Sistema de Gestión para la Protección de Datos Personales del Instituto Nacional Electoral

(Resumen del Anexo Único del Acuerdo INE-CT-ACG-PDP-001-2019)

Primera Edición
12-12-2019

Unidad Técnica de Transparencia y Protección de Datos Personales

CONTENIDO

Sistema de Gestión para la Protección de Datos Personales del Instituto Nacional Electoral

INTRODUCCIÓN

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 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.

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

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

Características:

- 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.

Beneficios:

a) <u>A las personas titulares de los datos:</u>
    - 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;
- 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 de la Ley General y artículo 32 del Reglamento del Instituto en materia de Protección de Datos Personales).

Compatibilidad con otros estándares de sistemas de gestión

La definición de la estructura del Sistema de Gestión se basa en lo establecido en el **Anexo SL de 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 Nacional Electoral.

Base regulatoria

1 ALCANCE

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.

2 REFERENCIAS NORMATIVAS

Las referencias normativas se dividen en: obligatorias y opcionales.

a) Obligatorias

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

b) Opcionales

- Convenio 108+. Convenio para la protección de las personas con respecto al procesamiento de datos personales.
- Las que se consideren necesarias de acuerdo con la normativa particular que aplique a la organización y a sus funciones.

3 TÉRMINOS, DEFINICIONES Y ABREVIACIONES

Para el propósito de este documento, los términos y definiciones a aplicar corresponden a los señalados en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de la normativa interna y/o especializada.

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

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

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

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 y demás normatividad que de ella derive.

e) **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.

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

g) **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.

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

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

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

k) **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.

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

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

n) **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.

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

p) **Proceso:** conjunto de actividades interrelacionadas o interactivas para transformar entradas en salidas. Conjunto de actividades mutuamente relacionadas o que interactúan, que utilizan las entradas para proporcionar un resultado previsto.

q) **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.

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

s) **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.

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

u) **SGPDP**: Sistema de Gestión para la Protección de los Datos Personales.

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 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 y demás normativa que de ellas derive;

b) **Parcial**, cuando abarque sólo algunos principios, deberes y obligaciones previstas en la Ley General 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.

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.

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 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 Evaluación de riesgos en la protección de los datos personales

La organización debe realizar un proceso de evaluación de riesgos en seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, integridad u disponibilidad de los datos personales, con base en su ciclo de vida y con el alcance establecido en SGPDP.

La organización debe aplicar una Evaluación de Impacto en la protección de los datos personales para identificar los riesgos relacionados al procesamiento de los datos personales 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.

La organización debe mantener la información documentada sobre las evaluaciones de riesgo de los datos personales y de las Evaluaciones de impacto.

6.1.3 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.

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.

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

La organización debe ejecutar evaluaciones de riesgos enfocados a los datos personales 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 establecidos en el 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 TRATAMIENTO DE RIESGOS DE DATOS PERSONALES

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

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

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.

9.3 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.

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.

APÉNDICE A.

CATÁLOGO DE CONTROLES PARA LA PROTECCIÓN DE DATOS PERSONALES

El Catálogo de controles provee a las áreas propietarias/dueñas, custodias, usuarias y todas las involucradas en el tratamiento de los datos personales, las **actividades** específicas para dar cumplimiento a un control.

Tabla 1. 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	Política organizacional 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 y normativos. Actividades de control 1. Prácticas de conducta organizacional para la protección de datos personales 2. Las necesidades organizacionales, amenazas, vulnerabilidades y normatividad 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 de los Órganos 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,

