RECOMENDACIONES

para la elaboración de **Políticas internas de gestión y tratamiento de datos personales**

(Sector Público)

inai

CONTENIDOS

DIRECTORIO

Blanca Lilia Ibarra Cadena
Comisionada Presidenta

Francisco Javier Acuña Llamas
Comisionado

Adrián Alcalá Méndez
Comisionado

Norma Julieta Del Río Venegas
Comisionada

Josefina Román Vergara
Comisionada

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

Avenida Insurgentes Sur 3211, Colonia Insurgentes Cuicuilco, Alcaldía Coyoacán, Código Postal 04530, Ciudad de México

DEFINICIONES Y ABREVIATURAS

Activo. Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización[1].

Bases de datos. El conjunto ordenado de datos personales referentes a una persona física identificada o identificable.

Custodios. Son aquéllos con responsabilidad funcional sobre los activos, como: los responsables del departamento de datos, administradores de sistemas o responsables de un proceso o de un proyecto en específico, entre otros.[2]

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

Documento de Seguridad. Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

1 INCIBE, Glosario de términos de ciberseguridad, una guía de aproximación para el empresario. Fecha de consulta: 25/04/2022. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

2 INAI, (2015, junio), Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, Consulta realizada el 25/04/2022. p.4. Disponible en https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

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

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

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

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

Organización. Conjunto de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones[3], para efectos de esta guía, se refiere a los Sujetos Obligados.

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

Riesgo. Combinación de la probabilidad de un evento y su consecuencia desfavorable[4].

Identificar el riesgo. Proceso para encontrar, enlistar y describir los elementos del riesgo.[5]

Valorar el riesgo. Proceso para asignar valores a la probabilidad y consecuencias del riesgo (impacto)[6].

3 Ibidem

4 Ibidem

5 Ibidem p. 5

6 Ibidem

Tratar el riesgo. Procesos que se realizan para modificar el nivel de riesgo[7].

Seguridad de la información. Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

Confidencialidad. Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.[8]

Disponibilidad. Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.[9]

Integridad. La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales[10].

Sistema de Gestión de Seguridad de Datos Personales (SGSDP). Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el trata-

7 Ibidem

8 INCIBE Glosario de términos de ciberseguridad, una guía de aproximación para el empresario. p. 30 Fecha de consulta: 25/04/2022. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

9 Ibidem p. 38

10 Ibidem p.52

miento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.

Sujeto obligado. Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, fideicomisos y fondos públicos, del ámbito federal y partidos políticos que en el ejercicio de sus atribuciones y funciones lleven a cabo tratamientos de datos personales de personas físicas, en términos de lo dispuesto en la Ley General y los Lineamientos Generales, incluyendo al INAI y los organismos garantes.

Titular. La persona física a quien corresponden los datos personales.

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

1. INTRODUCCIÓN

La presente recomendación, busca orientar a los sujetos obligados en la elaboración de sus políticas de gestión y tratamiento de datos personales a que refieren los artículos 30, fracciones II y IV, 33, fracción I, de la LGPDPPSO, así como los artículos 46, 47, 51 y 56 de los Lineamientos Generales.

De acuerdo con dicha disposición, los sujetos obligados deberán incorporar a su normativa políticas que aseguren el buen manejo y tratamiento de los datos personales y los sistemas que los soportan, que sean eficaces y útiles, y que establezcan pautas, obligaciones y responsabilidades para el personal que trata dichos datos personales. Ello, como un mecanismo para el cumplimiento del principio de responsabilidad, pero también del deber de seguridad establecidos en la Ley General, ya que las políticas de gestión y tratamiento de datos, así como políticas de seguridad complementarias son medidas de seguridad administrativas conforme a lo establecido en el artículo 3, fracción XXI.

Estas políticas que son obligación legal para los responsables, deben ser también resultado de la labor realizada durante la implementación de un Sistema de Gestión de Protección de Datos Personales, en tanto que este tiene como objetivo proveer un marco de trabajo para el tratamiento de datos personales que permita mantener vigente y mejorar la protección de datos personales para el cumplimiento de la legislación y fomentar las buenas prácticas.

El SGSDP se basa en el ciclo PDCA, por sus siglas en inglés (Plan, Do, Check, Act) y traducido al español PHVA (Planear, Hacer, Verificar, Actuar)[11], donde se consi-

[11] INAI, (2015, junio), Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, Consulta realizada el 25/04/2022. p. 7-8. Disponible en https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

deran diferentes pasos y objetivos de acuerdo a cada fase del ciclo, que pueden observarse en la siguiente tabla:

Ciclo	Fases		Pasos	Objetivos Específicos
	Planificar	Planear el SGSDP	1. Alcance y objetivos 2. Política de gestión de datos personales 3. Funciones y obligaciones de quienes traten datos personales 4. Inventario de datos personales 5. Análisis de riesgos de los datos personales 6. Identificación de las medidas de seguridad y análisis de brecha	Definir los objetivos, políticas, procesos y procedimientos relevantes del SGSDP para gestionar los riesgos de los datos personales, con el fin de cumplir con la legislación sobre protección de datos y obtener resultados acordes con las políticas y objetivos generales del sujeto obligado.
	Hacer	Implementar y operar el SGSDP	7. Implementación de las medidas de seguridad aplicables a los datos personales	Implementar y operar las políticas, objetivos, procesos y procedimientos del SGSDP, así como sus controles o mecanismos con indicadores de medición.
	Verificar	Monitorear y revisar el SGSDP	8. Revisiones y auditoría	Evaluar y medir el cumplimiento del proceso de acuerdo con la legislación de protección de datos personales, la política, los objetivos y la experiencia práctica del SGSDP, e informar los resultados al Comité de Transparencia para su revisión.
	Actuar	Mejorar el SGSDP	9. Mejora continua y Capacitación	Para lograr la mejora continua se deben adoptar medidas correctivas y preventivas, en función de los resultados obtenidos de la revisión por parte del Comité de Transparencia, las auditorías al SGSDP y de la comparación con otras fuentes de información relevantes, como actualizaciones regulatorias, riesgos e impactos organizacionales, entre otros. Adicionalmente, se debe considerar la capacitación del personal.

