiliza para proteger a los dispositivos de cargas eléctricas. Algunos dispositivos, sin estar equipados de una jaula de Faraday actúan como tal, por ejemplo: los ascensores, los coches, los aviones, entre otros; por esta razón se recomienda permanecer en el interior del coche durante una tormenta eléctrica, su carrocería metálica actúa como una jaula de Faraday, lo que significa que en el interior el campo es nulo y lo hace seguro.

activos (modificación, destrucción y creación de datos). Por lo que es necesario proteger las conexiones de los usuarios..."[98]. Por tanto la UIT plantea que es necesario identificar a los usuarios, localizarlos y conocer sus flujos de aplicación.

Ante ello, plantea el uso de la encriptación de los datos a nivel de «red» pese al aumento del ancho de banda y rendimiento de la red, pues su ventaja es *"...la independencia de la aplicación y de los mecanismos de encriptación vinculados al transporte que son ahora completamente transparentes para el usuario*[99]*."*; sin embargo, este tipo de transacciones encriptadas sin un hash podría modificar *"...la propia aplicación y los datos se encriptan antes de entregarse al protocolo de red que se encargará de su encaminamiento*[100]*."*.

En cuanto al Sistema Operativo, la UIT considera el uso de *"...protección en las tarjetas de red, el soporte de protocolos de aplicación en modo seguro (transmisión de ficheros protegidos, mensajería segura) y las operaciones de replicación (mirroring) y duplicación (duplexing) de la información, redundancia de las operaciones de escritura y de los equipos*[101]*"*. Lo cual equivale a seguridad en la infraestructura del transporte y de la aplicación: en los procesos y usuarios autenticados; uso de la encriptación / desencriptación y su gestión de claves.

4.1.8 Gestión adecuada

Dependiendo de la naturaleza de la información tratada, los encargados definen las actividades de gestión de las plataformas ante la disponibilidad e implementación de la seguridad para su óptimo rendimiento. Adicionalmente de las tareas de monitoreo y respuesta inmediata ante algún incidente interno o falla interna.

> *"...una buena gestión de la red contribuye a que las infraestructuras, servicios y datos estén disponibles de una manera eficaz. Gracias a la gestión de la red, y especialmente de las funciones de gestión de las configuraciones, del rendimiento y de los incidentes, pueden alcanzarse los objetivos de la seguridad a saber, la disponibilidad y la integridad".*
>
> *"La gestión de la red permite disponer de todos los datos necesarios no sólo para la facturación a los usuarios sino también para la*

[98] (Telecomunicaciones, Guía de ciberseguridad para los países en desarrollo, 2007). [Versión digital], [Consulta en agosto 2020]. Véase en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2007-PDF-S.pdf
[99] Ibidem. Página 75
[100] Ibidem. Página 75
[101] Ibidem. Página 75

implementación de las funciones de vigilancia y auditoría que tienen una importancia primordial en materia de seguridad. Esto permite verificar las acciones con fines de prueba o de no rechazo."[102].

A ello se adiciona la confidencialidad en la transmisión de la información (aislamiento con las Jaulas de Faraday), minimización de accesos no autorizados a los datos y control de tratamiento de los datos en aras de su integridad y seguridad de la información.

Para la protección de la red, la UIT determina imprescindible protegerla de cualquier modificación por terceros y con detección de acciones como: direcciones en las tablas de encaminamiento como paquetes IP; modificación a los caminos y copias ilegales de los datos transportados; vigilancia de los flujos; desvío, modificación y destrucción de los paquetes de datos; y denegación de servicio.

Es importante poder asegurar el proceso de encaminamiento de los datos a través de las redes de telecomunicación. Los proveedores del servicio «red» deben proteger todas las entidades que intervienen en este proceso y muy especialmente los encaminadores y los servidores de nombres para que la calidad del servicio de encaminamiento satisfaga los criterios de seguridad, de disponibilidad (que el servicio sea operacional), de confidencialidad (que los datos se entreguen a los destinatarios correctos) y de integridad (que los datos no se modifiquen durante su transferencia).

Cabe señalar que si bien es cierto que la entrega de la información fidedigna no se garantiza por la red a la dirección correcta, por lo que es necesario el uso de un «control de acceso» y/o el uso de la codificación de la información *"...pueden ser comprensibles para terceros no autorizados. Cuando se trata de* ***datos sensibles es necesario encriptarlos para que resulten ininteligibles****"*.

Bajo esta precisión, es de destacar que las entidades deben aplicar una vigilancia constante a la red para *"...garantizar que la calidad de servicio de la red sea aceptable sino también detectar problemas, incidentes, errores y anomalías que degraden la eficacia de la red y que puedan llegar a afectar a la seguridad de los recursos para responder lo más rápidamente posible y de manera adaptada a los problemas de funcionamiento…"*, ello es similar a la auditoría de lo registrado y

[102] *Ibidem, p.*

crear planes de contención y de respuesta ante vulneraciones o incidentes para los usuarios, la seguridad interna e integridad de la información.

4.2 Estrategia de ciberseguridad en México

En México existe la Estrategia Nacional de Ciberseguridad (ENCS)[103], cuyo objetivo es establecer acciones de ciberseguridad en el ámbito social, económico y político ante el uso de las Tecnologías de la Información y Comunicación (TIC) por parte del Estado Mexicano. Sus objetivos estratégicos de protección son:

a. la sociedad y sus derechos, para la generación de condiciones para el ejercicio de las actividades y derechos de la población
b. la economía e innovación, con el fin de propiciar el desarrollo e innovación tecnológica así como el impulso a la ciberseguridad
c. las instituciones públicas, en aras de la salvaguarda de la información y los sistemas informáticos de las instituciones públicas
d. la seguridad pública, orientado a incrementar las capacidades para la prevención e investigación de conductas delictivas en el ciberespacio
e. la seguridad nacional, dirigido al desarrollo de capacidades para prevenir riesgos y amenazas en el ciberespacio que atenten contra la independencia, integridad y soberanía nacional

Para ello, se consideran ejes transversales *en la cultura de la ciberseguridad, desarrollo de capacidades, coordinación y colaboración de organizaciones, personas y tecnología, investigación y desarrollo en TIC, adopción de estándares y criterios técnicos, marco jurídico y medición y seguimiento de resultados basados en Derechos Humanos, gestión de riesgos y con colaboración multidisciplinaria*.

Dicho lo anterior, se recomienda:

- leer los acuerdos de confidencialidad, contratos laborales y cualquier otro acuerdo para evitar la comisión de un delito o incentivar la difamación de las actividades
- determinar la recaudación de los datos personales y realizar auditorías para minimizar el riesgo de filtración de información

[103] Estrategia Nacional de Ciberseguridad (ENCS), [Versión digital], [Consulta en agosto de 2020]. [Versión digital], [Consulta en agosto 2020]. Véase en: https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf
Modelo de Madurez de Capacidad de Seguridad Cibernética para las Naciones (CMM), Global Cyber Security Capacity Centre University of Oxford, 3/31/2016

- Utilizar sitios con protocolo HTTPs y aplicarlo en las páginas web
- Actualizar el software periódicamente
- Realizar copias de seguridad periódicas
- Habilitar firewall para proteger la conexión a Internet
- Establecer políticas de seguridad en la navegación desde dispositivos propios y empresariales
- Cree una estrategia de respuesta frente a incidentes
- En caso de violación a los sistemas internos, informe a la autoridad a razón de la información que pudiera ser comprometida
- Investigue la posibilidad de contratación de las pólizas de seguro que ampare la pérdida de datos o información
- Se recomienda a las empresas evaluar la posibilidad de contratar hackers éticos para la protección de los sistemas internos
- Se recomienda a las empresas a tener diferentes puntos de conexión al sistema con la finalidad de que en caso de violación de seguridad, el atacante o posea el control total del sistema
- Adopte “buenas prácticas” o certificaciones de seguridad de los sistemas

4.3 Recomendación de infraestructura jurídica

En este apartado verificaremos que la protección de datos personales en relación al tratamiento por un tercero y deben de ser conocimiento de los encargados y los responsables de la seguridad de la información.

Como se ha mencionado en capítulos anteriores, el tratamiento de datos personales es parte del derecho humano de la dignidad, derivando de ahí otros derechos tal como el de la privacidad. En el caso mexicano, está plenamente contemplado en nuestra Carta Magna y se derivaron las leyes correspondientes al sector privado y al público; así como se han creado legislaciones que por su naturaleza conllevan la combinación de otras actividades reconocidas como el comercio electrónico, uso de imagen en redes públicas y creación de perfiles o audiencias para las actividades de comercio, por mencionar algunas.

4.3.1 Actividades de comercio

En el caso de la creación y concentración de bases de datos por algún particular, este debe atender a la protección de la información con base en la Ley Federal de

Protección de Datos Personales en Posesión de Particulares (LFPDPPP), observancia de los Principios de Tratamiento, denotación del Aviso de Privacidad y herramientas para el ejercicio de los Derechos ARCO de los titulares y demás premisas anteriormente señaladas.

Actualmente, y con especial mención a la presente pandemia originada por el virus conocido como coronavirus la Asociación Mexicana de Venta Online (AMVO) señaló que se detectó un incremento del 35% las compras digitales[104], mismas contempladas en el Código de Comercio en el Capítulo 1 de los mensajes de datos, *pues estas actividades son sometidas a la interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa*[105].

Por otro lado y como lo refiere el Código de Comercio, para cualquier acto de comercio en el que se establezcan métodos de certificación de comunicación (art.49) se debe observar la Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos[106] que refiere a las que medidas que garanticen que los actos de comercio dentro del país contengan la efectiva información para lograr la efectiva protección del consumidor y los requisitos para la conservación de los mensajes de datos que *"...consignen contratos, convenios o compromisos y que en consecuencia originen el surgimiento de derechos y obligaciones."* por cualquier medio electrónico o tecnología.

