INE
Instituto Nacional Electoral

Base Regulatoria

Sistema de Gestión para la Protección de Datos Personales

(Tercera edición)

Junio 2024

CONTROL DE VERSIONES

Versión	Descripción	Fecha	Documento de actualización
Primera edición	Presentación y aprobación al Comité de Transparencia	12-12-2019	No aplica
Segunda edición	Presentación de las actualizaciones al Comité de Transparencia	10-03-2022	Consultar
Tercera edición	Presentación y aprobación de las actualizaciones al Comité de Transparencia	25-06-2024	Consultar

CONTENIDO

GLOSARIO

Para los efectos del presente documento, se tomarán las definiciones establecidas en la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados, el Programa para la Protección de Datos Personales del Instituto Nacional Electoral (en adelante el Programa) y, sin perjuicio de lo previsto en la normatividad aplicable en la materia, se entenderá por:

a) **Alcance material**: Número de procesos de negocio que involucran el tratamiento de datos personales realizado por el responsable o encargado que contempla el esquema de mejores prácticas.[1]

b) **Alcance normativo**: Principios, deberes y obligaciones previstas en la Ley General de Datos que abarca el esquema de mejores prácticas. Puede ser total o parcial.[2]

c) **Base regulatoria**: Marco normativo del Sistema de Gestión de Protección de Datos Personales del Instituto Nacional Electoral.

d) **Certificación**: Procedimiento que lleva a cabo un organismo de certificación para evaluar la conformidad de un esquema de mejores prácticas o sistema de gestión y su implementación, así como productos y servicios tecnológicos de tratamiento de datos personales, con relación con lo dispuesto en la Ley General de Datos y demás normatividad que de ella derive.[3]

e) **Ciclo Deming o de mejora continua**: Conocido también por sus siglas en inglés como el ciclo PDCA *(Plan, Do, Check, Act).* Metodología que describe las etapas para la implementación de un sistema de gestión, producto o servicio.[4]

[1] Parámetros de mejores prácticas en materia de protección de datos personales del sector público, artículo 12, aprobado por el INAI mediante acuerdo ACT-PUB/11/09/2019.07
[2] Ibid., artículo 11
[3] Ibid., artículo 2 fracción III.
[4] PDSA Cycle, The Deming Institute, URL: https://deming.org/explore/p-d-s-a

f) **Control**: Acciones de protección de datos personales resultado de las obligaciones de la normativa en la materia. Es una medida que modifica el riesgo del dato personal.[5]

g) **Dato**: En su acepción informática se define como "la información dispuesta de manera adecuada para su tratamiento por una computadora".[6] Se define, además, como los elementos primarios de la información, que, por sí solos, son irrelevantes para la toma de decisiones (de la Peña Santillán, 2010).

h) **Dato personal**: 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.[7]

a) **Dominio**: Procesos para la protección de los datos personales que una organización realiza.

b) **Esquema de mejores prácticas**: Conjunto de acciones, reglas, criterios y procedimientos con finalidades definidas para la protección de los datos personales.[8]

c) **Información**: En el contexto de seguridad de la información, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. [9]

d) **Ley General de Datos o LGPDPPSO**: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

---

[5] ISO/IEC 27000:2018, Information Technology – Security Techniques- Information security system – Overview and vocabulary.
[6] Definición tomada del Diccionario de la Lengua española en línea, URL: https://dle.rae.es/dato
[7] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 3, fracc. IX. 2017.
[8] Parámetros de mejores prácticas en materia de protección de datos personales del sector público, artículo 8, aprobado por el INAI mediante acuerdo ACT-PUB/11/09/2019.07
[9] Portal del ISO 27001 en español, URL: http://iso27000.es/iso27000.html

e) **Marco de referencia o *framework***: Conjunto estandarizado de conceptos, prácticas y criterios de un tipo de problemática particular que sirve como referencia para enfrentar y resolver nuevos problemas de índole similar.[10]