Tabla 1. Dominios y objetivos de control

		transmisión y seguridad de los datos personales 6. Descripción de su publicación a través de medios de comunicación organizacionales. 7. Forma de comunicar a los terceros involucrados en el tratamiento de los datos personales. 8. Disponer de un mecanismo que permita verificar que la política fue leída y entendida por personal interno y terceros involucrados en el tratamiento de los datos personales.
D1.2	Revisión de la política para la protección de datos personales.	*Control* Las políticas para la protección de datos personales deben ser revisadas con una frecuencia determinada o cuando exista un cambio significativo, para asegurar su eficacia. Actividades de control 9. Control de cambios con las fechas de revisión/actualización de la política. 10. Evidencia de la publicación a través de medios de comunicación organizacionales. 11. Evidencia de la comunicación a los terceros involucrados en el tratamiento de los datos personales.
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:

Tabla 1. Dominios y objetivos de control

		12. Identificación de las partes interesadas internas y externas. 13. Disponer de una matriz de responsabilidades y participación en la protección de los datos personales de las partes interesadas identificados. 14. Designar a un Oficial de Protección de Datos Personales.
D2.2	Contacto con las autoridades	*Control* Conocer temas actuales sobre la protección de los datos personales y buenas prácticas internacionales. Actividades de control: 15. Procedimiento de comunicación y colaboración con el Órgano Garante 16. Listados de autoridades (Órgano Garante, organismos de denuncia de vulneraciones, organismos de investigación de delitos electorales, entre otros). 17. Participar en estudios sobre mejores prácticas para el SGPDP
D2.3	Contacto con grupos de interés especial	*Control* Mantener contacto permanente con el Órgano Garante y otros organismos especializados en la materia. Actividades de control: 18. Evidencia de asistencia a foros, conferencias o eventos de asociaciones de grupos de expertos de protección de datos personales. 19. Reportes de seguimiento de fuentes de información legal respecto a la protección de los datos personales.

Tabla 1. Dominios y objetivos de control

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: 20. Inclusión del riesgo de los datos personales como parte de los riesgos de cumplimiento organizacionales. 21. 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: 22. Documentos que acrediten la capacitación especializada en la materia por organizaciones nacionales o internacionales: • Maestrías • Doctorados • Especializaciones • Certificaciones • Asistencia a congresos/seminarios/foros 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 programas de concientización permanentes, en materia de protección de datos personales, para todos los empleados de la organización, así como

Tabla 1. Dominios y objetivos de control

		la inclusión de capacitación en datos personales a los nuevos empleados. Actividades de control: 23. Objetivo de capacitación 24. Necesidades de capacitación para las áreas responsables del tratamiento de datos personales. 25. Medios y recursos 26. Diseñados para la especialización en la materia. 27. La medición de resultados y 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 con los principios de la protección de datos		
D3.1	Inventario de base de datos personales	*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: 28. Nombre de la base de datos 29. Proceso de negocio 30. Propietario / dueño de la base de datos 31. Datos personales y su categorización 32. Sistema (s) de tratamiento
D3.2	Categorización de los datos personales tratados	*Control* Identificar la naturaleza de los datos personales (estándar, sensible, especial) recabados. Actividades de control:

Tabla 1. Dominios y objetivos de control

		33. Esquema de categorización de datos personales atendiendo a la legislación y normatividad aplicable de la organización. 34. 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 la autoridad de protección de datos personales de la organización	*Control* Disponer de un registro actualizado de las bases de datos personales utilizadas en los procesos/servicios y sus sistemas de tratamiento. Actividades de control: 35. Inclusión del registro de las bases de datos en las políticas de protección de datos personales 36. Procedimiento para el registro de las bases de datos por parte de los responsables 37. Aviso de privacidad del tratamiento de los datos personales 38. Cédula de identificación del sistema de tratamiento
D3.4	Diagramas de flujo en el tratamiento de los datos personales	*Control* Conocer el flujo de tratamiento de los datos personales durante todo su ciclo de vida entre sistemas, procesos, países, etc. Actividades de control: 39. El tratamiento de los datos personales durante todas las fases de su ciclo de vida 40. La identificación de sistemas de tratamiento, activos secundarios y roles.