En el caso particular de los actos de comercio, los comerciantes deben resguardar los mensajes en formato ASN versión 1 (Notación Abstracta de Sintaxis) y en cualquier otro formato sin perjuicio de cualquier otro ordenamiento aplicable; si es información en medio físico, se podrá migrar al formato mencionado siempre y cuando se aplique un cotejo por un tercero legalmente

---

[104] (Herrera, 2020) Herrera Esther, Por Covid-19, ventas online se disparan, publicación del Diario Milenio, 31 de marzo de 2020. [Versión digital] [Consulta en agosto 2020]. Véase en: https://www.milenio.com/negocios/coronavirus-nuevoleon-pandemia-dispara-ventas-online

[105] (Comercio, 1989) Código de Comercio, Capítulo 1 de los mensajes de datos, Capítulo adicionado y publicado en el Diario Oficial de la Federación el 29 de agosto de 2003. [Versión digital] [Consulta en agosto 2020]: http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_de_Comercio.pdf

[106] (NOM-151-SCFI-2002, 2002) Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos, publicación en el Diario Oficial de la Federación el 20 de marzo de 2002. [Versión digital], [Consulta en agosto 2020]. Véase en: https://www.dof.gob.mx/nota_detalle_popup.php?codigo=727725

autorizado quien constatará que la migración "...se realice íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva...".

En caso de que sea necesario sujetar a análisis algún trato comercial vía mensaje, la propia Norma contiene las disposiciones y formas de interpretación de la información.

4.3.2 Contratos digitales

Independientemente de que el comercio como tal es un contrato, los contratos con alineación electrónica en el Código Civil Federal[107] (CCF) conlleva el uso de un Aviso de Privacidad y Acuerdo de Confidencialidad, este último en razón a las actividades primarias del origen del contrato; por lo cual se comparten principios con el Aviso de privacidad con algunas diferencias:

- consentimiento.- en el artículo 1803 indica que este podrá ser expreso o tácito:
    - *"...será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos"*, y
    - *"...el tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo…*"
- en el caso de la oferta de la celebración de un contrato a la que se le notifique un plazo de aceptación *"...queda ligada por su oferta hasta la expiración del plazo…"* (art. 1804); en embargo, en los casos en que no se señale un plazo de aceptación, *"...el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata."* (art. 1805).
- en el caso de la certeza de propuesta y aceptación por medios electrónicos, ópticos u otras tecnologías no necesariamente requiere una estipulación por el escrito previa para que cause efectos (último párrafo del art. 1811).

El Código señala que cuando sea exigible la impresión y firma de los interesados se requiere la impresión de la huella digital (art. 1834); sin embargo,

[107] (Federal, 1928) Código Civil Federal, publicación del 26 de mayo, 14 de julio, 3 y 31 de agosto de 1928. Última reforma 27 de marzo de 2020, [Versión digital], [Consulta en agosto 2020]. Véase en: http://www.diputados.gob.mx/LeyesBiblio/pdf/2_270320.pdf

en el caso del uso de los medios electrónicos, ópticos u otra tecnología la información generada o comunicada *"...en forma íntegra, a través de dichos medios sea atribuible a las personas obligadas y accesible para su ulterior consulta."* (Art. 1834 bis). Cuando la Ley o el caso exija su formalidad ante un acto jurídico las partes podrán realizar un tratamiento de la información (generar, enviar, recibir, archivar o comunicar) que contenga los términos exactos de las obligaciones estipuladas por los medios digitales, por lo que el fedatario público hará constar el origen de dicha información y conservar una versión íntegra de la misma para su ulterior consulta.

Aplicado al caso sobre el tratamiento de datos personales contenidos en los contratos resulta complicado intentar generalizar el uso de Avisos de privacidad para el tratamiento de la información pues como se ha vislumbrado, es necesario considerar diversas variables de los interesados y el alcance de las obligaciones contraídas en el caso en particular. Sin embargo, el obviar la negativa del uso de un Aviso de Privacidad y/o cláusula.

4.3.3 Certeza en la autenticidad de los mensajes de datos

La norma NOM-151-SCFI-2002[108] está dedicada a los mensajes de datos y digitalización de documentos y esta es perfectamente aplicable al momento en que las entidades digitalizan sus procesos y con ello, garantizar la integridad de la información. Cabe señalar, que el Código de Comercio considera el uso de los sellos digitales y el uso del hash como certificación de integridad de la información. Asimismo, los documentos signados con la firma electrónica pueden ser almacenados en la nube de los comprobantes de las transacciones, pues este tipo de documentos cuentan con diversas capas de seguridad.

En ese sentido, la Norma es de observancia general para los comerciantes que debían conservar los mensajes de datos con formato ASN 1 y *"...mostrados a través de un vaciado hexadecimal de su contenido en formato BER. Se incluyen las claves de criptografía que se usaron en la creación de los ejemplos con el propósito de que se pueda verificar la implantación de la presente Norma Oficial Mexicana..."*[109] que den origen a derechos y obligaciones en razón a

[108] (NOM-151-SCFI-2002, 2002). [Versión digital], [Consulta en agosto 2020]. Véase en: http://www.informatica-juridica.com/norma/norma-oficial-mexicana-nom-151-scfi-2002/
[109] *Ibidem, p.*

compromisos, contratos y/o convenios; por lo que la propiedad de la autoría de un algoritmo y ser atribuible inequívocamente del mensaje.

4.3.4 Expedientes electrónicos

En el caso de la integración de los expedientes electrónicos, la NOM señala se debe crear un mensaje ASN.1, la cual debe de observar las siguientes premisas:

- el nombre del expediente debe coincidir con el nombre con el que se identifica en el sistema de información en donde está o estuvo almacenado
- contener un índice y contenga el nombre y el compendio de cada archivo parcial que integra el expediente
- la identificación del operador del sistema de conservación, y
- su firma digital conforme a la Norma

4.3.5 Verificación de la autenticidad

De acuerdo a la NOM 151, la verificación de la autenticidad de una constancia se realiza mediante un sistema conforme a los pasos siguientes:

1. verificar la firma digital del servicio de certificación en la constancia
2. verificar la firma digital del operador del sistema de conservación en el expediente contenido en la constancia, y
3. recalcular el compendio de él o los archivos parciales y verificar que coincidan con los compendios asentados en el expediente.

La secuencia del ASN 1 para verificar, en forma ejemplificativa, es la siguiente:

```
Definición ASN.1
NCI-NOM-000-SECOFI DEFINITIONS : :=
BEGIN
.....................
nomIdentificacion OBJECT IDENTIFIER ::= {nom 373}
nomIPersonaFisica     OBJECT     IDENTIFIER     ::=
{nomIdentificacion 1}
nomIF-NOMBRE       OBJECT       IDENTIFIER       ::=
{nomIPersonaFisica 1}
nomIF-IFE OBJECT IDENTIFIER ::= {nomIPersonaFisica
2}
```

```
nomIF-CURP OBJECT IDENTIFIER ::= {nomIPersonaFisica
3}
nomIF-PASAPORTE      OBJECT      IDENTIFIER      ::=
{nomIPersonaFisica 4}
nomIF-CEDULAFISCAL     OBJECT     IDENTIFIER     ::=
{nomIPersonaFisica 5}
nomIPersonaMoral      OBJECT      IDENTIFIER      ::=
{nomIdentificacion 2}
nomIM-NOMBRE       OBJECT       IDENTIFIER       ::=
{nomIPersonaMoral 1}
nomIM-CURP OBJECT IDENTIFIER ::= {nomIPersonaMoral
2}
nomIM-CEDULAFISCAL     OBJECT     IDENTIFIER     ::=
{nomIPersonaMoral 3}
NombrePersonaFisica ::= SEQUENCE {
  nombreIdP PrintableString,
apellido1IdP PrintableString,
apellido2IdP PrintableString
}
IdentificadorPersona ::= SEQUENCE {
nombreIdP NombrePersonaFisica,
  tipoIdP OBJECT IDENTIFIER,
  contenidoIdP PrintableString
}
NumeroCertificado ::= PrintableString
IdentificadorUsuario ::= SEQUENCE {
personaFisicaMoral OBJECT IDENTIFIER,
nombreRazonSocialIdU  CHOICE  {NombrePersonaFisica,
PrintableString},
  tipoIdU OBJECT IDENTIFIER,
  contenidoIdU PrintableString,
numeroCertificadoU NumeroCertificado,
representanteIdU  IdentificadorPersona  OPTIONAL  --
Este campo es para el -- representante legal
```

```
}
AlgorithmIdentifier ::= SEQUENCE {
  algorithm OBJECT IDENTIFIER,
  NULL
}
NombreConstanciaOP ::= PrintableString
FirmaUsuarioOP ::= SEQUENCE {
algoritmoFirma AlgorithmIdentifier,
  firma BIT STRING
}
FirmaConstanciaOP ::= SEQUENCE {
algoritmoFirma AlgorithmIdentifier,
  firma BIT STRING
}
ResumenOP ::= SEQUENCE {
  algoritmoresumen AlgorithmIdentifier,
  resumen BIT STRING
}
Folio-UsuarioOP ::= INTEGER
ArchivoParcial ::= SEQUENCE {
titulo NombreOP,
tipo TipoOP,
contenido BIT STRING
}
Entrada-al-Indice ::= SEQUENCE {
titulo NombreOP,
resumen ResumenOP
}
Expediente ::= SEQUENCE {
nombre-expediente PrintableString,
indice SET OF Entrada-al-Indice,
id-usuario IdUsuarioOP,
firma-usuario FirmaUsuarioOP
}
```

```
Sello ::= SEQUENCE {
  estampa-de-tiempo UTCTime,
emisor EmisorOP,
folio-usuario Folio-UsuarioOP
}
Constancia ::= SEQUENCE {
nombre-de-la-constancia NombreConstanciaOP,
expediente Expediente,
marca-de-tiempo Sello,
firma-constancia FirmaConstanciaOP
}
END
==========================================
```

Como puede observarse, el código conlleva una estructura técnico-lógica, desglosada de la siguiente forma:

- Contiene identificadores del tipo de archivo conforme a la NOM 151
- El campo “firma-usuario del objeto expediente” es la firma digital de los campos “nombre-expediente, índice e id-usuario” -en ese orden- y son mostrados en bytes
- En el objeto sello, el campo “estampa-de-tiempo” estipula la fecha y hora en formato GMT o IMT con el que se creó el sello; el emisor es el representante del prestador de servicios de certificación que creó el sello. El “folio-usuario” es un número secuencial ascendente otorgado a cada usuario del prestador de servicios de certificación de cada operación registrada
- El objeto Constancia contiene un campo “nombre-de-la-constancia” que almacena el nombre del archivo de computadora en la que se guardará la constancia en el sistema del prestador de servicios. La certificación contiene el tipo “Expediente” con el que es guardado con el ente certificador con un sello fechado y emitido por este, al momento de crear la Constancia. El campo firma-constancia es la firma digital de los campos “nombre-de-la-constancia”, “expediente”, “marca-de-tiempo” en ese orden y presentados en una secuencia de bytes.