Tabla 2. Objetivos del SGSDP dentro de las fases del ciclo PHVA

Como se observa, la elaboración de las políticas de gestión de tratamientos de datos personales, se encuentra en la primera fase de un SGSDP, esto es, en la planeación, y debe ser el resultado de haber analizado el contexto del sujeto obligado en cuanto a sus procesos donde se tratan datos personales o se operan sistemas de tratamiento, el alcance del sistema, esto es, las unidades administrativas que participan en el tratamiento de datos u operan estos sistemas, o bien que participan en algún momento del ciclo de vida de los datos; asimismo, deberán identificarse los activos, en este caso los datos personales y los sistemas de tratamiento, su ciclo de vida; las personas servidoras públicas que participan en los procesos de tratamiento, los custodios de los activos, el análisis de riesgos, las medidas de seguridad actuales así como saber identificar las que se pretenden implementar de acuerdo a los valores obtenidos del riesgo residual.

Se debe señalar que si bien la política de gestión y tratamiento de datos personales se establece para efectos didácticos como el segundo paso a seguir del proceso de planeación de un SGSDP, no se puede considerar como un requisito finalizarla para continuar con los siguientes pasos, sino que puede comenzar a redactarse de forma general en cuanto se tiene el alcance y los objetivos del SGSDP, sin embargo, esta debe irse construyendo a lo largo de todo el proceso de planeación, e incluso deberán elaborarse políticas adicionales de acuerdo a las medidas de seguridad identificadas que deben comenzar a operar en la Institución como resultado del análisis de riesgos y el análisis de brecha, así como procedimientos específicos por Unidad Administrativa como complemento a esas políticas, de acuerdo al contexto y las necesidades del sujeto obligado.

En ese orden, será útil para los sujetos obligados trabajar en conjunto con el Documento de Seguridad que ya integra toda la información anteriormente señalada. Por lo que éste puede ocuparse como materia prima para la elaboración de las políticas de gestión de datos personales.

Es importante precisar que, el Documento de Seguridad y el SGSDP si bien constituyen deberes conforme a la LGPDPPSO y están interrelacionados, no son lo mismo. El

primero, es la documentación propiamente dicha de los contenidos que indica la Ley: inventario de datos personales y sistemas de tratamiento, las funciones y obligaciones de las personas que traten datos personales, el análisis de riesgos; el análisis de brecha; el plan de trabajo; los mecanismos de monitoreo y revisión de las medidas de seguridad, y el programa general de capacitación, documento con el que los responsables del tratamiento deben demostrar el cumplimiento de sus obligaciones; y el segundo, se trata de un proceso continuo que deben operar los sujetos obligados, entendiéndose el SGSDP como un conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos, como se observa las políticas de gestión y tratamiento de datos personales van a ser parte del resultado de operar el SGSDP.

Ahora bien, para entender qué es y cómo debe realizarse una Política de Gestión de Datos Personales, se debe señalar qué es una política de seguridad en el ámbito de seguridad de la información, y es aquel documento "que describe los requisitos o reglas específicas que deben cumplirse en una organización. Presenta una declaración formal, breve y de alto nivel, que abarca las creencias generales de la organización, metas, objetivos y procedimientos aceptables para un área determinada. "

Esta definición debemos trasladarla al contexto del sector público, para los Sujetos Obligados, así como al contexto particular del derecho de protección de datos personales, que, conforme a la Ley General se denominan políticas de gestión de datos personales y son aquellos documentos que describen los requisitos o reglas específicas que deben cumplirse al interior del sujeto obligado.

En el desarrollo de las presentes recomendaciones, se especificarán las características que deben tener y los requisitos mínimos para elaborar una Política General, asimismo se orientará en caso de que se requieran establecer otras políticas específicas.

2. OBJETIVO

El objetivo de este documento es describir el proceso y los requisitos mínimos que deben tomarse en cuenta para crear las Políticas de Gestión de Tratamiento de Datos Personales adecuadas, eficaces y útiles para el sujeto obligado, y que estas sean acordes con su propio contexto, sus objetivos, sus finalidades y su competencia, y estén armonizadas con la implementación del SGSDP.

3. ANTECEDENTES

Es oportuno precisar, que la elaboración de las Políticas de Gestión de Datos Personales es parte de la implementación del SGSPD, para lo cual deberá trabajarse en conjunto el propio Sistema y preferiblemente el Documento de Seguridad, lo cual facilitará el trabajo, en tanto que se tiene la materia prima para redactarlas.

Previo a la elaboración de las políticas, deben definirse los alcances y objetivos de la gestión de datos personales, se trata de definir los límites en la aplicación del sistema de gestión de la seguridad de los datos personales.

Definir el alcance se refiere a entender qué actividades, qué unidades administrativas, qué procesos va a cubrir el SGSDP, qué requiere ser protegido, definir los requisitos de seguridad de los datos personales, considerar la criticidad de los datos y los sistemas del tratamiento que pueden causar un gran impacto en los titulares como resultado de pérdidas de confidencialidad, integridad o disponibilidad; asimismo, se deben definir el alcance y los límites de la Tecnología de la Información y Comunicación (TIC) que se utiliza para el tratamiento de datos personales; el alcance físico y los límites de las instalaciones o ubicaciones, se deben considerar también, las actividades externalizadas así como las interfaces y dependencias requeridas por ejemplo, puede haber instituciones donde hay muchas áreas que no traten datos personales por lo que se debe considerar si se integrarán al sistema o se dejarán fuera de este.

Para ello es indispensable entender el contexto de la institución tanto interno como externo, sus objetivos y sus valores.

El alcance correcto del SGSDP ayudará a las Instituciones a cumplir sus requisitos de seguridad y planificar la implementación del propio sistema. Para efectos de la política de seguridad esta primera parte del desarrollo del SGSDP ayudará a que

se identifique qué se quiere proteger, y se alineen los requisitos de seguridad de la entidad con los ejercicios de análisis y evaluación de riesgos.

Algunas preguntas que se pueden hacer quienes van a redactar las políticas, son:

- ¿Qué datos personales y sistemas de tratamiento en el sujeto obligado estarán cubiertos por el SGSDP?

- Considerar sus ubicaciones, el formato en qué se conservan, es decir archivo físico, digitalizado o electrónico, el tipo de tecnologías que se utilizan.

