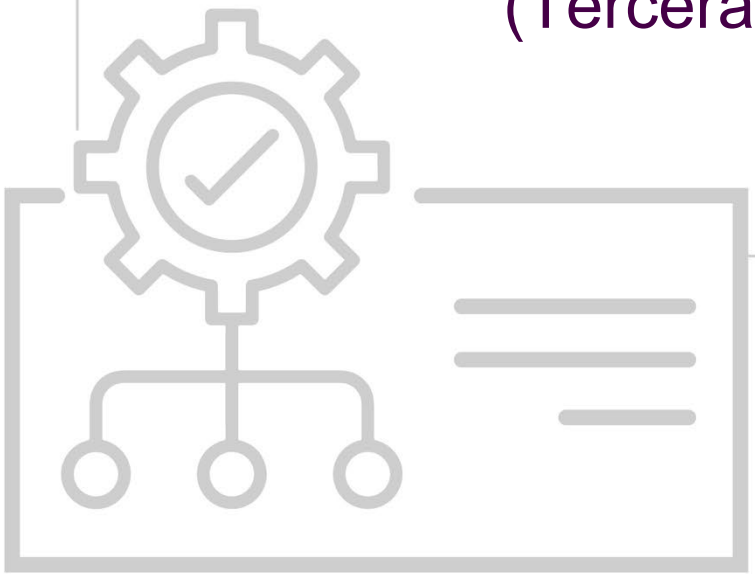
INE
Instituto Nacional Electoral

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

ANTECEDENTES

Primer ciclo del Sistema de Gestión para la Protección de Datos Personales

La implementación de los sistemas de gestión se rige bajo el ciclo de Deming[17] o mejora continua, que se basa en cuatro etapas que conforman un ciclo; al concluir, el ciclo reinicia. En este sentido, el Sistema de Gestión para la Protección de Datos Personales del INE (en adelante, Sistema de Gestión o SiPRODAP) inició su primer ciclo en 2019, concluyendo en 2023, por lo que iniciará el segundo ciclo en 2024.

En función de ello, el 30 de enero de 2024, el Comité de Transparencia aprobó mediante el acuerdo INE-CT-ACG-PDP-001-2024, el Plan de Acción para la conformación de los instrumentos rectores del segundo ciclo respecto de la operación y supervisión de la Protección de Datos Personales en el INE,[18] que incluye la actualización del SiPRODAP.

El Sistema de Gestión cuenta con dos ediciones en su primer ciclo, como se visualiza en la siguiente tabla.

Ciclo del SiPRODAP	Edición	Año
Primer ciclo	Primera	2019
	Segunda	2022
Segundo ciclo	Tercera	2024

Los resultados del primer ciclo pueden ser consultados en los informes publicados en el Apartado virtual de protección de datos personales del Instituto Nacional Electoral sección Sistema de Gestión (SiPRODAP).

[17] The Deming Institute (2023). The PDSA Cycle. Disponible en https:// deming.org/explore/pdsa/
[18] Consultar el informe.

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

El INE, a través de la Unidad Técnica de Transparencia y Protección de Datos Personales (en adelante, Unidad de Transparencia o UTTyPDP) diseñó, en 2019, un modelo que le permitiera cumplir con el principio de responsabilidad en materia de Protección de datos personales desde un enfoque proactivo, denominado "*Modelo de operación para el cumplimiento de principios y deberes en materia de protección de datos personales*" (en adelante, Modelo de operación).

El Modelo de operación indica al Instituto la ruta a seguir para cumplir de manera sistemática y atemporal sus obligaciones respecto de los principios y deberes, no solo en atención a las disposiciones normativas vigentes, sino también tomando en consideración otros elementos y documentos rectores que contemplen su correcta aplicación.

Consta de dos componentes**,** cada uno con sus instrumentos de apoyo (ver figura 1)**:**

I. **Programa para la Protección de Datos Personales**.

   Conformado por las Estrategias para el cumplimiento de Principios [19], Deberes y *Fortalecimiento de la Cultura en Protección de Datos Personales,* como un eje Transversal, que hace referencia de manera específica a la capacitación, concientización y actualización especializada en la materia.

II. **Sistema de Gestión para la Protección de Datos Personales** (en adelante, Sistema de Gestión o SiPRODAP). Atiende al principio de responsabilidad.

Este documento hace referencia al segundo componente del Modelo de operación.

[19] La Estrategia para el cumplimiento de los Principios, abarca los principios de licitud, lealtad, calidad, finalidad, proporcionalidad, información, consentimiento, dejando fuera el principio de responsabilidad, el cual se opera a través del Sistema de Gestión para la Protección de Datos Personales.

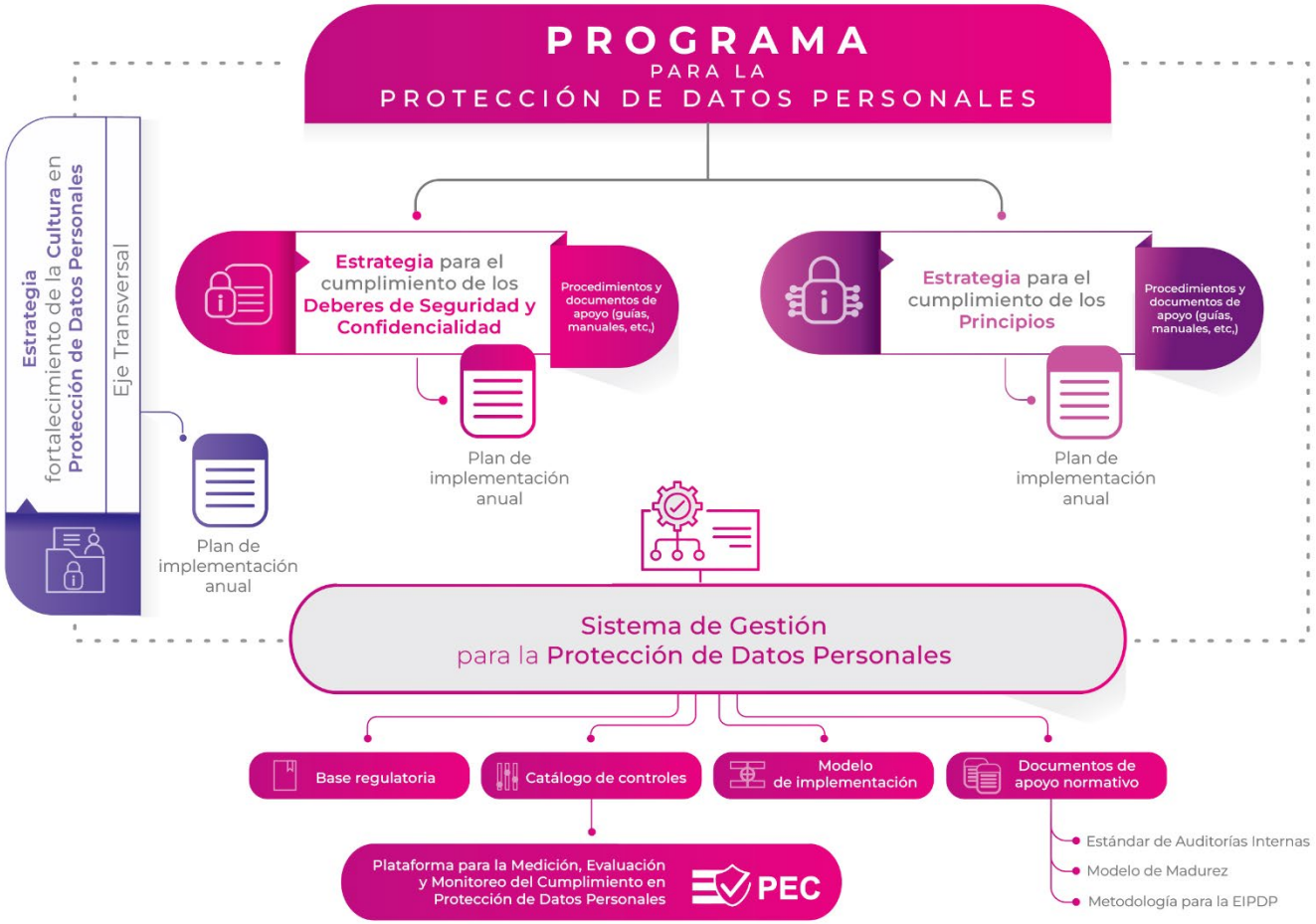


Figura 1. Modelo de operación para el cumplimiento de principios y deberes en materia de protección de datos personales

Sistema de Gestión para la Protección de Datos Personales (tercera edición)

PREÁMBULO

El valor del dato personal

Las organizaciones deben mantener una gestión adecuada de sus bases de datos, llevar a cabo un debido monitoreo que les permita tener control sobre la información que poseen, informar a los individuos el propósito del tratamiento, qué datos personales son o serán procesados y las acciones mediante las cuales los protegen durante la recolección, el procesamiento y el destino final; es decir, durante todo su ciclo de vida.

De esta manera, promueven la transparencia, generando confianza en el tratamiento de los datos personales y, al mismo tiempo, un impacto positivo, como la buena reputación.

Hablar de transparencia -en materia de protección de datos personales- también implica que una organización incluye a todo su personal en la política de protección de datos personales, asigna responsabilidades y roles e implementa reglas de manera clara.[20]

Los datos se han vuelto la materia prima más valiosa; hay quienes afirman que han superado al petróleo para convertirse en el recurso más valioso del mundo[21]; sin embargo, el dato en sí mismo carece de sentido -al ser la unidad mínima de información-, pero cuando se reúne un conjunto de datos, se convierte en información y es cuando toma sentido.[22]

En materia de datos personales, los datos aislados no poseen valor, sino el tener diversos datos que se conviertan en información que permita identificar o hacer identificable a una

[20] Van Lieshout, M., & Emmert, S. (2018). RESPECT4 - Privacy as Innovation Opportunity. En M. Medina, A. Mitrakas, K. Rannenberg, E. Schweighofer, N. Tsouroulas, & (Eds.), Privacy Technologies and Policy. 6th Annual Privacy Forum, APF pp. 43-60. Barcelona, Spain: Springer.
[21] IIPSI. (s.f.). El petróleo de la era digital: OPEN DATA. Recuperado el 28 de agosto de 2019, de Instituto Internacional de Privacidad y Seguridad de la Información: https://privacidadyseguridad.org/el-petroleo-de-la-era-digital-open-data/
[22] García, L. (29 de noviembre de 2018). Datos personales: El usuario como mercancía. Recuperado el 28 de agosto de 2019, de Quinto poder: https://quinto-poder.mx/opinion/datos-personales-el-usuario-como-mercancia/

persona; tener ese tipo de información sobre cientos de millones de personas y poder procesarlos, es lo que otorga valor.

Aunque no es posible asignar un valor preciso a los datos personales – debido a que esto está en función del tipo de dato personal, su actualización, utilidad para posibles interesados, la complejidad de conseguirlos, entre otros- existen diversas metodologías para medir y estimar el valor de los datos personales desde una perspectiva "monetaria"[23], o la llamada "monetización" a los datos personales.[24]

Los datos son la materia prima indispensable para comprender, predecir e influir en el comportamiento de las personas. Es por ello que las bases de datos personales han adquirido un valor cada vez más importante, no sólo para publicistas y mercadólogos, sino también para políticos, que las utilizan para apuntalar sus estrategias de comunicación en segmentos específicos, así como para influenciar en la toma de decisiones de las personas, por lo que muchas empresas y organizaciones están dispuestas a pagar por ellas.[25]

Lo anterior deja ver el peligro que implica, en términos de privacidad, poseer datos personales, debido a que pueden ser obtenidos por medios fraudulentos y utilizados para otros fines, sin el consentimiento del titular y sin considerar métodos legales establecidos en la legislación nacional.

Al ser los datos personales, hoy en día, el activo más importante -y un recurso sin el cual el crecimiento económico no sería posible- las organizaciones deberán sujetarse a las leyes y normativas de protección de datos personales.[26]

El Instituto Nacional Electoral, como la máxima autoridad electoral del Estado Mexicano, es responsable de recabar una diversidad de información personal necesaria para realizar actividades lícitas y legítimas con el objetivo de ejercer sus funciones. Proteger los datos

[23] Dennedy, M., & Leizerov, S. (26 de september de 2017). Series: On monetizing personal information. Recuperado el 25 de septiembre de 2019, de IAPP: https://iapp.org/resources/article/series-on-monetizing-personal-information/
[24]La Secretaría de Economía y la Asociación Mexicana de Internet A.C. (AMIPCI), en 2016, publicaron el "*Estudio sobre el valor económico de los datos personales*" (AMIPCI; SE, 2016), el cual integra resultados acerca del valor que se asigna al dato personal. En México, identificaron diversas empresas con servicios de venta y comercialización de bases de datos empresariales y consumidores que contienen datos personales.
[25] IIPSI. (s.f.). El petróleo de la era digital: OPEN DATA. Recuperado el 28 de agosto de 2019, de Instituto Internacional de Privacidad y Seguridad de la Información: https://privacidadyseguridad.org/el-petroleo-de-la-era-digital-open-data/
[26] García, L. (29 de noviembre de 2018). Datos personales: El usuario como mercancía. Recuperado el 28 de agosto de 2019, de Quinto poder: https://quinto-poder.mx/opinion/datos-personales-el-usuario-como-mercancia/

personales y prevenir que sean vulnerados representa un enorme reto, que ha venido afrontando desde su constitución como IFE, hasta el día de hoy, como INE, a través de la implementación de diversas acciones.

Sin embargo, con el surgimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Instituto, como un sujeto obligado de esta Ley, requiere de mecanismos que le permitan no solo cumplir con la normativa en la materia, sino demostrar que la cumple, esto enmarcado en el principio de responsabilidad o conocido internacionalmente como *accountability* o responsabilidad proactiva con el objetivo de proteger los derechos y libertades de las personas titulares de los datos.

Protección de Datos Personales como Derecho Humano

La protección de los datos personales es un derecho humano que comprende un conjunto de principios, deberes, derechos y obligaciones que las organizaciones deben cumplir para rendir cuentas sobre el tratamiento de los datos personales en su posesión; desde 1980 adquiere una dimensión internacional que se encuentra prevista en diversos instrumentos internacionales, entre los que destacan:

- Las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OECD)[27],
- El Convenio 108 del Consejo de Europa (Consejo de Europa, 1981),
- La Resolución 45/95 de la Asamblea General de la ONU[28],
- Las Directrices para la Armonización de la regulación de la protección de Datos en la Comunidad Iberoamericana[29],

[27] OECD. (23 de septiembre de 1980). Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales. Recuperado el 27 de marzo de 2018, de Organización de los Estados Americanos: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf
[28] Consejo de Europa. (28 de enero de 1981). Convenio No. 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de daros de carácter personal. Recuperado el 25 de enero de 2018, de INAI: http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf
[29] Red Iberoamericana de Protección de Datos. (2007). Directrices para la armonización de la Protección de Datos en la Comunidad Iberoamericana.

- Estándar Internacional para la protección de los datos personales y la privacidad (Resolución de Madrid)[30].

- Los Estándares de protección de datos personales para los Estados Iberoamericanos.[31]

En México, la protección de los datos personales es un derecho humano fundamental, reconocido en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos; por lo tanto, el Estado Mexicano impone un conjunto de obligaciones a las entidades -públicas y privadas- que los tratan.

Obligaciones en materia de Protección de Datos Personales

De manera particular, para las entidades públicas, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), señala que las instituciones deben cumplir con todas las obligaciones que en dicha norma se establecen; esto a través del principio de responsabilidad (artículos 29 y 30, LGPDPPSO), el cual también es aplicable a los encargados de realizar tratamiento de datos personales a solicitud del responsable, y al momento de realizar transferencias nacionales o internacionales.

En los Lineamientos Generales de Protección de Datos Personales para el Sector Público -emitidos por el INAI- (en adelante Lineamientos), referente al principio de responsabilidad, se establecen las siguientes obligaciones que el responsable deberá cumplir:

a) Adoptar políticas e implementar mecanismos para asegurar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

b) Establecer mecanismos para evidenciar el cumplimiento ante los titulares y el INAI.

[30] Agencia Española de Protección de Datos. (2009). Estándares internacionales sobre protección de datos personales y privacidad: Resolución de Madrid: Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con el tratamiento de Datos de Carácter. Madrid, España

[31] RIPD. (20 de junio de 2017). Estándares de Protección de Datos Personales para los Estados Iberoamericanos. Recuperado el 8 de septiembre de 2018, de Red Iberoamericana de Protección de Datos: http://www.redipd.org/noticias_todas/2017/novedades/common/Estandares_Esp_Con_logo_RIPD.pdf#Testo%20en%20espa%C3%B1ol

También establece que, para el cumplimiento de estas obligaciones, el responsable podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de mejores prácticas o cualquier otro mecanismo que determine adecuado para tales fines.

Por otra parte, a nivel internacional el Grupo de Trabajo Artículo 29[32] -ahora reemplazado por el Comité Europeo de Protección de Datos (*European Data Protection Board, EDPB*)[33], en su Opinión 3/2010 referente al principio de responsabilidad, señaló que es necesario aplicar en la práctica medidas apropiadas y efectivas que brinden los resultados de los principios de protección de datos personales. Como ejemplo de tales medidas, cita procedimientos para:

- Garantizar la identificación de todas las operaciones de procesamiento de datos,
- Responder a las solicitudes de acceso,
- La asignación de recursos, incluida la designación de las personas responsables de la organización del cumplimiento de la protección de datos.

Por qué un sistema de gestión

La adopción de un sistema de gestión representa el mecanismo para rendir cuentas a las personas titulares de los datos y al órgano garante nacional sobre el tratamiento de los datos personales, a través del cual también se materializa la implementación del principio de responsabilidad –pero que engloba la acreditación del cumplimiento del resto de los principios, deberes y demás obligaciones establecidas en la *LGPDPPSO*-.

Mediante un sistema de gestión (SG) es posible estructurar los elementos que conformarán la protección de los datos personales mediante un enfoque sistémico para lograr la mejora continua –con base en los objetivos de protección de datos personales en la organización y la normatividad aplicable-.

[32] Grupo de trabajo europeo independiente que se ocupó de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (entrada en aplicación del RGPD). URL: https://ec.europa.eu/newsroom/article29/news-overview.cfm
[33] Organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de la UE. URL: https://edpb.europa.eu/edpb_es

Un SG está conformado por una serie de procesos, acciones y tareas que se llevan a cabo sobre un conjunto de elementos (personas, procedimientos, estrategias, planes, recursos, productos, etc.) [34] para que una organización logre sus objetivos. [35], como lo es, la protección de los datos personales [36].

La protección de los datos personales establece el cumplimiento de derechos, principios, deberes y diversas obligaciones. En este sentido, el INAI desarrolló la *Guía para la implementación de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP)*, para cumplir con lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)[37], que también puede ser utilizada para cumplir con el artículo 34 de la LGPDPPSO [38], no obstante, dicho modelo está acotado a la implementación de la seguridad (Deberes) de los datos personales, dejando fuera los principios, derechos y demás obligaciones.

En este sentido, es importante mencionar que, si bien las buenas prácticas de seguridad ayudan a gestionar el riesgo tecnológico –*incidentes de seguridad*- y riesgos de cumplimiento -*legal*- al proteger la información en general, **existen otros riesgos que pueden surgir de cómo las organizaciones recopilan, almacenan, usan y comparten los datos personales para cumplir con su misión u objetivo de negocio**; es decir, pueden suscitarse riesgos para los derechos y libertades de las personas cuyos datos son sujetos de tratamiento; o sea, la protección de los datos personales y la seguridad de la información son conceptos distintos pero que se encuentran interrelacionados.

Derivado de lo anterior, la UTTyPDP propone el diseño de un Sistema de Gestión para la Protección de los Datos Personales (SGPDP o Sistema de Gestión), el cual proveerá al Instituto las bases para cumplir con los principios, deberes, derechos y demás obligaciones señaladas en la normativa aplicable, permitiendo:

---

[34] Giraldo Giraldo, R. A. (2017). Mejoramiento del proceso de compras de la constructora SSINCO S.A.S. Recuperado el 5 de septiembre de 2019, de Repositorio de la Universidad Católica de Manizales: http://repositorio.ucm.edu.co:8080/jspui/bitstream/handle/10839/1885/Ricardo%20Alberto%20Giraldo.pdf?sequence=1&isAllowed=y

[35] ISO/IEC. (s.f.). Management system standards. Recuperado el 22 de noviembre de 2018, de ISO.ORG: https://www.iso.org/management-system-standards.html

[36] Estos objetivos pueden relacionarse con diversos temas, que incluyen la calidad del producto o servicio, la eficiencia operativa, el desempeño ambiental, la salud, la seguridad, entre otros.

[37] INAI. (junio de 2015). Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales. Recuperado el 7 de enero de 2018, de INAI: http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

[38] Artículo 34. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

- 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[39] de la Ley General de Datos y artículo 32[40] del Reglamento del Instituto en materia de Protección de Datos Personales).

[39] 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.
[40] 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.

OBJETIVO DEL SISTEMA DE GESTIÓN

Apartado actualizado versión 3.0

Garantizar que los datos personales en posesión del Instituto Nacional Electoral sean tratados con estricto apego de la normativa aplicable en la materia, atendiendo al principio de responsabilidad proactiva para evaluar la eficacia y eficiencia del Programa para la Protección de Datos Personales, mediante el uso de mejores prácticas, estándares internacionales y procesos organizados que permitan la mejora continua.

ESTRUCTURA DEL DOCUMENTO

Este documento está conformado por tres apartados y un apéndice:

- **Apartado I**. Metodología empleada para el diseño del Sistema de Gestión.
- **Apartado II**. Describe la estructura del Sistema de Gestión, resultado del diseño.
- **Apartado III**. Explica las fases a través de las cuales será implementado el Sistema de Gestión, por parte de la UTTyPDP.
- **Apéndice Único**. Contiene el detalle de las actividades que la UTTyPDP desarrolló para el diseño del Sistema de Gestión.