f) **Partes interesadas**, **grupos de interés o *stakeholders*.** Persona u organización que puede afectar, ser afectada o se percibe asimismo a ser afectada por una decisión o actividad.[11]

g) **Proceso:** Conjunto de fases sucesivas de un fenómeno natural o de una operación artificial.[12] Conjunto de actividades mutuamente relacionadas o que interactúan, que utilizan las entradas para proporcionar un resultado previsto.[13]

h) **Proceso de negocio**: Procesos que prescriben la forma en la que se utilizan los recursos -datos, capital, personas- de una organización para lograr sus objetivos de negocio.[14]

i) **Sistema de gestión**: Conjunto de elementos interrelacionados o interactivos de una organización que establecen políticas, objetivos y procesos para alcanzar sus objetivos.[15] Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.[16]

---

[10] ¿Qué es una Infraestructura Digital o 'Framework'?, URL: http://www.ictea.com/cs/index.php?rp=/knowledgebase/8991/Que-es-una-Infraestructura-Digital-o-andsharp039Frameworkandsharp039.html
[11] Gestión de Calidad. Universidad Santiago de Cali, URL: https://www.usc.edu.co/index.php/gestion-de-calidad/terminos-y-definiciones
[12] Diccionario de la Lengua española en línea, URL: https://dle.rae.es/proceso
[13] Gestión de Calidad. Universidad Santiago de Cali, URL: https://www.usc.edu.co/index.php/gestion-de-calidad/terminos-y-definiciones
[14] F. Leymann and W. Altenhuber, "Managing business processes as an information resource," in *IBM Systems Journal*, vol. 33, no. 2, pp. 326-348, 1994.
doi: 10.1147/sj.332.0326
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5387316&isnumber=5387310
[15] Gestión de Calidad. Universidad Santiago de Cali, URL: https://www.usc.edu.co/index.php/gestion-de-calidad/terminos-y-definiciones
[16] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 34, párrafo 2. 2017