- ¿Cómo y por qué esos datos y esos sistemas son críticos? Aquí deberá analizarse los tipos de datos personales que se tratan, es decir si son datos personales sensibles, la cantidad de datos personales que se tratan, el posible impacto a las personales titulares, y las demás consideraciones del artículo 32, de la Ley General.

- ¿Va a requerir que partes externas, proveedores cumplan con su SGSDP? Se refiere a si, por ejemplo, personal externo, de limpieza, proveedores que ingresen a las instalaciones requerirán estar integrados al SGSDP, esto será así si por cualquier razón durante su ingreso o interacción con el sujeto obligado tienen acceso a los datos personales.

- ¿Las actividades realizadas por la organización requieren de interfaces o dependencias externas o de actividades realizadas por terceros? ¿si es así, deberían ser considerados dentro del alcance del SGSDP?

- Debe considerarse, por ejemplo, si se ha contratado servicios en la nube, o servicios técnicos que tengan acceso remoto a los datos personales o a los sistemas de tratamiento.

Para contestar muchas de estas preguntas los responsables pueden apoyarse en el Documento de Seguridad, si ya se ha realizado este, en tanto que puede reutilizarse el inventario de datos personales y sistemas de tratamiento, así como el análisis y evaluación del riesgo de los datos personales y los sistemas de tratamiento, los cuales orientan para determinar su inclusión en el alcance del SGSDP.

Además de lo anterior debe considerarse el contexto externo de la Institución, en el caso particular las leyes aplicables, esto es, la LGPDPPSO, y los Lineamientos Generales, pero también las leyes especiales que apliquen al sujeto obligado en lo particular y que contenga normativa relativa a la seguridad de datos personales.

Por cuanto, a los objetivos de seguridad, se debe tener en cuenta qué queremos conseguir con el SGSDP, para ello se debe considerar el cumplimiento de la LGDPPSO y los Lineamientos Generales, que en este caso será el cumplimiento de los deberes, obligaciones y principios contenidos en dicha normativa.

Una vez que han sido definidos los alcances y objetivos de la gestión de los datos personales, un equipo autorizado y coordinado por el Comité de Transparencia (de conformidad con lo establecido en la fracción V, del artículo 84, de la LGPDPPSO), deberá comenzar a redactar una política general de gestión y seguridad que ayude al logro de los objetivos planteados, sin embargo, hay que tener claro que esta se irá consolidando durante todo el proceso de implantación del SGSDP, teniendo en cuenta que se trata de un sistema con el que se busca la mejora continua y que se requerirán múltiples políticas de gestión y tratamiento de datos, como se verá adelante.

4. POLÍTICAS DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DE ACUERDO CON LA LGPDPPSO Y LOS LINEAMIENTOS GENERALES: CONTENIDO MÍNIMO Y REQUISITOS.

La Ley General menciona por una parte en el artículo 30, perteneciente al Título Segundo, Capítulo Primero de los Principios, que entre los mecanismos que debe implementar el responsable del tratamiento para cumplir con el principio de responsabilidad, es la elaboración de políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable. Se debe recordar que "al principio de responsabilidad se le conoce también como el principio de rendición de cuentas, ya que establece la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación y demostrar ante los titulares y la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales" [12]
.

Posteriormente, en el artículo 33, perteneciente al mismo Título Segundo, Capítulo Segundo de los Deberes, señala que para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar actividades interrelacionadas, entre ellas, crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.

En ese sentido, podemos observar que la LGPDPPSO reitera las políticas tanto para

[12] INAI. (2016, junio). Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, p. 63. Fecha de consulta: 25/04/2022. Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_lfpdppp_junio2016.pdf

el cumplimiento del principio de responsabilidad, mediante el cual el sujeto obligado debe demostrar que cumple con la Ley, pero también las menciona como un deber que los sujetos obligados deben incorporar para establecer y cumplir con las medidas de seguridad.

Respecto a lo anterior, los Lineamientos Generales señalan en el artículo 46 que el responsable tiene la obligación de adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General, asimismo, deben establecer mecanismos para evidenciar su cumplimiento ante los titulares y ante el Instituto. Asimismo, deberá realizar lo anterior cuando los datos personales en su posesión sean tratados por parte de encargados del tratamiento, así como cuando se realicen transferencias nacionales o internacionales de datos.

De igual manera, señala que, en la adopción de las políticas e implementación de mecanismos para evidencia el cumplimiento, se deberá considerar de manera enunciativa más no limitativa, el desarrollo tecnológico y las técnicas existentes, la naturaleza, contexto, alcance y finalidades del tratamiento de los datos personales, así como las atribuciones y facultades con la que cuenta el responsable y demás cuestiones que considere convenientes, y para ello el responsable puede valerse de mecanismos de autorregulación como estándares, mejores prácticas nacionales o internacionales, esquemas de mejores prácticas, o cualquier otro mecanismo que determine adecuado para tales fines.

De lo anterior se observa que los Lineamientos Generales agregan que dichas políticas deben regir y considerar como parte del alcance, a las relaciones que se tengan con terceros, en particular cuando se contraten encargados del tratamiento, así como las transferencias que se realicen. Aunado a ello, en la creación de las políticas se debe considerar la naturaleza, el contexto, el alcance y las finalidades del tratamiento, así como el desarrollo tecnológico y las técnicas o la forma en que se tratan los datos dentro de la Institución, es decir, que las políticas deben tener un sentido lógico y ser congruentes con el contexto del sujeto obligado.

Por su parte, el artículo 47 de los Lineamientos Generales, establece, que el responsable debe elaborar e implementar políticas y programas de protección de datos personales que busquen establecer los elementos y actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de sus funciones y obligaciones, impliquen un tratamiento de datos personales a efecto de proteger estos de manera sistemática y continua. Dichas políticas y programas deben ser aprobados, coordinados y supervisados por el Comité de Transparencia, y el responsable del tratamiento puede autorizar recursos para su implementación y cumplimiento.

Así las cosas, las políticas deben establecer las pautas directivas y operativas, a nivel de procedimiento, conforme a las que se llevarán a cabo los tratamientos de datos personales, a efecto de proteger de manera sistemática y continua los datos personales.