- La línea "========" enmarca el principio y fin del archivo ASN 1, no pertenece al archivo

La función lógica de la codificación se ejemplifica de la siguiente forma: primero se presentan dos archivos a conservar; posteriormente, se construyen cada uno de los objetos ASN.1 correspondientes: *"archivos parciales", "expediente"* almacenado con nombre y formato "*docusuario.ber*" y la "constancia" en el archivo "*recibo.ber*". Así, los nombres de los archivos que almacenan el expediente, constancia y archivos parciales están almacenados en los campos *"nombre-expediente", "nombre-de-la-constancia"* y *"título*".

Cabe mencionar que se utilizan claves privadas para verificar los objetos ASN.1 y con ello, constatar las firmas de los documentos mencionados. Al momento de la generación de las claves, no se genera una clave pública y no se pierden los datos de las claves, por lo que las claves y resultados pueden ser usadas solo para verificar los formatos.

4.3.6 Uso del Front End de Comunicaciones

El Front End Comunicaciones (FEC) es un programa desarrollado para el uso de las comunicaciones de aplicaciones con arquitectura cliente/servidor para el intercambio de mensajes en tiempo real; en palabras técnicas, permite especificar el protocolo de comunicación entre los clientes del prestador de servicios de certificación y los sistemas de la NOM 151; en otras palabras, el FEC es un mecanismo de enlace entre clientes y servidores. Es de destacar, que la Secretaría de Economía tiene un sistema de referencia estandarizado para los prestadores de servicios de certificación y su uso correcto.

Visto su uso en transacciones de comercio y celebración de contratos y/o convenios entre particulares que conllevan el uso de los datos personales, este protocolo tiene los siguientes objetivos principales:

- Simplificar la programación de los sistemas con arquitectura cliente/servidor, descartando la estipulación del manejo de las comunicaciones
- Permita un ambiente de operación flexible para la interacción de programas de creados en distintas plataformas, sistemas operativos y lenguajes
- Los sistemas utilizados operen en tiempo real

- Suple actividades de un servidor, tales como: autenticar a los clientes, notificar la conexión o desconexión de un cliente, notificar a los clientes si un servidor está en servicio o no, y verificar el estado de clientes y servidores conectados

Con esta información el FEC provee transparencia en la localización de clientes y servidores, permite la interacción de programas de distintas plataformas y minimiza el uso de recursos de la red de comunicaciones.

La operación del FEC comienza con la aceptación de conexiones de los clientes, su identificación y notificación de la conexión con el cliente con el servicio deseado.

La descripción básica de su función es la siguiente:

```
Cliente <—> FEC <—> Servidor
```

Cabe señalar que los mensajes constan de dos partes: “encabezado” y “cuerpo” construidos con los tipos de lenguaje de programación: char, int, short, string y su funcionamiento se basa en acordar el tipo de formato del mensaje.

```
Encabezado            Destino + Acción + Tamaño
FEC$Cliente      1 byte  1 byte  1 byte
```

Explicada la estructura, el campo de “Destino Servidor o Cliente” es el destinatario del mensaje; la “Acción” es la instrucción a realizar; y “Tamaño” es la longitud en bytes del cuerpo del mensaje, sin incluir el encabezado.

El encabezado tiene una longitud de 12 bytes y la siguiente estructura:

```
Encabezado= Origen+Acción+Año+Mes+ Día + Hora + Tamaño
FEC=> 1 byte 1 byte 2 byte 2 byte 2 byte 2 byte 2 byte
```

Los elementos que del encabezado se desglosan de la siguiente forma: “Origen” del mensaje; “Acción” o instrucción a aplicar, “Año, Mes, Día” que el FEC recibió el mensaje; “Hora” que el FEC recibió el mensaje; y “Tamaño” en bytes del mensaje. Es de señalar que existen dos tipos de encabezado a razón del registro detallado de los mensajes transferidos a los servidores mediante el FEC y provee seguridad de la fecha y hora de recepción certificada. Es importante señalar que el protocolo de comunicación del FEC es abierto y la información viaja en formato de red.

Con la base de la información presentada actualmente, al momento de que alguna entidad requiera la aplicación de la NOM 151 podrá verificar el lenguaje,

los mensajes reservados del FEC y el tipo de respuestas que puede presentar el FEC.

Para el objeto de uso de esta información y/o aplicación de la NOM 151 en operaciones transaccionales por comercio electrónico y la celebración de contratos y/o convenios, las entidades físicas y morales deben de observar los formatos y medios de conservación con el objetivo de garantizar la integridad de la información y de los mensajes de datos, como forma de respeto a los derechos de los consumidores e interesados, así como certeza jurídica. Lo cual coadyuva a la ciberseguridad; pues permite *"...la implementación de un conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual."*[110].

4.3.7 Uso de la firma electrónica avanzada

En México fue publicada la Ley de Firma Electrónica Avanzada[111] (FIEL) para la celebración de actos contemplados en la legislación y la emisión de certificados digitales a personas físicas. Con esta herramienta se genera un "certificado digital", una "clave pública" y una "clave privada" para la verificación de la autenticidad de la firma y por consiguiente, la constatación de la voluntad del signatario.

> *Artículo 2, fracción XIII: Firma Electrónica Avanzada: el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa;*

Asimismo, dicha legislación mexicana señala que el mensaje de datos es toda información transmitida por medios electrónicos:

> *Artículo 2, fracción XVII: Mensaje de Datos: la información generada, enviada, recibida, archivada o comunicada a través de medios de*

[110] Diccionario Oxford, Definición de ciberseguridad. [Versión digital]. [Consulta en agosto 2020]. Véase en: https://www.lexico.com/es/definicion/ciberseguridad

[111] Ley de Firma Electrónica Avanzada, publicación del 11 de enero de 2012, [Versión digital], [Consulta en agosto 2020]. Véase en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf

comunicación electrónica, que puede contener documentos electrónicos;

Considerando que la normativa reconoce que el uso de la firma electrónica avanzada es equiparable al uso de la firma autógrafa, su uso es limitado conforme a los actos lícitos y lo que existan por dictamen; no obstante, las disposiciones de esta Ley no son aplicables en materia fiscal, aduanera y financiera (art.4). En los actos de comercio e inscripciones en el Registro Público de Comercio, el uso de la FIEL se rige por el Código de Comercio y ordenamientos aplicables en la materia, sin perjuicio de la aplicación de lo dispuesto en esta Ley.

Artículo 7. La firma electrónica avanzada podrá ser utilizada en documentos electrónicos y, en su caso, en mensajes de datos. Los documentos electrónicos y los mensajes de datos que cuenten con firma electrónica avanzada producirán los mismos efectos que los presentados con firma autógrafa y, en consecuencia, tendrán el mismo valor probatorio que las disposiciones aplicables les otorgan a éstos.

Para ello, la Firma atiende una serie de principios a cumplir contemplados en el numeral 8 de la presente Ley:

I. *Equivalencia Funcional* en un documento electrónico o en un mensaje de datos, satisfaciendo el requisito de firma al igual que la firma autógrafa;

II. *Autenticidad de la firma* en un documento digital o mensaje de datos otorga certeza jurídica de la voluntad del firmante y sus consecuencias jurídicas;

III. *Integridad y originalidad* del contenido del documento o mensaje de datos desde su firma ante la comunicación del archivo;

IV. *Neutralidad Tecnológica* aplicada para la emisión de certificados digitales y los servicios relacionados sin favorecer o excluir alguna tecnología;

V. *No Repudio* la firma en los documentos digitales o mensajes garantiza la autoría e integridad de la información, y la firma es atribuible al firmante, y;

VI. *Confidencialidad*, pues su cifrado sólo puede ser abierto y visto correctamente por el firmante y el receptor

Bajo estos principios, el artículo 9 indica que para que la FIEL pueda ser utilizada en cualquier forma jurídicamente contemplada, debe de contar con un *"certificado digital vigente, emitido u homologado"* en términos de la propia Ley y una "*llave privada*" de uso exclusivo del titular.

Para el uso de la Firma Electrónica en entidades gubernamentales, conforme al artículo 13, *"Cada dependencia y entidad creará y administrará un sistema de trámites electrónicos que establezca el control de accesos, los respaldos y la recuperación de información, con mecanismos confiables de seguridad, disponibilidad, integridad, autenticidad, confidencialidad y custodia…"*, siendo la Secretaría quién dicte los lineamientos para su cumplimiento. Ello concatena con la información pública a reserva de lo dispuesto en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y responsabilidad de la entidad para su manejo, seguridad y protección de la información (artículo 14).

Respecto a la conservación de la información y mensajes digitales, la Ley de Firma Electrónica Avanzada refiere su conservación a la Norma contemplada en el artículo 49 del Código de Comercio: la NOM 151 (artículo 15).

Finalmente, la interpretación de esta Ley está a cargo de la Secretaría de Economía y el Servicio de Administración Tributaria (SAT) y ante la suplencia normativa se atenderá la Ley Federal de Procedimiento Administrativo, el Código Civil Federal y el Código Federal de Procedimientos Civiles.

Como hemos visto a lo largo de este apartado, la Firma Electrónica Avanzada es una forma de certificación de la voluntad en documentos digitales y certificación de mensajes; pues al ser de uso exclusivo del titular y con los aditamentos para la no refutación y autenticidad de la misma, es casi inefable la refutación de la misma. Así, para posibles consultas de los particulares y/o de la autoridad podrá realizarse con certeza jurídica con la aplicación de la Norma 151, cumpliendo así con los principios de la ciberseguridad.

Lo anterior denota la inefabilidad de la inmersión de la tecnología y la automatización de los procesos de las entidades en relación a la vida humana; pues la simplificación de los procesos y minimización de riesgos y costos permite que el ciclo de la economía continúe mediante las nuevas tecnologías de la información. Asimismo, al amparo de la normativa mexicana toda actividad debe acreditar su legitimidad jurídica.

4.3.8 Avisos de privacidad

Aunado a una estructura jurídica adecuada para la salvaguarda de la información y respeto a los derechos de las personas, en México es un requisito de Ley, el tratamiento de los datos personales y la información; los avisos de privacidad coadyuvan a certeza jurídica y minimización de riesgos para las entidades en relación a las actividades que estos desarrollen, por lo que la creación de este documento no debe subestimarse y debe implementarse de forma correcta e idónea.