1 APARTADO I. METODOLOGÍA EMPLEADA PARA EL DISEÑO DEL SISTEMA DE GESTIÓN

Para el diseño de un Sistema de Gestión para la Protección de Datos Personales (en adelante SGPDP), en 2019, la UTTyPDP desarrolló una metodología sustentada en marcos internacionales sobre privacidad y protección de datos personales, sistemas de gestión y la legislación nacional en la materia para el sector público, con la finalidad de identificar los elementos que debe poseer un sistema de gestión con características de protección de datos personales para organismos públicos que, a la postre, permita verificar y demostrar que las **medidas** utilizadas por los responsables de la protección de los datos personales son **eficaces, eficientes y apropiadas de acuerdo con el riesgo inherente del dato personal** y de esta forma maximizar la protección de los derechos y libertades de los titulares.

Si bien existen marcos internacionales que homologan los principios, deberes, derechos y demás obligaciones, cada legislación en la materia incluye obligaciones específicas de acuerdo con el contexto económico, cultural, democrático y social, por lo que fue necesario un análisis para determinar la estructura, procesos, acciones y actividades de control de protección de datos personales para demostrar el cumplimiento mediante el SGPDP, considerando el ámbito nacional.

En este contexto, y para que el sistema de gestión contara con las características anteriores, la UTTyPDP realizó lo siguiente:

a) **Análisis normativo, para identificación de los elementos –procesos, acciones y actividades-** en materia de protección de datos personales, considerando:

- los principios, deberes, derechos y demás obligaciones establecidas en la normativa y regulación nacional en la materia aplicable a los Sujetos Obligados;
- las mejores prácticas de los estándares y marcos internacionales de privacidad y protección de datos personales;
- los procesos y procedimientos organizacionales utilizados para el cumplimiento.

b) **Identificación de las partes interesadas** en la protección de los datos personales para definir sus **funciones y atribuciones** con la finalidad de designar roles y responsabilidades de la información clave de negocio en materia de protección de los datos personales.

c) **Definición de la estructura del Sistema de Gestión** con base en lo establecido por la Organización de Estándares Internacionales (ISO, por sus siglas en inglés) para lograr la compatibilidad con otros sistemas de gestión que se encuentren implementados en el Instituto.

1.1 ANÁLISIS NORMATIVO

Apartado actualizado versión 3.0

1.1.1 Análisis de la normativa nacional

- Análisis de la LGPDPPSO. De un total de 168 artículos, la UTTyPDP identificó **61 artículos** que los responsables deben cumplir[41].

- Análisis de los Lineamientos Generales de protección de datos personales para el sector público: De un total de 253 artículos, fueron identificados **130 artículos** para su cumplimiento por parte de los responsables.

- Análisis del Reglamento del Instituto Nacional Electoral en materia de Protección de Datos Personales: De un total de 60 artículos, fueron identificados **48 artículos** para su cumplimiento por parte de los responsables.

La matriz se puede consultar en el Apéndice Único, “4.1 Normativa Nacional” de este documento.

1.1.2 Análisis de la normativa internacional

- Análisis del Convenio 108+. De un total de 31 artículos se identificaron **13 artículos** para su integración.

[41] Para ello, tomamos como base el Análisis normativo desarrollado por la propia UTTyPDP en 2017.

- Análisis del Reglamento General de Protección de Datos de la Unión Europea (RGPD). De un total de 99 artículos, se identificaron **41 artículos** para su integración.

Si bien, la normativa internacional fue considerada para el diseño del sistema de gestión, esto no implica que serán consideras como criterios de auditoría.

La matriz se puede consultar en el Apéndice Único, “4.2 Normativa Internacional” de este documento.

1.2 Identificación de las acciones de protección de datos personales

Derivado del análisis en 2019, se identificaron 75 acciones de protección de datos personales, denominadas controles**,** resultado de las obligaciones de la protección de los datos personales, sin embargo, **debido a la actualización en 2022 (ver documento “Actualización al Anexo Único 2022) actualmente se cuenta con 90 acciones de protección de datos personales**.

Cabe señalar que el Instituto ya ha ejecutado parte de estas acciones (o está en proceso de ejecución), sin embargo, el valor añadido de esta actividad es su sistematización y la maduración a una perspectiva institucional.

La matriz se puede consultar en el Apéndice Único, “4.3 Identificación de las obligaciones de protección de datos personales” de este documento.

1.3 Análisis de buenas prácticas

De la identificación de las obligaciones de protección de datos personales que debe cumplir el Instituto en su carácter de responsable, la UTTyPDP realizó la verificación comparada con las buenas prácticas internacionales y *frameworks* de privacidad; específicamente, las siguientes:

- ISO/IEC 27701:2019. Estándar que forma parte del marco de gestión de la seguridad de la información *ISO/IEC 27000 – Information technology – Security techniques – Information security management system. Es una* extensión al estándar internacional ISO/IEC 270001 e ISO/IEC 27002 con el objetivo de especificar los requisitos y proporcionar orientación para establecer, implementar,

mantener y mejorar continuamente un Sistema de Gestión de Información de Privacidad (PIMS, por sus siglas en inglés)[42].

- *ISO/IEC 29100:2024 -Information technology, Security techniques, Privacy framework*. Marco de alto nivel para la protección de la información de identificación personal (PII, por sus siglas en inglés) dentro de los sistemas de tecnología de la información y comunicación (TIC), que involucra aspectos organizacionales, técnicos y de procedimiento en un marco de privacidad general.[43] *Apartado actualizado versión 3.0*

- *Privacy Management Accountability Framework*. Este marco es desarrollado por NYMITY[44] y está dirigido para el cumplimiento de la CCPA -California Consumer Privacy Act y la RGPD –Reglamento General de Protección de Datos Personales de la Unión Europea-.

El análisis se puede consultar en el Apéndice Único, “4.4 Identificación de las obligaciones de protección de datos personales” de este documento.

1.4 IDENTIFICACIÓN DE LA PARTES INTERESADAS

Las buenas prácticas y marcos internacionales señalan que es necesario identificar a los grupos, entidades o áreas, internas o externas, que juegan un rol específico en la protección de los datos personales o que tienen alguna relación con funciones de soporte para ello, con el objetivo de establecer a qué tipo de información tendrán acceso y cuáles son sus responsabilidades respecto de ésta.

- Partes interesadas internas:

    - **Alta dirección**. Se refiere la persona o grupo de personas que dirige y controla la organización al más alto nivel; son las áreas que toman las decisiones del negocio: Consejo General, Direcciones Ejecutivas, Unidades técnicas.

[42] ISO/IEC 27701. (Agosto de 2019). Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines. Switzerland.
[43] ISO/IEC. (15 de diciembre de 2011). Information technology - Security techniques - Privacy frameworks. International Standard ISO/IEC 29100. Suiza.
[44] Compañía global líder en investigación especializada en cumplimiento normativo y en la implementación y gestión efectiva de programas de protección de datos personales. Página web: https://latam.nymity.com/nosotros.aspx

- **Otros órganos colegiados**: Comités, comisiones o equivalentes.
- **Órganos en materia de transparencia**: Comité de Transparencia o equivalente.
- **Áreas responsables del cumplimiento**: unidades administrativas/negocio o instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento y ser responsables o encargadas de los datos personales[45], como pueden ser:
  - Área responsable del tratamiento de los datos personales: Órganos Ejecutivos, Técnicos, de Control o equivalentes, Dirección de área o equivalentes
  - Áreas de seguridad de la información.
  - Áreas de tecnologías de la información y comunicación.

- Partes interesadas externas:
  - **Autoridades de protección de datos**
    - Nacionales: Organismos garantes.
    - Internacionales: Autoridades de Control o equivalentes.
  - **Encargados**: Persona física o jurídica, pública o privada ajena a la organización del responsable, que sola o en conjunto con otras, trate datos personales a nombre y por cuenta del responsable.[46]
  - **Otros sujetos obligados**. Los señalados en la LGPDPPSO.
  - **Titulares**. Persona física a la que corresponden los datos personales.

[45] Definición tomada del artículo 3, fracc. I de la LGPDPPSO.
[46] Definición tomada del artículo 3, fracc. XV de la LGPDPPSO

Referente al Sistema de Gestión se identifica la generación, uso o aprobación de la siguiente información[47]:

a) Gestión del Programa de protección de datos personales.

b) Presupuesto para la protección de datos personales.

c) Gestión de proyectos de datos personales.

d) Políticas, estándares y procedimientos de datos personales.

e) Requerimientos para la protección de los datos personales (técnicos y normativos).

f) Materiales de capacitación y concientización.

g) Reportes de cumplimiento en la protección de datos personales.

h) Gestión de riesgos de los datos personales.

i) Tablero (*dashboard*) del sistema de gestión para la protección de los datos personales.

La nomenclatura empleada para describir la participación de las partes interesadas con respecto a la información del sistema de gestión es la siguiente:

- A – Aprobador. Área que verifica que la actividad se cumpla sin tener que ejecutarla.
- C – Creador. Área que genera o desarrolla la actividad.
- I – Informado. Área a quien debe ser informada de la actividad
- U – Usuario de la información. Área que utilizará la información.
- NP – No participa

A continuación, se presenta el resumen del análisis.

[47] ISACA. (2017). Implementing a Privacy Protection Program: Using COBIT 5 Enablers with the ISACA Privacy Principles. Illinois.

Tabla 1. Proceso de protección de datos y su relación con las partes interesadas.

Apartado actualizado versión 3.0

Partes interesadas	Gestión del programa de protección de datos personales	Presupuesto para la protección de datos	Gestión de proyectos de datos personales	Políticas, estándares y procedimientos de datos personales	Requerimientos para la protección de los datos personales	Materiales de capacitación y concientización	Reportes de cumplimiento en la protección de datos personales	Gestión de riesgos de los datos personales	Tablero (dashboard) del sistema de gestión para la protección de los datos personales
Internas									
Alta dirección	I/U	A	NP	I	NP	NP	NP	I	I
Órganos en materia de transparencia	C/A	C	C	C/A	C/A	C/A	C/A	C	C
Otros Órganos colegiados	U	NP	A	NP	NP	NP	NP	I	A
Áreas responsables	U	NP	NP	U	U	U	I	C	I
Áreas de Seguridad de la Información	NP	NP	NP	U	U	U	U	U	NP
Áreas de TI	NP	NP	NP	U	U	NP	U	U	NP

Partes interesadas	Gestión del programa de protección de datos personales	Presupuesto para la protección de datos	Gestión de proyectos de datos personales	Políticas, estándares y procedimientos de datos personales	Requerimientos para la protección de los datos personales	Materiales de capacitación y concientización	Reportes de cumplimiento en la protección de datos personales	Gestión de riesgos de los datos personales	Tablero (dashboard) del sistema de gestión para la protección de los datos personales
Externas									
Autoridades de protección de datos	NP	I	NP	NP	NP	NP	NP	NP	I
Encargados	NP	NP	NP	U	U	NP	NP	NP	NP
Titulares	NP	NP	NP	I	NP	NP	NP	NP	NP
Otros sujetos obligados	NP	NP	NP	U	U	NP	NP	NP	NP

1.5 Definición de la estructura del Sistema de Gestión

El Sistema de Gestión para la Protección de Datos Personales del Instituto Nacional Electoral, se conformará de dos apartados (con base en el Anexo SL[48] de las normas ISO/IEC): la Base regulatoria y el Catálogo de Controles.

1.5.1 Base regulatoria

Tiene como objetivo que el Sistema de Gestión esté alineado y sea compatible con las normas de sistemas de gestión internacionales, simplificando posibles duplicidades con otros sistemas de gestión que se encuentren implementados; además, posee la cualidad de poder agregar requisitos adicionales específicos de la disciplina según sea necesario[49] -que en este caso serían requisitos en materia de protección de datos personales-.

Características generales:

- Apartado fijo, con periodos de revisión anuales o cuando exista un cambio en la normativa de protección de datos personales;
- Conformado por Cláusulas que servirán de guía para su implementación.
- Impersonal, es decir, no hace referencia a una organización pública en particular;
- Atemporal, no señala plazos ni tiempos;
- Holístico, ya que es aplicable a toda la organización del sujeto obligado;

La UTTyPDP agrega una característica más:

- Sujeto a aprobación y revisión del Comité de Transparencia.

El uso del Anexo SL provee a cualquier sistema de gestión:

- un texto central idéntico,
- términos comunes, y

[48] La ISO, en el 2012, publicó el ANEXO SL –en las Directivas ISO/IEC parte 1 (Suplemento consolidado ISO – Procedimientos específicos para ISO). Es una estructura de alto nivel (HLS, por sus siglas en inglés) para todos los sistemas de gestión de las normas ISO que sirve para definir estándares de sistemas de gestión.
[49] ISO/IEC. (2015). ISO/IEC Directives, Part 1. Consolidated ISO Supplement - Procedures specific to ISO. Recuperado el 3 de diciembre de 207, de DV BENCHMARK.

- definiciones centrales,

Considerando el Anexo SL, **la Base regulatoria se estructurará en 10 cláusulas o secciones**.

Las tres primeras cláusulas son introductorias, mientras que las cláusulas cuatro a diez se incluyen los requisitos necesarios para el Sistema de Gestión en materia de protección de datos personales (BSI Group) (ISO/IEC, 2015):

- **Cláusula 1: Objeto y campo de aplicación**. El alcance establece los resultados esperados del Sistema de Gestión. Los resultados son específicos del tipo de organización y deben ser coherentes con su contexto (cláusula 4).

- **Cláusula 2: Referencias normativas**. Proporciona detalles sobre las normas de referencia o publicaciones relevantes en relación con la norma concreta.

- **Cláusula 3: Términos y Definiciones.** Detalla términos y definiciones aplicables a la norma específica, además de cualquier otro término o definición relacionado con la norma.

- **Cláusula 4: Contexto de la organización**. Consta de cuatro sub-cláusulas:

    - 4.1 Entendimiento de la organización y de su contexto.

    - 4.2 Identificación de necesidades y expectativas de las partes interesadas.

    - 4.3 Determinación del alcance del sistema de gestión.

    - 4.4 Sistema de gestión.

    Determina por qué la organización está donde está; debe identificar las cuestiones internas y externas que pueden influir en los resultados esperados, así como a todas las partes interesadas y sus necesidades. Es necesario determinar el apetito del riesgo de la organización, así como los aspectos legales y regulatorios que le sean de aplicación.

    Además, debe documentar su alcance y establecer los límites del sistema de gestión –todo en línea con los objetivos del negocio-.

- **Cláusula 5: Liderazgo**. Esta cláusula consta de tres sub-cláusulas:
    - 5.1 Liderazgo y compromiso.
    - 5.2 Política.
    - 5.3 Roles, responsabilidades y autoridades en la organización.

    Esta estructura hace hincapié especial en el liderazgo. La alta dirección tiene una mayor responsabilidad y participación en el sistema de gestión de la organización. Los requisitos del sistema de gestión se deben integrar en los procesos de negocio, asegurar que el SG logra los resultados previstos y asignar los recursos necesarios. La alta dirección también es responsable de comunicar la importancia del sistema de gestión y aumentar la toma de conciencia y la participación de los empleados.

- **Cláusula 6: Planificación**. Consta de dos sub-cláusulas:
    - 6.1 Acciones para tratar los riesgos y oportunidades.
    - 6.2 Objetivos del sistema de gestión y planificación para lograrlos.

    Esta cláusula proporciona la manera directa de tratar el riesgo. Una vez que la organización ha definido los riesgos y oportunidades en la cláusula 4, tiene que establecer cómo van a ser tratados a través de la planificación. Este enfoque proactivo sustituye a la acción preventiva y reduce la necesidad de acciones correctivas posteriores. Se pone especial atención en los objetivos del sistema de gestión, los cuales deben ser medibles, objeto de seguimiento, comunicados, coherentes con la política del sistema de gestión y actualizados cuando sea necesario.

- **Cláusula 7: Soporte**. Consta de cinco sub-cláusulas:
    - 7.1 Recursos.
    - 7.2 Competencia.
    - 7.3 Toma de conciencia.
    - 7.4 Comunicación.

- 7.5 Información documentada.

  La organización debe analizar el soporte necesario para cumplir con las metas y objetivos. Esto incluye los recursos, comunicaciones internas y externas, así como la información documentada -que reemplaza los términos utilizados anteriormente como documentos, documentación y registros-. Exige que todas las personas en la organización estén conscientes de las políticas asociadas.

- **Cláusula 8: Operación**. Consta de una sub-cláusulas:

  - 8.1 Planificación y control operacional.

    La mayor parte de los requisitos del sistema de gestión se encuentran dentro de esta cláusula. Aborda tanto los procesos internos como los contratados externamente; la gestión del proceso global incluye criterios adecuados para el control de estos procesos, así como formas de gestionar el cambio planificado y el no previsto.

- **Cláusula 9: Evaluación del rendimiento**. Consta de tres sub-cláusulas:

  - 9.1 Seguimiento, medición, análisis y evaluación.

  - 9.2 Auditoría interna.

  - 9.3 Revisión por la dirección.

    Para dar cumplimiento a este requisito, las organizaciones deben determinar qué, cómo y cuándo ha de ser supervisado, medido, analizado y evaluado el SG. La auditoría interna también es parte de este proceso, para asegurar que el sistema de gestión se ajusta a los requisitos de la organización, así como a los de la norma, y se ha implementado y mantenido con éxito. En la revisión por la alta dirección se analiza si el sistema de gestión es aprobado, adecuado y eficaz.

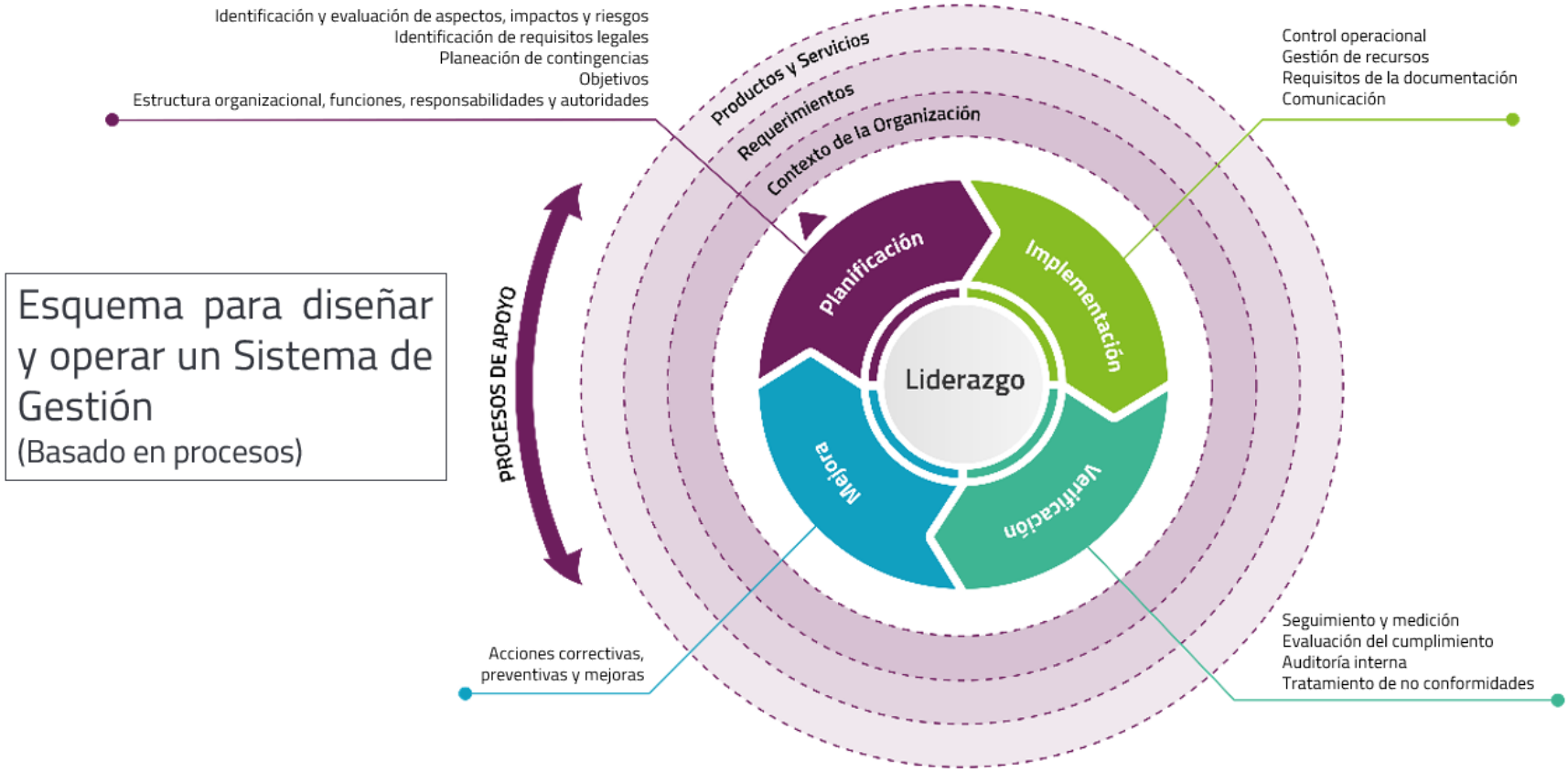
- **Cláusula 10: Mejora**. Consta de dos sub-cláusulas:

  - 10.1 No conformidad y acción correctiva.

  - 10.2 Mejora continua.

Esta cláusula analiza las formas de hacer frente a las no conformidades y acciones correctivas, así como a las estrategias de mejora continua.