Tabla 1. Dominios y objetivos de control

D3.5	Políticas para la transferencia o remisión de datos personales	*Control* En el caso de que sea necesario realizar una transferencia o remisión de datos personales se debe contar con lineamientos generales para tal fin. Actividades de control: 41. La prevención de, al menos, la intercepción, copia, modificación, destrucción de los datos personales. 42. El uso de técnicas criptográficas para proteger la confidencialidad e integridad de los datos personales. 43. Los medios físicos y electrónicos aceptados para la transferencia o remisión de los datos personales.
D3.6	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: 44. Evidencia de los mecanismos utilizados: • Instrumentos jurídicos • Normas vinculantes • Convenios de colaboración • Códigos de conducta 45. En caso de excepciones, que están sean manifestadas de forma clara.
D3.7	Limitación del alcance del tratamiento de los datos personales	*Control* El tratamiento de los datos personales debe ser únicamente para las finalidades para las que fueron recabados y en procesos en los requeridos. Actividades de control:

Tabla 1. Dominios y objetivos de control

		46. Datos personales tratados con el consentimiento del interesado 47. Datos personales tratados sin el consentimiento del interesado 48. Especificar de manera clara la finalidad para la que los datos personales serán utilizados 49. Comunicar al titular cuando se haya modificado el alcance del tratamiento 50. Procedimientos de comunicación, en caso de existir modificación al alcance del tratamiento.
Dominio 4. Protección de datos personales en la operación		
Objetivo: Disponer de políticas y/o procedimientos que contemplen las acciones necesarias para la protección de los datos personales durante su ciclo de vida.		
D4.1	Procedimientos de verificación para la obtención lícita de los 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: 51. Existencia de procedimientos para verificar que los datos son obtenidos y tratados en estricto apego y cumplimiento a las atribuciones o facultades que la normatividad le confiera al responsable. 52. Contar con evidencia de la ejecución de los procedimientos. 53. Los procedimientos deben describir de manera detallada la forma y tiempos en que el responsable verifica la licitud.
D4.2	Políticas y/o procedimientos para la recolección de datos personales	*Control* Contar con políticas o procedimientos que describan el proceso de recolección de datos personales, señalando el tipo de medios a emplear para tal fin.

Tabla 1. Dominios y objetivos de control

		Actividades de control: 54. Definición de finalidad(es) del tratamiento. 55. El proceso de recolección/captación del área responsable, roles y responsabilidades. 56. Identificación de encargados y/o terceros que intervengan en el proceso de recolección/captación. 57. La normatividad que faculta al área responsable para la recolección y el uso de los datos personales. 58. La justificación que únicamente son recabados los datos personales necesarios para las finalidades establecidas y para su tratamiento relevante y necesario. 59. Implementación de medidas de seguridad durante su recolección y uso. 60. Medios de obtención del consentimiento. 61. Formatos de recolección y/o sistemas utilizados. 62. Descripción de cualquier otro medio utilizado para la recolección de los datos personales.
D4.3	Políticas y/o procedimientos para la recolección y uso de datos personales de niños, niñas y menores	*Control* Disponer de la evidencia necesaria para demostrar que los datos recabados de niños, niñas y menores cuenten con la más alta protección, estableciendo claramente las responsabilidades y el debido tratamiento de esta información. Actividades de control: 63. 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 menores de edad. 64. El registro del consentimiento de los padres o tutores.