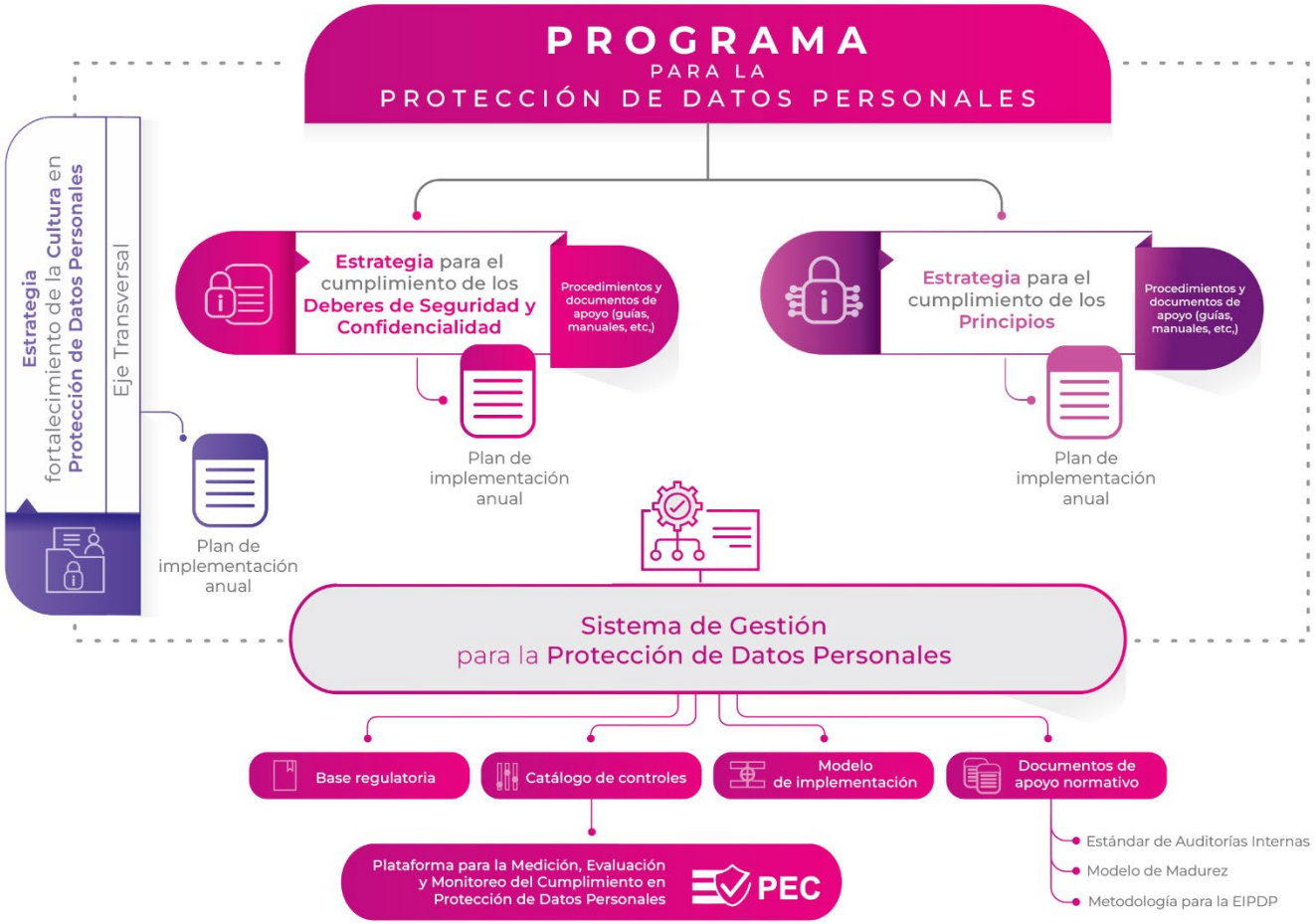

Figura 1. Modelo de operación para el cumplimiento de principios y deberes en materia de protección de datos personales

1 INTRODUCCIÓN

El Sistema de Gestión para la Protección de los Datos Personales (SiPRODAP) provee al INE las bases para cumplir con los principios, deberes, derechos y demás obligaciones señaladas en la normativa aplicable, permitiendo:

- Verificar que las medidas implementadas para el cumplimiento de la normatividad son eficaces, eficientes y apropiadas de acuerdo con el riesgo inherente del dato personal;
- Demostrar la conformidad de las actividades de tratamiento;
- Medir el aprovechamiento eficaz y permanente de los recursos destinados para el logro de objetivos de protección de datos personales; e,
- Integrar a toda la organización en la protección de los datos personales.

Entre las características consideradas para el diseño del SGPDP, se encuentran las siguientes:

- Integrado por las buenas prácticas nacionales e internacionales en protección de datos, privacidad y seguridad de la información;
- Sustentado en la LGPDPPSO;
- Considera la mejora continua;
- Escalable, con relación al alcance del sistema de gestión, para que las medidas sean coherentes con los riesgos del procesamiento y la naturaleza del dato personal;
- Compatible con otros sistemas de gestión; y,
- Adaptable a diversos organismos públicos.

Disponer de un Sistema de Gestión para la Protección de los Datos Personales proporcionará:

a) A las personas titulares de los datos:

- Transparencia en los mecanismos implementados para el debido tratamiento de sus datos personales.
- Confianza en el debido tratamiento de sus datos personales.

b) Al Instituto,

De manera general:

- Las bases para homologar los procesos, acciones y actividades de protección de los datos personales;
- Facilitar la transferencia segura entre sujetos obligados u organizaciones internacionales;
- Un habilitador clave para lograr la protección de datos por diseño y por defecto;
- Un esquema de mejores prácticas, conforme a lo señalado en el artículo 72 de la Ley General de Datos;
- Conocimiento de los mecanismos de protección de datos que son implementados;
- Las bases para una mejor gestión de los riesgos en el tratamiento de los datos personales;
- Medir del nivel de madurez en la protección de los datos personales.