En el esquema de la página siguiente, se observa de manera gráfica -en términos de procesos- la interrelación de cada una de las cláusulas que integran la Base regulatoria:


Identificación y evaluación de aspectos, impactos y riesgos
Identificación de requisitos legales
Planeación de contingencias
Objetivos
Estructura organizacional, funciones, responsabilidades y autoridades
Productos y Servicios
Requerimientos
Contexto de la Organización
Control operacional
Gestión de recursos
Requisitos de la documentación
Comunicación
Esquema para diseñar y operar un Sistema de Gestión
(Basado en procesos)
PROCESOS DE APOYO
Planificación
Implementación
Liderazgo
Mejora
Verificación
Acciones correctivas, preventivas y mejoras
Seguimiento y medición
Evaluación del cumplimiento
Auditoría interna
Tratamiento de no conformidades

1.5.2 Catálogo de Controles

El objetivo del Catálogo de controles es proveer a las áreas propietarias/dueñas, custodias y usuarias, las **actividades** específicas para dar cumplimiento a un control, las cuales serán posteriormente **evaluadas para medir cuantitativamente el nivel de cumplimiento**.

Cabe señalar que las actividades del control proveen las bases para que, además de medir cuantitativamente el nivel de cumplimiento, sea posible conocer el si el control es eficiente, efectivo y de acuerdo con el riesgo inherente al dato personal, que son las características que permiten cumplir con el principio de responsabilidad.

Las 90 obligaciones o **controles** identificadas en el apartado **1.1 Análisis normativo** se agruparon en **13 Dominios** que **corresponden a los procesos** de protección de datos personales, los cuales se listan a continuación:

1) Política organizacional de protección de datos personales
2) Aspectos organizacionales de la protección de datos personales
3) Gestión de datos personales y mecanismos de transferencia y remisiones
4) Protección de datos personales en la operación
5) Protección de datos personales de los recursos humanos
6) Gestión de la seguridad en el tratamiento de los datos personales
7) Riesgos con encargados
8) Avisos de Privacidad
9) Solicitudes ARCOP
10) Evaluaciones de impacto en la protección de datos personales
11) Gestión de vulneraciones
12) Monitoreo de la protección de los datos personales
13) Cumplimiento normativo

Cada Dominio tiene un objetivo general y, a su vez, los controles cuentan con sus objetivos específicos. La declaración de objetivos tiene la finalidad de describir lo que se debe lograr como resultado de la implementación de controles.

Características generales del Catálogo de controles:

- Apartado semi-fijo, con periodos de revisión semestrales o cuando exista un cambio en la normativa de protección de datos personales;
- Conformado por Controles que podrán ser seleccionados por la organización en el desarrollo de su Sistema de Gestión para la Protección de Datos Personales;
- Impersonal, es decir, los controles son aplicables a cualquier sujeto obligado;
- Atemporal, no señala plazos ni tiempos;
- Holístico, ya que es aplicable a toda la organización del sujeto obligado.

La UTTyPDP agrega la siguiente característica:

- Las revisiones y actualizaciones serán informadas al Comité de Transparencia.

Las actividades por cada control se pueden consultar en el Apéndice Único, “4.5 Descripción del Catálogo de controles” de este documento.

A continuación, se presenta la estructura del Sistema de Gestión para la Protección de Datos Personales de forma gráfica.

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

2 APARTADO II. DESARROLLO DE LA ESTRUCTURA DEL SISTEMA DE GESTIÓN

Como resultado del Apartado I, la UTTyPDP elaboró la estructura del Sistema de Gestión, que se presenta en este apartado, la cual se tomará como base para su implementación (Apartado III. Modelo de Implementación del Sistema de Gestión, de este documento).

2.1 BASE REGULATORIA

Introducción

En este apartado, la organización[50] 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.

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

- 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.
- 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.

2.2 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 **Apartado III. 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.

La siguiente tabla muestra los 13 dominios con sus objetivos generales y los 90 controles que integran cada dominio.

Apartado actualizado versión 3.0

Dominios y controles	
Dominio 1. Política organizacional de protección de datos personales	Objetivo: Verificar que la organización disponga de pautas y criterios generales para la protección de los datos personales.
Controles: 1. Políticas organizacionales para la protección de datos personales. 2. Programas organizacionales para la protección de datos personales. 3. Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales.	

<table>
<tr><th colspan="2">Dominios y controles</th></tr>
<tr><td>Dominio 2. Aspectos organizacionales de la protección de datos personales</td><td>Objetivo: Identificar, a nivel organizacional, los límites y alcances de las responsabilidades de los involucrados en la protección de los datos personales.</td></tr>
<tr><td colspan="2">Controles:

1. Asignación de responsabilidades organizacionales de protección de datos personales.
2. Contacto con las autoridades.
3. Contacto con grupos de interés especial.
4. Integración de la protección de datos personales en la gestión de riesgos del negocio.
5. Educación continua al personal del Área de Protección de Datos Personales.
6. Concientización y capacitación en materia de protección de datos personales.</td></tr>
<tr><td>Dominio 3. Gestión de datos personales y mecanismos de transferencia y remisiones</td><td>Objetivo: Conocer los datos personales tratados, así como los procesos, propietarios, usuarios, custodios, encargados o terceros que intervienen durante su ciclo de vida, para verificar el cumplimiento de la protección de datos.</td></tr>
<tr><td colspan="2">Controles:

1. Inventario de base de datos personales.
2. Categorización de datos personales tratados.
3. Registro de las bases de datos ante el Órgano en materia de transparencia del responsable.
4. Cédula de identificación del sistema de tratamiento.
5. Ciclo de vida de los datos personales.
6. Políticas para la transferencia o remisión de datos personales.
7. Registro de los mecanismos empleados para transferencias internacionales de datos personales.
8. Limitación del alcance del tratamiento de los datos personales.
9. Supresión de archivos temporales.</td></tr>
<tr><td>Dominio 4. Protección de datos personales en la operación</td><td>Objetivo: Disponer de instrumentos que contemplen las acciones necesarias para la</td></tr>
</table>

Dominios y controles	
	protección de los datos personales durante su ciclo de vida.
Controles: 1. Instrumentos para verificar el tratamiento lícito de datos personales. 2. Medios para la recolección de datos personales. 3. Instrumentos para la recolección de datos personales de niños, niñas y adolescentes. 4. Instrumentos para la recolección de datos personales de personas en estado de interdicción o de incapacidad. 5. Instrumentos para la disociación de los datos personales. 6. Políticas y/o procedimientos para verificar la calidad de los datos personales. 7. Delimitación del tratamiento de datos personales en finalidades primarias y secundarias, atendiendo al principio de proporcionalidad. 8. Mecanismos para obtener el consentimiento de forma válida. 9. Políticas, métodos y técnicas para la supresión y/o bloqueo de datos personales. 10. Uso de cookies y mecanismos de rastreo y geolocalización. 11. Mecanismos para la protección de datos personales en el uso de dispositivos móviles personales en el lugar de trabajo (BYOD). 12. Protección de datos personales derivado de la revelación de información a las autoridades. 13. Identificación de roles y responsabilidades en el tratamiento de datos personales. 14. Políticas o procedimientos para el uso de procesos automatizados de tratamiento de datos personales para la elaboración de perfiles. 15. Políticas para la obtención y tratamiento de datos personales de instancias de seguridad, procuración y administración de justicia. 16. Conservación de registros de actividades de tratamiento.	
Dominio 5. Protección de datos personales de los recursos humanos	Objetivo: Determinar las acciones mínimas para que los datos personales recabados, relacionados con los recursos humanos del responsable sean debidamente tratados.
Controles: 1. Códigos de conducta organizacional que incluya aspectos de protección de datos personales. 2. Protección de datos personales en los contratos del personal.	

<table>
<tr><th colspan="2">Dominios y controles</th></tr>
<tr><td colspan="2">3. Procedimientos de protección de datos personales para los expedientes de contratación.
4. Avisos de privacidad relacionados con los recursos humanos.
5. Protección de datos personales en las prácticas de monitoreo de empleados y en el uso de sistemas de video-vigilancia.
6. Protección de datos personales en las prácticas de vigilancia de la salud en el entorno laboral.</td></tr>
<tr><td>Dominio 6. Gestión de la seguridad en el tratamiento de los datos personales</td><td>Objetivo: Llevar un control de las medidas de seguridad físicas, técnicas y administrativas mínimas para la protección de los datos personales.</td></tr>
<tr><td colspan="2">Controles:

1. Inclusión de la protección de datos personales en la política de seguridad de la información.
2. Medidas de seguridad físicas.
3. Medidas de seguridad administrativas.
4. Medidas de seguridad técnicas.
5. Auditorías de seguridad de la información que incluyan datos personales.
6. Análisis de brecha de seguridad de los datos personales.
7. Análisis de riesgos de los datos personales tratados.
8. Plan de trabajo.
9. Inventario de datos personales y de los sistemas de tratamiento.
10. Funciones y obligaciones de las personas que tratan datos personales.
11. Programa integral de capacitación.
12. Documento de seguridad.
13. Monitoreo y supervisión continuo de las medidas de seguridad implementadas.</td></tr>
<tr><td>Dominio 7. Riesgos con encargados</td><td>Objetivo: Verificar que los encargados protejan los datos personales bajo su resguardo.</td></tr>
<tr><td colspan="2">Controles:

1. Acciones de cumplimiento de protección de datos personales para encargados.
2. Cláusulas contractuales.
3. Procesos de debida diligencia (due diligence) en las prácticas de protección de datos con encargados.</td></tr>
</table>

<table>
<tr><th colspan="2">Dominios y controles</th></tr>
<tr><td colspan="2">4. Instrumentos para la contratación de prestadores de servicios de cómputo en la nube.
5. Subcontratación de servicios.
6. Mecanismos para determinar acciones por incumplimiento contractual.
7. Auditorías de debida diligencia sobre prácticas de protección de datos con encargados.</td></tr>
<tr><td>Dominio 8. Avisos de Privacidad</td><td>Objetivo: Verificar que la organización dispone de avisos de privacidad con los requisitos que marca la normativa aplicable en la materia para cumplir con el principio de información.</td></tr>
<tr><td colspan="2">Controles:

1. Instrumentos de apoyo para generar avisos de privacidad.
2. Avisos de privacidad integral con el detalle sobre el manejo de los datos personales.
3. Avisos de privacidad simplificados, con el resumen sobre el manejo de los datos personales.
4. Disposición del aviso de privacidad en todos los puntos de recolección de datos personales.
5. Disposición de los avisos de privacidad en medios visibles.
6. Disposición de avisos de privacidad en los contratos y términos de uso.
7. Capacitación a empleados para explicar o dar a conocer el aviso de privacidad.
8. Medidas compensatorias para dar a conocer el aviso de privacidad.</td></tr>
<tr><td>Dominio 9. Solicitudes ARCOP</td><td>Objetivo: Verificar que el responsable dispone de procedimientos que provean eficiencia al proceso de atención a solicitudes ARCOP.</td></tr>
<tr><td colspan="2">Controles:

1. Instrumento para atender solicitudes o proveer mecanismos para que los titulares ejerzan sus derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales.
2. Solicitud para el ejercicio de los derechos ARCOP.
3. Medidas especiales para personas con discapacidad y hablantes de lengua indígena.
4. Instrumentos para el acceso a datos personales.</td></tr>
</table>

<table>
<tr><th colspan="2">Dominios y controles</th></tr>
<tr><td colspan="2">5. Instrumentos para la rectificación de datos personales.
6. Instrumento para la cancelación de datos personales.
7. Instrumento para la oposición (revocación) de datos personales.
8. Instrumento para responder solicitudes sobre portabilidad de datos personales.
9. Procedimientos para la atención de recursos de revisión.</td></tr>
<tr><td>Dominio 10. Evaluaciones de impacto en la protección de datos personales</td><td>Objetivo: Verificar que los datos personales cuyo tratamiento implica un alto riesgo cuenten con una estrategia de tratamiento.</td></tr>
<tr><td colspan="2">Controles:

1. Evaluaciones de Impacto en la Protección de Datos (EIPDs) para nuevos programas, sistemas y procesos o modificados.
2. Instrumentos para llevar a cabo EIPDs.
3. Involucrar a encargados como parte del proceso de EIPDs.</td></tr>
<tr><td>Dominio 11. Gestión de vulneraciones</td><td>Objetivo: Verificar la existencia, vigencia y uso de procedimientos que permitan actuar de manera oportuna en caso de presentarse alguna vulneración de la seguridad de los datos personales.</td></tr>
<tr><td colspan="2">Controles:

1. Plan de respuesta a vulneraciones a la seguridad de datos personales.
2. Verificación, revisión y evaluación del Plan de Respuesta a vulneraciones de la seguridad de datos personales.
3. Notificación de las vulneraciones de seguridad a la persona titular.
4. Monitoreo, reporte y bitácoras de vulneraciones.</td></tr>
<tr><td>Dominio 12. Monitoreo de la protección de los datos personales</td><td>Objetivo: Verificar la adecuada gestión en la protección de datos personales con base en lo establecido en el sistema de gestión.</td></tr>
<tr><td colspan="2">Controles:</td></tr>
</table>

<table>
<tr><th colspan="2">Dominios y controles</th></tr>
<tr><td colspan="2">1. Auditorías internas y autoevaluaciones al sistema de gestión de datos personales.
2. Auditorías internas en materia de protección de los datos personales (monitoreo y supervisión) de las políticas, planes, procesos, y procedimientos del responsable.
3. Revisión independiente de la protección de datos personales.
4. Atención de dudas y quejas de los titulares.</td></tr>
<tr><td>Dominio 13. Cumplimiento normativo</td><td>Objetivo: Verificar el cumplimiento normativo en la materia.</td></tr>
<tr><td colspan="2">Controles:

1. Tratamiento de datos personales de acuerdo con las finalidades y atribuciones.
2. Apartado virtual de protección de datos personales en los sitios de internet del responsable.</td></tr>
</table>

3 APARTADO III. MODELO DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN

Apartado actualizado versión 3.0

La UTTyPDP deberá desarrollar e integrar la documentación a la que hace referencia la Base regulatoria conforme a los tiempos y formas establecidas en este modelo, en una **memoria** que servirá, además, como evidencia de su cumplimiento.

3.1 DEFINICIÓN DEL MODELO DE IMPLEMENTACIÓN, SEGUNDO CICLO

La UTTyPDP será la responsable de implementar y operar el Sistema de Gestión, a través de un Modelo de implementación que consta de cuatro etapas (basado en el ciclo de Deming o de mejora continua), mismas que se muestran en la figura 3.

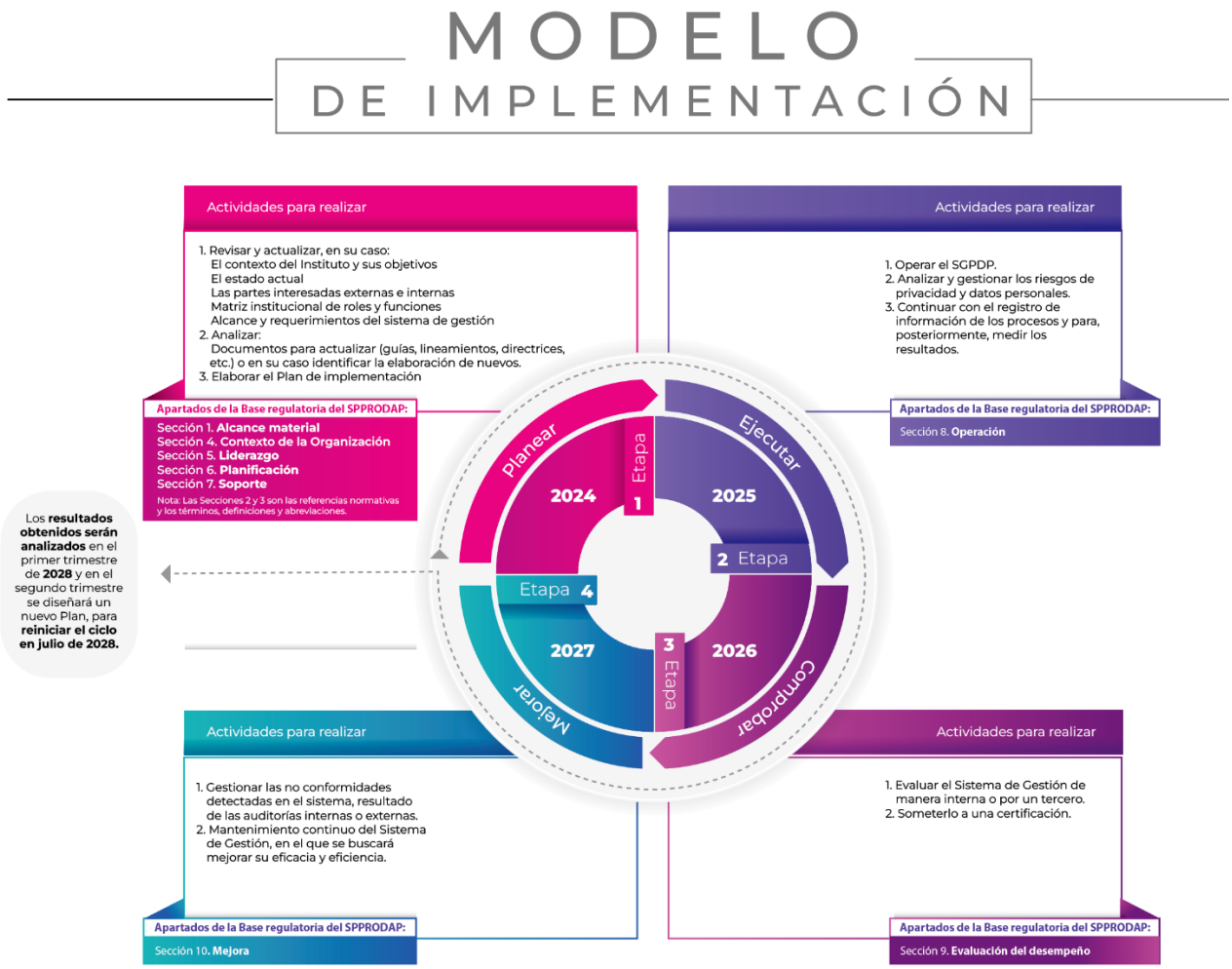


Figura 3. Modelo de implementación del segundo ciclo del SiPRODAP

De manera general, cada etapa se describe a continuación:

- **Etapa 1. Planear**.

  Objetivo: Establecer los objetivos, procedimientos y políticas relacionadas con la protección de datos personales, así como el alcance del Sistema de Gestión, los roles y funciones.

  Actividades para realizar de acuerdo con lo señalado en la Base regulatoria (en materia de protección de datos personales):

  1. Preliminares. Revisar y actualizar, en su caso:
     a. El contexto del Instituto y sus objetivos.
     b. El estado actual.
     c. Las partes interesadas externas e internas.
     d. Matriz institucional de roles y funciones.
     e. Alcance y requerimientos del sistema de gestión.
     f. Los riesgos.
  2. Analizar documentos para actualizar (guías, lineamientos, directrices, etc.) o en su caso identificar la elaboración de nuevos.
  3. Elaborar el Plan de implementación.

- **Etapa 2. Ejecutar**.

  Objetivo: Implantar el sistema de gestión a través de lo descrito en el Plan de implementación a fin de gestionar los datos personales del Instituto de conformidad con la normativa aplicable en la materia.

  Actividades para realizar:

  1. Operar el SiPRODAP.
  2. Analizar y gestionar los riesgos de privacidad y datos personales.

3. Continuar con el registro de información de los procesos y para, posteriormente, medir los resultados.

- **Etapa 3. Comprobar.**

  Objetivo: Evaluar y revisar la efectividad del Sistema de Gestión a través de una evaluación interna o por parte de un tercero experto para mejorar el proceso y, en su caso, someterlo a una certificación.

  En materia de protección de datos personales la **evaluación** se refiere a una **auditoría**, que puede ser:

  a) voluntaria, según lo previsto en el artículo 151 de la Ley General de Datos, y es realizada por el INAI.

  b) Interna, ejecutada por el equipo auditor de la Unidad de Transparencia.

  La **certificación** tiene como objeto evaluar la conformidad de sistemas de gestión desarrollados e implementados por los responsables y encargados.

  En función de lo anterior, las actividades para realiza son:

  1. Evaluar el Sistema de Gestión de manera interna o por un tercero.

  2. Analizar someterlo a una certificación.

- **Etapa 4. Mejorar**.

  Objetivo: Determinar las acciones correctivas y preventivas a partir de los resultados obtenidos con la finalidad de mejorar de forma continua el Sistema de Gestión.

  Actividades para realizar:

  1. Gestión de las no conformidades detectadas en el sistema, resultado de las auditorías internas o externas.

  2. Mantenimiento continuo del Sistema de Gestión, en el que se buscará mejorar su eficacia y eficiencia.

  Con los resultados obtenidos se deberá diseñar un nuevo Plan y reiniciar el ciclo.

3.2 RESPONSABILIDADES

Durante las cuatro etapas del Modelo, la UTTyPDP deberá:

a) Establecer un Plan de trabajo correspondiente a cada etapa, en el mes de enero de cada año, que describa el proceso para su ejecución, con base en los recursos anuales aprobados por el Instituto para el Proyecto T181010 Programa Integral de Gestión de Datos Personales[51].

b) Someter a aprobación ante el Comité de Transparencia (CT), en el mes de febrero, el Plan de trabajo de cada etapa que corresponda.

c) Informar al CT, en diciembre de cada año, el avance de ejecución de cada etapa.

[51] La ejecución de cada etapa está sujeta a que la UTTyPDP disponga de los recursos materiales, financieros y humanos.