Tabla 1. Dominios y objetivos de control

		65. Todas las que aplican al control "Políticas y/o procedimientos para la recolección y uso de datos personales".
D4.4	Políticas y/o procedimientos para la recolección y uso de datos personales de personas en estado de interdicción o de incapacidad	*Control* Disponer de la evidencia necesaria para demostrar que la recolección y el uso de los datos personales están alineados con lo que señala la normativa aplicable en la materia y/o buenas prácticas o leyes internacionales. Actividades de control: 66. 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. 67. El registro del consentimiento del representante legal. 68. Todas las que aplican al control "Políticas y/o procedimientos para la recolección y uso de datos personales".
D4.5	Políticas y/o procedimientos para la disociación de los datos personales	*Control* Disponer en los procesos o políticas establecidos para disociar los datos personales un protocolo que permita eliminar o reducir al mínimo los riesgos de re-identificación de los datos personales. Actividades de control: 69. Cláusulas que especifiquen claramente los casos en los que los responsables deben disociar los datos personales 70. Evidencia de la implementación de controles para la disociación 71. Periodos de verificación de los controles implementados 72. Uso o implementación de alguno de los siguientes mecanismos:

Tabla 1. Dominios y objetivos de control

		• Aleatorización: adición de ruido, permutación, privacidad diferencial. • Generalización: Agregación y anonimato k, Diversidad l y proximidad t.
D4.6	Políticas y/o procedimientos para la calidad de los datos personales	*Control* Las políticas o procedimientos deben incluir la forma en que los propietarios aseguran la calidad de los datos recabados. Actividades de control: 73. Minimizar el tratamiento manual de los datos personales. 74. Utilizar elementos de tecnológicos de captura que permita recabar los datos personales sin transcribirlos. 75. Validación de la completitud y exactitud de los datos personales capturados antes de su almacenamiento en la base de datos. 76. Corroborar con el titular la correcta captura de sus datos personales.
D4.7	Políticas y procedimientos para el uso de datos personales (finalidades primarias y secundarias)	*Control* Las políticas y procedimientos deben asegurar el uso adecuado de los datos personales, durante todo su ciclo de vida, y en los que se especifique la identificación del tipo de finalidad (primarias y secundarias). Actividades de control: 77. La recolección, almacenamiento, uso, circulación o supresión de los datos personales por parte de la organización. 78. El aviso de privacidad de conformidad con lo establecido en la normativa aplicable 79. Derechos de los titulares y procedimientos para su ejercicio 80. Cumplimiento a los Deberes de seguridad que garanticen su integridad, disponibilidad y confidencialidad

Tabla 1. Dominios y objetivos de control

		81. Para finalidades secundarias: • Cláusulas que señalen los mecanismos para la protección y uso de los datos personales en casos como investigaciones, auditorías o minería de datos, por mencionar algunos, y en cuáles se debe dar aviso a los titulares. • Procedimientos con información necesaria para dar el aviso a los titulares, cuando se determine que el propósito del tratamiento de los datos personales es distinto a los fines primarios.
D4.8	Políticas y/o procedimientos para obtener el consentimiento de forma válida	*Control* Los mecanismos o procedimientos deben 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 debe llevar a cabo. Actividades de control: 82. El consentimiento libre, previo, expreso e informado de los titulares. 83. Los diferentes mecanismos y formas para obtener la autorización, garantizando que en todo momento sea posible rectificar dicha autorización. 84. El mantenimiento de los registros físicos o tecnológicos de la obtención del consentimiento. 85. En caso de existir excepciones, deben ser señaladas de manera explícita.
D4.9	Políticas y procedimientos para la supresión y/o bloqueo de datos personales	*Control* Los procedimientos o políticas deben integrar los métodos empleados para la supresión segura, o bloqueo en su caso, de

Tabla 1. Dominios y objetivos de control

		los datos personales, tanto en medios físicos como digitales. Actividades de control: 86. Un proceso de identificación de los soportes documentales que contengan datos personales 87. Las características del medio de almacenamiento para conocer la capacidad de recuperación de los datos personales 88. Las diferentes técnicas de supresión segura con base en los soportes documentales, que especifique el algoritmo utilizado. 89. Las herramientas para la supresión de la información y la validación de no recuperación 90. La destrucción de los metadatos asociados a los datos personales 91. Registros de auditoria generados durante el proceso de supresión segura. 92. Documentación del proceso de supresión (recolección, transporte, destrucción, emisión de informe) El control debe considerar para el bloqueo: 93. Definir los métodos para limitar el tratamiento de los datos personales 94. Impedir el acceso de los usuarios a los datos personales seleccionados para bloqueo. 95. Retirar temporalmente los datos publicados de un sitio de internet 96. Definir los medios técnicos utilizados para que los datos personales no sean objeto de operaciones de tratamiento o modificaciones posterior al bloqueo. 97. Indicar de forma clara en el sistema que el tratamiento de los datos personales está limitado.