De manera particular:

- La gestión del Programa de Protección de Datos Personales Institucional.
- Disponer de un sistema de gestión que incluya las medidas de seguridad implementadas para proteger los datos personales (artículo 34[17] de la Ley

[17] Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

General de Datos y artículo 32[18] del Reglamento del Instituto en materia de Protección de Datos Personales).

El SiPRODAP está conformado de dos apartados: la Base regulatoria y el Catálogo de Controles.

Figura 2. Esquema general del Sistema de Gestión para la Protección de Datos Personales

Este documento contiene la descripción de la Base regulatoria.

[18] La Unidad de Transparencia implementará el Sistema de Gestión en el que quedarán documentadas y contenidas las acciones que los Órganos del Instituto desarrollen para mantener tales medidas de seguridad.

2 BASE REGULATORIA

Introducción

En este apartado, la organización[19] deberá desarrollar una breve introducción referente a la misma y sus objetivos de protección de los datos personales.

Sección 1. Alcance material

El objetivo es señalar el alcance material del sistema de gestión de la organización para establecer, implementar, mantener y mejorar la protección de los datos personales.

El **alcance material** será de dos formas: total o parcial.

a) **Total,** cuando abarque todos los procesos de negocio que involucran el tratamiento de datos personales del responsable o encargado adherido;

b) **Parcial**, si abarca algunos procesos de negocio que involucran el tratamiento de datos personales del responsable o encargado adherido.

Sección 2. Referencias normativas

Las referencias normativas se dividen en: obligatorias y opcionales.

a) Obligatorias

- Ley General de Protección de Datos en Posesión de Sujetos Obligados.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Normativa interna en la materia, generada por el sujeto obligado.

b) Opcionales

- Convenio 108+. Convenio para la protección de las personas con respecto al procesamiento de datos personales.

[19] El término “organización” hace referencia al INE.

- Las que se consideren necesarias de acuerdo con la normativa particular que aplique a la organización y a sus funciones.

Sección 3. Términos, definiciones y abreviaciones (Glosario)

El objetivo es señalar el uso de las definiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y, en caso de considerarse necesario, definiciones de la normativa interna y/o especializada.

Incluir, si se considera necesario, las siguientes:

a) **Alta dirección**: áreas que toman las decisiones del negocio: Consejo, Dirección General o equivalentes.

b) **Desempeño**: resultado medible. Puede relacionarse con las actividades de gestión, procesos, productos y servicios, sistemas u organizaciones.

c) **Información documentada**: información requerida para ser controlada y mantenida por una organización y el medio en el cual está contenida. Evidencia de los resultados logrados (registros). La información documentada puede ser en cualquier formato y medio y desde cualquier fuente.

d) **Monitoreo**. Determinar el estado de un sistema, un proceso o una actividad.

e) **No conformidad**. Incumplimiento de un requisito.

f) **Objetivos**: resultado a alcanzar. En el contexto de la Protección de los datos personales, la organización establece los objetivos de protección de los datos, de acuerdo con la política de protección de datos personales, para lograr resultados específicos.

g) **Organización**: persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.

h) **Órgano**: Persona o conjunto de personas que actúan en representación de una organización o persona jurídica en un ámbito de competencia determinado.

i) **Partes interesadas**: llamadas también grupos de interés o ***stakeholders***. Persona u organización que puede afectar, ser afectada por o se percibe asimismo a ser afectada por una decisión o actividad. Incluye a los ciudadanos, partidos políticos y los órganos garantes en materia de Transparencia, Acceso a la Información y Protección de Datos Personales.

j) **Política**: Intenciones y dirección de una organización, formalmente expresadas por los órganos de dirección.

k) **Proceso**: conjunto de actividades interrelacionadas o interactivas para transformar entradas en salidas.