4 APÉNDICE ÚNICO

4.1 NORMATIVA NACIONAL

4.1.1 Análisis de la LGPDPPSO

En la tabla que se muestra a continuación, se observa el análisis realizado a la LGPDPPSO

Artículos de la LGPDPPSO que derivan en obligaciones para el sujeto obligado		
Título	**Capítulo**	**Artículos**
Primero. Disposiciones generales.	I. Del objeto de la ley. Artículos 1 al 9.	Art. 7
Segundo. Principios y deberes.	I. De los principios. Artículos 16 al 30.	Todos
	II. De los deberes. Artículos 31 al 42.	Todos
Tercero. Derechos de los titulares y su ejercicio.	II. Del ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Artículos 48 al 56.	Art. 48 al 55
	III. De la portabilidad de los datos. Artículo 57.	Art. 57
Cuarto. Relación del responsable y encargado.	Único. Responsable y encargado. Artículos 58 al 64.	Todos excepto el 62
Quinto. Comunicaciones de datos personales.	Único. De las transferencias y remisiones de datos personales. Artículos 65 al 71.	Art. 65 al 69
Sexto. Acciones preventivas en materia de protección de datos personales.	I. De las mejores prácticas. Artículos 72 al 79.	Art. 74, 77, 78 y 79
	II. De las bases de datos en posesión de instancias de seguridad, procuración y administración de justicia. Artículo 80 al 82.	Todos

Artículos de la LGPDPPSO que derivan en obligaciones para el sujeto obligado		
Título	**Capítulo**	**Artículos**
Séptimo. Responsables en materia de protección de datos personales en posesión de los sujetos obligados.	I. Comité de Transparencia. Artículos 83 y 84.	Art. 84
	II. De la Unidad de Transparencia. Artículos 85 al 87.	Art. 85 y 86
Octavo. Organismos garantes.	III. De la Coordinación y Promoción del Derecho a la Protección de Datos Personales. Artículos 92 y 93.	Art. 92
Noveno. De los procedimientos de impugnación en materia de protección de datos personales en posesión de sujetos obligados.	II. Del recurso de revisión ante el Instituto y los Organismos Garantes. Artículos 103 al 116.	Art. 103

4.1.2 Análisis de los Lineamientos Generales de protección de datos personales para el sector público

Artículos de los Lineamientos que derivan en obligaciones para el sujeto obligado		
Título	**Capítulo**	**Artículos**
Primero. Disposiciones generales.	Único. Del objeto y ámbitos de validez subjetivo y objetivo de los lineamientos generales. Artículos 1 al 6.	Art. 4 y 5
Segundo. Principios y deberes.	I. De los principios de protección de datos personales. Artículos 7 al 54.	Todos
	II. De los deberes. Artículos 55 al 72.	Todos

Artículos de los Lineamientos que derivan en obligaciones para el sujeto obligado		
Título	**Capítulo**	**Artículos**
Tercero. Derechos de los titulares y su ejercicio.	Único. De ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Artículos 73 al 107.	Todos
Cuarto. Relación del responsable y encargado.	Único. Del encargado. Artículos 108 al 112.	Art. 109 al 112
Quinto. Transferencias de datos personales.	Único. De los requerimientos para la realización de transferencias nacionales y/o internacionales. Artículos 113 al 118.	Art. 113 al 116
Sexto. Acciones preventivas en materia de protección de datos personales.	Único. De los esquemas de mejores prácticas, evaluaciones de impacto en la protección de datos personales y el oficial de protección de datos personales. Artículos 119 al 122.	Todos
Séptimo. Medios de impugnación.	II. De la sustanciación del recurso de revisión. Artículos 136 al 159.	Art. 138 y 151
	III. Del cumplimiento de las resoluciones recaídas a los recursos de revisión. Artículos 160 al 162.	Art. 160 y 161
Octavo. Facultad de verificación del Instituto.	IV. Del cumplimiento de las resoluciones recaídas a los procedimientos de verificación. Artículos 215 a 217.	Art. 215 y 216
	V. Auditorías voluntarias. Artículos 218 al 231.	Art. 218, 221 y 230 *Actualizado versión 3.0*
Décimo. De la evaluación del desempeño de los responsables respecto del cumplimiento de la Ley General de Datos. *Actualizado versión 3.0*	Único. Sistema de evaluación del desempeño. Artículos 246 al 253.	Art. 250

4.1.3 Análisis del Reglamento del Instituto Nacional Electoral en materia de Protección de Datos Personales

Apartado nuevo versión 3.0

Artículos del Reglamento que derivan en obligaciones para el sujeto obligado		
Título	**Capítulo**	**Artículos**
Primero. Disposiciones generales.	Artículos 1 al 12.	Art. 2, 7, 8 y 12
Segundo. De los órganos del instituto en materia de protección de datos personales.	I. Atribuciones del Comité. Artículo 13.	Art. 13
	II. Atribuciones de la Unidad de Transparencia. Artículo 14.	Art. 14
Tercero. De los principios y deberes.	I. Principios. Artículo 16 al 30.	Todos
	II. De los deberes. Artículos 31 al 36.	Todos
Cuarto. De los derechos arco y su ejercicio.	II. Del ejercicio de los derechos. Sección primera. De las reglas generales. Artículos 39 al 41.	Todos
	III. Procedimiento para el ejercicio de los derechos ARCO. Artículos 42 al 50.	Todos
	IV. Recurso de revisión. Artículos 51 al 59.	Todos

4.2 NORMATIVA INTERNACIONAL

4.2.1 Convenio 108+

Apartado actualizado versión 3.0

Artículos del Convenio 108 que derivan en obligaciones	
Capítulo	**Artículos**
II. Principios básicos para la protección de datos. Artículos 4 al 13.	Art. 4 al12
III. Flujos transfronterizos de datos. Artículo 14.	Todos
IV. Autoridades de control. Artículos 15. *Actualizado versión 3.0*	Todos
V. Cooperación y asistencia mutua. Artículos 16 al 21. *Actualizado versión 3.0*	Art. 16 y 17

4.2.2 RGPD

Artículos de la RGPD que derivan en obligaciones		
Capítulo	**Sección**	**Artículos**
II. Principios.	Única. Artículos 5 al 11.	Art. 5 al 9
III. Derechos del interesado.	1. Transparencia y modalidades. Artículo 12.	Art. 12
	2. Información y acceso a los datos personales. Artículos 13 al 15.	Todos
	3. Rectificación y supresión. Artículos 16 al 20.	Todos

Artículos de la RGPD que derivan en obligaciones		
Capítulo	**Sección**	**Artículos**
	4. Derecho de oposición y decisiones individuales automatizadas. Artículos 21 y 22.	Todos
	5. Limitaciones. Artículo 23.	Todos
IV. Responsables del tratamiento y encargado del tratamiento.	1. Obligaciones generales. Artículo 24 al 31.	Todos excepto el 27
	2. Seguridad de los datos personales. Artículos 32 al 34.	Todos
	3. Evaluación de impacto relativa a la protección de datos y consulta previa. Artículos 35 y 36.	Todos
	4. Delegado de protección de datos. Artículo 37 al 39.	Todos
V. Transferencias de datos personales a terceros países u organizaciones internacionales.	Único. Artículos 44 al 50.	Art. 45 al 50
IX. Disposiciones relativas a situaciones específicas de tratamiento.	Único. Artículos 85 al 91.	Art. 88 y 89

4.3 IDENTIFICACIÓN DE LAS OBLIGACIONES DE PROTECCIÓN DE DATOS PERSONALES

4.3.1 Matriz de acciones

Apartado actualizado versión 3.0

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
1.	Políticas organizacionales para la protección de datos personales	Art. 30 Fracc. II	Art. 47 56	No contiene información.	No contiene información	Art. 5, 24,89
2.	Programas organizacionales para la protección de datos personales	Art. 30 Fracc. II	Art. 47, 56	Art.57 *Actualizado versión 3.0*	No contiene información	Art. 5, 24, 89
3.	Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales	Art. 30 Fracc. I	Art. 47, 56	No contiene información	No contiene información	Art. 5, 24, 89
4.	Asignación de responsabilidades organizacionales de protección de datos personales	Art. 33, Fracc. I, 85	Art. 56, 57, 121, 122	Artículo 2 *Actualizado versión 3.0*	Art. 4	Art. 26 27, 37, 38, 39 *Actualizado versión 3.0*
5.	Contacto con las autoridades	No contiene información	No contiene información	No contiene información	Art. 16, 17	Art. 31
6.	Contacto con grupos de interés especial	No contiene información	No contiene información	No contiene información	NA	Art. 50
7.	Integración de la protección de datos	No contiene información	No contiene información	No contiene información	Art. 6 numeral 2, 7	Art. 25, 32

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
	personales en la gestión de riesgos del negocio				*Actualizado versión 3.0*	*Actualizado versión 3.0*
8.	Educación continua al personal del Área de Protección de Datos Personales	Art. 30 Fracc. III	Art. 64	No contiene información	No contiene información	No contiene información
9.	Concientización y capacitación en materia de protección de datos	Art. 30 Fracc. III, 33 Fracc. VIII, 84, 92	Art. 48, 64	No contiene información	No contiene información	No contiene información
10.	Inventario de base de datos personales	Art. 33 fracc III, 35 Fracc. I	Art. 58	No contiene información	No contiene información	Art. 5
11.	Categorización de datos personales tratados	Art. 35 Fracc. I	No contiene información	No contiene información	Art. 8 numeral 1 inciso c) *Actualizado versión 3.0*	Art. 5, 14 d), 15 b) *Actualizado versión 3.0*
12.	Registro de las bases de datos ante el Órgano en materia de transparencia del responsable	No contiene información	No contiene información	Art.8 *Actualizado versión 3.0*	No contiene información	Art. 30
13.	Cédula de identificación del sistema de tratamiento	No contiene información	No contiene información	No contiene información	No contiene información	No contiene información
14.	Ciclo de vida de los datos personales	Art 33 Fracc. I	Art. 56 Fracc. IV, 59	No contiene información	No contiene información	No contiene información

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
		Actualizado versión 3.0	*Actualizado versión 3.0*			
15.	Políticas para la transferencia o remisión de datos personales	Art. 66, 67, 68, 69, 70	No contiene información	Art. 53 *Actualizado versión 3.0*	Art. 14	Art. 45, 46, 47, 48, 49
16.	Registro de los mecanismos empleados para transferencias internacionales de datos personales	Art. 66, 67, 68, 69, 70	Art. 113, 114, 115, 116, 117	No contiene información	Art. 14	Art. 45, 46, 47, 48, 49
17.	Limitación del alcance del tratamiento de los datos personales	Art. 66	Art. 113	Art. 53 *Actualizado versión 3.0*	Art. 14	Art. 45, 46, 47, 48, 49
18.	Supresión de archivos temporales	Art. 24, 64 Fracc. II d) *Actualizado versión 3.0*	Art. 23, 59, 94	Art. 12 *Actualizado versión 3.0*	No contiene información	No contiene información
19.	Instrumentos para verificar el tratamiento lícito de datos personales	Art. 17, 19 *Actualizado versión 3.0*	Art. 8, 11 *Actualizado versión 3.0*	Art. 16 *Actualizado versión 3.0*	Art. 5	Art. 5, 6 *Actualizado versión 3.0*
20.	Medios para la recolección de datos personales	Art. 7	Art. 53	Art. 20 *Actualizado versión 3.0*	Art. 6	Art. 8, 9
21.	Instrumentos para la recolección de datos personales de niños, niñas y adolescentes	Art. 7, 20	Art. 5, 78, 79, 80, 81	Art.21, 22, 23	Art. 6	Art. 8, 9, 12

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
				Actualizado versión 3.0		
22.	Instrumentos para la recolección de datos personales de personas en estado de interdicción o de incapacidad	Art. 20	Art. 78, 79, 80, 81	Art.21 *Actualizado versión 3.0*	Art. 6	Art. 9
23.	Instrumentos para la disociación de los datos personales	No contiene información	No contiene información	No contiene información	No contiene información	Art. 89
24.	Políticas y/o procedimientos para verificar la calidad de los datos	Art. 23	Art. 21, 23	Art.24 *Actualizado versión 3.0*	Art. 5	Art. 5
25.	Delimitación del tratamiento de datos personales en finalidades primarias y secundarias, atendiendo al principio de proporcionalidad	Art. 18	Art. 9, 10	Art.25 *Actualizado versión 3.0*	Art. 5, 8 *Actualizado versión 3.0*	Art. 6, 13, 14
26.	Mecanismos para obtener el consentimiento de forma válida	Art. 20, 21, 22, 65	Art. 12, 13, 16, 18, 19, 20	Art. 8, 17, 19, 20, 21 *Actualizado versión 3.0*	Art. 5, 8 *Actualizado versión 3.0*	Art. 6, 7, 8, 13, 14 *Actualizado versión 3.0*
27.	Políticas, métodos y técnicas para la supresión y/o bloqueo de datos personales	Art. 24	Art. 23	Art.12 *Actualizado versión 3.0*	Art. 9	Art. 6, 7, 13, 14, 15 numeral 1 inciso e), 17

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
						Actualizado versión 3.0
28.	Uso de cookies y mecanismos de rastreo y geolocalización	Art.25	Art. 24, 25	Art. 12, 25 *Actualizado versión 3.0*	Art. 5	Art. 6, 7, 13, 14
29.	Mecanismos para la protección de datos en el uso de dispositivos personales en el lugar de trabajo (BYOD)	Art. 31	No contiene información	No contiene información	No contiene información	No contiene información
30.	Protección de datos personales derivado de la revelación de información a las autoridades	No contiene información	No contiene información	No contiene información	No contiene información	No contiene información
31.	Identificación de roles y responsabilidades en el tratamiento de datos personales	Art. 33, 34	Art. 56, 57	Art. 2 *Actualizado versión 3.0*	Art. 4 *Actualizado versión 3.0*	Art. 30
32.	Políticas o procedimientos para el uso de procesos automatizados de tratamiento de datos personales para la elaboración de perfiles	No contiene información	No contiene información	No contiene información	Art. 9	Art. 22
33.	Políticas para la obtención y tratamiento de	Art. 80, 81, 82	No contiene información	No contiene información	Art. 9	Art. 10

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
	datos personales de instancias de seguridad, procuración y administración de justicia					
34.	Conservación de registros de actividades de tratamiento	Art. 33, 34, 35, 36	Art. 56, 57, 58, 59, 65	Art. 31, 32 *Actualizado versión 3.0*	Art. 9	Art. 30
35.	Códigos de conducta organizacional que incluya aspectos de protección de datos personales	Art. 30 Fracc. II, 42	No contiene información	Art. 31, 36 *Actualizado versión 3.0*	No contiene información	No contiene información
36.	Protección de datos personales en los contratos del personal	Art. 30 Fracc. II, 42	No contiene información	No contiene información	No contiene información	No contiene información
37.	Procedimientos de protección de datos personales para los expedientes de contratación	No contiene información	No contiene información	No contiene información	No contiene información	No contiene información
38.	Avisos de privacidad relacionados con los recursos humanos	No contiene información	No contiene información	No contiene información	No contiene información	No contiene información
39.	Protección de datos personales en las prácticas de monitoreo de empleados y en el uso de sistemas de video-vigilancia	No contiene información	No contiene información	No contiene información	No contiene información	No contiene información

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
40.	Protección de datos personales en las prácticas de vigilancia de la salud en el entorno laboral	No contiene información	No contiene información	No contiene información	No contiene información	No contiene información
41.	Inclusión de la protección de datos en la política de seguridad de la información	Art. 33	No contiene información	Art. 31 *Actualizado versión 3.0*	Art. 7	Art. 32
42.	Medidas de seguridad físicas	Art. 33	Art. 55	Art. 31 *Actualizado versión 3.0*	Art. 7, 10	Art. 32
43.	Medidas de seguridad administrativas	Art. 33	Art. 55	Art. 31 *Actualizado versión 3.0*	Art. 7, 10	Art. 32
44.	Medidas de seguridad técnicas	Art. 33	Art. 55	Art. 31 *Actualizado versión 3.0*	Art. 7, 10	Art. 32
45.	Auditorías de seguridad de la información que incluya datos personales	Art. 33 Fracc.VII	Art. 63	Art.59 *Actualizado versión 3.0*	No contiene información	Art. 32
46.	Análisis de brecha de seguridad de los datos personales	Art. 33 Fracc. V	Art. 61	No contiene información	No contiene información	Art. 32
47.	Análisis de riesgos de los datos personales tratados	Art. 33 Fracc IV	Art. 60	No contiene información	Art. 10	Art. 32

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
					Actualizado versión 3.0	
48.	Plan de trabajo	Art. 33 Fracc.VI	Art. 62	No contiene información	No contiene información	Art. 32
49.	Inventario de datos personales y de los sistemas de tratamiento	Art. 33 Fracc. III	Art. 58	No contiene información	No contiene información	Art. 32
50.	Funciones y obligaciones de las personas que tratan datos personales	Art. 33 Fracc. II	Art. 57	Art. 8 *Actualizado versión 3.0*	No contiene información	Art. 32
51.	Programa integral de capacitación	Art. 33 Fracc.VIII	Art. 64	No contiene información	No contiene información	Art. 32
52.	Documento de seguridad	Art. 35, 36	No contiene información	Art. 31 *Actualizado versión 3.0*	No contiene información	NA
53.	Monitoreo y supervisión continuo de las medidas de seguridad implementadas	Art. 33 Fracc. I.	Art. 63	No contiene información	No contiene información	Art. 32
54.	Acciones de cumplimiento de protección de datos personales para encargados	Art. 58, 59, 61, 62	Art. 108, 109, 110	Art. 54 *Actualizado versión 3.0*	No contiene información	Art. 28, 29
55.	Cláusulas contractuales	Art. 59	Art. 109	Art. 54 *Actualizado versión 3.0*	No contiene información	Art. 57

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
56.	Procesos de debida diligencia (*due diligence*) en las prácticas de protección de datos con encargados	Art. 58, 59	Art. 108, 109, 110	Art. 54 *Actualizado versión 3.0*	No contiene información	Art. 28, 29
57.	Instrumento para la contratación de prestadores de servicios de cómputo en la nube	Art. 63, 64	Art. 111	Art. 54 *Actualizado versión 3.0*	No contiene información	Art. 28, 29
58.	Subcontratación de servicios	Art. 59, 61, 62 *Actualizado versión 3.0*	Art. 109, 110 *Actualizado versión 3.0*	Art. 56 *Actualizado versión 3.0*	No contiene información	Art. 28, 29
59.	Mecanismos para determinar acciones por incumplimiento contractual	Art. 60	Art. 112	Art. 55 *Actualizado versión 3.0*	No contiene información	Art. 28, 29
60.	Auditorías de debida diligencia sobre prácticas de protección de datos con encargados	Art. 60	Art. 109	No contiene información	No contiene información	Art. 28, 29
61.	Instrumentos de apoyo para generar avisos de privacidad	Art. 26, 27, 28	Art. 13, 14, 15, 16, 17, 18, 19, 26, 27, 40, 42	Art. 27, 28, 29 *Actualizado versión 3.0*	No contiene información	Art. 12, 13, 14
62.	Avisos de privacidad integral con el detalle sobre el manejo de los datos personales	Art. 26, 28	Art. 34, 35, 36, 37, 38, 39, 40, 41	Art. 27, 28 *Actualizado versión 3.0*	Art. 8	Art. 5, 12, 13, 14 *Actualizado versión 3.0*

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
63.	Avisos de privacidad simplificados con el resumen sobre el manejo de los datos personales	Art. 27	Art.30, 31, 32, 33	Art. 27, 28 *Actualizado versión 3.0*	Art. 8	N/A *Actualizado versión 3.0*
64.	Disposición del aviso de privacidad en todos los puntos de recolección de datos personales	Art. 26, 27, 28	Art. 29, 43, 44	Art. 28 *Actualizado versión 3.0*	Art. 8	Art. 5, 7, 12, 13, 21
65.	Disposición de los avisos de privacidad en medios visibles	Art. 26, 27, 28	Art. 43,44	Art. 28 *Actualizado versión 3.0*	Art. 8	Art. 5, 7, 12, 13, 21
66.	Disposición de avisos de privacidad en los contratos y términos de uso	Art. 26, 27, 28, 67, 68, 69	Art. 43,44	No contiene información	Art. 8	Art. 21
67.	Capacitación a empleados para explicar o dar a conocer el aviso de privacidad	No contiene información	No contiene información	No contiene información	No contiene información	No contiene información
68.	Medidas compensatorias para dar a conocer el aviso de privacidad	Art. 26	Art. 43,44	Art. 29 *Actualizado versión 3.0*	Art. 8	No contiene información
69.	Instrumento para atender solicitudes o proveer mecanismos para que los titulares	Art. 28 Fracc. V, 48, 51, 52, 53, 54, 55, 56, 85	Art. 83, 84, 92, 93, 94, 95	Art. 39 al 50 *Actualizado versión 3.0*	Art. 9	Art. 15, 16, 17, 18, 19 *Actualizado versión 3.0*

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
	ejerzan sus derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales *Actualizado versión 3.0*					
70.	Solicitud para el ejercicio de los derechos ARCOP	Art. 52	Art. 83	Art. 41 *Actualizado versión 3.0*	Art. 9	Art. 15, 16, 17, 18, 19,21 *Actualizado versión 3.0*
71.	Medidas especiales para personas con discapacidad y hablantes de lengua indígena	Art. 52	Art. 84, 85	No contiene información	Art. 9	Art. 15, 16, 18, 19
72.	Instrumentos para el acceso a datos personales	Art. 52	Art. 92	Art. 42, 43, 45 *Actualizado versión 3.0*	Art. 9	Art. 15, 16, 18, 19
73.	Instrumentos para la rectificación de datos personales	Art. 52	Art. 93	Art. 42, 43 *Actualizado versión 3.0*	Art. 9	Art. 15, 16, 18, 19
74.	Instrumento para la cancelación de datos personales	Art. 51, 52, 53, 54, 55, 85	Art. 94	Art. 42, 43 *Actualizado versión 3.0*	Art. 9	Art. 17