En este punto, es importante mencionar que las propias políticas son un control o medida de seguridad a valorar en el SGSDP, y el objetivo de estas es regir o regular las acciones permitidas y no permitidas respecto al tratamiento de datos personales, los roles y responsabilidades, y las consecuencias ante el incumplimiento, así como reiterar los principios y obligaciones que tienen todas las personas servidoras públicas que realicen tratamiento de datos personales y establecer las medidas de seguridad a operar dentro del sujeto obligado para la seguridad de los datos.

En ese sentido, es recomendable que se realice una Política General de Gestión y Tratamiento de Datos, que rija en lo general y se elaboren múltiples políticas complementarias en función de los controles o medidas de seguridad que se mantengan e implementen en la institución derivado del Sistema de Gestión de Datos Personales, e incluso podrían elaborarse procedimientos o manuales por unidad administrativa, o bien por proceso de tratamiento de datos donde se establezcan los controles específicos y la forma de operarlos, en caso de ser necesario (Véase la figura 1).

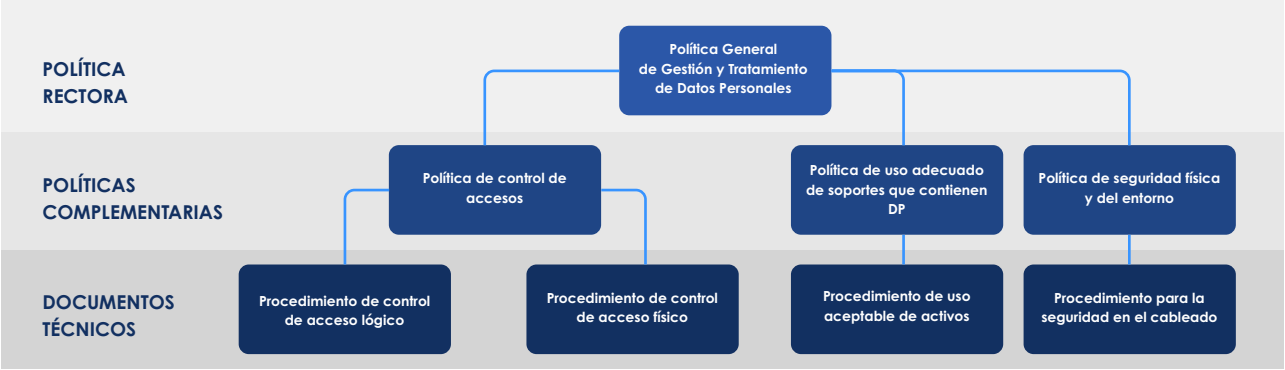


Figura 1. Ejemplo

- **Política rectora o general.** Es un documento de alto nivel que denota el compromiso de los órganos directivos del sujeto obligado con la seguridad de los datos personales, establece la importancia de salvaguardarlos, contiene los principios y deberes para la protección de los datos personales, el qué y por qué la institución planea protegerlos (los objetivos). Debe ser enriquecida con otras políticas dependientes, guías y procedimientos.

- **Políticas técnicas complementarias.** Son más detalladas que la política rectora y definen los elementos necesarios para asegurar los datos personales. Estas políticas atienden a las preguntas qué se debe proteger a mayor detalle, quién, cuándo y dónde. Describe lo que se debe hacer, pero no la manera de llevarlo a cabo, esto se reserva para las instrucciones, manuales y procedimientos.

- **Instrucciones, manuales y procedimientos.** Desglosan los pasos a seguir para llevar a cabo los enunciados de las políticas técnicas. Son documentos adjuntos que están escritos en un siguiente nivel de granularidad, en tanto que describen cómo se deben hacer las cosas. Generalmente, están redactados en un lenguaje técnico avanzado debido a que está dirigido a personal operativo.

4.1 CONTENIDO DE LA POLÍTICA GENERAL DE GESTIÓN Y TRATAMIENTO DE DATOS

El artículo 56 de los Lineamientos Generales señala que los requisitos mínimos que deben contener las políticas internas para la gestión y el tratamiento de los datos personales son

- Dar cumplimiento a todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General y los Lineamientos Generales.

- Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen.

- Las sanciones en caso de incumplimiento;

- La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados;

- El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales, y

- El proceso general de atención de los derechos ARCO.

En ese sentido, se debe puntualizar lo señalado previamente en tanto que es recomendable realizar una política general o rectora que contenga los principios generales, las obligaciones y deberes que deben observar las personas servidoras públicas y personal externo en el tratamiento de los datos personales, así como los requisitos del referido artículo 56 de los Lineamientos Generales, que se explican a continuación.

- **El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General y los Lineamientos Generales.**

  La política debe establecer el compromiso de cumplir con la legislación en protección de datos personales por parte de todos los involucrados en el tratamiento, por lo que debe ser comunicada a los mismos, e incluir al menos las siguientes reglas:

  - El cumplimiento de todos los principios que establece el artículo 16, de la Ley General: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, conforme a lo que señala dicho ordenamiento, los Lineamientos Generales y demás normativa aplicable; todas las personas servidoras públicas que por algún motivo trate datos personales deberán hacerlo conforme a los principios y deberes.

  - Tratar y recabar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley General, los Lineamientos Generales y demás normativa aplicable (principio de licitud).

  - Sujetar el tratamiento de datos personales al consentimiento de la persona titular, salvo las excepciones previstas por la Ley General y los Lineamientos Generales (principio de consentimiento).

  - Informar a las personas titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad (principio de información).

  - Procurar que los datos personales tratados sean correctos, completos y actualizados (principio de calidad).

  - Suprimir los datos personales cuando hayan dejado de ser necesa-

rios para el cumplimiento de las finalidades previstas en el aviso de privacidad y para las cuales se obtuvieron (principio de calidad).

- Tratar datos personales estrictamente el tiempo necesario para propósitos legales, regulatorios o legítimos organizacionales (principio de calidad).
- Limitar el tratamiento de los datos personales al cumplimiento de las finalidades previstas en el aviso de privacidad (principio de finalidad).

- No obtener los datos personales a través de medios fraudulentos (principio de lealtad).

- Respetar la expectativa razonable de privacidad de la persona titular (principio de lealtad).

- Tratar los menos datos personales posibles, y sólo aquéllos que resulten necesarios, adecuados y relevantes en relación con las finalidades previstas en el aviso de privacidad (principio de proporcionalidad).