Existen recomendaciones internacionales para la presentación del documento y los requisitos estipulados en la legislación mexicana, tal como se refirió en el capítulo anterior, por lo que enunciare los principios aplicados a nuestra normativa referenciados en la Ley de la materia a los tipos de Avisos de Privacidad:

En mi consideración, los primeros pasos para la creación del correcto Aviso de Privacidad es determinar la entidad y naturaleza jurídica; el giro o actividades estipuladas para la creación; en listado de las tecnologías o plataformas electrónicas internas y externas aplicadas para su funcionamiento; determinación del tipo de datos personales utilizados y su nivel de riesgo; grado de acercamiento o contacto con los titulares de los datos; existencia o no de la tercerización o transferencia de datos personales a entidades dentro del país o uso de las transferencias internacionales; y en especial consideración, la descripción del flujo de la información y/o proceso operacional, -ello permite detectar los factores de riesgo-; y la determinación de las garantías del respeto de los Derechos de las personas.

Persona Física/Persona moral:

Giro/actividad principal:

Tecnologías/Plataformas de uso:

Plataformas externas:

Operación general de la empresa:

Tercerización del tratamiento de datos personales:

Transferencias internacionales de los datos personales:

Flujo de la información-proceso:

Ante ello, se presentan algunas propuestas sobre el uso general de los diferentes tipos de Avisos de Privacidad; sin embargo, es necesario adecuar al

giro y conforme al nivel de riesgo de la información, dar expresa protección y seguridad de la información a los titulares.

4.3.8.1 Aviso Integral

Fundamentación: Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), artículos 8, 15, 16, 33 y 36. Reglamento de la Ley (RLFPDPPP), artículos 14, 30, 41, 68, 90 y 102. Título vigésimo de los presentes Lineamientos y Decimoctavo de los Lineamientos de los Avisos de Privacidad (Publicación del 17 de enero de 2013 del Diario Oficial de la Federación).

Propuesta del Aviso de Privacidad Integral

De conformidad con lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[112] *(LFPDPPP) y el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*[113] *(RLFPDPPP), publicada en el Diario Oficial de la Federación el 5 de Julio de 2010, la persona física o moral* _____ *, que en lo consiguiente se le denominará "el responsable" y/o sus empresas afiliadas, subsidiarias o relacionadas, por este medio informan las finalidades del tratamiento de los datos personales y sensibles mediante consentimiento tácito o expreso de los titulares derivado de las actividades industriales, comerciales y de servicios realizadas dentro de los Estados Unidos Mexicanos y sus medios de garantía para el acceso, protección, integridad y confidencialidad de la información.*

Para los efectos del presente Aviso de Privacidad se entenderá por Datos Personales (art 3, fr. V LFPDPPP) cualquier información concerniente a una persona física identificada o identificable. Serán datos sensibles (art. 3 fr. VI LFPDPPP) son todos los datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, tal como origen racial o étnico, estado de salud presente y futuro, información genética,

[112] Ley Federal de Protección de Datos Personales…

[113] Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Publicación del Diario Oficial de la Federación el 21 de diciembre de 2011. [Versión digital] [Consultado en agosto de 2020]. Véase en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Los titulares podrán limitar el uso, divulgación o realizar el ejercicio pleno de sus derechos de Acceso Revocación, Cancelación y Oposición de sus derechos (ARCO) de su tratamiento en cualquier momento sin efectos retroactivos mediante el envío de la solicitud al correo electrónico: privacidad@sfe.com.mx o al domicilio legal señalado (art. 16 fr. III y art.33 LFPDPPP y art. 90 RLFPDPPP).

Para los efectos relacionados con el presente aviso de privacidad, "el responsable" asumirá su compromiso jurídico en los términos previstos por la Ley (art. 15, fr. I) del tratamiento que dé a dichos Datos Personales y/o Datos Personales Sensibles y señala como domicilio para efectos legales el ubicado en _____ (puede ser el domicilio legal u otro distinto).

Los datos sujetos a tratamiento (art. 15) por parte del responsable" son: identificación (nombre completo, CURP, RFC, cédula profesional, pasaporte, etc.), domicilio, información recabada del titular (datos bancarios, datos patrimoniales, y datos de contacto).

**Si se realizara un tratamiento de datos sensibles sujetos a tratamiento se encuentran, se enlista la siguiente información a recabar: (información sobre su estado de salud, enfermedades prescritas o padecidas, uso de medicamentos o tratamientos, uso de datos biométricos). Mismos que serán recabados de la siguiente forma: _____.*

Las finalidades del tratamiento (art. 16 fr. II) serán utilizados para fines de: (venta, estadísticos, realización de encuestas, consultas, investigaciones, revisiones y seguimiento relacionados con los servicios prestados y productos comercializados por "el responsable" (art. 30 RLFPDPPP), así como para contacto de clientes, usuarios y/o proveedores para cualquier tema relacionado con dichos productos y servicios, participación en programas de adhesión a tratamientos, llamadas de cortesía, etc.).

Declara "el responsable" que no realiza tratamiento de datos personales para finalidades distintas o no compatibles o análogas con

las finalidades expuestas, a excepción de las que permita de forma explícita la ley o reglamento, o se haya obtenido el consentimiento del titular para el nuevo tratamiento (art. 43 RLFPDPPP).

Para efectos de consentimiento del tratamiento de los datos personales (art.8 LFPDPPP, y el art.14 del RLFPDPPP), "el responsable" se valdrá del consentimiento expreso, el brindado de forma verbal, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Asimismo, se valdrá el consentimiento tácito cuando el titular no se oponga a su tratamiento ante la puesta a su disposición el presente Aviso de privacidad.

**Para el tratamiento de datos sensibles (art. 9), "el responsable" obtendrá el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.*

Declara "el responsable" que las bases de datos creadas con los datos sensibles de los titulares únicamente tendrán como finalidad: (control interno para comercialización de los bienes y servicios, control de acceso, etc.).

Al proporcionar datos personales a "el responsable", si el titular no manifiesta su negativa para el tratamiento de su información, se entenderá que ha otorgado su consentimiento para su tratamiento (art. 14, párrafo 3).

Respecto a la transferencia de datos personales y/o datos personales sensibles (art. 16 fr. V y 36 LFPDPPP y art. 68 RLFPDPPP), "el responsable podrá" transferir a: (sociedades subsidiarias, filiales, afiliadas y controladoras de "el responsable", proveedores, etc). La información que podrá ser transferida es: (datos de identificación, datos de contacto, empresas de mercadotecnia para fines publicitarios, empresas de mensajería, etc.).

___ Acepto la transferencia de los datos personales (art. 36, párrafo segundo)

Declara "el responsable" que ha adoptado y mantiene las medidas de seguridad, administrativas, técnicas y físicas, necesarias para proteger sus datos personales y datos personales sensibles contra daño,*

pérdida, alteración, destrucción o el uso, acceso a tratamiento no autorizados.

El Aviso de Privacidad se encuentra disponible (art. 14 y 102 RLFPDPPP) en nuestra página de internet: _____ y/o en _____. Cualquier modificación a este aviso de privacidad estará disponible en dichas páginas de Internet.

4.3.8.2 Aviso simplificado

Fundamentación: artículo 17, fracción II de la LFPDPPP y el numeral 27 de su Reglamento, y Trigésimo cuarto de los Lineamientos de los Avisos de Privacidad, (Publicación del 17 de enero de 2013 del Diario Oficial de la Federación).

De conformidad con lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP), publicada en el Diario Oficial de la Federación el 5 de Julio de 2010, la sociedad y/o sus empresas afiliadas, subsidiarias o relacionadas, por este medio informan las finalidades del tratamiento de los datos personales y sensibles mediante consentimiento tácito o expreso de los titulares derivado de las actividades industriales, comerciales y de servicio realizadas dentro de los Estados Unidos Mexicanos y sus medios de garantía para el acceso, protección, integridad y confidencialidad de la información.*

Para los efectos relacionados con el presente aviso de privacidad, la persona física o moral, en lo consiguiente, "el responsable" asumirá las obligaciones jurídicas en los términos previstos por la Ley (art. 15, fr. I) del tratamiento que dé a dichos Datos Personales y Datos Personales Sensibles y señala como domicilio para efectos legales el ubicado en: _____.

Las finalidades del tratamiento (art. 16 fr. II) serán utilizados para: (fines de venta, estadísticos, realización de encuestas, consultas, investigaciones, revisiones y seguimiento relacionados con los servicios prestados y productos comercializados por "el responsable" - fines de

prospección comercial - (art. 30 RLFPDPPP), así como para contacto de nuestros clientes, usuarios y/o proveedores para cualquier tema relacionado con dichos productos y servicios, llamadas de cortesía, etc.) o cualquier otro enunciado en el presente Aviso de Privacidad.
Declara "el responsable" no realizar tratamiento de datos personales para finalidades distintas o no compatibles o análogas con las finalidades expuestas, a excepción de las que permita de forma explícita la ley o reglamento, o se haya obtenido el consentimiento del titular para el nuevo tratamiento (art. 43 RLFPDPPP).

El Aviso de Privacidad integral se encuentra disponible (art. 14 y 102 RLFPDPPP) en nuestra página de internet: _____ y/o _____. Cualquier modificación a este aviso de privacidad estará disponible en dichas páginas de Internet.
(Cuando el aviso de privacidad simplificado se haga del conocimiento de los titulares por medios remotos o locales de comunicación electrónica, óptica u otra tecnología, por ese mismo medio deberá ponerse a disposición el aviso de privacidad integral. Sin perjuicio de que el titular pueda solicitar el aviso de privacidad integral por un medio distinto al indicado en el aviso de privacidad simplificado, en ejercicio de su derecho de acceso, art. 23 de la LFPDPPP.)

4.3.8.3 Aviso corto

Fundamentación: artículo 28 del RLFPDPPP y Decimoctavo de los Lineamientos de los Avisos de Privacidad, (Publicación del 17 de enero de 2013 del Diario Oficial de la Federación).