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
75.	Instrumento para la oposición (revocación) de datos personales	Art. 28 Fracc. V, 48 al 56, 85	Art. 95	Art. 42, 43 *Actualizado versión 3.0*	Art. 9 *Actualizado versión 3.0*	Art. 16, 17, 21
76.	Instrumento para responder solicitudes sobre portabilidad de datos	Art. 57.	No contiene información	No contiene información	No contiene información	Art. 20
77.	Procedimientos para la atención de recursos de revisión	Art. 103	Art. 106	Art 51, 52 *Actualizado versión 3.0*	No contiene información	No contiene información
78.	Evaluaciones de Impacto en la Protección de Datos (EIPDs) para nuevos programas, sistemas y procesos o modificados	Art. 74, 75, 76, 77	Art. 120	Art. 58 *Actualizado versión 3.0*	Art. 10	Art. 25, 35 *Actualizado versión 3.0*
79.	Instrumentos para llevar a cabo EIPDs	Art. 74, 75, 76, 77	Art. 120	No contiene información	Art. 10	Art 25, 35 *Actualizado versión 3.0*
80.	Involucrar a encargados como parte del proceso de EIPDs	No contiene información	No contiene información	No contiene información	Art. 10	Art. 24, 35
81.	Plan de respuesta a vulneraciones a la seguridad de datos personales	Art. 37, 38	Art. 66,67, 68, 69	Art. 33, 34 *Actualizado versión 3.0*	No contiene información	Art. 33, 34

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
82.	Verificación, revisión y evaluación del Plan de respuesta a vulneraciones de la seguridad de datos personales	Art. 37, 38	Art. 66, 67, 68, 69	No contiene información	No contiene información	Art. 33, 34
83.	Notificación de las vulneraciones de seguridad a la persona titular.	Art. 40, 41	Art. 66,67, 68, 69	Art. 34, 35 *Actualizado versión 3.0*	No contiene información	Art. 33, 34
84.	Monitoreo, reporte y bitácoras de vulneraciones	Art. 39	Art. 66, 67, 68, 69	Art. 33 *Actualizado versión 3.0*	No contiene información	Art. 33, 34
85.	Auditorías internas y autoevaluaciones al sistema de gestión de datos personales	Art. 29, 30	Art. 65	No contiene información	No contiene información	No contiene información
86.	Auditorías internas en materia de protección de los datos personales (monitoreo y supervisión) de las políticas, planes, procesos, y procedimientos del responsable	Art. 30 Fracc. V, 84	Art. 63	No contiene información	No contiene información	No contiene información
87.	Revisión independiente de la protección de datos personales	Art. 29, 30	No contiene información	No contiene información	No contiene información	Art. 51

Matriz de acciones						
Num	**Acciones (Control)**	**Nacional**			**Internacional**	
		LGPDPPSO	**Lineamientos**	**Reglamento**	**Convenio 108+**	**RGPD**
88.	Atención de dudas y quejas de los titulares	Art. 30 Fracc. VI	Art. 50	No contiene información	No contiene información	No contiene información
89.	Tratamiento de datos personales de acuerdo con las finalidades y atribuciones *Actualizado versión 3.0*	Art. 17, 18	Art. 8, 9 *Actualizado versión 3.0*	Art. 16, 17 *Actualizado versión 3.0*	Art. 5	Art. 6
90.	Apartado virtual de protección de datos personales en los sitios de internet del responsable	No contiene información	Art. 250	No contiene información	No contiene información	No contiene información

4.4 ESTÁNDARES Y *FRAMEWORKS* INTERNACIONALES

4.4.1 Matriz de acciones

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
1.	Política organizacional para la protección de datos personales.	*6.2.1.1 Policies for information security*	*4.6 Privacy policies*	*3. Maintain Internal Data Privacy Policy*
2.	Programas organizacionales para la protección de datos personales	*6.2.1.1 Policies for information security*	*4.6 Privacy policies*	*3. Maintain Internal Data Privacy Policy*
3.	Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales	*6.2.1.1 Policies for information security*	*4.6 Privacy policies*	*3. Maintain Internal Data Privacy Policy*
4.	Asignación de responsabilidades organizacionales en protección de datos personales.	*6.3.1.1 Information Security Roles and Responsibilities* *6.3.1.2 Segregation of duties* *7.2.7 Joint PII controller*	*4.2 Actors and roles*	*1. Maintain Governance Structure*
5.	Contacto con las autoridades	*6.3.1.3 Contact with authorities*	*4.5.1 Legal and regulatory factors*	*1. Maintain Governance Structure*

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
6.	Contacto con grupos de interés especial	*6.3.1.4 Contact with special interest groups*	No contiene información	*1. Maintain Governance Structure*
7.	Integración de la protección de datos personales en gestión de riesgos del negocio	*5.6.2 Information security risk assessment*	*4.5 Privacy safeguarding requirements*	*1. Maintain Governance Structure*
8.	Educación continua al personal del Área de Protección de Datos Personales	*6.4.2.2 Information security awareness, education and training*	*5.10 Accountability*	*5. Maintain Training and Awareness Program*
9.	Concientización y capacitación en materia de protección de datos personales	*6.4.2.2 Information security awareness, education and training*	*5.10 Accountability*	*5. Maintain Training and Awareness Program*
10.	Inventario de base de datos personales	*6.5.1.1 Inventory of assets*	No contiene información	*2. Maintain Personal Data Inventory and Data Transfer Mechanisms*
11.	Categorización de los datos personales tratados	*6.5.2.1 Classification of information*	*4.2.2 PII controllers*	*2. Maintain Personal Data Inventory and Data Transfer Mechanisms*
12.	Registro de las bases de datos ante el Órgano en materia de transparencia del responsable	*6.5.1.2 Ownership of assets*	No contiene información	*2. Maintain Personal Data Inventory and Data Transfer Mechanisms*

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
13.	Cédula de identificación del sistema de tratamiento	No contiene información	No contiene información	No contiene información
14.	Diagramas de flujo en el tratamiento de los datos personales	*7.2.8 Records related to processing PII*	*4.3 Interactions*	*2. Maintain Personal Data Inventory and Data Transfer Mechanisms*
15.	Políticas para la transferencia o remisión de datos personales	*6.10.2.1 Information transfer policies and procedures* *7.5.1 Identify basis for PII transfer between jurisdictions* *8.5.1 Basis for PII transfer between jurisdictions*	*4.5.1 Legal and regulatory factors* *5.6 Use, retention and disclosure limitation* *5.10 Accountability*	*2. Maintain Personal Data Inventory and Data Transfer Mechanisms*
16.	Registro de los mecanismos empleados para transferencias internacionales de datos personales	*7.5.1 Identify basis for PII transfer between jurisdictions* *7.5.3 Records of transfer of PII*	*4.5.1 Legal and regulatory factors*	*2. Maintain Personal Data Inventory and Data Transfer Mechanisms*
17.	Limitación del alcance del tratamiento de los datos personales	*7.4.2 Limit processing*	*5.3 Purpose legitimacy and specification*	*4. Embed Data Privacy Into Operations*
18.	Supresión de archivos temporales	*7.4.6 Temporary files*	No contiene información	*4. Embed Data Privacy Into Operations*

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
19.	Instrumentos para verificar el tratamiento lícito de datos personales	*7.2.2 Identify lawful basis*	*5.2 Consent and choice*	*3. Maintain Internal Data Privacy Policy*
20.	Medios para la recolección de datos personales	*7.2.1 Identify and document purpose* *7.3.2 Determining information for PII principals*	*5.4 Collection limitation*	*4. Embed Data Privacy Into Operations*
21.	Instrumentos para la recolección y uso de datos personales de niños, niñas y adolescentes	*7.2.3 Determine when and how consent is to be obtained* *7.2.4 Obtain and record consent* *7.4.1 Limit processing* *7.2.2 Identify lawful basis*	*5.2 Consent and choice*	*4. Embed Data Privacy Into Operations*
22.	Instrumentos para la recolección y uso de datos personales de personas en estado de interdicción o de incapacidad	*7.2.2 Identify lawful basis*	*5.2 Consent and choice*	*4. Embed Data Privacy Into Operations*
23.	Instrumentos para la disociación de los datos personales	*7.4.5 PII de-identification and deletion at the end of processing*	No contiene información	*4. Embed Data Privacy Into Operations*

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
24.	Políticas y/o procedimientos para verificar la calidad de los datos personales	*7.4.3 Accuracy and quality*	*5.7 Accuracy and quality*	*4. Embed Data Privacy Into Operations*
25.	Delimitación del tratamiento de datos personales en finalidades primarias y secundarias, atendiendo al principio de proporcionalidad	*7.2.1 Identify and document purpose*	*5.3 Purpose legitimacy and specification* *5.6 Use, retention and disclosure limitation*	*8. Maintain Notices*
26.	Mecanismos para obtener el consentimiento de forma válida	*7.2.3 Determine when and how consent is to be obtained* *7.2.4 Obtain and record consent*	*5.2 Consent and choice*	*4. Embed Data Privacy Into Operations*
27.	Políticas y procedimientos para la supresión y/o bloqueo de datos personales	*7.4.8 Disposal*	*5.5 Data minimization*	*4. Embed Data Privacy Into Operations*
28.	Uso de cookies y mecanismos de rastreo y localización	*7.4.6 Temporary files*	*4.5.4 Other factors*	*4. Embed Data Privacy Into Operations*
29.	Mecanismos para la protección de datos personales en el uso de dispositivos móviles personales en el lugar de trabajo (BYOD)	*6.3.2.1 Mobile device policy*	No contiene información	*4. Embed Data Privacy Into Operations*

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
30.	Protección de datos personales derivado de la revelación de información a las autoridades	*7.5.4 Records of PII disclosure to third parties* *8.5.4 Notification of PII disclosure requests*	*5.6 Use, retention and disclosure limitation*	*4. Embed Data Privacy Into Operations*
31.	Identificación de roles y responsabilidades en el tratamiento de los datos personales	*6.3.1.1 Information Security Roles and Responsibilities*	*4.2 Actors and roles*	*1. Maintain Governance Structure*
32.	Políticas o procedimientos para el uso de procesos automatizados de tratamiento de datos personales para la elaboración de perfiles	*7.3.10 Automated decision making*	No contiene información	*4. Embed Data Privacy Into Operations*
33.	Políticas para la obtención y tratamiento de datos personales de instancias de seguridad, procuración y administración de justicia	No contiene información	*5.4 Collection limitation*	*4. Embed Data Privacy Into Operations*
34.	Conservación de registros de actividades de tratamiento	*7.2.8 Records related to processing PII*	*5.11 Information security*	*4. Embed Data Privacy Into Operations*
35.	Códigos de conducta organizacional que incluya aspectos de protección de datos personales	6.4.2.1 Management responsibilities	No contiene información	3. Maintain Internal Data Privacy Policy

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
36.	Protección de datos personales en los contratos del personal	6.4.1.2 Terms and conditions of employment	4.5.2 Contractual factors	3. Maintain Internal Data Privacy Policy
37.	Procedimientos de protección de datos personales en los expedientes de contratación	7.2.3 Determine and how consent is to be obtained 7.4.4 PII minimization objectives	No contiene información	3. Maintain Internal Data Privacy Policy
38.	Avisos de privacidad relacionado con los recursos humanos	7.3.1 Determining and fulfilling obligations to PII principals 7.3.2 Determining information for PII principals 7.3.3 Providing information to PII principals 7.3.4 Providing mechanism to modify or withdraw consent 7.3.5 Providing mechanism to object to PII processing 7.3.6 Access, correction and/or erasure 7.3.8 Providing copy of PII processed	No contiene información	8. Maintain Notice

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
		7.3.9 Handling requests		
39.	Protección de datos personales en las prácticas de monitoreo de empleados y en el uso de sistemas de video-vigilancia	No contiene información	No contiene información	4. Embed Data Privacy Into Operations
40.	Protección de datos personales en las prácticas de vigilancia de la salud en el entorno laboral	No contiene información	No contiene información	4. Embed Data Privacy Into Operations
41.	Inclusión de la protección de datos personales en la política de seguridad de la información	6.2.1.1 Policies for information security	4.6 Privacy policies	6.Manage Information Security Risk
42.	Medidas de seguridad físicas	6 PIMS-specific guidance related to ISO/IEC 27002	4.7 Privacy Controls 5.11 Information security	6.Manage Information Security Risk
43.	Medidas de seguridad administrativas	6 PIMS-specific guidance related to ISO/IEC 27002	4.7 Privacy Controls 5.11 Information security	6.Manage Information Security Risk
44.	Medidas de seguridad técnicas	6 PIMS-specific guidance related to ISO/IEC 27002	4.7 Privacy Controls	6.Manage Information Security Risk

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
			5.11 Information security	
45.	Auditorías de seguridad de la información que incluya datos personales	6.9.7.1 Information system audit controls 6.15.2.1 Independent review of information security	5.12 Privacy compliance	12 Monitor Data Handling Practices
46.	Análisis de brecha de seguridad de los datos personales	No contiene información	No contiene información	11. Maintain Data Privacy Breach Management Program
47.	Análisis de riesgos de los datos personales	5.6.2 Information security risk assessment	5.11 Information security	6.Manage Information Security Risk
48.	Plan de trabajo	5.6.3 Information security risk treatment	No contiene información	6.Manage Information Security Risk
49.	Inventario de datos personales y de los sistemas de tratamiento	7.2.8 Records related to processing PII	No contiene información	6.Manage Information Security Risk
50.	Funciones y obligaciones de las personas que tratan datos personales	7.3.1 Determining and fulfilling obligations to PII principals	No contiene información	6.Manage Information Security Risk

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
51.	Programa integral de capacitación	7.2.2, Information security awareness, education and training,	No contiene información	6.Manage Information Security Risk
52.	Documento de seguridad	No contiene información	4.5.1 Legal and regulatory factors	No contiene información
53.	Monitoreo y supervisión continuo de las medidas de seguridad implementadas	7.3.5 Providing mechanism to object to PII processing	No contiene información	6.Manage Information Security Risk
54.	Acciones de cumplimiento de protección de datos personales para encargados	6.12.1.1 Information security policy for supplier relationships 8.2.1 Customer agreement	4.5.2 Contractual factors	7. Manage Third-Party Risk
55.	Cláusulas contractuales	6.12 Supplier relationships	4.5.2 Contractual factors	7. Manage Third-Party Risk
56.	Procesos de debida diligencia (due diligence) en las prácticas de protección de datos con encargados	7.2. Contracts with PII processors	No contiene información	7. Manage Third-Party Risk
57.	Política de contratación de prestadores de servicios de cómputo en la nube	7.2.6 Contracts with PII processors	No contiene información	7. Manage Third-Party Risk

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
58.	Subcontratación de servicios	6.12 Supplier relationships	4.5.2 Contractual factors	7. Manage Third-Party Risk
59.	Mecanismos para determinar acciones por incumplimiento contractual	8.2.4 Infringing Instruction	No contiene información	7. Manage Third-Party Risk
60.	Auditorías de debida diligencia sobre prácticas de protección de datos con encargados	6.12.2 Supplier service delivery management	5.12 Privacy compliance	7. Manage Third-Party Risk
61.	Instrumentos de apoyo para generar avisos de privacidad	7.3.1 Determining and fulfilling obligations to PII principals 7.3.2 Determining information for PII 7.3.3 Providing information to PII principals 7.3.4 Providing mechanism to modify or withdraw consent. 7.3.5 Providing mechanism to object to PII processing 7.3.6 Access, correction and/or erasure	5.8 Openness, transparency and notice	8. Maintain Notices

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
		7.3.7 PII controllers obligations to inform third parties		
62.	Avisos de privacidad integral con el detalle sobre el manejo de los datos personales	7.3.2 Determining information for PII 7.3.6 Access, correction and/or erasure	5.8 Openness, transparency and notice	8. Maintain Notices
63.	Aviso de privacidad simplificado con el resumen sobre el manejo de los datos personales	7.3.2 Determining information for PII 7.3.6 Access, correction and/or erasure	5.8 Openness, transparency and notice	8. Maintain Notices
64.	Disposición del aviso de privacidad en todos los puntos de recolección de datos personales	7.3.3 Providing information to PII principals	5.9 Individual participation and access	8. Maintain Notices
65.	Disposición de los avisos de privacidad en medios visibles	7.3.1 Determining and fulfilling obligations to PII principals	5.9 Individual participation and access	8. Maintain Notices
66.	Disposición de avisos de privacidad en los contratos y términos de uso	7.3.3 Providing information to PII principals	5.9 Individual participation and access	8. Maintain Notices
67.	Capacitación a empleados para explicar o dar a conocer el aviso de privacidad	6.4.2.2 Information security awareness, education and training	No contiene información	5. Maintain Training and Awareness Program

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
68.	Medidas compensatorias para dar a conocer el aviso de privacidad	7.3.2 Determining information for PII principals	No contiene información	8. Maintain Notices
69.	Instrumento para atender solicitudes o proveer Procedimientos o guías para atender solicitudes o proveer mecanismos para que los titulares ejerzan sus derechos de acceso, rectificación, cancelación y oposición de datos personales	7.3.4 Providing mechanism to modify or withdraw consent 7.3.5 Providing mechanism to object to PII processing 7.3.6 Access, correction and/or erasure 7.3.9 Handling requests	5.9 Individual participation and access	9. Respond to Requests and Complaints from individuals
70.	Solicitud para el ejercicio de los derechos ARCO	7.3.5 Providing mechanism to object to PII processing 7.3.6 Access, correction and / or erasure	5.9 Individual participation and access	9. Respond to Requests and Complaints from individuals
71.	Medidas especiales para personas con discapacidad y hablantes de lengua indígena	No contiene información	No contiene información	No contiene información
72.	Instrumentos para el acceso a datos personales	7.3.5 Providing mechanism to object to PII processing 7.3.6 Access, correction and / or erasure	5.9 Individual participation and access	9. Respond to Requests and Complaints from individuals

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
73.	Instrumentos para la rectificación de datos personales	7.3.5 Providing mechanism to object to PII processing 7.3.6 Access, correction and / or erasure	5.9 Individual participation and access	9. Respond to Requests and Complaints from individuals
74.	Instrumento para la cancelación de datos personales	7.3.5 Providing mechanism to object to PII processing 7.3.6 Access, correction and / or erasure	5.9 Individual participation and access	9. Respond to Requests and Complaints from individuals
75.	Instrumento para la oposición (revocación) de datos personales	7.3.5 Providing mechanism to object to PII processing 7.3.6 Access, correction and / or erasure	5.9 Individual participation and access	9. Respond to Requests and Complaints from individuals
76.	Procedimientos para responder solicitudes sobre portabilidad de datos personales	7.3.9 Handling requests	No contiene información	9. Respond to Requests and Complaints from individuals
77.	Procedimientos para la atención de recursos de revisión	No contiene información	No contiene información	No contiene información
78.	Evaluaciones de Impacto en la Protección de Datos (EIPDs) para nuevos	7.2.5 Privacy impact assessment	4.5 Privacy safeguarding requirements	10. Monitor for New

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
	programas, sistemas y procesos o modificados			Operational Practices
79.	Instrumentos para llevar a cabo EIPDs	7.2.5 Privacy impact assessment	4.5 Privacy safeguarding requirements	10. Monitor for New Operational Practices
80.	Involucrar a encargados como parte del proceso de EIPDs	7.2.5 Privacy impact assessment	4.5.2 Contractual factors 4.5.3 Business factors	10. Monitor for New Operational Practices
81.	Plan de respuesta a vulneraciones a la seguridad de datos personales	6.13.1.1 Responsibilities and procedures	5.10 Accountability	11. Maintain Data Privacy Breach Management Program
82.	Verificación, revisión y evaluación del Plan de respuesta a vulneraciones de la seguridad de datos personales	6.13.1.1 Responsibilities and procedures	No contiene información	11. Maintain Data Privacy Breach Management Program
83.	Protocolo de notificación (a los titulares afectados) y de reportes (a las autoridades de protección de datos) sobre vulneraciones	6.13.1.4 Assessment of and decisions on information security events	No contiene información	11. Maintain Data Privacy Breach Management Program

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
84.	Monitoreo, reporte y bitácoras de vulneraciones	6.13.1.6 Learning from information security incidents	No contiene información	11. Maintain Data Privacy Breach Management Program
85.	Auditorías internas y autoevaluaciones al sistema de gestión de datos personales	5.7.2 Internal Audit	5.12 Privacy compliance	12. Monitor Data Handling Practices
86.	Auditorías internas en materia de protección de los datos personales (monitoreo y supervisión) de las políticas, planes, procesos, y procedimientos del responsable	6.9.1.1 Documenting operating procedures	5.12 Privacy compliance	12. Monitor Data Handling Practices
87.	Revisión independiente de la protección de datos personales	6.15.2.1 Independent review of information security	No contiene información	12. Monitor Data Handling Practices
88.	Atención de dudas y quejas de los titulares	7.3.9 Handling requests	No contiene información	9. Respond to Requests and Complaints from individuals
89.	Cambios regulatorios y de cumplimiento	7.2.2 Identify lawful basis	4.5.1 Legal and regulatory factors	13. Track External Criteria
90.	Apartado virtual de protección de datos	No contiene información	No contiene información	No contiene información

Estándares y *frameworks*				
Num	**Control**	**ISO/IES 27701:2019**	**ISO/IEC 29100:2024**	**NYIMITY Framework**
	personales en los sitios de internet del responsable			

4.5 DESCRIPCIÓN DEL CATÁLOGO DE CONTROLES

Apartado actualizado versión 3.0

Dominios y objetivos de control		
Dominio 1. Política organizacional de protección de datos personales		
Objetivo: Verificar que la organización disponga de pautas y criterios generales para la protección de los datos personales		
D1.1	Políticas organizacionales para la protección de datos personales.	*Control.* Disponer de una política de protección de datos personales, con base en los objetivos de protección de datos organizacionales. Actividades de control 1. Prácticas de conducta organizacional para la protección de datos personales. 2. Las necesidades organizacionales, amenazas, vulnerabilidades y normativa aplicable para los datos personales. 3. El contexto en el que ocurre el tratamiento y el ciclo de vida de los datos personales. 4. Hoja de firmas con la aprobación de las políticas por parte del Órgano en materia de transparencia. 5. Periodos para la revisión y/o actualización de la política: • al menos una vez al año o • cuando exista un cambio significativo en el marco normativo o legal aplicable, en los procesos organizacionales, en la infraestructura que soporta el tratamiento, almacenamiento, transmisión y seguridad de los datos personales. 6. Publicación a través de medios de comunicación organizacionales.