l) **Requerimiento**: Necesidad o expectativa establecida, generalmente implícita u obligatoria.

m) **Riesgo**: Efecto de incertidumbre. El efecto puede ser una desviación de lo esperado, ya sea positiva o negativa. La incertidumbre es un estado o de deficiencia de información relacionada a entender o conocer de un evento sus consecuencias o probabilidad. El riesgo a menudo es expresado en términos de la combinación de las consecuencias de un evento y la probabilidad de ocurrencia asociada.

n) **Sistema de gestión**: conjunto de elementos interrelacionados o interactivos de una organización que establecen políticas, objetivos y procesos para alcanzar sus objetivos.

Sección 4. Contexto de la organización

4.1 Entendimiento de la organización y su contexto

La organización tiene el rol de responsable; por lo tanto, debe identificar y analizar los problemas externos e internos que sean relevantes para su propósito y que afecten su capacidad para lograr los resultados previstos de su sistema de gestión para la protección de los datos personales, los cuales pueden incluir:

a) Legislación aplicable en protección de datos personales o privacidad;

b) Regulación aplicable;

c) Decisiones judiciales aplicables;

d) Contexto organizacional, gobernanza, políticas y procedimientos aplicables;

e) Decisiones administrativas aplicables;

f) Requerimientos contractuales aplicables.

4.2 Identificación de necesidades y expectativas de las partes interesadas

La organización debe determinar:

a) las partes interesadas que son relevantes para el sistema de gestión para la protección de los datos personales;

b) los requisitos pertinentes de estas partes interesadas.

4.3 Determinar el alcance normativo del Sistema de Gestión

La organización debe determinar los límites y la aplicabilidad del sistema de gestión para la protección de los datos personales para establecer el **alcance normativo**.

El **alcance normativo** será de dos formas: total o parcial.

a) **Total,** cuando abarque todos los principios, deberes y obligaciones previstos en la Ley General de Datos y demás normativa que de ellas derive;

b) **Parcial**, cuando abarque sólo algunos principios, deberes y obligaciones previstas en la Ley General de Datos y demás normativa que de ella derive.

Para determinar este alcance, la organización debe considerar:

a) las cuestiones externas e internas mencionadas en 4.1;
b) los requisitos mencionados en 4.2.

La organización debe mantener la información documentada acerca del alcance.

4.4 Sistema de Gestión para la Protección de los Datos Personales

La organización debe establecer, implementar, mantener y mejorar continuamente un SGPDP, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de esta Base regulatoria.

Sección 5. Liderazgo

5.1 Liderazgo y compromiso organizacional

La organización deberá demostrar liderazgo y compromiso con respecto al sistema de gestión para la protección de los datos personales a través de:

a) asegurar que la política de protección de datos personales y los objetivos de protección de datos estén establecidos y sean compatibles con la organización;

b) garantizar la integración de los requisitos del sistema de gestión para la protección de los datos personales en los procesos de la organización;

c) asegurar que los recursos necesarios para el sistema de gestión para la protección de los datos personales estén disponibles;

d) comunicar la importancia de una gestión eficaz de la protección de los datos personales y de cumplir con los requisitos del sistema de gestión de protección de datos personales;

e) garantizar que el sistema de gestión para la protección de los datos personales logre los resultados previstos;

f) dirigir y apoyar a las personas para que contribuyan a la efectividad del sistema de gestión para la protección de los datos personales;

g) promoción de la mejora continua;

Apoyar otras funciones de gestión relevantes para demostrar su liderazgo tal como se aplica a sus áreas de responsabilidad.

5.2 Políticas

La organización debe establecer una política de protección de datos personales que:

a) sea apropiada para el propósito de la organización;

b) proporcione un marco para establecer los objetivos de la protección de los datos personales;

c) incluya un compromiso para satisfacer los requisitos aplicables;

d) incluya un compromiso con la mejora continua del sistema de gestión para la protección de los datos personales.