De conformidad con lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP), publicada en el Diario Oficial de la Federación el 5 de Julio de 2010, la persona física o moral: _____, en lo consiguiente "el responsable" y/o sus empresas afiliadas, subsidiarias o relacionadas, por este medio informan las

finalidades del tratamiento de los datos personales y sensibles mediante consentimiento tácito o expreso de los titulares derivado de las actividades industriales, comerciales y de servicios realizadas dentro de los Estados Unidos Mexicanos y sus medios de garantía para el acceso, protección, integridad y confidencialidad de la información.*

Para los efectos relacionados con el presente aviso de privacidad, la persona física o moral: _____ será responsable, en los términos previstos por la Ley (art. 15, fr. I) del tratamiento que dé a dichos Datos Personales y Datos Personales Sensibles y señala como domicilio para efectos legales el ubicado en: _____.

Las finalidades del tratamiento (art. 16 fr. II) serán utilizados para: (fines de venta, estadísticos, realización de encuestas, consultas, investigaciones, revisiones y seguimiento relacionados con los servicios prestados y productos comercializados por "el responsable", fines de prospección comercial, contacto de nuestros clientes, usuarios y/o proveedores para cualquier tema relacionado con dichos productos y servicios, llamadas de cortesía, etc.), o cualquier otro estipulado en el presente Aviso (art. 30 RLFPDPPP).

Declara "el responsable" que no realiza tratamiento de datos personales para finalidades distintas o no compatibles o análogas con las finalidades expuestas, a excepción de las que permita de forma explícita la ley o reglamento, o se haya obtenido el consentimiento del titular para el nuevo tratamiento (art. 43 RLFPDPPP).

Usted podrá conocer el Aviso de Privacidad Integral en: _____ (art. 14 y 102 RLFPDPPP). Cualquier modificación a este aviso de privacidad estará disponible en dichas páginas de Internet.

(La divulgación inmediata de la información antes señalada no exime al responsable de la obligación de proveer los mecanismos para que el titular conozca el contenido del aviso de privacidad integral).

Anotación de uso del Aviso de Privacidad Corto: "...Cuadragésimo. Al considerar que el aviso de privacidad corto se utiliza cuando el espacio para la obtención de los datos personales y para difundir el aviso de privacidad es mínimo y limitado, y los datos personales recabados son mínimos.".

En ese sentido, es necesario diferenciar el concepto de “transmisión” y “transferencia” de datos personales, jurídicamente ambos conceptos son completamente diferentes, ya que:

- la Transmisión de Información se lleva a cabo cuando se comunican datos para que un tercero o encargado realice un tratamiento de estos a razón de un contrato, por lo cual asumirá las obligaciones del responsable, y
- la Transferencia de Información se perfecciona cuando el responsable se ubique en un país y envíe los datos a otro fuera del país; lo cual quedará a reserva de los países el tratamiento de los datos en función a los acuerdos internacionales y su legislación

De forma general un contrato de Transmisión de datos personales, debe de considerar:

- Las medidas de seguridad tecnológicas o físicas sobre los canales de transmisión
- Las finalidades de uso autorizado por el titular
- Las medidas de seguridad a implementar por el encargado para evitar la alteración, sustracción y / o destrucción no autorizados
- Los canales para ejercer los derechos del titular
- El uso de la información al término del contrato
- La responsabilidad jurídica por el incumplimiento del contrato ante el tratamiento de los datos, fugas, alteraciones y/o acceso no autorizado

Cabe mencionar que algunos países adoptaron la figura de “encargado interno” de las organizaciones con la finalidad de formalizar su responsabilidad y atender el marco legislativo aplicable a la materia; no obstante, queda un punto de reflexión para su cumplimiento ante el uso de las nuevas tecnologías de la información para la obtención, uso, transmisión y destrucción de esta información.

4.3.9 Punto disruptivo ante la Inteligencia artificial (AI) y aprendizaje automatizado (*machine learning*)

De acuerdo con la Doctora en BigData y Protección de Datos, Elena Gil González, existe una tensión entre la transparencia exigida por el Reglamento vs los avances tecnológicos, tal como la BigData o el aprendizaje computacional, pues al ser “alimentadas” por bases de datos generados mediante dispositivos inteligentes, la huella digital generada y el comercio electrónico plenamente no

son considerados todos los usos posibles al momento de la recopilación, por lo que se realiza un tratamiento automatizado por algoritmos[114].

En ese sentido, Gil explica que anteriormente se exigía que los datos fueren tratados “de manera leal y lícita”; sin embargo, el artículo 5 del Reglamento General de Protección de Datos (RGPD) establece que éstos sean tratados “de manera lícita, leal y transparente”, lo cual figura a la transparencia como un principio básico de la protección de datos.

Asimismo, refiere que el especialista Puyol Montero asegura que los principios de protección de datos constituyen el contenido esencial de este derecho, y que, a través de los mismos, se configura un sistema de tutela que garantiza una utilización más racional de los datos personales. Lo cual se traduce en el empoderamiento de los titulares y la transparencia sobre la información a entregar al interesado (RGDP, artículos 13 y 14).

Aunado a lo señalado en la legislación mexicana, el Reglamento apunta que la transparencia sobre la información dirigida al público o interesado debe ser concisa, de fácil acceso y de lenguaje sencillo con orientación informativa sobre el tratamiento de datos y sus finalidades (art. 12, 29, 58 y 60 del Reglamento).

Sin embargo, la Directiva de Protección de Datos de la Unión Europea de 1995 (Directiva 95/46/EC) se amplió la obligación de informar al interesado sobre la existencia de las decisiones automatizadas (artículo 15 de la Directiva y numeral 22 del RGPD en relación a los artículos 13, 15 y 71), la elaboración de perfiles (art. 13.2.f), art. 14.2.g) y art. 15.1.h)), y la obligación de brindar al interesado la información en los casos en los que el responsable proyecte el uso ulterior de datos personales para un fin no contemplado originalmente (art. 13.3 y art. 14.4).

Doctrinarios como Veale y Edwards, 2017; Wachter et al, 2016; y Hildebrandt, 2016 señalan que pese a las nuevas obligaciones de transparencia de los responsables del tratamiento de información personal y sus posibles consecuencias. No obstante, esto podría verse entorpecido ante el funcionamiento técnico-lógico de los algoritmos.

---

[114] Gil González Elena, Big data, privacidad y protección de datos, Agencia Española de Protección de Datos, XIX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos, publicación 2015, [Versión digital], [Consulta septiembre 2020]. Véase en: https://www.aepd.es/sites/default/files/2019-10/big-data.pdf

Ante ello, la Doctora Elena Gil resalta la **necesidad de definir la temporalidad de la creación de las bases de datos**, pues la información proporcionada antes (ex ante) de definir el modelo algorítmico y cualquier decisión automatizada sobre una persona. Y en segundo término estaría el posterior a la creación del modelo del algoritmo (ex post), la recopilación de datos de una persona y la toma de decisiones automatizadas[115]. Por lo que al considerarse los artículos 13, 14 y 15 del Reglamento aparentemente refieren a la proporción ex ante sobre el algoritmo y no al ex post sobre las decisiones automatizadas y la elaboración de perfiles.

Para ello, para Gil resulta necesario considerar que el responsable tiene el máximo de información de los sujetos y si no se han producido consecuencias, es momento de transparentar e informar del funcionamiento del algoritmo y sus consecuencias. De esta forma, la toma de decisiones automatizadas se fundamentaría en el consentimiento explícito en un contrato y el principio de transparencia de la información en aras de la *"...prevención de acumulación de datos y las desviaciones de sus finalidades ya que el principal riesgo es la acumulación de información…"*[116].

Gil resalta que al momento de la decisión automatizada se requiere instaurar garantías relativas al derecho del interesado sobre expresar su opinión ante la interpretación y la potencia predictiva, pues el aprendizaje computacional no es un oráculo capaz de predecir con certeza una realidad futura basado en una lógica definida. Sin embargo, el Reglamento Europeo señala que el Derecho a no ser objeto de decisiones automatizadas (art. 22 y 71) siempre y cuando exista un contrato entre el titular y el encargado; y la actividad sea permitida por el Estado para el respeto a los derechos e intereses legítimos del interesado.

En conclusión, se considera que el Reglamento atiende primordialmente a la transparencia y la protección de los sujetos en relación con la toma de decisiones automatizadas; sin embargo, la ambigüedad de conceptos permite la flexibilidad del uso de técnicas para el tratamiento de la información y su limitante es el interés del titular sobre la existencia de decisiones automatizadas, el funcionamiento de los sistemas y las garantías para el ejercicio u oposición en este tipo de decisiones.

---

[115] Ibidem. p. 41
[116] *Ibidem, p. 41*

4.3.10 Precisiones y recomendaciones de seguridad jurídica para el Tratamiento de Datos Personales

El Instituto Nacional de Acceso a la Información y Protección de Datos (INAI) con el marco facultativo del artículo 38 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) podrá *"...difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente Ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento."* (Artículo 38).

Para efectos de interpretación, emitir criterios y recomendaciones (art. 39), así como divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información y tratamiento de los datos personales e imponer las sanciones ante violaciones a la Ley, entre otras.

La Secretaría de Economía (SE) difunde información sobre las obligaciones de la protección de datos personales en la iniciativa privada nacional e internacional con actividad comercial en México. Promueve mejores prácticas comerciales respecto a la economía digital y el desarrollo económico nacional. Además, podrá emitir lineamientos de contenido y alcance de los avisos de privacidad en coadyuvancia con el INAI; celebrar convenios con cámaras de comercio, asociaciones y organismos empresariales en la materia; elaborar estudios y políticas de comercio electrónico y promover el desarrollo de las Tecnologías de la Información y Comunicación; tiene la facultad de participar en procedimientos sancionadores, así como de las mejores prácticas internacionales y la obligación de adoptar Acuerdos Internacionales ratificados en el país.

4.3.11 Uso de los Drones y la protección de datos

La Agencia Española de Protección de Datos (AEPD) emitió un comunicado[117] sobre el uso de vehículos aéreos sin tripulación, mejor conocidos como *drones*, en la que refiere que el uso de estos dispositivos por civiles y autoridades implican el uso del *Global System Position* (GPS) y una cámara de vídeo adaptada a distintas funcionalidades (cámaras termográficas, de visión nocturna, escáner 3D,

[117] (Datos, Drones y protección de datos, 2019) Agencia Española de Protección de Datos, Drones y Protección de Datos, publicación de septiembre de 2019. [Versión digital], [Consulta en julio 2020] Véase en: https://www.aepd.es/sites/default/files/2019-09/guia-drones.pdf

dispositivos WIFI y/o Bluetooth, sistemas de detección de dispositivos móviles, etc.), por lo que es necesario garantizar el derecho a la protección de datos.