Dominios y objetivos de control		
		7. Forma de comunicar a los terceros involucrados en el tratamiento de los datos personales, en caso de ser necesario. 8. Mecanismo que permita verificar que la política fue leída y entendida por personal interno y terceros involucrados en el tratamiento de los datos personales, en caso de aplicar. 9. Revisión de la política para la protección de datos personales.
D1.2	Programas organizacionales para la protección de datos personales	*Control* Disponer de un Programa de protección de datos personales que tengan por objeto establecer los elementos y actividades de dirección, operación y control de todos los procesos que traten datos personales, con base en los objetivos de protección de datos organizacionales. Actividades de control 10. Coordinación y supervisión por parte del Órgano en materia de transparencia. 11. Planes para la implementación del Programa de Protección de Datos Personales.
D1.3	Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales	*Control* Previsión y autorización de recursos para la implementación y cumplimiento de las políticas y programas. Actividades de control 12. Documentación referente a los recursos destinados, firmada por los responsables.

Dominios y objetivos de control		
		13. Informe de actividades implementadas con los recursos aprobados.
Dominio 2. Aspectos organizacionales de la protección de datos personales		
Objetivo: Identificar, a nivel organizacional, los límites y alcances de las responsabilidades de los involucrados en la protección de los datos personales		
D2.1	Asignación de responsabilidades organizacionales de protección de datos personales	*Control* Especificar y delimitar las responsabilidades organizacionales de la protección de datos personales. Actividades de control: 14. Identificación de las partes interesadas internas y externas. 15. Disponer de una matriz de responsabilidades y participación en la protección de los datos personales de las partes interesadas identificadas. 16. Designar a un Oficial de Protección de Datos Personales.
D2.2	Contacto con las autoridades	*Control* Mantener contacto permanente con el Órgano Garante y otros organismos especializados en la materia. Actividades de control: 17. Comunicación y colaboración con el Órgano Garante. 18. Listados de autoridades (Órgano Garante, organismos de denuncia de vulneraciones, organismos de investigación de delitos electorales, entre otros). 19. Participar en estudios sobre mejores prácticas para el SGPDP.

Dominios y objetivos de control		
D2.3	Contacto con grupos de interés especial	*Control* Conocer temas actuales sobre la protección de datos personales y buenas prácticas internacionales. Actividades de control: 20. Asistencia a foros, conferencias o eventos de asociaciones de grupos de expertos de protección de datos personales. 21. Boletines informativos de fuentes de información respecto a la protección de datos personales.
D2.4	Integración de la protección de datos personales en la gestión de riesgos del negocio	*Control* Los riesgos de la protección de los datos personales, que puedan afectar a los objetivos organizacionales, deben considerarse como un elemento más en la gestión de riesgos de negocio. Actividades de control: 22. Inclusión del riesgo de los datos personales como parte de los riesgos de cumplimiento organizacionales. 23. Inclusión del riesgo de datos personales en las evaluaciones de riesgo de seguridad de la información.
D2.5	Educación continua al personal del Área de Protección de Datos Personales	*Control* Los conocimientos del personal del área responsable de protección de datos personales deben mantenerse actualizados para una toma de decisiones acertada. Actividades de control: 24. Documentos que acrediten la capacitación especializada en la materia

Dominios y objetivos de control		
		por organizaciones nacionales o internacionales: • Maestrías; • Doctorados; • Especializaciones; • Certificaciones; • Asistencia a congresos, seminarios, foros, cursos en protección de datos personales o seguridad de la información.
D2.6	Concientización y capacitación en materia de protección de datos personales	*Control* Disponer de planes y/o programas de concientización permanentes, en materia de protección de datos personales, para todos los empleados de la organización, así como la inclusión de capacitación en datos personales a los nuevos empleados. Actividades de control: 25. Objetivo de capacitación. 26. Necesidades de capacitación para las áreas responsables del tratamiento de datos personales. 27. Medios y recursos diseñados para la especialización en la materia. 28. La medición de resultados. 29. El impacto de la capacitación en el cumplimiento de la protección de los datos personales.
Dominio 3. Gestión de datos personales y mecanismos de transferencia y remisiones		
Objetivo: Conocer los datos personales tratados, así como los procesos, propietarios, usuarios, custodios, encargados o terceros que intervienen durante su ciclo de vida, para verificar el cumplimiento de la protección de datos.		
D3.1	Inventario de base de datos personales	*Control*

Dominios y objetivos de control		
		Identificar qué datos personales son recabados y utilizados en la(s) bases(s) de datos(s) para su uso en un proceso y especificar en dónde residen física y lógicamente. Actividades de control: 30. Nombre de la base de datos. 31. Proceso de negocio. 32. Propietario de la base de datos. 33. Datos personales que contienen categorizados. 34. Sistema (s) de tratamiento a través del cual se tratan los datos personales (herramienta informática).
D3.2	Categorización de datos personales tratados	*Control* Identificar la naturaleza de los datos personales (estándar, sensible, especial) recabados en, al menos, documentos, contratos, medios de almacenamiento. Actividades de control: 35. Esquema de categorización de datos personales atendiendo a la legislación y normatividad aplicable del responsable. 36. Inclusión de la categorización en, al menos: • Documentos de requerimientos de servicios de TIC; • Contrataciones con encargados; • El etiquetado de medios de almacenamiento en los que residan datos personales;
D3.3	Registro de las bases de datos ante el Órgano en materia de transparencia del responsable	*Control* Disponer de un registro actualizado de las bases de datos personales utilizadas en los procesos/servicios.

Dominios y objetivos de control		
		Actividades de control: 37. Procedimiento para el registro de las bases de datos por parte de los responsables. 38. Constancia de registro de la base de datos ante el Órgano en materia de transparencia.
D3.4	Cédula de identificación del sistema de tratamiento	*Control* Disponer de una cédula que permita identificar los sistemas de tratamiento (herramienta informática) utilizados en los procesos/servicios. Actividades de control: 39. Identificación y datos del responsable del sistema de tratamiento 40. Fechas de creación del sistema y actualización de la cédula. 41. Publicación de la cédula en el apartado de protección de datos personales del responsable.
D3.5	Ciclo de vida de los datos personales	*Control* Conocer el flujo de tratamiento de los datos personales durante todo su ciclo de vida entre sistemas, procesos, países, mediante un diagrama que contemple las etapas correspondientes y su descripción. Actividades de control: 42. La obtención de los datos personales. 43. El almacenamiento de los datos personales. 44. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento.

Dominios y objetivos de control		
		45. Los sistemas físicos y/o electrónicos utilizados para su tratamiento. 46. La divulgación de los datos personales considerando las remisiones y transferencias, que en su caso se efectúen. 47. El bloqueo de los datos personales, en caso de que aplique. 48. La cancelación, supresión o destrucción de los datos personales 49. Breve descripción de cada una de las etapas.
D3.6	Políticas para la transferencia o remisión de datos personales	*Control* Asegurar que las comunicaciones de datos personales sean acordes con la normativa en la materia. Actividades de control: 50. En transferencias fuera del territorio nacional el tercero receptor debe proteger los datos personales conforme a los principios y deberes que establece la normativa en la materia y las disposiciones que resulten aplicables. 51. Comunicar el aviso de privacidad respectivo al tercero receptor en las transferencias nacionales e internacionales que se realicen y, en su caso, sus modificaciones. 52. Manifestación por escrito del tercero receptor internacional a través del cual se obliga a proteger los datos personales conforme a los principios y deberes que establece la normativa en la materia y las disposiciones que resulten aplicables.

Dominios y objetivos de control		
D3.7	Registro de los mecanismos empleados para transferencias internacionales de datos personales	*Control* Mantener toda la documentación de cumplimiento como cláusulas contractuales, políticas corporativas, acuerdos, regulaciones, etc. Actividades de control: 53. Mecanismos utilizados, de manera enunciativa: • Instrumentos jurídicos; • Normas corporativas vinculantes; • Convenios de colaboración; • Códigos de conducta; • En caso de haber excepciones, estas deben ser justificadas de forma clara. 54. Los mecanismos deben especificar, al menos: • Sólo tratar los datos que hayan sido transferidos al responsable para las finalidades para las cuales le hayan sido comunicados, según lo establecido en el aviso de privacidad proporcionado, así como garantizar la confidencialidad de los datos personales; • Sólo se tratan los datos personales para las finalidades para las cuales fueron transferidos; • Contar con controles de seguridad para la transferencia de los datos personales; • Los medios físicos y electrónicos aceptados para la transferencia o remisión de los datos personales;
D3.8	Limitación del alcance del tratamiento de los datos personales	*Control* El tratamiento de los datos personales debe ser únicamente para las finalidades para las

Dominios y objetivos de control		
		que fueron recabados y en los procesos requeridos. Actividades de control: 55. Datos personales tratados con el consentimiento del interesado. 56. Datos personales tratados sin el consentimiento del interesado. 57. Especificar de manera clara la finalidad para la que los datos personales serán utilizados. 58. Comunicar al titular cuando se haya modificado el alcance del tratamiento. 59. Procedimientos de comunicación, en caso de existir modificación al alcance del tratamiento.
D3.9	Supresión de archivos temporales	*Control* Los archivos físicos y electrónicos utilizados o generados temporalmente que contengan datos personales deben suprimirse concluida su finalidad en los procesos requeridos. Actividades de control: *60.* Documento que certifique la eliminación segura de los archivos de acuerdo con el procedimiento de supresión establecido por la organización, con al menos, la especificación de ○ El algoritmo de borrado seguro empleado; ○ Medios eliminados; ○ Técnica utilizada; ○ Persona que aprueba.

Dominios y objetivos de control		
Dominio 4. Protección de datos personales en la operación		
Objetivo: Disponer de instrumentos que contemplen las acciones necesarias para la protección de los datos personales durante su ciclo de vida.		
D4.1	Instrumentos para verificar el tratamiento lícito de datos personales	*Control* Verificar que los datos personales son obtenidos con el consentimiento del titular o sobre alguna base legítima para su tratamiento. Actividades de control: 61. Existencia de instrumentos (procedimientos, lineamientos, guías, manuales) para verificar que los datos son obtenidos y tratados en estricto apego y cumplimiento a las atribuciones o facultades que la normativa le confiera al responsable. 62. La normativa específica que faculta al área responsable para tratar los datos personales. 63. Los instrumentos deben describir de manera detallada la forma en que el responsable verifica la licitud.
D4.2	Medios para la recolección de datos personales	*Control* Describir claramente el proceso de recolección de datos personales, señalando el tipo de medios a emplear para tal fin. Actividades de control: 64. Definición de finalidad(es) del tratamiento. 65. El proceso de recolección/captación del área responsable, roles y responsabilidades. 66. Identificación de encargados y/o terceros que intervengan en el proceso de recolección/captación.

Dominios y objetivos de control		
		67. La justificación que únicamente son recabados los datos personales necesarios para las finalidades establecidas y para su tratamiento relevante y necesario. 68. Implementación de medidas de seguridad durante su recolección y uso. 69. Medios de obtención del consentimiento, en caso de aplicar. 70. Formatos de recolección y/o sistemas utilizados o descripción de cualquier otro medio utilizado para la recolección de los datos personales.
D4.3	Instrumentos para la recolección de datos personales de niños, niñas y adolescentes	*Control* Los datos recabados de niños, niñas y adolescentes deben contar con la más alta protección, estableciendo claramente las responsabilidades y el debido tratamiento de esta información. Actividades de control: 71. La obtención del consentimiento de los padres o tutores, de forma libre, específica e informada que autorice el tratamiento de los datos personales de las niñas, niños y adolescentes. 72. Responsabilidades de quien trate datos personales de niños, niñas y adolescentes. 73. Especificar claramente el tratamiento de los datos personales.
D4.4	Instrumentos para la recolección de datos personales de personas en estado de interdicción o de incapacidad	*Control* La recolección de datos personales de personas en estado de interdicción o de incapacidad está alineada con la normativa aplicable en la materia y/o buenas prácticas o leyes internacionales. Actividades de control:

Dominios y objetivos de control		
		74. La obtención del consentimiento del representante legal, de forma libre, específica e informada que autorice el tratamiento de los datos personales de personas en estado de interdicción o de incapacidad. 75. Responsabilidades de quien trate datos personales de personas en estado de interdicción o de incapacidad. 76. Especificar claramente el tratamiento de los datos personales.
D4.5	Instrumentos para la disociación de los datos personales	*Control* Disociar los datos personales de tal forma que permita eliminar o reducir al mínimo el riesgo de re-identificación. Actividades de control: 77. Especificación de los casos en los que los responsables deben disociar los datos personales. 78. Medidas de seguridad implementadas para la disociación. 79. Periodos de revisión de las medidas implementadas. 80. Especificar el mecanismo de disociación (de manera enunciativa, Aleatorización: adición de ruido, permutación, privacidad diferencial; Generalización: Agregación y anonimato k, Diversidad l y proximidad t.).
D4.6	Políticas y/o procedimientos para verificar la calidad de los datos personales	*Control* Asegurar la calidad de los datos personales recabados por la organización. Actividades de control: 81. Minimizar el tratamiento manual de los datos personales mediante el uso de

Dominios y objetivos de control		
		elementos tecnológicos de captura que permita recabar los datos personales sin transcribirlos. 82. Validación de la completitud y exactitud de los datos personales capturados antes de su almacenamiento en la base de datos. 83. Corroborar con el titular la correcta captura de sus datos personales. 84. Mecanismo mediante el cual se comunica a las personas titulares mantener actualizados sus datos personales.
D4.7	Delimitación del tratamiento de datos personales en finalidades primarias y secundarias, atendiendo al principio de proporcionalidad	*Control* Asegurar el uso adecuado de los datos personales, durante todo su ciclo de vida, identificando el tipo de finalidad (primarias y secundarias). Actividades de control: 85. Instrumento mediante el cual se verifique que los datos personales son adecuados, relevantes y estrictamente necesarios para las finalidades del tratamiento. 86. Implementar medidas técnicas y administrativas para garantizar que sean objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos, limitando a lo necesario el plazo de conservación y su accesibilidad, en atención del criterio de minimización. 87. El aviso de privacidad debe establecer claramente las finalidades primarias y secundarias. 88. Cláusulas que señalen los mecanismos para la protección de los datos personales en casos como investigaciones, auditorías o minería de

Dominios y objetivos de control		
		datos, por mencionar algunos, y en cuáles se debe avisar a los titulares para finalidades secundarias. 89. Procedimientos con información necesaria para avisar a los titulares del uso de los datos personales para finalidades secundarias. 90. Instrumento mediante el cual se obtenga el consentimiento expreso para el tratamiento de los datos personales para finalidades secundarias. 91. Especificar de manera clara las excepciones al consentimiento; en caso de que aplique para finalidades secundarias.
D4.8	Mecanismos para obtener el consentimiento de forma válida	*Control* Describir cómo se obtiene el consentimiento válido de los titulares, es decir, libre, específico, no ambiguo, explícito e informado y en qué momento de la recolección de los datos se lleva a cabo. Actividades de control: 92. Medio a través del cual se solicita el consentimiento libre, previo, expreso e informado de los titulares. 93. El mantenimiento de los registros físicos o tecnológicos de la obtención del consentimiento. 94. Señalar las excepciones de manera explícita, en caso de existir. 95. Mecanismos para obtener consentimiento tácito garantizando que en todo momento sea posible rectificar dicha autorización. 96. Mecanismos para obtener consentimiento expreso garantizando que en todo momento

Dominios y objetivos de control		
		sea posible rectificar dicha autorización.
D4.9	Políticas, métodos y técnicas para la supresión y/o bloqueo de datos personales	*Control* Procedimientos establecidos y documentados para la conservación y, en su caso, bloqueo y supresión de los datos personales, tanto en medios físicos como digitales. Actividades de control: 97. Procedimientos y plazos que contemplen, al menos: ○ Identificación de los soportes documentales que contengan datos personales. ○ Las características del medio de almacenamiento para conocer la capacidad de recuperación de los datos personales. ○ Mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales. ○ Las diferentes técnicas de supresión segura con base en los soportes documentales, que especifique el algoritmo utilizado, con al menos los siguientes atributos: irreversibilidad, seguridad y confidencialidad, favorable al medio ambiente. 98. Revisión periódica sobre la necesidad de conservar los datos personales. 99. La destrucción de los metadatos asociados a los datos personales, en caso de que aplique. 100. Registros de auditoría generados durante el proceso de supresión segura.

Dominios y objetivos de control		
		101. Documentación que certifique el proceso de supresión y en su caso bloqueo, si aplica. 102. Documentación que certifique el proceso de conservación, en caso de que aplique. El control debe considerar para el bloqueo: 103. Métodos para limitar el tratamiento de los datos personales para el bloqueo. 104. Métodos para impedir el acceso de los usuarios a los datos personales seleccionados para bloqueo. 105. Retirar temporalmente los datos publicados en internet que se encuentren bloqueados. 106. Medios técnicos utilizados para que los datos personales no sean objeto de operaciones de tratamiento o modificaciones posterior al bloqueo. 107. Indicar de forma clara en el sistema que el tratamiento de los datos personales está limitado por bloqueo.
D4.10	Uso de cookies y mecanismos de rastreo y geolocalización	*Control* Regular el uso de cookies o de geolocalización a través de la definición de mecanismos, asegurando el uso transparente de los mismos, o en su defecto, permitir su desactivación. Actividades de control: 108. Documento que regule o informe sobre el uso de cookies o geolocalización. 109. Procedimientos para solicitar, por parte del titular de los datos, su desactivación.

Dominios y objetivos de control		
		110. Descripción sobre tipo de cookies utilizadas. 111. Inclusión en el apartado en el aviso de privacidad integral que informe sobre el uso de cookies y mecanismos de rastreo y localización. 112. Medios empleados para la obtención del consentimiento.
D4.11	Mecanismos para la protección de datos personales en el uso de dispositivos móviles personales en el lugar de trabajo (BYOD)	*Control* Proteger los datos personales de posibles vulneraciones a su seguridad debido al uso de dispositivos móviles personales. Actividades de control: 113. Análisis de riesgos de los dispositivos portátiles utilizados (SmartPhones, computadoras portátiles, discos duros, USB, etc.). 114. Registro de los dispositivos móviles que serán utilizados. 115. Especificación de las medidas de seguridad físicas, técnicas y administrativas. 116. Autorización de uso de dispositivos móviles personales en el lugar de trabajo.
D4.12	Protección de datos personales derivado de la revelación de información a las autoridades	*Control* Las políticas, procedimientos o protocolos deben incluir información acerca de la entrega de datos personales en caso de que éstos sean requeridos por una autoridad competente y en el ejercicio de sus funciones. Actividades de control: 117. Inclusión de cláusulas en las políticas, protocolos o

Dominios y objetivos de control		
		procedimientos que definan las medidas de seguridad físicas, técnicas y administrativas -con base en el riesgo del dato- para guardar la confidencialidad e integridad de la información. 118. Cláusulas en las políticas, protocolos o procedimientos que integren, al menos, la siguiente información: • Datos personales revelados. • Justificación legal y normativa de la revelación.
D4.13	Identificación de roles y responsabilidades en el tratamiento de datos personales	*Control* Las responsabilidades de los usuarios, custodios o propietarios, que intervienen en cualquier fase del ciclo de los datos personales, o información que contiene datos personales deben estar debidamente identificadas. Actividades de control: 119. Identificación de propietarios, custodios y usuarios de cada proceso que trate datos personales. 120. Asignación de responsabilidades en el tratamiento de los datos personales en función del rol identificado. 121. Integración de los roles y responsabilidades en los procedimientos, protocolos, lineamientos, convenios, contratos o cualquier otro instrumento establecido que haga referencia al tratamiento del dato personal.
D4.14	Políticas o procedimientos para el uso de procesos automatizados de tratamiento	*Control* Cuando los datos personales sean utilizados en la elaboración de perfiles, se debe comunicar al titular de los datos sobre todas

Dominios y objetivos de control		
	de datos personales para la elaboración de perfiles	las actividades concretas del tratamiento automatizado de sus datos personales, aunque estos se hayan obtenido de una fuente distinta al propio titular. Actividades de control: 122. Cláusulas referentes a la licitud del tratamiento. 123. Procedimientos para informar al titular de los datos personales sobre la elaboración de perfiles. 124. En caso de que un encargado realice el tratamiento, considerar todos los controles requeridos para el encargado. 125. Autorización expresa del titular para el tratamiento. 126. Especificar los procedimientos matemáticos o estadísticos empleados para la elaboración de perfiles. 127. Aplicar las medidas técnicas y administrativas para garantizar que no existan inexactitudes en los datos personales. 128. Verificar que los perfiles generados no tengan efectos discriminatorios en los titulares debido al uso de datos sensibles.
D4.15	Políticas para la obtención y tratamiento de datos personales de instancias de seguridad, procuración y administración de justicia	*Control* Proteger el tratamiento de los datos personales, así como el uso y almacenamiento de las bases de datos de instancias de seguridad, procuración y administración de justicia. Actividades de control:

Dominios y objetivos de control		
		129. Cláusulas que especifiquen la obtención y tratamiento limitados a los supuestos y categorías de datos que resulten necesarios. 130. Considerar todos los controles requeridos para la gestión de la seguridad en el tratamiento de los datos personales.
D4.16	Conservación de registros de actividades de tratamiento	*Control* Contar con registros o bitácoras de las operaciones aplicadas a los datos personales en los sistemas de tratamiento manuales o automatizados. Actividades de control: 131. Medidas de seguridad para garantizar la disponibilidad, confidencialidad e integridad de los registros y de sus copias de seguridad. 132. Tiempos de conservación de los registros o bitácoras. 133. Señalar las operaciones registradas en las bitácoras.
Dominio 5. Protección de datos personales de los recursos humanos		
Objetivo: Determinar las acciones mínimas para que los datos personales recabados, relacionados con los recursos humanos del responsable sean debidamente tratados.		
D5.1	Códigos de conducta organizacional que incluya aspectos de protección de datos personales	*Control* La obligación de salvaguardar los datos personales a los que el personal tiene acceso como parte de sus funciones de trabajo debe integrarse en los estatutos correspondientes. Actividades de control:

Dominios y objetivos de control		
		134. Inclusión de cláusulas referentes a la obligación de la protección de datos personales por parte de las áreas responsables de administración del personal en políticas, procedimientos o instrumentos similares. 135. Inclusión de cláusulas referentes a las sanciones por incumplimiento de la protección de datos personales en políticas, procedimientos o instrumentos similares. 136. Diseñar funciones y responsabilidades de las personas en función de su relación con el tratamiento de datos personales del personal. 137. Mecanismos para que las personas involucradas en el tratamiento de los datos personales del personal, guarde la confidencialidad antes, durante y después de realizada la contratación. 138. Sensibilización y capacitación de quienes tratan datos personales que fomente el compromiso con su protección.
D5.2	Protección de datos personales en los contratos del personal	*Control* Detallar la responsabilidad adquirida con respecto a los datos personales en los contratos celebrados con el personal, con independencia del tipo de contratación y temporalidad. Actividades de control: 139. Cláusulas que garanticen la secrecía de la información que contenga datos personales durante y al concluir la relación laboral. 140. Verificación de las referencias.