Tabla 1. Dominios y objetivos de control

D4.10	Protección de datos personales en el uso de cookies y mecanismos de rastreo y localización	*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: 98. Políticas o normas generales sobre el uso de cookies o geolocalización. 99. Procedimientos para solicitar, por parte del titular de los datos, su desactivación. 100. Guía sobre tipo de cookies utilizadas 101. Evidencia del cumplimiento de las siguientes obligaciones: • Principio de información • Obtención de consentimiento • Responsabilidades en el uso de las cookies
D4.11	Políticas y/o procedimientos para la protección de datos personales en el uso de dispositivos móviles personales en el lugar de trabajo (BYOD)	*Control* Las políticas de uso de dispositivos móviles personales deben contener la implementación de controles que protejan la información contra un incidente de datos personales. Actividades de control: 102. Análisis de riesgos de los dispositivos portátiles utilizados (SmartPhones, computadoras portátiles, discos duros, USB, etc.). 103. Registro de los dispositivos móviles que serán utilizados. 104. Especificación de las medidas de seguridad físicas, técnicas y administrativas. 105. Autorización de uso de dispositivos móviles personales en el lugar de trabajo.

Tabla 1. Dominios y objetivos de control

D4.12	Protección de datos personales para la revelación de información a las autoridades	*Control* La 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: 106. Inclusión de cláusulas en las políticas, protocolos o procedimientos que definan: ○ las medidas de seguridad físicas técnicas y administrativas -con base en el riesgo del datado- para guardar la confidencialidad e integridad de la información, ○ 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 los 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: 107. Identificación de propietarios, custodios y usuarios de cada proceso que trate datos personales. 108. Asignación de responsabilidades en el tratamiento de los datos personales en función del rol identificado. 109. Integración de los roles y responsabilidades en los

Tabla 1. Dominios y objetivos de control

		procedimientos, protocolos, lineamientos, convenios, contratos o cualquier otro instrumento establecido que haga referencia al tratamiento del dato personal.
D4.14	Políticas para el uso de procesos automatizados de tratamiento de datos personales para la elaboración de perfiles	*Control* Cuando los datos personales sean utilizados en la elaboración de perfiles, se debe comunicar al titular de los datos sobre todas 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: 110. Cláusulas referentes a la licitud del tratamiento 111. Procedimientos para informar al titular de los datos personales sobre la elaboración de perfiles 112. En caso de que un encargado realice el tratamiento, considerar todos los controles requeridos para el encargado. 113. Autorización expresa del titular para el tratamiento. 114. Especificar los procedimientos matemáticos o estadísticos empleados para la elaboración de perfiles. 115. Aplicar las medidas técnicas y administrativas para garantizar la que no existan inexactitudes en los datos personales 116. Disponer de un procedimiento para verificar que los perfiles generados no tengan efectos discriminatorios en los titulares, debido al uso de datos sensibles.