La política de protección de datos personales deberá:

a) estar disponible como información documentada;

b) ser comunicada dentro de la organización;

c) estar disponible para las partes interesadas, según corresponda.

5.3 Roles organizacionales, responsabilidades y autoridades

La organización debe garantizar que las responsabilidades y autoridades para los roles relevantes se asignen y comuniquen dentro de la organización.

La organización debe asignar la responsabilidad y la autoridad para:

a) asegurar que el sistema de gestión para la protección de los datos personales cumpla con los requisitos de esta Base regulatoria;

b) informar sobre el desempeño del sistema de gestión para la protección de los datos personales a la organización.

Sección 6. Planificación

6.1 General

6.1.1 Acciones para tratar riesgos y oportunidades

Al planificar el sistema de gestión para la protección de los datos personales, la organización debe considerar los problemas mencionados en 4.1 y los requisitos mencionados en 4.2 y determinar los riesgos y oportunidades que deben abordarse para:

a) asegurar que el sistema de gestión para la protección de los datos personales puede lograr los resultados previstos;

b) prevenir o reducir efectos no deseados en el tratamiento de los datos personales durante todo su ciclo de vida;

c) lograr la mejora continua.

La organización debe planificar:

a) acciones para abordar estos riesgos y oportunidades;

b) cómo:

- integrar e implementar las acciones en sus procesos del sistema de gestión para la protección de los datos personales;
- evaluar la efectividad de estas acciones.

6.1.2 Tratamiento de riesgos

La organización debe, con forme al alcance del SGPDP:

a) Seleccionar las opciones de tratamiento de riesgo, de acuerdo con el resultado de la evaluación de riesgos de los datos personales;

b) Determinar los controles necesarios para implementar las opciones de tratamiento de riesgo seleccionadas;

c) Verificar que los controles incluyan, al menos, los descritos en el Anexo A;

d) Elaborar un Estado de Aplicabilidad de los controles de protección de datos personales, en el que se señalen los controles implementados y los que no fueron implementados, con su justificación correspondiente;

e) Formular el plan de tratamiento de riesgos de datos personales;

f) Obtener la aprobación del plan de tratamiento de riesgos por parte de los dueños/propietarios del tratamiento de los datos.

La organización debe mantener la información documentada sobre el tratamiento de los riesgos referente a los datos personales.

6.2 Objetivos de protección de datos personales y planificación para alcanzarlos

La organización debe establecer los objetivos para la protección de los datos personales, con forme al alcance del SGPDP.

Los objetivos para la protección de los datos personales deberán:

a) ser coherentes con la política de protección de datos personales;

b) ser medibles (si es posible);

c) tener en cuenta los requisitos aplicables;

d) ser monitoreados;

e) ser comunicados;

f) ser actualizados según corresponda.

La organización debe retener información documentada sobre los objetivos de protección de los datos personales.

Al planificar cómo lograr sus objetivos, la organización debe determinar:

- qué se hará;
- qué recursos se requerirán;

- quién será responsable;
- cuándo se completará;
- cómo se evaluarán los resultados.

Sección 7. Soporte

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión para la protección de los datos personales.

7.2 Competencias

La organización debe:

- determinar la competencia necesaria de la (s) persona (s) que realizan el trabajo bajo su control que afecta su desempeño en la protección de los datos personales;
- garantizar que estas personas sean competentes sobre la base de una educación, formación o experiencia adecuadas;
- cuando corresponda, tomar medidas para adquirir la competencia necesaria y evaluar la efectividad de las acciones tomadas;
- retener información documentada apropiada como evidencia de la competencia.

7.3 Sensibilización

Las personas que trabajen bajo el control de la organización deben tener en cuenta:

- la política de protección de datos personales;
- su contribución a la efectividad del sistema de gestión para la protección de los datos personales, incluidos los beneficios de un mejor desempeño en la protección de los datos;
- las implicaciones de no cumplir con los requisitos del sistema de gestión para la protección de los datos personales.