Dominios y objetivos de control		
		141. Acciones disciplinarias y sanciones en caso de incumplir alguna de las cláusulas o infringir la legislación y normatividad aplicable.
D5.3	Procedimientos de protección de datos personales para los expedientes de contratación	*Control* Integrar disposiciones para la generación, uso, acceso, retención y seguridad de los expedientes físicos y electrónicos del personal. Actividades de control: 142. Especificaciones de las medidas de seguridad físicas para garantizar la confidencialidad, integridad y disponibilidad de los expedientes físicos y electrónicos del personal contratado. 143. Especificaciones de las medidas de seguridad técnicas para garantizar la confidencialidad, integridad y disponibilidad de los expedientes físicos y electrónicos del personal contratado. 144. Especificaciones de las medidas administrativas para garantizar la confidencialidad, integridad y disponibilidad de los expedientes físicos y electrónicos del personal contratado.
D5.4	Avisos de privacidad relacionados con los recursos humanos	*Control* El aviso de privacidad de los recursos humanos informa cómo la organización recabará, usará y procesará los datos personales de los recursos humanos -y en su caso de familiares o personas relacionadas-. Actividades de control: 145. Disponer de avisos de privacidad integral y simplificado o inclusión de un apartado en los existentes para el

Dominios y objetivos de control		
		personal, con independencia del esquema de contratación, con los requisitos de la normativa en la materia. 146. Disponer de avisos de privacidad integral y simplificado o inclusión de un apartado en los existentes para aspirantes (candidatos), con los requisitos de la normativa en la materia. 147. Disponer de avisos de privacidad integral y simplificado o inclusión de un apartado en los existentes para concursos de selección de personal, con los requisitos de la normativa en la materia. 148. Disponer de avisos de privacidad integral y simplificado o inclusión de un apartado en los existentes para prestadores de servicio social y/o prácticas profesionales con los requisitos de la normativa en la materia. 149. Disponer de avisos de privacidad integral y simplificado o inclusión de un apartado en los existentes para el servicio profesional de carrera, con los requisitos de la normativa en la materia.
D5.5	Protección de datos personales en las prácticas de monitoreo de empleados y en el uso de sistemas de video-vigilancia	*Control* Las finalidades en el uso de Circuito Cerrado de Televisión (CCTV) u otro medio de monitoreo en áreas específicas la organización, así como las medidas de protección, temporalidad, acceso, entre otras están claramente definidas. Actividades de control: 150. Informa al personal de esta medida mediante un aviso de privacidad para el monitoreo de empleados y el uso de sistemas de video-vigilancia.

Dominios y objetivos de control		
		151. Contar con un análisis de riesgos y, eventualmente, de la evaluación de impacto, si fuera necesaria. 152. Especificar las pautas de conducta de los empleados en los diferentes medios de comunicación organizacionales. 153. Actualización de las políticas respecto de la video-vigilancia, en caso de existir, que atiendan a la normativa actual de protección de datos personales. 154. La especificación clara de los fines que justifican el monitoreo. 155. El momento y circunstancias por las cuales se hará uso de la información obtenida del monitoreo y de los sistemas de video-vigilancia. 156. Aplicar el principio de minimización mediante: ○ La limitación del número de cámaras para cumplir con la función de vigilancia; ○ Análisis de requisitos técnicos de las cámaras (el zoom y las cámaras domo pueden afectar este principio). 157. Excluir la instalación de sistemas de imagen y/o sonido en lugares destinados al descanso o esparcimiento del personal (vestuario, aseos, comedores, y análogos).
D5.6	Protección de datos personales en las prácticas de vigilancia de la salud en el entorno laboral	*Control* Que las prácticas de vigilancia de la salud para la prevención de riesgos laborales se encuentren alineadas a la normativa en materia de protección de datos personales.

Dominios y objetivos de control		
		Actividades de control: 158. Informar en el aviso de privacidad sobre el tratamiento de datos de salud. 159. Disponer de una base jurídica para el tratamiento de datos de salud. 160. Informar claramente al personal de esta medida mediante el aviso de privacidad. 161. Instrumento que contenga el consentimiento expreso del personal en caso de que el reconocimiento médico permita averiguar datos no vinculados estrictamente con la aptitud laboral. 162. Definición precisa de los perfiles de acceso y las funciones de quienes intervienen en el tratamiento de los datos de salud. 163. Medidas de seguridad físicas, técnicas y administrativas específicas para la salvaguarda de la historia clínica del personal que acude al servicio médico del responsable.
Dominio 6. Gestión de la seguridad en el tratamiento de los datos personales		
Objetivo: Llevar un control de las medidas de seguridad físicas, técnicas y administrativas mínimas para la protección de los datos personales.		
D6.1	Inclusión de la protección de datos personales en la política de seguridad de la información	*Control* La Política de seguridad de la información organizacional, debe incluir una cláusula referente a la protección de los datos personales. Actividades de control: 164. Cláusula que especifique la protección de los datos personales en

Dominios y objetivos de control		
		las directrices o políticas de seguridad de la información organizacional. 165. Distribución de las directrices o políticas de seguridad de la información.
D6.2	Medidas de seguridad físicas	*Control* Tener debidamente identificadas, implementadas y monitoreadas las acciones y mecanismos para protección del entorno físico del tratamiento de los datos personales. Actividades de control: 166. Referencia al estándar, framework o buena práctica del control implementado. 167. Descripción de las medidas de seguridad, especificando el riesgo de datos personales que tratan. 168. Eficiencia del control implementado.
D6.3	Medidas de seguridad administrativas	*Control* Tener debidamente identificadas, implementadas y monitoreadas las políticas, directrices, procedimientos o documentos similares para la gestión, soporte y revisión de la seguridad de los datos personales. Actividades de control: 169. Referencia al estándar, framework o buena práctica del control implementado. 170. Descripción de las medidas de seguridad, especificando el riesgo de datos personales que tratan. 171. Eficiencia del control implementado.
D6.4	Medidas de seguridad técnicas	*Control* Tener debidamente identificadas, implementadas y monitoreadas las acciones

Dominios y objetivos de control		
		y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital y los recursos involucrados en el tratamiento de los datos personales. Actividades de control: 172. Referencia al estándar, framework o buena práctica del control implementado. 173. Descripción de las medidas de seguridad, especificando el riesgo de datos personales que tratan. 174. Eficiencia del control implementado.
D6.5	Auditorías de seguridad de la información que incluyan datos personales	*Control* Se deben efectuar revisiones, internas o externas, periódicas de las medidas de seguridad implementadas, incluyendo las amenazas y vulneraciones a las que pueden estar expuestos los datos personales. Actividades de control: 175. Disponer de un plan de auditoría de seguridad de la información. 176. La inclusión, dentro del alcance del plan de auditoría de seguridad de la información de los datos personales que son tratados. 177. Plan de seguimiento de la auditoría, de existir no conformidades relacionadas con datos personales. 178. Contar con pruebas de seguridad (*pentest*) o pruebas de vulnerabilidades.
D6.6	Análisis de brecha de seguridad de los datos personales	*Control* Identificar las medidas de seguridad de los datos personales existentes y efectivas, las faltantes o nuevas.

Dominios y objetivos de control		
		Actividades de control: 179. Definición de un estándar o marco internacional u organizacional de seguridad de la información para la aplicación del análisis de brecha. 180. Documentación de la aplicación del análisis de brecha por lo menos cada dos años. 181. Identificación de las medidas de seguridad existentes y efectivas. 182. Identificación de las medidas de seguridad faltantes. 183. Identificación de medidas de seguridad nuevas, en caso de aplicar.
D6.7	Análisis de riesgos de los datos personales tratados	*Control* Identificar los riesgos de los datos personales tratados durante su ciclo de vida. Actividades de control: 184. Especificación de requerimientos regulatorios, códigos de conducta, mejores prácticas del sector específico. 185. Los datos personales previamente clasificados. 186. El valor de los datos personales de acuerdo con su clasificación y su ciclo de vida. 187. El valor y exposición de los activos involucrados en el tratamiento de los datos personales. 188. Las consecuencias negativas (daño a la privacidad) para los titulares que pudieran derivar en una vulneración de seguridad.
D6.8	Plan de trabajo	*Control*

Dominios y objetivos de control		
		Las acciones a implementar, de acuerdo con el resultado obtenido en los análisis de riesgos y de brecha, deben estar definidas en planes de trabajo. Actividades de control: 189. Especificar fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes, recursos y áreas responsables. 190. Listado de las medidas de seguridad a implementar priorizando de acuerdo a su relevancia. 191. Periodos de revisión del avance de la implementación de las medidas de seguridad.
D6.9	Inventario de datos personales y de los sistemas de tratamiento	Control Disponer de un inventario con la información básica de cada tratamiento de datos personales. Actividades de control: 192. Catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales. 193. Las finalidades de cada tratamiento. 194. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no. 195. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales. 196. La lista de personas que tienen acceso a los sistemas de tratamiento. 197. El nombre completo o denominación o razón social del encargado y el

Dominios y objetivos de control		
		instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, en caso de aplicar. 198. Los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que la justifiquen, en caso de aplicar.
D6.10	Funciones y obligaciones de las personas que tratan datos personales	Control Establecer y documentar roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales. Actividades de control: 199. Documentos que establezcan los roles, responsabilidades y la cadena de rendición de cuentas. 200. Documentos que señalen las funciones y obligaciones de quienes participan en cualquier parte del tratamiento de los datos personales.
D6.11	Programa integral de capacitación	Control Capacitar al personal considerando sus roles y responsabilidades en el tratamiento y seguridad de los datos personales y el perfil de sus puestos. Actividades de control: 201. Requerimientos y actualizaciones del sistema de gestión. 202. Legislación vigente en materia de protección de datos personales y las mejoras prácticas relacionadas con el tratamiento de éstos. 203. Las consecuencias del incumplimiento de los requerimientos

Dominios y objetivos de control		
		legales o requisitos organizacionales. 204. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.
D6.12	Documento de seguridad	*Control* Disponer de un documento de seguridad que incorpore el resumen de todas las medidas de seguridad implementadas. Actividades de control: 205. El inventario de datos personales y de los sistemas de tratamiento: 206. Las funciones y obligaciones de las personas que tratan datos personales. 207. El análisis de riesgos. 208. Análisis de brecha. 209. El plan de trabajo. 210. Los mecanismos de monitoreo y revisión de las medidas de seguridad. 211. El programa general de capacitación. 212. Documento que acredite su presentación ante el Órgano en materia de transparencia del responsable.
D6.13	Monitoreo y supervisión continuo de las medidas de seguridad implementadas	*Control* Que la evaluación y medición de los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales sean verificados a través de un Programa de seguridad de la información que incorpore las acciones correspondientes.

Dominios y objetivos de control		
		Actividades de control: 213. Nuevos activos que se incluyan en la gestión de riesgos. 214. Modificaciones necesarias a los activos, -cambio o migración tecnológica, entre otras-. 215. Nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas. 216. Posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes. 217. Vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir. 218. Cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo. 219. Incidentes y vulneraciones de seguridad ocurridas.
Dominio 7. Riesgos con encargados		
Objetivo: Verificar que los encargados protejan los datos personales bajo su resguardo		
D7.1	Acciones de cumplimiento de protección de datos personales para encargados	*Control* Disponer de instrumentos jurídicos que establezcan los requerimientos que deben cumplir los encargados al realizar el tratamiento de los datos personales. Actividades de control:

Dominios y objetivos de control		
		220. Descripción de obligaciones de protección de datos personales que debe cumplir el encargado. 221. De ser posible, adhesión al código de conducta del responsable por parte de los empleados del encargado. 222. Permitir al Órgano Garante y a la organización realizar verificaciones en el lugar o establecimiento donde lleve a cabo el tratamiento de los datos personales. 223. Colaborar con el Órgano Garante en las investigaciones previas y verificaciones que se lleven a cabo, proporcionando toda la información y documentación que se estime necesaria para tal efecto. 224. Generar, actualizar y conservar la documentación necesaria que acredite el cumplimiento de sus obligaciones. 225. Participación en auditorías de protección de datos personales para verificar su cumplimiento. 226. Establecimiento de cláusulas de confidencialidad. 227. Firma de convenios de confidencialidad de los empleados del encargado que participen en el tratamiento de los datos personales. 228. Que los acuerdos entre el responsable y el encargado no contravengan la normativa aplicable en la materia. 229. Especificar que, en caso de requerirse subcontratación, medie autorización expresa del responsable.

Dominios y objetivos de control		
D7.2	Cláusulas contractuales	*Control* Verificar que el documento jurídico que formaliza la relación con el encargado contenga las disposiciones enmarcadas en la normativa aplicable y que permita acreditar su existencia, alcance y contenido. Actividades de control: 230. Tratar los datos personales conforme a las instrucciones del responsable. 231. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. 232. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables. 233. Informar al responsable cuando ocurra una vulneración a los datos personales, de conformidad con los procedimientos establecidos por la organización. 234. Guardar confidencialidad respecto de los datos personales tratados. 235. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable. 236. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
D7.3	Procesos de debida diligencia (*due diligence*) en las prácticas de protección de datos con encargados	*Control* Verificar, antes de llevar a cabo la contratación, que los encargados atienden las buenas prácticas nacionales e internacionales en protección de datos

Dominios y objetivos de control		
		personales y/o seguridad de la información, así como la normativa en la materia. Actividades de control: 237. Certificaciones de seguridad o de protección de datos personales del encargado o del personal involucrado en el tratamiento de los datos. 238. Cumplimiento de la legislación y normatividad aplicable en materia de protección de datos personales nacional o internacional (en caso de aplicar). 239. Registros de incidentes de seguridad y/o vulneraciones que el encargado haya presentado en otras organizaciones, en caso de aplicar. 240. Investigación por parte del responsable de fuentes externas acerca de la ocurrencia de incidentes de seguridad y/o vulneraciones antes de la contratación del encargado.
D7.4	Instrumentos para la contratación de prestadores de servicios de cómputo en la nube	*Control* Garantizar que los prestadores de servicios de cómputo cumplan sus obligaciones de protección de datos personales. Actividades de control: 241. Disponer de políticas de protección de datos personales afines a los principios y deberes de la normativa aplicable en la materia. 242. Aplicar las políticas de protección de datos personales afines a los principios y deberes de la normativa aplicable en la materia. 243. Instrumentos para generar, actualizar y conservar la

Dominios y objetivos de control		
		documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones. 244. Especificaciones de la existencia de subcontrataciones relacionadas con la información sobre la que se preste el servicio. 245. Abstenerse de incluir condiciones que autoricen o permitan asumir la titularidad o propiedad de la información sobre los que se preste el servicio. 246. Mecanismos para guardar la confidencialidad de los datos personales. 247. Mecanismos definidos para dar a conocer cambios en sus políticas de privacidad o condiciones del servicio, aplicación o infraestructura. 248. Mecanismos definidos para limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio. 249. Especificaciones de las medidas de seguridad para la protección de los datos personales. 250. Mecanismos definidos para garantizar la supresión de los datos personales una vez concluido el servicio prestado. 251. Especificar el establecimiento de mecanismos de control de acceso a los datos personales que impidan el acceso a los datos personales a personas que no cuenten con privilegios de acceso. 252. Solicitud fundada y motivada de autoridad competente referente a los accesos a los datos personales a terceros, en caso de aplicar. 253. Informes de acceso al responsable.

Dominios y objetivos de control		
		254. Formación y educación de los empleados del encargado sobre protección de datos personales.
D7.5	Subcontratación de servicios	*Control* Alineación en la subcontratación de servicios por parte del encargado atendiendo a la protección de los datos personales a los que tenga acceso. Actividades de control: 255. Instrumento que formalice la relación entre el encargado y el tercero a quien subcontratará. 256. Realizar el tratamiento de los datos personales conforme a las instrucciones del encargado. 257. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el encargado. 258. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables. 259. Informar al encargado cuando ocurra una vulneración a los datos personales que trata por sus instrucciones. 260. Guardar confidencialidad respecto de los datos personales tratados. 261. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el encargado, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. 262. Abstenerse de transferir los datos personales salvo en el caso de que el encargado así lo determine (por instrucciones del responsable).

Dominios y objetivos de control		
		263. Permitir al Órgano Garante y a la organización realizar verificaciones en el lugar o establecimiento donde lleve a cabo el tratamiento de los datos personales. 264. Colaborar con el Órgano Garante en las investigaciones previas y verificaciones que se lleven a cabo, proporcionando toda la información y documentación que se estime necesaria para tal efecto. 265. Generar, actualizar y conservar la documentación necesaria que acredite el cumplimiento de sus obligaciones.
D7.6	Mecanismos para determinar acciones por incumplimiento contractual	*Control* Contar con mecanismos (procedimientos, guías, cláusulas, entre otros) que permitan determinar si existe incumplimiento a lo establecido para la protección de datos personales en los contratos celebrados con los encargados. Actividades de control: 266. Especificar las causas de incumplimiento. 267. La normativa aplicable. 268. Tipos de sanciones.
D7.7	Auditorías de debida diligencia sobre prácticas de protección de datos con encargados	*Control* Contar con un calendario de auditorías que permita verificar de manera permanente el cumplimiento de las políticas, criterios contractuales o de cualquier mecanismo implementado para asegurar el debido tratamiento de los datos por parte de encargados. Actividades de control:

Dominios y objetivos de control		
		269. Plan de auditorías internas y/o externas que integre: ○ Personas responsables de la ejecución de la auditoría; ○ Temporalidad de las auditorías; ○ Cualificaciones de los auditores en materia de protección de datos personales; ○ Fecha de presentación del informe de la auditoría; 270. Presentación del informe de auditoría. 271. Seguimiento al cumplimiento de las no conformidades. 272. Especificación de la metodología empleada para la auditoría.
Dominio 8. Avisos de Privacidad		
Objetivo: Verificar que la organización dispone de avisos de privacidad con los requisitos que marca la normativa aplicable en la materia para cumplir con el principio de información.		
D8.1	Instrumentos de apoyo para generar avisos de privacidad	*Control* Avisos de privacidad elaborados con los requisitos de la normatividad aplicable. Actividades de control: 273. Explicar qué es un aviso de privacidad. 274. Normativa que regula los avisos de privacidad. 275. Características. 276. Tipos de avisos. 277. Obligaciones generales. 278. Elementos que conforman el aviso de privacidad simplificado o integral. 279. Informar los medios a través de los cuales se hará del conocimiento del

Dominios y objetivos de control		
		titular el aviso de privacidad simplificado o integral. 280. Formato tipo o modelos de avisos de privacidad integral y simplificado. 281. Ejemplos.
D8.2	Avisos de privacidad integral con el detalle sobre el manejo de los datos personales	*Control* Los avisos de privacidad integrales incluyen todos los elementos que detalla la normativa aplicable. Actividades de control: 282. El sitio, lugar o mecanismo implementado para conocer el aviso de privacidad integral. 283. Información al titular de las transferencias nacionales e internacionales que: ○ requieran de su consentimiento, indicando: los destinatarios o terceros receptores; finalidades de las transferencias. ○ no requieran de su consentimiento, indicando: los destinatarios o terceros receptores; finalidades de las transferencias; el fundamento legal. 284. El domicilio completo, que incluya: la calle, número, colonia, ciudad, municipio o delegación/alcaldía, código postal y entidad federativa (es posible incluir otros datos de contacto por ejemplo dirección de la página de internet, correo electrónico y número telefónico). 285. Los tipos de datos personales que se recaban, distinguiéndolos expresamente de los datos personales de carácter sensible.