- Velar por el cumplimiento de estos principios y adoptar las medidas necesarias para su aplicación (principio de responsabilidad).

- Establecer y mantener medidas de seguridad (deber de seguridad).

- Guardar la confidencialidad de los datos personales (deber de confidencialidad).

- Identificar el flujo y ciclo de vida de los datos personales: por qué medio se recaban, en qué procesos de la organización se

utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen.

- Mantener un inventario actualizado de los datos personales o de sus categorías que maneja el responsable.

- Respetar los derechos de las personas titulares en relación con sus datos personales.

- Desarrollar e implementar un SGSDP de acuerdo con la política de gestión de datos personales.

- Definir las partes interesadas y miembros del sujeto obligado con responsabilidades específicas y a cargo de la rendición de cuentas para el SGSDP.

En general, deberán considerarse todos los principios que constan en los artículos 16 a 30 de la LGPDPPSO, desarrollados en los artículos 7 a 54 de los Lineamientos Generales, y los deberes contenidos en los artículos 31 a 42 de la misma Ley General, descritos en los artículos 55 a 72 de los Lineamientos Generales.

- **Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen.**

  En este punto será muy importante que en la política general se establezca el compromiso en cuanto a que se cubrirán las necesidades operativas y técnicas para mantener la adecuada seguridad de los datos personales conforme a la LGPDPPSO, del responsable del tratamiento, incluidos los órganos directivos del sujeto obligado y el Comité de Transparencia.

Asimismo, se deben asignar las responsabilidades para llevar a cabo las tareas específicas de seguridad de los datos personales, designando a las personas adecuadas dentro del sujeto obligado, para ello, es posible nombrar a los responsables para la seguridad de los datos personales para todo el sujeto obligado, además de los responsables de sistemas de tratamiento y custodios de la información que contiene datos, especificando la cadena de custodia de los mismos, conforme al artículo 57 de los Lineamientos generales.

Podrá utilizarse la documentación que integra el Documento de Seguridad, específicamente la fracción II del artículo 35 de la Ley General, que refiere a las funciones y obligaciones de las personas que tratan datos personales.

- **Las sanciones en caso de incumplimiento.**

Respecto a las sanciones, debe tenerse en cuenta que la LGPDPPSO establece en su artículo 163 que serán causas de sanción por incumplimiento a las obligaciones que dicho ordenamiento legal prevé, las siguientes:

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

  - Incumplir los plazos de atención previstos en la Ley General para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate.
  - Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.

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

- No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la Ley General, según sea el caso, y demás disposiciones que resulten aplicables en la materia.

- Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales.
- Incumplir el deber de confidencialidad establecido en el artículo 42 de la Ley General.

- No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33, de la LGPDPPSO.

- Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la Ley General.

- Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO.
- Obstruir los actos de verificación de la autoridad.

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

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

- Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.

Asimismo, debe precisarse que los incumplimientos de la Ley General pueden derivar, además de en faltas administrativas, en delitos y responsabilidades civiles, dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

- **La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados.**

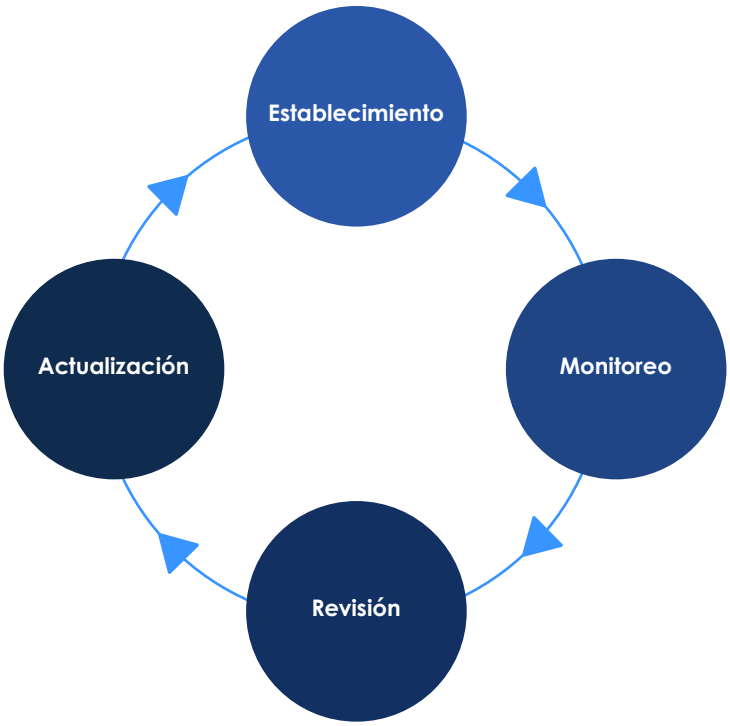
  Sobre este punto, podrán utilizarse los insumos del Documento de Seguridad para la elaboración del inventario de datos personales y sistemas de tratamiento conforme a los artículos 58 y 59 de los Lineamientos Generales e integrarse como anexo de la política general.

- **El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales.**

  Respecto a este punto, deberá definirse en la política el proceso general

para el establecimiento de las medidas de seguridad, así como el monitoreo, revisión y actualización de estas.

Debe comprenderse que, en materia de seguridad de la información, el establecimiento, monitoreo, revisión y actualización debe verse como un proceso de mejora continua, en ese sentido se deben establecer las pautas generales respecto a dichas acciones.



Autoría propia

a. El establecimiento de las medidas de seguridad

Respecto al establecimiento de las medidas de seguridad, se deberá señalar el procedimiento que indica la propia Ley General en los artículos 33, 34 y 35, referen-

te a medidas de seguridad, Sistema de Gestión de Seguridad de los Datos Personales, y el Documento de Seguridad, en tanto que las medidas de seguridad son el resultado de la elaboración del Sistema de Gestión de Seguridad de los Datos Personales y el Documento de Seguridad, particularmente lo que resulta del análisis de riesgos, análisis de brecha y el plan de trabajo.

b. La monitorización o monitoreo de las medidas de seguridad

El monitoreo conlleva la vigilancia de las medidas de seguridad. Para ello es indispensable que se lleve un control y se vigilen constantemente los activos, sus vulnerabilidades, las amenazas a las que están expuestos, los riesgos, asimismo, servirá saber el impacto de las vulneraciones ocurridas, ya que en la medida en que se tenga conocimiento de esta información sabremos si los activos están correctamente protegidos, si las medidas de seguridad son pertinentes y podremos evaluar su cumplimiento dentro de la entidad. Es por ello por lo que, el presente apartado señala que deberán monitorizarse las medidas de seguridad con base en el análisis de riesgo previamente elaborado.