Considerando que un dato personal es toda información sobre una persona física identificada o identificable por lo que cualquier operador registre o procese imágenes, videos, sonido, datos biométricos y/o datos de geolocalización están sujetos a la normativa de protección de datos.

La Agencia refiere que los principales usos de estos dispositivos es para la video vigilancia, inspección de infraestructuras, levantamientos topográficos, uso en la agricultura, fotografía y video, por mencionar algunos; sin embargo, en México, existe la Ley de Aviación Civil[118] que apunta únicamente a:

- Tratamiento de datos personales: para video vigilancia o vigilancia por sensores (por ejemplo, el seguimiento de dispositivos móviles) y,
- Operaciones sin uso de datos personales para la inspección de terrenos e infraestructuras, topografía, fotografía y vídeo.

Ante este contexto, se puede determinar que cualquier imagen o vídeo captado por un dron puede transgredir los derechos a la protección de datos, en caso de que las personas que ahí se visualicen sean identificables.

De forma enunciativa, el marco normativo es la Ley de Aviación Civil (LAC) en su numeral 2 fracciones 1 Bis al Sexies; artículo 6 fracción XVIII y artículo 88 Bis; la Circular Obligatoria CO AV-23/10 R4; respecto a los requisitos para operar un sistema de aeronave pilotada a distancia (RPAS) se enuncia en el Proyecto de Norma PROY-NOM-107-SCT3-2016, publicada el 20 de septiembre de 2017. Asimismo, existen Reglas de vuelo de la Dirección General de Aeronáutica Civil[119].

Para la instalación de video vigilancia por drones en lugares públicos debe considerar lo siguiente:

- La responsabilidad de la grabación fue por mandato de un tercero, este es el que tiene la responsabilidad del tratamiento de datos
- Aplicar el principio de recopilación mínima de datos para anonimizar
- Implementar protocolos de comunicación seguro a fin de prevenir el acceso a las transmisiones, y aplicación del cifrado de los datos, y

[118] (Civil, 1995) Ley de Aviación Civil, publicación del 12 de mayo de 1995. [Versión digital], [Consulta en julio 2020]. Véase en: http://www.diputados.gob.mx/LeyesBiblio/pdf/25_180618.pdf

[119] (Transportes, 2017) Secretaría de Comunicaciones y Transportes, Dirección General de Aeronáutica Civil, Requerimientos para operar un sistema de aeronave pilotada a distancia (RPAS) en el Espacio aéreo mexicano, publicado el 25 de julio de 2017. [Versión digital], [Consulta en agosto 2020]. Véase en: http://www.sct.gob.mx/fileadmin/DireccionesGrales/DGAC-archivo/modulo3/co-av-23-10-r4.pdf

- Habilitar mecanismos del RGPD con la finalidad de adoptar las medidas adecuadas para el adecuada privacidad por defecto y los mecanismos de oposición para los posibles afectados

4.3.12 Protección de Datos personales de personas morales

En el caso de México, la Suprema Corte de Justicia de la Nación (SCJN) emitió una tesis número 2005522, publicada en la Gaceta del Semanario Judicial de la Federación, nombrada: ***PERSONAS MORALES. TIENEN DERECHO A LA PROTECCIÓN DE LOS DATOS QUE PUEDAN EQUIPARARSE A LOS PERSONALES, AUN CUANDO DICHA INFORMACIÓN HAYA SIDO ENTREGADA A UNA AUTORIDAD*** [120].

Con ello, la Corte refirió que con base en el párrafo segundo del artículo 16 de la Constitución -sobre el derecho a la protección de datos personales- para el control de los titulares ante el tratamiento de su información y se salvaguarda su derecho a la privacidad, por lo que ante la imposibilidad de que una empresa tenga derecho a la intimidad o la vida privada; sin embargo, estas poseen información -económica, comercial o relativa a su identidad- susceptible de transmisión arbitraria que pueda afectar o anular sus derechos o desarrollo.

Por ello, los entes jurídicos tienen derecho a la privacidad y de protección de datos que le sean inherentes, independientemente a sus obligaciones en materia de transparencia e información pública -principio de máxima publicidad y disponibilidad-. En ese sentido, cualquier entidad gubernamental tiene la obligación de dar tratamiento *confidencial* a la información *cuando tenga el carácter de privada* solo por poseer datos que pudieran equipararse a los personales.

> ***PERSONAS MORALES. TIENEN DERECHO A LA PROTECCIÓN DE LOS DATOS QUE PUEDAN EQUIPARARSE A LOS PERSONALES, AUN CUANDO DICHA INFORMACIÓN HAYA SIDO ENTREGADA A UNA AUTORIDAD****. El artículo 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos reconoce el derecho a la protección de datos personales, consistente en el*

[120] (Personas Morales. Tienen Derecho A La Protección De Datos Que Puedan Equiparse A Los Personales, Aún Cuando Dicha Información Haya Sido Entregada A Una Autoridad, Tesis: P. II/2014 (10a.), pub, 2014) Suprema Corte de Justicia de la Nación, tesis aislada 2005522, Tesis: P. II/2014 (10a.), publicación Libro 3, Febrero de 2014, Tomo I, página 274. [Versión digital] [Consulta en agosto 2020]. Véase en: https://sjf.scjn.gob.mx/SJFSem/Paginas/Reportes/ReporteDE.aspx?idius=2005522&Tipo=1

control de cada individuo sobre el acceso y uso de la información personal en aras de preservar la vida privada de las personas. En ese sentido, el derecho a la protección de datos personales podría entenderse, en primera instancia, como una prerrogativa de las personas físicas, ante la imposibilidad de afirmar que las morales son titulares del derecho a la intimidad y/o a la vida privada; sin embargo, el contenido de este derecho puede extenderse a cierta información de las personas jurídicas colectivas, en tanto que también cuentan con determinados espacios de protección ante cualquier intromisión arbitraria por parte de terceros respecto de cierta información económica, comercial o relativa a su identidad que, de revelarse, pudiera anular o menoscabar su libre y buen desarrollo. Por tanto, los bienes protegidos por el derecho a la privacidad y de protección de datos de las personas morales, comprenden aquellos documentos e información que les son inherentes, que deben permanecer ajenos al conocimiento de terceros, independientemente de que, en materia de transparencia e información pública, opere el principio de máxima publicidad y disponibilidad, conforme al cual, toda información en posesión de las autoridades es pública, sin importar la fuente o la forma en que se haya obtenido, pues, acorde con el artículo 6o., en relación con el 16, párrafo segundo, constitucionales, la información entregada a las autoridades por parte de las personas morales, será confidencial cuando tenga el carácter de privada por contener datos que pudieran equipararse a los personales, o bien, reservada temporalmente, si se actualiza alguno de los supuestos previstos legalmente.

Contradicción de tesis 56/2011. Entre las sustentadas por la Primera y la Segunda Salas de la Suprema Corte de Justicia de la Nación. 30 de mayo de 2013. Mayoría de siete votos de los Ministros Margarita Beatriz Luna Ramos, José Fernando Franco González Salas, Arturo Zaldívar Lelo de Larrea, Jorge Mario Pardo Rebolledo, Sergio A. Valls Hernández, Olga Sánchez Cordero de García Villegas y Alberto Pérez Dayán; votaron en contra: Alfredo Gutiérrez Ortiz Mena, José Ramón Cossío Díaz, Luis María Aguilar Morales y Juan N. Silva Meza.

Ponente: Sergio A. Valls Hernández. Secretarios: Laura García Velasco y José Álvaro Vargas Ornelas. El Tribunal Pleno, el veintitrés de enero en curso, aprobó, con el número II/2014 (10a.), la tesis aislada que antecede. México, Distrito Federal, a veintitrés de enero de dos mil catorce.

Con esa precisión, se recomienda la aplicación de las recomendaciones y protocolos de seguridad en el presente trabajo para la protección de los datos equiparables a los personales de un ente jurídico. Pues con la lógica enunciada y la normativa nacional, así como las recomendaciones internacionales para la ciberseguridad de los datos personales en Tecnologías de la Información.

4.3.13 Protección de datos en medios electrónicos para fines periodísticos

Actualmente es común que todo usuario de dispositivos electrónicos cuentan con medios para la toma de audiovisuales y con conexión a Internet, lo cual puede vulnerar los derechos humanos de las personas en aras de la libre expresión y máxima publicidad de la información, con las excepciones constitucionales para ello (Artículo 16, segundo párrafo de la Constitución Mexicana - seguridad nacional, orden público, la supremacía y protección de la seguridad y salud públicas).

Por lo cual existen distintos tipos de interés afectados: “interés público”, el “interés social” o la “utilidad pública”, por lo que la Suprema Corte indica realizar la ponderación para justificar la exposición de la vida privada de una persona (Amparo directo 3/2011. TA, 10ª época[121]).

Por ello, la persona que realice publicaciones e impliquen el tratamiento de datos personales, y que en el ejercicio de la libertad de expresión debe prevalecer la protección a la vida privada (evitar “intromisiones innecesarias”) e “instrumentar medidas de diligencia” para evitar acusaciones ante “negligencia inexcusable”.

Asimismo, el Observatorio Iberoamericano de Protección de Datos (OIPD) recomienda: atender lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de Particulares[122] y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[123], correspondientemente.

---

[121] (Resolución de la Sentencia del caso Lydia Caho, 2013) Resolución de la Sentencia del caso Lydia Cacho, No. 017/2013, publicación del 31 de enero de 2013. [Versión digital] [Consulta en agosto 2020]. Véase en: http://www.pudh.unam.mx/perseo/sentencia-del-caso-lydia-cacho/

[122] Ley Federal de Protección de Datos…

[123] Ley General de Protección de Datos..

De forma relacionada, existe el Código Deontológico relativo al tratamiento de datos personales en el ejercicio de la actividad periodística o "Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica"[124] elaborado por el "Garante para la protección de datos personales" de Italia respecto a las figuras públicas.

A continuación, resaltare las más notorias a mi parecer:

- La vida privada de las personas públicas debe ser respetada si los hechos o noticias no tienen que ver con su vida pública (Artículo 6, párrafo 2)
- Se debe privilegiar dos principios de la protección de datos personales: el consentimiento y la licitud; sin embargo, es necesario que los periodistas en observancia a la información, responsabilidad y de deber de seguridad, debe de debe dar a conocer su identidad, su profesión y la finalidad del acopio (artículo 10), por lo que resulta útil el uso del Aviso de Privacidad Corto.
- En cuanto a los derechos de imagen por la publicación de visuales, los periodistas no deben de perder la objetividad, dar a conocer el Aviso de Privacidad Corto y obtener el consentimiento del titular.
- En el tratamiento de datos personales de menores o incapaces: a los padres o tutores debe de entregarse un Aviso de Privacidad y la obtención del consentimiento e informar el objeto de la información de interés público. Pues de lo contrario puede derivar en la comisión de un delito (art. 7).