Dominios y objetivos de control		
		286. El o los artículos, apartado, fracciones, incisos y nombre de los ordenamientos o disposiciones normativas vigentes, precisando: ○ fecha de publicación, ○ fecha de última reforma o modificación. 287. Información sobre los mecanismos, medios y procedimientos habilitados para atender las solicitudes de los derechos ARCO.
D8.3	Avisos de privacidad simplificados, con el resumen sobre el manejo de los datos personales.	*Control* Los avisos de privacidad simplificados incluyen todos los elementos que detalla la normativa aplicable. Actividades de control: 288. Denominación completa del responsable. 289. Descripción puntual de las finalidades del tratamiento de los datos personales con las características siguientes: ○ el listado debe ser completo y no utilizar frases ambiguas; ○ ser específicas y redactadas con claridad; ○ identificación de las finalidades que requieran el consentimiento del titular y las que no. 290. Identificación de las transferencias que requieran el consentimiento del titular, indicando: ○ autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales;

Dominios y objetivos de control		
		○ finalidades de las transferencias. 291. Incluir o informar sobre mecanismos y medios para manifestar la negativa del tratamiento por parte del titular. 292. Fecha de última reforma o modificación.
D8.4	Disposición del aviso de privacidad en todos los puntos de recolección de datos personales	*Control* Los avisos de privacidad son publicados en todos los puntos a través de los cuales se lleva a cabo la recolección de los datos. Actividades de control: 293. Disposición al titular del aviso de privacidad simplificado. 294. Publicación del aviso de privacidad integral de manera permanente, en el sitio o medio que se informe en el aviso de privacidad simplificado. 295. Disposición al titular del nuevo aviso de privacidad cuando: cambie su identidad, requiera recabar datos personales sensibles adicionales, cambie las finalidades, modifique las condiciones de las transferencias o se pretendan realizar transferencias no previstas inicialmente y el consentimiento del titular sea necesario. 296. Disposición del aviso de privacidad en diferentes formatos: ○ físicos ○ electrónicos ○ sonoros ○ audiovisuales ○ braille ○ otra tecnología que permita su comunicación eficaz 297. Disposición del aviso de privacidad en lenguas indígenas:

Dominios y objetivos de control		
		○ náhuatl ○ mixteco ○ otomí ○ mazateco ○ zapoteco ○ mazahua 298. Cuando se recaben de manera indirecta los datos personales de un titular: ○ enviar el aviso de privacidad correspondiente a los titulares; ○ informar al titular sobre los 5 días hábiles que tiene para manifestar su negativa, y ○ solicitar el consentimiento expreso, en caso de que se requiera, y los datos personales se tratan sólo si se cuenta con el mismo.
D8.5	Disposición de los avisos de privacidad en medios visibles	*Control* Los avisos de privacidad deben colocarse en todos los puntos a través de los cuales se lleva a cabo la recolección de los datos personales. Actividades de control: 299. Avisos de privacidad integrales en páginas web, chats, redes sociales con ligas accesibles y visibles y/o ventanas emergentes, grabaciones telefónicas, entre otros. 300. Aviso de privacidad simplificado en espacios visibles en páginas web, chats, redes sociales, ventanas emergentes, grabaciones telefónicas, entre otros. 301. Avisos de privacidad impresos con letra legible. 302. Ubicación de avisos de privacidad impresos en lugares accesibles para

Dominios y objetivos de control		
		personas en sillas de ruedas o de baja estatura.
D8.6	Disposición de avisos de privacidad en los contratos y términos de uso	*Control* En los contratos y términos de uso, los avisos de privacidad deben disponerse en lugares fáciles de acceder y que puedan ser consultados. Actividades de control: 303. Incorporación de una cláusula que señale la ubicación del aviso de privacidad del responsable o señalar como obligatorio que el aviso forme parte de los anexos a los contratos o términos de uso.
D8.7	Capacitación a empleados para explicar o dar a conocer el aviso de privacidad	*Control* El personal debe estar capacitado para que conozca a detalle el aviso de privacidad y pueda explicarlo, o resolver dudas en cuanto a su contenido, principalmente a quien recaba los datos personales. Actividades de control: 304. Integración en las capacitaciones/sensibilizaciones del personal de nuevo ingreso información referente a los avisos de privacidad. 305. Capacitación especializada sobre la conformación del aviso de privacidad al personal que por sus funciones tiene contacto directo con los titulares de los datos. 306. Inclusión en los scripts de la información referente al aviso de privacidad. 307. Disponer de material de reforzamiento:

Dominios y objetivos de control		
		○ manuales ○ infografías ○ cursos virtuales ○ folletos
D8.8	Medidas compensatorias para dar a conocer el aviso de privacidad	*Control* Disponer de políticas o procedimientos para especificar los mecanismos alternos para dar a conocer el aviso de privacidad. Actividades de control: 308. Motivos por los cuales el responsable hará uso de medidas compensatorias de comunicación masiva u otros mecanismos de amplio alcance. 309. Las modalidades para la aplicación de medidas compensatorias y sus procedimientos de instrumentación. 310. Difusión en medios de comunicación masivos: ○ Diario Oficial de la Federación o diarios de circulación nacional; ○ Diarios o gacetas oficiales de las entidades federativas, o diarios de circulación regional o local, o bien, revistas especializadas; ○ Página de Internet o cualquier otra plataforma o tecnología oficial del responsable; ○ Carteles informativos; ○ Cápsulas informativas radiofónicas; ○ Cualquier otro medio alterno de comunicación masivo. 311. Criterios para seleccionar el medio para difundir el aviso de privacidad. 312. Criterios para la publicación del aviso de privacidad en los diferentes medios de comunicación.

Dominios y objetivos de control		
Dominio 9. Solicitudes ARCOP		
Objetivo: Verificar que el responsable dispone de procedimientos que provean eficiencia al proceso de atención a solicitudes ARCOP.		
D9.1	Instrumento para atender solicitudes o proveer mecanismos para que los titulares ejerzan sus derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales	*Control* Contar con un instrumento para la atención de las solicitudes ARCOP. Actividades de control: 313. En qué consisten los derechos ARCOP. 314. Personas facultadas para el ejercicio de los derechos ARCOP. 315. Los medios para la acreditación de la identidad del titular; la identidad y personalidad del representante. 316. Los medios para acreditar el interés jurídico en el supuesto de que el titular sea un menor de edad: ○ la copia del acta de defunción del menor; ○ el acta de nacimiento o identificación del menor; ○ la identificación de quien ejerce la patria potestad y/o tutela. 317. Los medios para acreditar el interés jurídico en el supuesto de que el titular sea una persona en estado de interdicción o incapacidad declarada por ley o por autoridad judicial: ○ copia de su acta de defunción; ○ el documento de su identificación oficial y de quien ejerce la tutela; ○ el instrumento legal de designación del tutor. 318. Disponer de un apartado referente al ejercicio de derechos ARCOP de menores de edad, que contenga los

Dominios y objetivos de control		
		medios para la acreditación de la identidad cuando: ○ sus padres ejercen la patria potestad; ○ una persona distinta a sus padres ejerce la patria potestad; ○ son representados por un tutor; 319. Disponer de un apartado referente al ejercicio de derechos ARCOP de personas en estado de interdicción o incapacidad declara por ley o por autoridad judicial. 320. Disponer de un apartado referente al ejercicio de derechos ARCOP de una persona fallecida que contenga: un procedimiento interno para tener en cuenta que, la persona que acredite tener un interés jurídico de conformidad con las leyes aplicables podrá ejercer los derechos ARCOP. 321. La persona que acredite tener un interés jurídico deberá presentar los siguientes documentos, según corresponda: ○ Acta de defunción del titular, en caso de que aplique; ○ Documentos que acrediten el interés jurídico de quien pretende ejercer el derecho, y ○ Documento de identificación oficial de quien solicita el ejercicio de los derechos ARCOP. 322. Medios de asistencia de la Unidad de Transparencia. 323. Registro de las solicitudes en el sistema electrónico habilitado para tal efecto por la autoridad de protección de datos nacional. 324. Plazos y procedimientos para la atención de las solicitudes, que incluya:

Dominios y objetivos de control		
		○ la prevención al titular; ○ causales de improcedencia; ○ medios de defensa. 325. Modalidades y costos de entrega. 326. Entrega al titular del acuse correspondiente. 327. Disposición del medio de reproducción con los datos solicitados y las constancias de ejercicio, por un plazo de 60 días. 328. Eliminación por un medio seguro, transcurrido el plazo de disposición sin que el titular o el responsable los hayan recogido. 329. Apartado que indique la reconducción de la vía -en caso de que se advierta que la solicitud para el ejercicio de derechos ARCOP corresponda a un derecho diferente- dentro de los 3 días siguientes a la presentación de la solicitud.
D9.2	Solicitud para el ejercicio de los derechos ARCOP	*Control* Verificar que no se impongan o solicitar mayores requerimientos a los señalados en la normativa. Actividades de control: 330. El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones. 331. Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante. 332. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud. 333. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los

Dominios y objetivos de control		
		derechos ARCOP, salvo que se trate del derecho de acceso. 334. La descripción del derecho ARCOP que se pretende ejercer, o bien, lo que solicita el titular, y *335.* Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.
D9.3	Medidas especiales para personas con discapacidad y hablantes de lengua indígena	*Control* Ejercer en igualdad de circunstancias los derechos ARCOP para personas con algún tipo de discapacidad o de lengua indígena. Actividades de control: 336. Acuerdos con instituciones públicas especializadas que pudieran auxiliar en la recepción y entrega de las respuestas a solicitudes para el ejercicio de los derechos ARCOP en lengua indígena, braille o cualquier formato que se requiera en función de la discapacidad del titular. 337. Equipos de cómputo con tecnología adaptada, escritura braille y lectores de texto. 338. Lugares de estacionamiento para personas con discapacidad. 339. Intérpretes oficiales de lenguas indígenas. 340. Utilización de lenguaje de señas o cualquier otro medio o modo de comunicación. 341. Facilidades para el acceso de perros guías o animales de apoyo. 342. Apoyo en la lectura de documentos. 343. Rampas para personas con discapacidad. 344. Medidas físicas o tecnológicas que ayuden a las personas con discapacidad y/o hablantes de

Dominios y objetivos de control		
		lengua indígena a ejercer sus derechos ARCOP.
D9.4	Instrumentos para el acceso a datos personales	*Control* Atender las solicitudes de los titulares sobre el acceso a datos personales. Actividades de control: 345. Formulario o algún otro mecanismo para que el titular pueda ejercer su derecho de acceso. 346. Constancia de notificación al titular sobre el acceso a sus datos personales que incluya, al menos: ○ Una copia de sus datos personales que son objeto del tratamiento; ○ Los fines del tratamiento; ○ Las categorías de datos personales que se traten; ○ Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular, los destinatarios en países terceros u organizaciones internacionales; ○ El plazo previsto de conservación de los datos personales, o si no es posible, los criterios utilizados para determinar este plazo; ○ La existencia del derecho del interesado a solicitar al responsable: la rectificación o supresión de sus datos personales, la limitación del tratamiento de sus datos personales u oponerse a ese tratamiento; ○ El derecho a presentar una reclamación ante una Autoridad

Dominios y objetivos de control		
		de protección de datos personales; ○ Cuando los datos personales no se hayan obtenido directamente del titular, cualquier información disponible sobre su origen; ○ La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y al menos en tales casos, información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de ese tratamiento para el interesado; ○ Cuando se transfieran datos personales a un tercer país o a una organización internacional, informar sobre las garantías en las que se realizan las transferencias.
D9.5	Instrumentos para la rectificación de datos personales	*Control* Atender las solicitudes de los titulares sobre la rectificación de los datos personales. Actividades de control: 347. Formulario o algún otro mecanismo para que el titular pueda ejercer su derecho de rectificación. 348. Plazos y procedimientos que incluyan que la notificación se entregará al titular o su representante, previa acreditación de la identidad y, en su caso, personalidad de este último, en el plazo de 15 días contados a partir del día siguiente a que se haya notificado la respuesta al titular.

Dominios y objetivos de control		
		349. Constancia de notificación al titular sobre sus datos rectificados que incluya, al menos: ○ Nombre completo del titular; ○ Especificar los datos personales corregidos; ○ La fecha a partir de la cual fueron rectificados los datos personales en sus registros, archivos, sistemas de información, expedientes, bases de datos o documentos en su posesión.
D9.6	Instrumento para la cancelación de datos personales.	*Control* Atender las solicitudes relacionadas con el derecho de cancelación. Actividades de control: 350. Formulario o algún otro mecanismo para que el titular pueda ejercer su derecho de cancelación. 351. Plazos y procedimientos que incluya la notificación de respuesta se entregará al titular o su representante, previa acreditación de la identidad y, en su caso, personalidad de este último, en el plazo de 15 días contados a partir del día siguiente a que se haya notificado. 352. Condiciones para ejercer el derecho de cancelación. 353. Causales de no procedencia. 354. Atención de dudas respecto al ejercicio del derecho de cancelación. 355. Constancia de notificación al titular que señale: ○ Los documentos, bases de datos personales, archivos, registros, expedientes y/o sistemas de tratamiento donde se encuentren

Dominios y objetivos de control		
		los datos personales objeto de cancelación; ○ El periodo de bloqueo de los datos personales, en su caso; ○ Las medidas de seguridad de carácter administrativo, físico y técnico implementadas durante el periodo de bloqueo, en su caso; ○ Las políticas, métodos y técnicas utilizadas para la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.
D9.7	Instrumento para la oposición (revocación) de datos personales	*Control* Atender las solicitudes de los titulares sobre la oposición (revocación) del consentimiento para el tratamiento de los datos personales. Actividades de control: 356. Formulario o algún otro mecanismo para que el titular pueda ejercer su derecho de oposición. 357. Personas facultadas para solicitar la revocación del consentimiento al tratamiento de los datos personales. 358. Plazos y procedimientos que incluya el tiempo de atención a la solicitud. 359. Causas por las cuales puede negarse la oposición. 360. Evitar como medio de manifestación para el titular el uso de cartas certificadas o similares, o el uso de otros medios que impliquen un costo adicional. 361. Informar a las personas titulares sobre las consecuencias de negar o retirar el consentimiento.

Dominios y objetivos de control		
		362. Constancia de cese del tratamiento donde el responsable notifique al titular, previa acreditación de su identidad y, en su caso, la identidad y personalidad de su representante, dentro del plazo de 15 días.
D9.8	Instrumento para responder solicitudes sobre portabilidad de datos personales	*Control* Contar con un instrumento que dé respuesta a las solicitudes sobre la portabilidad de datos personales. Actividades de control: 363. En qué consiste la portabilidad de datos personales. 364. Causales de no procedencia. 365. Requisitos para la presentación de una solicitud de portabilidad de datos personales. 366. Plazos. 367. Medios de entrega de la información y formato (audio, imagen, texto base de datos, video, etc). 368. Costos, en su caso. 369. Constancia de notificación al titular.
D9.9	Procedimientos para la atención de recursos de revisión	*Control* Disponer de mecanismos que permitan el monitoreo y la generación de reportes sobre el seguimiento a las posibles quejas en el ejercicio de los derechos ARCO. Actividades de control: 370. Personas facultadas para solicitar el recurso de revisión. 371. Documentos de acreditación. 372. Tiempo de atención a la solicitud.

Dominios y objetivos de control		
		373. Proceso de cumplimiento y plazos 374. Causales de procedencia. 375. Requisitos del escrito de recurso de revisión. 376. Medios de presentación. 377. Formato de solicitud o ejemplo. 378. Instrucciones de llenado del formato o solicitud de ejemplo. 379. Medios de impugnación.
Dominio 10. Evaluaciones de impacto en la protección de datos personales		
Objetivo: Verificar que los datos personales cuyo tratamiento implica un alto riesgo cuenten con una estrategia de tratamiento.		
D10.1	Evaluaciones de Impacto en la Protección de Datos (EIPDs) para nuevos programas, sistemas y procesos o modificados	*Control* Valorar los impactos reales respecto de determinado tratamiento, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares previstos en la normativa aplicable. Actividades de control: 380. Análisis para determinar si se requiere una evaluación de impacto. 381. Documento de evaluación de impacto, en caso de aplicar. 382. Procedimiento para atender las observaciones que en su caso realice el INAI, y justificar cuando ello no sea posible.
D10.2	Instrumentos para llevar a cabo EIPDs	*Control* Disponer de un instrumento que permita homologar el proceso de identificación, generación y presentación de las EIPDs. Actividades de control:

Dominios y objetivos de control		
		El instrumento debe contener al menos lo siguiente, 383. Qué es un tratamiento intensivo o relevante de datos personales. 384. Casos en los que se debe realizar una EIPD. 385. Elementos mínimos que debe incluir una EIPD establecidos por la normatividad aplicable. 386. Formatos o guías de apoyo. Además, 387. Integración de una cláusula de ejecución de EIPDs dentro de la política de protección de datos personales organizacional.
D10.3	Involucrar a encargados como parte del proceso de EIPDs	*Control* Considerar, en las evaluaciones de impacto, la integración de los encargados, en caso de que éstos intervengan en alguna parte del tratamiento. Actividades de control: 388. Inclusión en cláusulas contractuales de la cooperación del encargado en la ejecución de EIPDs.
Dominio 11. Gestión de vulneraciones		
Objetivo: Verificar la existencia, vigencia y uso de procedimientos que permitan actuar de manera oportuna en caso de presentarse alguna vulneración de la seguridad de los datos personales.		
D11.1	Plan de respuesta a vulneraciones a la seguridad de datos personales	*Control* Disponer de planes de respuesta a incidentes que involucren datos personales.

Dominios y objetivos de control		
		Actividades de control: 389. Plan de respuesta separado o integrado a los planes de respuesta de atención de incidentes de seguridad de la información. 390. Procedimientos para identificar y escalar las vulneraciones a la seguridad de datos personales. 391. Identificación de las vulneraciones a las que están expuestas los datos personales. 392. Roles y responsabilidades para la atención de las vulneraciones. 393. Recolección y preservación de evidencia. 394. Descripción de las actividades de atención de la vulneración (análisis, contención, erradicación, recuperación). 395. Protocolo o documento similar para la notificación de una vulneración al Órgano Garante y a los titulares, cuando corresponda, que contenga al menos, o Establecimiento de tiempos para la notificación. o Medios oficiales para la notificación. o Asignación del responsable de las notificaciones y reportes de las vulneraciones (contacto único de comunicación). o Información requerida en la notificación.
D11.2	Verificación, revisión y evaluación del Plan de Respuesta a vulneraciones de	*Control*

Dominios y objetivos de control		
	la seguridad de datos personales	Establecer los periodos de verificación, revisión y evaluación de los planes de respuesta a incidentes de datos personales. Actividades de control: 396. Documento que acredite las verificaciones, revisiones y evaluaciones, que contenga: ○ Fecha de la verificación, revisión y evaluación; ○ Responsable (nombre y cargo); ○ Firmas. 397. Descripción del resultado de las verificaciones, revisiones y evaluaciones.
D11.3	Notificación de las vulneraciones de seguridad a la persona titular.	*Control* Las notificaciones sobre las vulneraciones de seguridad deben contener elementos mínimos. Actividades de control: 398. La naturaleza del incidente o vulneración ocurrida; 399. Los datos personales comprometidos, 400. Las recomendaciones dirigidas al titular sobre las medidas que éste pueda adoptar para proteger sus intereses; 401. Las acciones correctivas realizadas de forma inmediata, 402. Los medios puestos a disposición del titular para que pueda obtener mayor información al respecto; 403. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y

Dominios y objetivos de control		
		404. Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.
D11.4	Monitoreo, reporte y bitácoras de vulneraciones	*Control* Llevar un registro de las vulneraciones ocurridas, así como el seguimiento a las acciones para su mitigación. Actividades de control: 405. Fecha en que ocurrió la vulneración. 406. El motivo. 407. Las acciones correctivas implementadas de forma inmediata. 408. Las acciones correctivas implementadas de forma definitiva. 409. Las acciones preventivas que, en su caso, puedan ser implementadas para vulneraciones posteriores. 410. Las consecuencias de la vulneración.
Dominio 12. Monitoreo de la protección de los datos personales		
Objetivo: Verificar la adecuada gestión en la protección de datos personales con base en lo establecido en el sistema de gestión.		
D12.1	Auditorías internas y autoevaluaciones al sistema de gestión de datos personales	*Control* Mejora continua del sistema de gestión de datos personales. Actividades de control: 411. Plan de auditorías internas al sistema de gestión. 412. Plan de trabajo para la atención de las no conformidades. 413. Presentación al Órgano en materia de transparencia del responsable el resultado de la autoevaluación del

Dominios y objetivos de control		
		sistema de gestión con el detalle de las revisiones y modificaciones aplicadas. 414. Revisiones por parte del Órgano en materia de transparencia del responsable de la atención de las no conformidades.
D12.2	Auditorías internas en materia de protección de los datos personales (monitoreo y supervisión) de las políticas, planes, procesos, y procedimientos del responsable	*Control* Asegurar que los procesos de negocio que tratan datos personales cumplen con la normatividad aplicable en la materia. Actividades de control: 415. Programa de auditorías internas. 416. Planes de auditorías con base en el Programa de auditorías para los procesos y procedimientos que traten datos personales. 417. Informe de auditoría. 418. Plan de seguimiento -o documento similar- para la atención de las no conformidades. 419. Revisiones del resultado de las auditorías por parte del Órgano en materia de transparencia del responsable. 420. Mecanismo para supervisar el cumplimiento del Documento de Seguridad por parte del Órgano en materia de transparencia del responsable.
D12.3	Revisión independiente de la protección de datos personales	*Control* Planificar la revisión, por parte de un tercero, para determinar el estado en el que se encuentra la protección de los datos personales en la organización. Actividades de control:

Dominios y objetivos de control		
		421. Revisiones independientes de la protección de datos personales. 422. Plan de trabajo -o documento similar- para atención de las recomendaciones. 423. Revisiones al proceso de atención de las recomendaciones por parte del Órgano en materia de transparencia.
D12.4	Atención de dudas y quejas de los titulares	*Control* Recibir y responder dudas y quejas de los titulares para cumplir con el principio de responsabilidad. Actividades de control: 424. Instrumento para recibir y responder las dudas y quejas de los titulares.
Dominio 13. Cumplimiento normativo		
Objetivo: Verificar el cumplimiento normativo en la materia.		
D13.1	Tratamiento de datos personales de acuerdo con las finalidades y atribuciones	*Control* Procesos y procedimientos de negocio que tratan datos personales alineados a la normativa aplicable. Actividades de control: 425. Instrumento que justifique las finalidades acordes a las atribuciones o facultades del responsable.
D.13.2	Apartado virtual de protección de datos personales en los sitios de internet del responsable	*Control* Disponer de un medio para acreditar el cumplimiento de las obligaciones en materia de protección de datos personales.

Dominios y objetivos de control		
		Actividades de control: 426. Sección de avisos de privacidad integrales. 427. Sección de datos de contacto de la unidad responsable de protección de datos personales del responsable. 428. Sección de información relevante en la materia.