Por su parte, el artículo 63 de los Lineamientos que abunda en el artículo 33, fracción VII, establece que el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Para ello, **el responsable debe monitorear constantemente**:

- Los nuevos activos que se incluyan en la gestión de riesgos;

- Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;

- Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;

- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;

- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

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

- Los incidentes y vulneraciones de seguridad ocurridas.

En ese sentido, el proceso recomendado a seguir para establecer dentro de la política es la revisión constante del inventario de activos, la elaboración del análisis de riesgos y análisis de brecha que conlleva a su vez la revisión de nuevas amenazas, las vulnerabilidades nuevas o incrementadas, el cambio en el impacto o consecuencia de las vulneraciones en los activos y en los titulares de los datos personales, y en general la advertencia de nuevos riesgos o su incremento, que deban tratarse.

c. La revisión de las medidas de seguridad

La revisión implica la evaluación de las medidas de seguridad, esto es, evaluar si las políticas y controles de seguridad realmente se estén aplicando dentro del sujeto obligado y si estas son necesarias y suficientes para el objetivo de tratamiento del riesgo planteado.

De este modo, se reitera lo que establece el primer párrafo del artículo 63 de los Lineamientos Generales: ***el responsable deberá evaluar y medir los resultados de***

las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Ahora bien, es importante observar que, para realizar la evaluación y medición de los resultados de las medidas de seguridad es necesario previamente haber monitoreado que dichas medidas realmente estén atendiendo los riesgos analizados, para así revisar objetivamente si las medidas de seguridad son eficaces, son suficientes e idóneas.

El proceso general para la revisión de medidas debe contemplar las auditorías internas y externas a las que refiere el artículo 30 fracciones IV y V de la Ley General, que establece que el responsable debe revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran y debe establecer un sistema de supervisión y vigilancia interna y/o externa, que incluya auditorías para comprobar el cumplimiento de las políticas de protección de datos personales; asimismo, el artículo 49 de los Lineamientos Generales, que abunda en las fracciones IV y V del artículo 30 de la Ley General, reitera que el responsable debe revisar las políticas y programas de seguridad al menos cada dos años, salvo que se realicen modificaciones sustanciales a los tratamientos de datos personales, por lo que se requieran actualizarse previamente las medidas de seguridad.

De acuerdo con lo anterior, la ley por medio del principio de responsabilidad establece que se debe implementar un sistema de supervisión y vigilancia para la comprobación del cumplimiento de las políticas internas de seguridad, dicha obligación debe observarse en armonía con los demás artículos que refieren a los mecanismos de monitorización de las medidas de seguridad incluyendo las políticas internas, en tanto que estas son medidas de seguridad administrativas.

Ahora bien, el último párrafo del artículo 63 señala que el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión. Se debe tomar en cuenta que la monitorización y revisión del Sistema de Gestión no solamente involucra la monitorización y revisión de las medidas de seguridad, sino que toda la planeación e implementación del propio Sistema. En ese sentido, se deberá establecer un programa de auditorías en particular para el SGSDP, siendo posible que los resultados de dichas auditorías incidan en la actualización de medidas de seguridad, o bien en modificaciones a todo el Sistema.

d. Actualización de las medidas de seguridad

La actualización es la consecuencia lógica y congruente de los incisos anteriores, al respecto, la Ley General y los Lineamientos Generales establecen los supuestos específicos donde se deben actualizar las medidas de seguridad que se señalarán adelante, sin embargo, es importante aclarar que no es necesario esperar a dichos momentos para hacerlo, ya que de implementarse bien un Sistema de Gestión, y que se monitoreen debidamente los activos, sus vulnerabilidades, amenazas y el riesgo en general, es probable que las políticas de seguridad se deban actualizar incluso antes de materializarse los supuestos a que refiere la normativa en la materia.

Respecto a los supuestos de actualización establecidos en la Ley, que deben estar contenidos en la política, debe mencionarse en primera instancia, el artículo 30 fracciones IV y V de la Ley General, que establece que el responsable deberá revisar las políticas y programas de seguridad y el sistema de supervisión y vigilancia implementado, al menos, cada dos años, salvo que realice modificaciones sustanciales a los tratamientos de datos personales que lleve a cabo y, en consecuencia, amerite una actualización previa a ese establecido. En congruencia con esto, el artículo 36 de la Ley General, refiere específicamente los momentos en que el responsable debe actualizar el Documento de Seguridad, y que son en particular, cuando:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;

- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;

- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida,

- Cuando se implementen acciones correctivas y preventivas ante una vulneración de seguridad

De la observación de estos supuestos, podemos concluir que las actualizaciones son consecuencia de lo realizado en la monitorización y revisión tanto de los activos y la valoración del riesgo, así como de la revisión de las medidas de seguridad. Asimismo, se debe comprender que la incidencia de la actualización del Documento de Seguridad en las medidas de seguridad es debido a que este es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee; y es por ello, que de actualizarse, se modificarían las medidas de seguridad dentro de las cuales se encuentran las políticas de datos personales, que son medidas administrativas en sí mismas.

Asimismo, pueden realizarse actualizaciones generadas por la propia actualización del Sistema de Gestión derivado de auditorías internas o externas en tanto que, con este, se busca la mejora continua del propio sistema que tiene como fin la seguridad de los datos personales; es indispensable que en todo momento las actualizaciones se reflejen tanto en el sistema de gestión como en el Documento de Seguridad.

- **El proceso general de atención de los derechos ARCO.**

  Este proceso viene referido en los artículos 43 a 57 de la Ley General, y desarrollados en los artículos 73 a 107 de los Lineamientos Generales. Se recomienda establecer en líneas generales el proceso para atender los derechos ARCO, y remitir ya sea a una política complementaria o procedimiento interno donde se especifique a profundidad los plazos internos y actuaciones que dependen de cada sujeto obligado.