7.4 Comunicación

La organización debe determinar las comunicaciones internas y externas relevantes para el sistema de gestión para la protección de los datos personales, que incluyan:

- sobre lo que comunicará;
- cuándo comunicarse;
- con quien comunicarse;
- cómo comunicarse.

7.5 Información documentada

7.5.1 General

El sistema de gestión para la protección de los datos personales de la organización debe incluir:

a) información documentada requerida por el SGPDP;

b) información documentada que la organización determine como necesaria para la efectividad del SGPDP.

7.5.2 Crear y actualizar

Al crear y actualizar la información documentada, la organización debe garantizar:

a) la identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia);

b) el formato (por ejemplo, idioma, versión de software, gráficos) y medios (por ejemplo, papel, electrónico);

c) la revisión y aprobación de idoneidad y adecuación.

7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión para la protección de los datos personales se controlará para garantizar que:

a) está disponible y es adecuada para su uso, donde y cuando sea necesario;

b) está adecuadamente protegido (por ejemplo, contra la pérdida de confidencialidad, uso indebido o pérdida de integridad).

Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda:

- distribución, acceso, recuperación y uso;
- almacenamiento y conservación, incluida la preservación de la legibilidad;
- control de cambios (por ejemplo, control de versiones);
- retención y disposición.

La documentación de la información de origen externo que la organización determine que es necesaria para la planificación y operación del sistema de gestión para la protección de los datos personales deberá identificarse, según corresponda, y controlarse.

Sección 8. Operación

8.1 Planificación y control operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos y para implementar las acciones determinadas en 6.1, mediante:

- establecer criterios para los procesos;
- implementar el control de los procesos de acuerdo con los criterios;
- mantener información documentada en la medida necesaria para tener la confianza de que los procesos se han llevado a cabo según lo planeado.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no intencionados, tomando medidas para mitigar los efectos adversos, según sea necesario.

La organización debe garantizar que los procesos tercerizados estén controlados.

8.2 Evaluaciones de riesgos en materia de protección de datos personales

Apartado actualizado versión 3.0

La organización debe ejecutar evaluaciones de riesgos de privacidad y datos personales en los procesos de negocio que implique su tratamiento en periodos establecidos, cuando ocurran cambios significativos, sean estos normativos u operacionales, en procesos ya

existentes o cuando surjan nuevos procesos, tomando en cuenta los criterios del numeral 6.1.1 Acciones para tratar riesgos y oportunidades, de este documento.

La organización debe retener información documentada apropiada como evidencia de los resultados.

8.3 Evaluación de impacto en la protección de datos personales

Apartado actualizado versión 3.0

La organización debe aplicar evaluaciones de impacto en la protección de datos personales para tratamientos de alto riesgo, en función de lo establecido en la legislación aplicable en la materia.

La organización debe:

- Evaluar las consecuencias potenciales que pueden resultar si el riesgo identificado se materializa para los titulares de los datos.
- Mantener la información documentada sobre las evaluaciones de impacto.

8.4 Tratamiento de riesgos en materia de protección de datos personales

Apartado actualizado versión 3.0

La organización debe implementar los planes de tratamiento de riesgos, informando el resultado de la implementación.

La organización debe mantener la información documentada como evidencia de la gestión de los riesgos.

Sección 9. Evaluación del desempeño del SG

9.1 Monitoreo, medición, análisis y evaluación

La organización debe determinar:

- lo que necesita ser monitoreado y medido;

- los métodos de monitoreo, medición, análisis y evaluación, según corresponda, para garantizar resultados válidos;

- cuándo se realizarán el seguimiento y la medición;

- cuándo se analizarán y evaluarán los resultados del monitoreo y la medición.

La organización debe mantener la información documentada apropiada como evidencia de los resultados.

La organización debe evaluar el desempeño en la protección de los datos personales y la efectividad del sistema de gestión para la protección de datos personales.