  Asimismo, con *"...el fin de proteger la personalidad de los menores involucrados en hechos noticiosos, el periodista no debe publicar sus nombres, ni proporcionar detalles capaces de llevar a su identificación..."*, por lo que la *"...protección de la personalidad del niño se extiende, considerando la calidad de las noticias y sus componentes, a todos los hechos que no son específicamente delitos..."*[125].
- En cuanto a la dignidad humana, el artículo 8º refiere que *"una vez preservada la información esencial, el periodista no debe proporcionar noticias ni publicar imágenes o fotografías de personas involucradas en hechos noticiosos que sean perjudiciales para la dignidad de la persona,*

[124] Código Deontológico relativo al tratamiento de datos personales en el ejercicio de la actividad periodística, publicación del 29 de noviembre de 2018. [Versión digital] [Consulta en agosto 2020]. Véase en: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9067692

[125] Ibidem. Artículo 7.

tampoco se detiene en detalles de violencia a menos que perciba alguna relevancia social de la noticia o de las imágenes (2) exceptuando cuando hay motivos de un relevante interés público o finalidad judicial o policiaca comprobada, el periodista no retoma ni produce imágenes o fotos de personas bajo arresto sin consentimiento del interesado (3) y no se puede presentar a las personas con cadenas o esposas, excepto cuando ello sea necesario para mostrar abusos"[126].

- La dignidad de las personas en el ámbito de la salud, los periodistas no deben publicar los datos analíticos de estricto interés clínico ni describir los hábitos sexuales de una persona identificada o identificable (art. 11).
- Se prevé Principios de Licitud y Calidad sobre la protección de datos personales, y el Deber de Seguridad para respaldo de las fuentes.

4.3.14 Marco de penalización por mal tratamiento de los datos personales

De acuerdo a la normativa de Protección de Datos Personales ante Particulares[127] y los Sujetos Obligados[128], existen diversas directrices sobre lo que jurídicamente se considera una violación a los derechos de protección.

De forma ejemplificativa, las vulneraciones a los datos personales son: incumplimiento a la solicitud de ejercicio de los derechos ARCO, actuación con negligencia o dolo en el trámite y respuesta de solicitudes, declarar dolosamente la inexistencia de datos personales y el responsable posea bases de datos totales o parciales, dar tratamiento a los datos personales en contravención a los principios legales, y omitir en el aviso de privacidad, alguno o todos los elementos del artículo 16 e informar los medios para ejercer los derechos ARCO.

Las sanciones para particulares pueden consultarse en el artículo 64 de la LFPDPPP; sin embargo, es de resaltarse que las infracciones por datos sensibles podrán incrementarse hasta por dos veces a lo establecidos.

Cabe señalar que el INAI fundará y motivará las resoluciones, considerando: la naturaleza del dato; la improcedencia de la negativa del responsable, para realizar los actos solicitados por el titular; el carácter intencional o no, de la acción u omisión constitutiva de la infracción; la capacidad económica

---

[126] *Ibidem, p.*

[127] Ley Federal de Protección de Datos Personales en Posesión de Particulares

[128] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas,

del responsable, y la reincidencia. Finalmente, el artículo 66 refiere a que las sanciones se impondrán sin perjuicio dela responsabilidad civil o penal que resulte.

Las infracciones de Sujetos obligados, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) refiere los Delitos ante el Tratamiento Indebido de Datos Personales, desde el artículo 67 al 69, lo cual conlleva:

- Imposición de tres meses a tres años de prisión al autorizado para tratar datos, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia[129] (art. 67)
- Prisión de seis meses a cinco años al que con ánimo de lucro indebido, mediante el engaño o uso del error del titular o la persona autorizada para transmitir la información[130] (art. 68)

Tratándose de datos personales sensibles, las penas referidas se duplicaran. En ambos casos, el INAI analizará la gravedad de la infracción sobre la gravedad del acto y considerará la capacidad económica y la reincidencia.

Respecto a los sujetos obligados y la materia penal, el Código Nacional de Procedimientos Penales (CNPP) en su artículo 106 refiere al concepto de "Reserva de identidad", el cual prohíbe realizar referencias a terceros sin legitimidad datos personales de personas sujetas a procedimientos penales. No obstante, existe la excepción para las personas en calidad de persecución.

> *"**Artículo 106.-** En ningún caso se podrá´ hacer referencia o comunicar a terceros no legitimados la información confidencial relativa a los datos personales de los sujetos del procedimiento penal o de cualquier persona relacionada o mencionada en este.*
>
> *Toda violación al deber de reserva por parte de los servidores públicos, será sancionada por la legislación aplicable.*
>
> *En los casos de personas sustraídas de la acción de la justicia, se admitirá la publicación de los datos que permitan la identificación del imputado para ejecutar la orden judicial de aprehensión o de comparecencia".*

[129] Ley General de Protección de Datos Personales… Artículo 67.
[130] Ley General de Protección de Datos Personales… Artículo 68.

Conclusiones

Conclusiones

Las tendencias y la evolución que actualmente se ha presentado para las empresas y las personas han impactado en distintos grados el uso de las Tecnologías, y es bien sabido por los conocedores del Derecho que las tecnologías avanzan más rápido que la materia; por lo que la medición del nivel de impacto y riesgo es relegado y muchas veces conocido hasta la presentación de un percance. Por ello, con un ambiente en constante evolución e incremento de las demandas, es necesario la implementación de sistemas de gestión y prevención de riesgos ante el uso de las TIC.

La necesidad de crear operaciones óptimas y con un parámetro mínimo de seguridad permitirá asumir los cambios y tendencias de una manera controlada, creando un ambiente de adaptación paulatina y se cree una cultura preventiva y concientización de la protección de datos en las tecnologías de la información.

La normalización y correcto conocimiento del ciclo de producción de un servicio o producto permite un análisis desde su inicio, su operación, el mantenimiento de la operación y la corrección bajo la óptica de operación de una ISO aplicado a la ciberseguridad de los datos personales conforme al interés principal de los encargados y responsables del tratamiento, y con ello incrementar su plusvalía, responsabilidad y minimización de los riesgos con alineación a sus objetivos.

El flujo de la información o ciclo de los procesos permitirá conocer el alcance e impacto sobre el control de la información de los interventores, con el desarrollo de una armonía y listo para la interacción con los usuarios finales.

En caso de que se detecten alertas de falla o riesgo, los responsables deben de adoptar medidas correctivas y aplicar planes de emergencia en caso de vulneraciones externas, lo que les permitirá a los equipos internos mayor control y conocimiento para las tareas de contención de falla.

Si bien las TIC son herramientas de operación, también son aplicaciones que requieren mantenimiento y actualización constante, por lo que es necesario concientizar a los operadores del correcto uso y desarrollo de capacitación para la atención de los requerimientos de los usuarios finales y la atención oportuna de los incidentes. Por lo que internamente, las entidades físicas o morales deben incentivar la capacitación constante, comunicación y actualización en las

tendencias tecnológicas, evitando así el “obviar” por el manejo de roles y responsabilidades como un todo.

Es importante señalar que la adopción de estándares y la concientización permite tener mayor flexibilidad y agilidad para la respuesta ante contingencias; en tanto externamente, se denota un punto más para competitividad y plusvalía comercial. Además, la adopción de medidas y recomendaciones como las que hace la Agencia Española entre las entidades que residen en México, permite la creación de una cadena de valor que conlleva la adopción de beneficios, mitigación de riesgos y la optimización de recursos.

La satisfacción de las medidas de seguridad de la información y al mismo tiempo, brindar los servicios y bienes a los usuarios mediante las TIC permitirá tener activo el ciclo económico y brindar una gestión efectiva de los servicios de TIC, incrementando así la confianza de los consumidores en tanto se acoplan los requerimientos técnicos y normativos del uso de las tecnologías.

5.1 Recomendaciones

En el proceso de elaboración de este proyecto, se recomienda la aplicación de un proceso de gestión del cambio y de mejora continua para crear un hábito en la constante evolución social, tecnológica y normativa, evitando así el rezago y pérdida de la valía de las entidades.

Asimismo, es importante incentivar la vanguardia en la tecnología, la normatividad y metodologías o marcos de referencia para la adaptación en los cambios a implementarse en la operación de las empresas.

Resulta necesario señalar, que el presente trabajo enumera una Guía para la adopción de las mejores prácticas de ciberseguridad aplicada a la protección de Datos Personales, por lo que es un planteamiento de una orientación inicial para todo aquel que requiera iniciar una gestión de los servicios de TIC y el inicio para una base de conocimiento en las condiciones actuales de México.

En palabras burdas, el conocimiento detallado de un ente sobre su propio ciclo de operación y conciencia del alcance y nivel de riesgo permite comprender la necesidad del uso correcto de las herramientas y roles, y con ello, asumir las necesidades de actualización, planes de contingencia, corrección preventiva y uso de las mejores prácticas conforme a las necesidades de la operación.

Finalmente, el uso del servicio de auditoría externa como medida preventiva y correctiva permite privilegiar el sentido de la operación y responsabilidad. Por lo que la optimización, la capacitación y la corrección son una meta constante y una cultura que todo ente que desee prevalecer en el mercado con una disminución de costos y riesgos jurídicos por la omisión del uso de buenas prácticas de normalización y recomendaciones internacionales.