  Aunado a los mínimos requeridos por la Ley General vistos con antelación, se recomienda que derivado del análisis de riesgos y de brecha, cuando se identifiquen las medidas de seguridad que van a operar dentro del sujeto obligado para la protección de los datos personales, se listen de manera general dentro de la política rectora, pero se detalle su operación en las políticas técnicas complementarias.

  Ahora bien, respecto a la forma de redactar la política general, se debe considerar que, al ser aplicable para todos los servidores públicos del sujeto obligado, incluso para personal externo, esta debe realizarse con un lenguaje claro y entendible para todos, debe ser concisa, asimismo, se recomienda que contenga el alcance y los objetivos donde se resuma el por qué sirve dicha política y su importancia.

  Será de suma relevancia que los responsables del tratamiento den a conocer dicha política a todo el personal tanto interno como externo del sujeto obligado, ya sea a la firma del contrato laboral o de servicios profesionales o contrato con proveedores correspondiente, o bien, durante el empleo, otorgando la política en físico o a través de medios electrónicos, cerciorándose que sea leída y comprendida, dejando constancia de ello a través de firma física o electrónica, o bien una casilla de confirmación de su lectura que otorgue constancia de la persona y el

momento donde se ha leído y comprendido, a fin de que sirva como prueba de cumplimiento del principio de responsabilidad y del deber de confidencialidad.

4.2 POLÍTICAS TÉCNICAS COMPLEMENTARIAS DE PROTECCIÓN DE DATOS

Las políticas complementarias son aquellas que detallan procedimientos y medidas de seguridad para la protección de los datos personales de manera más específica y técnica. Estas son importantes para operar un SGSDP y contribuyen a mejorar el deber de seguridad de los datos personales ya que son consecuencia de los resultados obtenidos del análisis de riesgos y el análisis de brecha, particularmente este último de donde se deben elegir las medidas de seguridad a mejorar y a implementarse priorizando la atención de los riesgos más graves, y dentro de estas medidas de seguridad se encuentran las administrativas referentes a políticas de seguridad de los datos personales, las cuales son complementarias a la política rectora o general de gestión y tratamiento de datos personales.

Las políticas técnicas complementarias deberán ser redactadas a detalle, por lo que en algunos casos serán más técnicas de acuerdo a la audiencia a la que se dirijan, por ejemplo, si se trata de la Política de control de acceso lógico, esta será sumamente técnica en tanto que quienes operarán los controles de acceso lógicos serán personas de la unidad administrativa correspondiente a IT, o el departamento de Tecnologías de la Información, o seguridad de la información, en su caso; sin embargo, también habrá personal que opere a nivel de usuario los sistemas de tratamiento y que no entienda tecnicismos, por lo que para estos últimos servirá una instrucción, manual o procedimiento de uso aceptable de los sistemas, en la que se utilice un lenguaje más sencillo donde se explique que está permitido, que no lo está, cómo reportar una falla, etcétera.

Algunos ejemplos de políticas complementarias son:

Política control de accesos lógicos.
Política de control de accesos físicos
Política de seguridad física y ambiental

Políticas, instrucciones, manuales o procedimientos orientadas al usuario, tales como:

Manual de uso aceptable de activos
Política de escritorio y pantalla limpios
Política de gestión de contraseñas seguras
Política de comunicación de información que contiene datos personales
Política de restricciones a las instalaciones y uso del software
Política de copia de seguridad
Política de protección contra software malicioso
Protocolo o procedimiento para la atención de incidentes de seguridad
Política de controles criptográficos
Política de seguridad de las comunicaciones
Protocolo para cumplimiento del deber de confidencialidad con proveedores y personal externo.

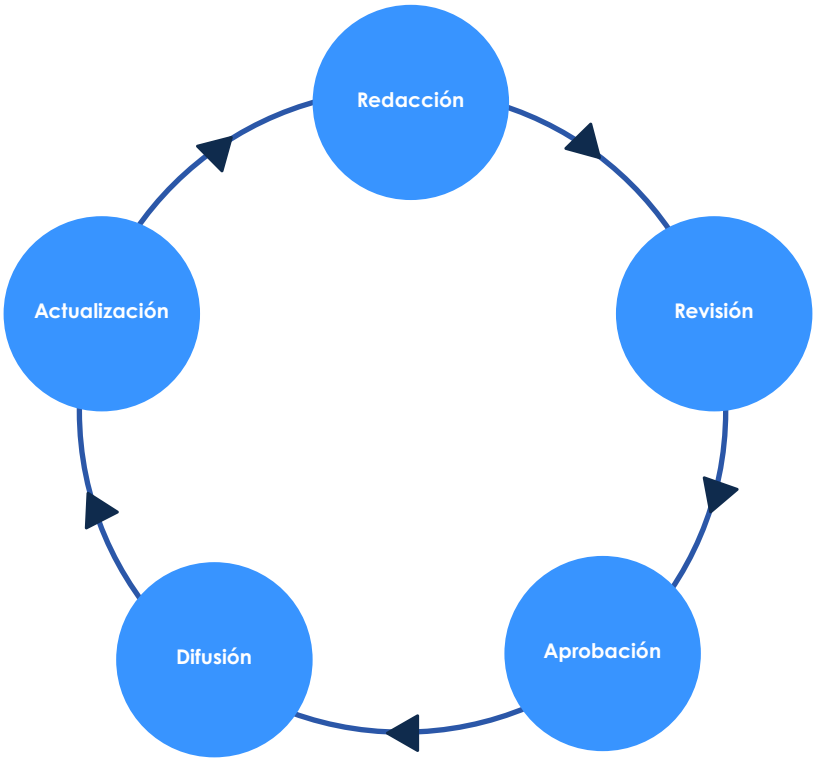
5. PERSONAL ENCARGADO DE REDACTAR LAS POLÍTICAS DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES

Respecto a quién debe redactar las políticas, si bien el proceso de elaboración debe estar aprobado, coordinado y supervisado por el Comité de Transparencia respectivo de cada sujeto obligado, como lo establece el artículo 47 de los Lineamientos Generales, se recomienda crear grupos multidisciplinarios donde confluya personal, por ejemplo, de las unidades administrativas que operan a nivel de usuarios, los custodios de los datos personales y quienes interactúan el tratamiento de los mismos, así como personal de la unidad administrativa correspondiente a Tecnologías de la Información o informática.