9.2 Auditorías

9.2.1 Auditorías internas.

La organización debe realizar auditorías internas a intervalos planificados para proporcionar información sobre el sistema de gestión para la protección de los datos personales:

a) conforme a los requisitos propios de la organización para su sistema de gestión para la protección de los datos personales;

b) que verifique se implementa y mantiene de manera efectiva.

9.2.2 Auditorías voluntarias

La organización puede solicitar, de manera voluntaria, auditorías por parte del Órgano Garante, con el objetivo de verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados.

9.2.3 La organización debe:

a) planificar, establecer, implementar y mantener un programa o programas de auditoría, incluida la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la presentación de informes, que deberán tener en cuenta la importancia de los procesos en cuestión y los resultados de auditorías anteriores;

b) definir los criterios de auditoría y el alcance de cada auditoría;

c) seleccionar auditores y realizar auditorías para asegurar la objetividad y la imparcialidad del proceso de auditoría;

d) garantizar que los resultados de las auditorías se comuniquen a las partes interesadas pertinentes;

e) retener información documentada como evidencia de la implementación del programa de auditoría y los resultados de la auditoría.

9.4 Revisión por parte de la alta dirección

La alta dirección debe revisar el sistema de gestión para la protección de los datos personales de la organización, a intervalos planificados, para garantizar su idoneidad, adecuación y eficacia continuas.

La revisión de la alta dirección incluirá la consideración de:

a) el estado de las acciones de revisiones administrativas anteriores;

b) cambios en los problemas externos e internos que son relevantes para el sistema de gestión para la protección de los datos personales;

c) información sobre el rendimiento en la protección de los datos personales, incluidas las tendencias en:

- no conformidades y acciones correctivas;
- resultados de monitoreo y medición;
- resultados de la auditoría;

d) oportunidades de mejora continua.

Los resultados de la revisión por la alta dirección deben incluir decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el sistema de gestión para la protección de los datos personales.

La organización debe mantener la información documentada como evidencia de los resultados de las revisiones de la alta dirección.

Sección 10. Mejora

10.1 No conformidad y acción correctiva

Cuando ocurre una no conformidad, la organización debe:

a) reaccionar ante la no conformidad y, según corresponda:

- tomar medidas para controlarlo y corregirlo;
- aceptar las consecuencias;

b) evaluar la necesidad de tomar medidas para eliminar la (s) causa (s) de la no conformidad, a fin de que no se repita u ocurra en otro lugar, mediante:

- revisión de la no conformidad;
- determinar las causas de la no conformidad;
- determinar si existen no conformidades similares, o si podrían ocurrir potencialmente;

c) implementar cualquier acción necesaria;

d) revisar la efectividad de cualquier acción correctiva tomada;

e) realizar cambios en el sistema de gestión para la protección de los datos personales, si es necesario.

Las acciones correctivas serán apropiadas a los efectos de las no conformidades encontradas.

La organización debe retener información documentada como evidencia de:

- la naturaleza de las no conformidades y cualquier acción posterior tomada;
- los resultados de cualquier acción correctiva.

10.2 Mejora continua

La organización debe mejorar continuamente la idoneidad, adecuación y efectividad del SGPDP.

3 CATÁLOGO DE CONTROLES PARA LA PROTECCIÓN DE DATOS PERSONALES

El Catálogo de controles provee a las áreas propietarias/dueñas, custodias y usuarias, las **actividades** específicas para dar cumplimiento a un control, que serán la base para **medir cuantitativamente el nivel de cumplimiento**.

Para la implementación de los controles, la UTTyPDP, deberá:

a) Diseñar una matriz de responsabilidades que identificará qué controles son responsabilidad de las áreas dueñas/propietarias, custodias y usuarias, atendiendo a los tiempos y formas establecidas en el **Modelo de implementación del Sistema de Gestión.**

b) Diseñar, cuando lo considere pertinente, un modelo de medición que permita conocer el nivel de madurez en la protección de los datos personales a nivel institucional.

Consultar el catálogo de controles en este enlace.