Bibliografía

Agencia Española de Protección de Datos, Drones y protección de datos, España, septiembre de 2019. https://www.aepd.es/sites/default/files/2019-09/guia-drones.pdf

Agencia Española de Protección de Datos, Guía Práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGDP, España, mayo de 2018. https://d3t4nwcgmfrp9x.cloudfront.net/upload/AnalisisDeRiesgosRGPD.pdf

Agencia Española de Protección de Datos, Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD, España, septiembre de 2019. https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

Arteaga Herrera José, Fernández Sacasas José A, El método clínico y el método científico, Cuba, 2010, volumen 8, número 5. http://medisur.sld.cu/index.php/medisur/article/view/1312

Asociación Española de Normalización y Certificación (AENOR), Uso y referencia a normas ISO e IEC en la reglamentación técnica, edición AENOR, España, Septiembre 2007. https://www.une.org/normalizacion_documentos/referencia_normas_iso_iec_reg_tecnica.pdf

Cruz Hernández Jeddú, Hernández García Pilar, Abraham Marcel Enrique, Dueñas Gobel Nancy, Salvato Dueñas Alena, Importancia del método científico, Cuba, Revista Cubana de Salud Pública versión impresa ISSN 0864-3466, septiembre de 2012. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-34662012000300009&lng=es

De León Jorge, Origen de las normas ISO, Revistas y publicaciones digitales, España. https://es.calameo.com/read/00280480692ccd26e5b3e

Diario Oficial de la Federación, Código Civil Federal, México, 31 de agosto de 1928. http://www.diputados.gob.mx/LeyesBiblio/pdf/2_270320.pdf

Diario Oficial de la Federación, Código de Comercio, México, publicación de octubre de 1989. http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_de_Comercio.pdf

Diario Oficial de la Federación, Declaratoria de vigencia de la Norma Mexicana NMX-I-27032-NYCE-2018, México, publicación del 26 de junio de 2018. https://dof.gob.mx/nota_detalle.php?codigo=5529046&fecha=26/06/2018

Diario Oficial de la Federación, Ley de Aviación Civil, México, publicación del 12 de mayo de 1995. http://www.diputados.gob.mx/LeyesBiblio/pdf/25_180618.pdf

Diario Oficial de la Federación, Ley de protección de datos personales en posesión de los particulares, México, 5 de julio de 2010. http://www.precisiontools.com.mx/LFPDPPP.pdf

Diario Oficial de la Federación, Ley Federal sobre Metrología y Normalización, México, 1992. : https://www.gob.mx/cms/uploads/attachment/file/107522/LEYFEDERALSOBREMETROLOGIAYNORMALIZACION.pdf

Diario Oficial de la Federación, Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos, México, 2002. https://www.dof.gob.mx/nota_detalle_popup.php?codigo=727725

Diario Oficial de la Federación, Reglamento de la ley de protección de datos personales en posesión de los particulares, México, 21 de diciembre de 2011. http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

Diario Oficial de la Federación, Reglamento de la Ley Federal sobre Metrología y Normalización, México, 1999. http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo88524.pdf

Diario Oficial de la Unión Europea, Decisión de Ejecución (UE) 2016/1250 de la Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del

Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. [notificada con el número C(2016) 4176], Comisión Europea, 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D1250&from=DE

Diario Oficial de la Unión Europea, Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Parlamento Europeo y del Consejo, publicación n° L 281 de 23/11/1995. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

Diario Oficial de la Unión Europea, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 26 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), Unión Europea, 27 de abril de 2016. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Dirección General de Aeronáutica Civil, Requerimientos para operar un sistema de aeronave pilotada a distancia (RPAS) en el Espacio aéreo mexicano, México, 25 de julio de 2017. http://www.sct.gob.mx/fileadmin/DireccionesGrales/DGAC-archivo/modulo3/co-av-23-10-r4.pdf

Donohue Brian, ¿Qué es un hash y cómo funciona?, publicación del 10 abril de 2020. Kaspersky Lab: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/#:~:text=10%20Abr%202014-Una%20funci%C3%B3n%20criptogr%C3%A1fica%20hash%2D%20usualmente%20conocida%20como%20%E2%80%9Chash%E2%80%9D%2D,tendr%C3%

Federación Nacional de Comerciantes (FENALCO), Superindustria se pronuncia sobre los elementos esenciales del contrato de transmisión de datos personales,

Colombia, [edición web], 2018. http://www.fenalco.com.co/gesti%C3%B3n-jur%C3%ADdica/superindustria-se-pronuncia-sobre-los-elementos-esenciales-del-contrato-de

Federal Register of Legislation, Privacy Act, 119 – Compilation No. 83, Australia, 16 de mayo de 2020. https://www.legislation.gov.au/Details/C2020C00168

Garante de la protección de datos personales, Normas deontológicas relativas al tratamiento de datos personales en el ejercicio de la actividad periodística publicadas de conformidad con el art. 20, párrafo 4, del Decreto Legislativo 10 de agosto de 2018, n. 101 - 29 de noviembre de 2018 (traducción Google Translate), Italia, enero 2019. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9067692

Gil Elena, Big Data privacidad y protección de datos, XIX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos, España, 2015. Agencia Española de Protección de Datos. : https://www.aepd.es/sites/default/files/2019-10/big-data.pdf

Great Place to Work México. ¿Quiénes somos?, México, 2019. https://greatplacetowork.com.mx/quienes-somos/

Herrera Esther, Por Covid-19, ventas online se disparan ¨, Monterrey, Edición digital Diario Milenio, publicación del 31 de marzo de 2020. : https://www.milenio.com/negocios/coronavirus-nuevoleon-pandemia-dispara-ventas-online

Instituto de Crédito Oficial (ICO), Personal Information online code of practice, traducción propia, España, ICO, mayo 2011. https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf

Instituto Nacional de Transparencia Acceso a la Información Pública Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, Conceptos, Ciudad de México, Publicación digital. : http://www.infodf.org.mx/index.php/protege-tus-datos-personales/preguntas-frecuentes.html

Kaspersky Lab, ¿Qué es la ciberseguridad?, publicación digital. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Ley Orgánica 3/2018 de Protección de Datos (LOPD), del 5 de diciembre de 2018, [Versión digital]. https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

MD5Hashing, Hash and Unhash, blog digital. https://md5hashing.net/hash

Ministerio de Asuntos Exteriores Unión Europea, Políticas Comunes de la Unión Europea, España, Octubre 2018). http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/UnionEuropea/Paginas/Pol%C3%ADticas-comunes-de-la-Uni%C3%B3n-Europea.aspx

Mundler Patrick, Bellon Stéphane, Sistemas de garantía participativa: ¿una alternativa a la certificación por organizaciones de terceros? (traducción Google Translate), Francia, Editorial Grep, páginas 57-65.

Muñoz Herrerías Oscar Agustín, Jaula de Faraday, Hidalgo, Publicación de la Universidad Autónoma de Hidalgo. https://www.uaeh.edu.mx/scige/boletin/prepa4/n10/r3.html

Nuñez E. Javier, Lima José Luis, Incentivos Reputacionales para la Autorregulación: Un análisis Experimental, Facultad de Economía de la Universidad de Chile, Publicación digital. http://www.econ.uchile.cl/uploads/publicacion/61f57e85-5657-4551-b53b-59a24c79baed.pdf

Oracle México, ¿Qué es cómputo en la nube?, México, publicación digital. https://www.oracle.com/mx/cloud/what-is-cloud-computing/

Organización Internacional de Estandarización (ISO), Origen de las normas ISO, Publicación digital, 26 de julio de 2015. https://www.isotools.org/2015/07/26/origen-normas-iso/

Organización Internacional de Normalización, Guía para los organismos nacionales de normalización de ISO, Suiza, Diciembre de 2010. https://www.iso.org/files/live/sites/isoorg/files/store/sp/PUB100269_sp.pdf

Parlamento Europeo, El defensor del pueblo europeo y los derechos de los ciudadanos, Eubarómetro, Sondeos de opinión del Parlamento Europeo, 2011. https://www.europarl.europa.eu/at-your-service/es/be-heard/eurobarometer/the-european-ombudsman-and-citizens-rights

Perseo, Programa Universitario de Derechos Humanos de la Universidad Autónoma de México, Sentencia del caso Lydia Cacho 017/2013, México,

Publicación número 1 de marzo de 2013. http://www.pudh.unam.mx/perseo/sentencia-del-caso-lydia-cacho/

Personales y garantía de los derechos digitales. Real Academia Española, Definición de soft law, España, marzo de 2020. https://dpej.rae.es/lema/soft-law#:~:text=Conjunto%20de%20normas%20o%20reglamentaciones,de%20conducta%2C%20principios%2C%20etc

Secretaría de Economía y la Cámara Nacional de la Industria Electrónica, Estudio de la Autoregulación en Materia de privacidad y Protección de Datos Personales en el Ámbito de las Tecnologías de la Información, México, 5a edición. https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_04.pdf

Secretaría de Economía, Organismos Nacionales de Normalización, México, 2010. http://www.2006-2012.economia.gob.mx/comunidad-negocios/normalizacion/nacional/procesos-de-normalizacion/organismo-nacionales

Secretaría de Economía, Organismos Nacionales de Normalización, México, julio de 2012. http://www.2006-2012.economia.gob.mx/files/comunidad_negocios/normalizacion/2012_07_31_ONN.pdf

Semanario Judicial de la Federación, Personas Morales. Tienen Derecho A La Protección De Datos Que Puedan Equiparse A Los Personales, Aún Cuando Dicha Información Haya Sido Entregada A Una Autoridad, México, Suprema Corte de Justicia de la Nación, 2014, Tesis: P. II/2014 (10a.), pub, Tesis aislada 2005522.

Versión digital en https://sjf.scjn.gob.mx/SJFSem/Paginas/Reportes/ReporteDE.aspx?idius=2005522&Tipo=1

SHA1, SHA1 and other hash functions online generator, 2020. http://www.sha1-online.com/

Thibault Aranda Javier, Aspectos jurídicos del teletrabajo, Revista del Ministerio de Trabajo y Asuntos Sociales: Revista del Ministerio de Trabajo e Inmigración, ISSN 1137-5868, No 11, 1998, págs. 93-108.

Unión Internacional de Telecomunicaciones, Guía de ciberseguridad para los países en desarrollo, Suiza, Edición 2007. https://www.itu.int/dms_pub/itu-d/opb/str/d-str-secu-2007-msw-s.doc

Unión Internacional de Telecomunicaciones, Informe de Tendencias en las Reformas de Telecomunicaciones de 2013, Suiza, publicación de 2013. https://www.itu.int/es/publications/ITU-D/pages/publications.aspx?parent=D-PREF-TTR.14-2013&media=electronic

Unión Internacional de Telecomunicaciones, Protección de datos y privacidad en la nube ¿Quién es el propietario de la nube?, Suiza, septiembre de 2015. https://itunews.itu.int/es/3702-Proteccion-de-datos-y-privacidad-en-la-nube-BR-Quien-es-el-propietario-de-la-nube.note.aspx