Lo anterior es así, ya que el desarrollo de políticas requiere de la participación de miembros del sujeto obligado directamente relacionados con los procesos esenciales del mismo, así como con el personal que conozca y opere medidas de seguridad físicas y técnicas.

Para decidir quiénes participarán en su redacción será indispensable tomar como referencia el inventario de datos personales y sistemas, el ciclo de vida de los datos, así como la determinación de roles, responsabilidades y cadena de custodia de los datos personales.

Ahora bien, la aprobación de las políticas requiere de la elaboración un procedimiento donde se redacten, revisen, aprueben, difundan y se actualicen, véase la figura 2.



Autoría propia

- Redacción. debe emplear un lenguaje conciso y fácil de comprender, de acuerdo con la audiencia a la que van dirigidas, como se mencionó anteriormente, si la política es general, va dirigida a todos los empleados y externos, debe ser en un lenguaje sencillo y entendible para todos; se deben redactar en infinitivo, y debe evitarse el uso de negaciones directas en los enunciados.

- Revisión. Para efectuar la revisión de las políticas se debe tomar en cuenta que debe haber un equilibrio entre la funcionalidad y la operatividad de estas; asimismo, se recomienda que se dé un proceso de retroalimentación con el personal usuario de sistemas de tratamiento y custodios de los datos personales a quienes le vaya a aplicar dicha política; y se

sugiere que en todo momento se involucren a los órganos de gobierno o directivos del sujeto obligado.

- Aprobación. La aprobación la debe realizar el Comité de Transparencia conforme al artículo 47, de los Lineamientos Generales. Se debe incluir la fecha de aprobación o en su caso de actualización.

- Difusión. Consiste en dar a conocer las políticas y su entrada en vigor, ello es fundamental para su funcionamiento. Por tal motivo, el responsable del tratamiento debe idear mecanismos para dar a conocerlas entre las audiencias, ya sea entregándolas físicamente a la suscripción del contrato laboral con los servidores públicos, para el personal de nuevo ingreso, pero también entregándola física o electrónicamente a todo el personal del sujeto obligado, así como a los externos. Será muy importante que el responsable del tratamiento pueda confirmar que las políticas han sido recibidas, leídas y comprendidas por el personal, contando con algún medio de prueba como firma de recepción, para efectos del cumplimiento del principio de responsabilidad.

  Además de lo anterior, el responsable puede realizar actividades como la creación de carteles, trípticos, sesiones informativas entre otros, para sensibilizar e informar al personal de la importancia del cumplimiento de las políticas.

- Actualización. La aplicación de políticas es una actividad permanente y de mejora continua, por lo que deben realizarse reajustes. La presencia recurrente de la violación de una política, el uso de nueva tecnología para el tratamiento de datos personales, vulneraciones o incidentes de seguridad son algunas de las razones por las cuales se deben actualizar, como se señala en el siguiente título.

6. REVISIÓN, EVALUACIÓN Y MEJORA DE LAS POLÍTICAS DE GESTIÓN Y TRATAMIENTO

Se deberá seguir el propio procedimiento general descrito en la propia política y que se describe en el punto 4.1. Contenido de la Política General de Gestión y Tratamiento de Datos, particularmente en el punto donde se detalla "El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales" de las presentes recomendaciones.

Además debe comprenderse que, las políticas de gestión y tratamiento de datos, como parte del sistema gestión de seguridad de los datos personales, pero también como obligación legal y como medida de seguridad administrativa, deben someterse a monitoreo, revisión y actualización constante, para lograr una eficiente seguridad de los datos personales y de los sistemas de tratamiento.

En ese sentido, es fundamental darles seguimiento a las políticas, mantener su implementación a través del tiempo y actualizar o realizar ajustes a las mismas cuando sea necesario, en particular conforme lo establece en los artículos 30 fracciones IV y V, 33 fracción VII, 34 y 35 fracción VI de la Ley General, los cuales debe ser interpretados de manera armónica y congruente, con lo establecido en los artículos 49 y 63 de los Lineamientos Generales. Finalmente, se debe recordar que podrán someterse a auditorías voluntarias por parte del Instituto o los Organismos garantes, según corresponda, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente Ley y demás normativa que resulte aplicable.

7. REFERENCIAS

INAI, coord. Davara F. de Marcos, Isabel. Diccionario de Protección de datos personales, conceptos fundamentales. Primera edición, noviembre 2019, México. Fecha de Consulta: 24 y 25/04/2022. Disponible en: https://transparencia.guadalajara.gob.mx/sites/default/files/DiccionarioProteccionDatosPersonales.pdf

INAI, coord. Solange Maqueo, María. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, comentada. Primera edición, noviembre 2018, México. Fecha de consulta: 24 y 25/04/2022. Disponible en: https://transparencia.guanajuato.gob.mx/bibliotecadigital/normatividad/Ley_General_de_Proteccion_de_Datos_Personales_en_Posesion_de_Sujetos_Obligados_comentada.pdf

INCIBE, Glosario de términos de ciberseguridad, una guía de aproximación para el empresario. Fecha de consulta: 24 y 25/04/2022 Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017. Fecha de consulta: 09/03/2022. Disponible en https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017)

Lineamientos Generales para la Protección de Datos Personales en el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018. Fecha de consulta: 09/03/2022. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018

Mendoza López, Miguel Ángel y Lorenzana Gutiérrez, Pablo Antonio (5 de marzo de 2013). Normatividad en las organizaciones: Políticas de seguridad de la información - Parte I | Revista. Seguridad (unam.mx), número 16, marzo-abril, ISSN 1 251

478 1 251 477. Fecha de consulta: 10/02/2022. Disponible: https://revista.seguridad.unam.mx/numero-16/normatividad-en-las-organizaciones-pol%C3%ADticas-de-seguridad-de-la-informaci%C3%B3n-parte-i

Universidad Internacional de la Rioja, 14 de abril de 2020, Claves de las Políticas de Seguridad de la Información, UNIR Revista. Fecha de consulta: 11/02/2022. Disponible en https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

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

RECOMENDACIONES

para la elaboración de Políticas internas de gestión y tratamiento de datos personales

(Sector Público)

Mayo 2022