Tabla 1. Dominios y objetivos de control

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: 117. Cláusulas que especifiquen la obtención y tratamiento limitados a los supuestos y categorías de datos que resulten necesarios. 118. Considerar todos los controles requeridos para la gestión de la seguridad en el tratamiento de los datos personales.
D4.16	Políticas y/o procedimientos para la conservación de registros de actividades de tratamiento	*Control* Mantener políticas o procedimientos que indiquen claramente el periodo de conservación de los registros o archivos de bitácoras de acceso a datos personales de los sistemas de tratamiento manuales o automatizados. Actividades de control: 119. Medidas de seguridad para garantizar la disponibilidad, confidencialidad e integridad de los registros y de sus copias de seguridad. 120. Tiempos de conservación de los registros o bitácoras.
Dominio 5. Protección de datos personales de los recursos humanos		
Objetivo: Determinar las acciones mínimas para que los datos personales recabados, relacionados con el personal de la organización, independientemente de su tipo de contratación, sean debidamente tratados		
D5.1	Códigos de conducta organizacional que incluya	*Control*

Tabla 1. Dominios y objetivos de control

	aspectos de protección de datos personales	La obligación de salvaguardar los datos personales a los que el personal tienen acceso como parte de sus funciones de trabajo debe integrarse en los estatutos correspondientes. Actividades de control: 121. La obligación de la protección de los datos personales de las áreas responsables de administración del personal. 122. Sanciones por el incumplimiento de la protección de los datos personales. 123. Descripción de mecanismos para informar a las áreas responsables de administración del personal los roles y responsabilidades de protección de datos personales. 124. Mecanismos para que, el personal que esté involucrado en el tratamiento de los datos personales del personal guarde la confidencialidad antes, durante y después de realizada la contratación
D5.2	Políticas de protección de datos personales en los contratos del personal	*Control* Los contratos celebrados con el personal, con independencia del tipo de contratación y temporalidad, deben incluir cláusulas que detallen la responsabilidad adquirida con respecto a los datos personales. Actividades de control: 125. Inclusión de responsabilidades generales y específicas (de acuerdo con el puesto) de quienes tratarán datos personales. 126. Acciones disciplinarias y sanciones en caso de incumplir alguna de las cláusulas o infringir la legislación y normatividad aplicable.

Tabla 1. Dominios y objetivos de control

		127. Verificación de las referencias. 128. Firmas de acuerdos de confidencialidad. 129. Responsabilidades posteriores al término de la relación laboral.
D53	Procedimientos de protección de datos personales en los expedientes de contratación	*Control* Integrar disposiciones para la recolección, uso, acceso, retención y seguridad de los expedientes físicos y electrónicos del personal. Actividades de control: 130. Especificaciones de las medidas de seguridad físicas, técnicas y administrativas para garantizar la confidencialidad, integridad y disponibilidad de los expedientes físicos y electrónicos del personal contratado. 131. Cláusulas que especifiquen guardar la confidencialidad de los datos personales recabados. 132. Consentimiento válido 133. Especificar de manera clara las excepciones al consentimiento. 134. Verificación de atención del criterio de minimización.
D5.4	Avisos de privacidad relacionado con la contratación del personal	*Control* Generar avisos de privacidad que especifiquen de qué forma la organización recabará, usará y procesará los datos del personal, así como el tipo de categorización asignada a los mismos. Actividades de control: 135. Disponer de avisos de privacidad para el tratamiento de los datos personales de los empleados cumpliendo todos los requisitos de la normativa en la materia.

Tabla 1. Dominios y objetivos de control

D5.5	Políticas de protección de datos en las prácticas de monitoreo de empleados y en el uso de sistemas de video-vigilancia	*Control* Se deben especificar las finalidades en caso de requerirse 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. Actividades de control: 136. Disponer de un aviso de privacidad para el monitoreo de empleados y el uso de sistemas de video-vigilancia. 137. Contar con una evaluación de impacto. 138. Especificar las pautas de conducta de los empleados en los diferentes medios de comunicación organizacionales 139. Actualización de las políticas, en caso de existir, que atiendan a la normativa actual de protección de datos personales. 140. La especificación clara de los fines que justifican el monitoreo. 141. El momento y circunstancias por las cuales se hará uso de la información obtenida del monitoreo y de los sistemas de video-vigilancia.
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:

Tabla 1. Dominios y objetivos de control

		142. Cláusula que especifique la protección de los datos personales en las directrices o políticas de seguridad de la información organizacional. 143. Evidencia de la 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: 144. Referencia al estándar, framework o buena práctica del control implementado. 145. Evidencia de la revisión de los controles por parte de las áreas responsables de seguridad de la información. 146. Descripción de las medidas de seguridad, especificando el riesgo de datos personales que tratan 147. Eficiencia del control implementado.
D6.3	Medidas de seguridad administrativas	*Control* Tener debidamente identificadas, implementadas y monitoreadas las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales. Actividades de control: 148. Referencia al estándar, framework o buena práctica del control implementado. 149. Evidencia de la revisión de los controles por parte de las áreas

Tabla 1. Dominios y objetivos de control

		responsables de seguridad de la información. 150. Descripción de las medidas de seguridad, especificando el riesgo que tratan. 151. Eficiencia del control implementado.
D6.4	Medidas de seguridad técnicas	*Control* Tener debidamente identificadas, implementadas y monitoreadas las acciones 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: 152. Referencia al estándar, framework o buena práctica del control implementado. 153. Evidencia de la revisión de los controles por parte de las áreas responsables de seguridad de la información. 154. Descripción de las medidas de seguridad, especificando el riesgo que tratan. 155. Eficiencia del control implementado.
D6.5	Auditorías de seguridad de la información que incluya 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: 156. Disponer de un plan de auditoría de seguridad de la información 157. La inclusión, dentro del alcance del plan de auditoría de seguridad de la información, de los datos personales que son tratados

Tabla 1. Dominios y objetivos de control

		158. Evidencia de la ejecución de las auditorías. 159. De existir no conformidades relacionadas con datos personales, contar con evidencia de su atención.
D6.6	Análisis de brecha de seguridad de los datos personales	*Control* Se deben ejecutar análisis de brecha de las medidas de seguridad de los datos personales existentes y efectivas, las faltantes o nuevas, en su caso y contar con la evidencia de ello. Actividades de control: 160. Definición de un estándar o marco internacional u organizacional de seguridad de la información para la aplicación del análisis de brecha. 161. Documentación de la aplicación del análisis de brecha por lo menos cada dos años. 162. Identificación las medidas de seguridad aplicables con base en el marco de referencia. 163. Identificación las medidas de seguridad existentes con base en el marco de referencia. 164. Identificación de la brecha de las medidas de seguridad.
D6.7	Análisis de riesgos de los datos personales	*Control* Llevar a cabo la ejecución de análisis de riesgos de los datos personales tratados durante su ciclo de vida, y contar con la evidencia de ello. Actividades de control: 165. Especificación de requerimientos regulatorios, códigos de conducta, mejores prácticas del sector específico 166. Los datos personales previamente clasificados.

Tabla 1. Dominios y objetivos de control

		167. El diagrama de ciclo de vida de los datos personales 168. Los activos involucrados en el tratamiento de los datos personales 169. Las consecuencias negativas para los titulares que pudieran derivar en una vulneración 170. Cantidad datos personales por titular y número de titulares 171. Metodología empleada para llevar a cabo el análisis de riesgos 172. Informe de la evaluación del riesgo.
D6.8	Plan de trabajo	*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: 173. Implementación de medidas de seguridad a corto, mediano y largo plazo, especificando el riesgo que mitigan. 174. El plan debe especificar: tiempos, recursos, áreas responsables para tratar el riesgo. 175. Priorización de las medidas de seguridad a implementar atendiendo a los análisis de riesgos y brecha. 176. Periodos de revisión del avance de la implementación de las medidas de seguridad. 177. Evidencia de la implementación de las medidas de seguridad.
D6.9	Documento de seguridad	*Control* Disponer de un documento de seguridad que incorpore el resumen de todas las medidas de seguridad implementadas. Actividades de control:

Tabla 1. Dominios y objetivos de control

		178. El inventario de datos personales y de los sistemas de tratamiento 179. Las funciones y obligaciones de las personas que tratan datos personales 180. El análisis de riesgos 181. Análisis de brecha 182. El plan de trabajo 183. Los mecanismos de monitoreo y revisión de las medidas de seguridad 184. El programa integral de capacitación
Dominio 7. Riesgos con encargados		
Objetivo: Verificar que los encargados protejan los datos personales bajo su resguardo		
D7.1	Políticas de cumplimiento de protección de datos personales para encargados	*Control* Disponer de políticas que establezcan puntualmente los requerimientos que deben cumplir los terceros o encargados al realizar el tratamiento de los datos personales. Actividades de control: 185. Descripción de obligaciones de protección de datos personales que debe cumplir el encargado. 186. Firma de convenios de confidencialidad de los empleados del encargado que participen en el tratamiento de los datos personales y de su adhesión al código de conducta de la organización. 187. Notificación de las vulneraciones 188. La disponibilidad para la atención de requerimientos del Órgano Garante y otras autoridades. 189. Auditorías de protección de datos personales para verificar su cumplimiento.
D7.2	Procesos de debida diligencia (*due diligence*) en las prácticas de protección de datos con encargados	*Control* Los terceros/encargados deben contar con certificaciones o similares en protección de datos personales -o al menos en seguridad

Tabla 1. Dominios y objetivos de control

		de la información- antes de llevar a cabo la contratación. Actividades de control: 190. Evidencia de certificaciones de seguridad o de protección de datos personales del encargado o del personal 191. Evidencia de cumplimiento de la legislación y normatividad aplicable en materia de protección de datos personales nacional o internacional (en caso de aplicar) 192. Registros de incidentes de seguridad y/o vulneraciones que el encargado haya presentado. 193. Evidencia de la investigación de fuentes externas acerca de la ocurrencia de incidentes de seguridad y/o vulneraciones.
D7.3	Políticas de contratación de prestadores de servicios de cómputo en la nube	*Control* Los prestadores de servicios de cómputo en la nube deben garantizar políticas de protección de datos personales. Actividades de control: 194. Que el encargado cuente con políticas de protección de datos personales afines a los principios y deberes de la normativa aplicable en la materia y su evidencia de aplicación 195. Especificaciones de la existencia de subcontrataciones relacionadas con la información sobre la que se presta el servicio 196. No incluir condiciones que autoricen o permitan asumir la titularidad o propiedad de la información sobre la que se presta el servicio

Tabla 1. Dominios y objetivos de control

		197. Evidencia de mecanismos para guardar la confidencialidad de los datos personales 198. Mecanismos definidos para dar a conocer cambios en sus políticas de privacidad o condiciones del servicio 199. Especificaciones de las medidas de seguridad para la protección de los datos personales 200. Mecanismos definidos para garantizar la supresión de los datos personales una vez concluido el servicio prestado. 201. Especificar el establecimiento de mecanismos de control de acceso a los datos personales. 202. La generación de la evidencia referente a los accesos a los datos personales a terceros: • Solicitud fundada y motivada de autoridad competente • Informes de acceso al responsable 203. Requisitos de cumplimiento de las normas nacionales sobre protección de datos personales 204. Requisitos de cumplimiento de las políticas organizacionales 205. Formación y educación de los empleados del encargado sobre protección de datos personales 206. Exigencia de cumplimiento a las políticas de tratamiento establecidas por la organización para subcontratistas 207. Acuerdos de cumplimiento de las políticas de la organización por parte del encargado
D7.4	Procedimientos para determinar acciones por incumplimiento contractual	*Control* Contar con procedimientos o guías que ayuden a determinar si existe incumplimiento a lo establecido para la

Tabla 1. Dominios y objetivos de control

		protección de los datos personales en los contratos celebrados con los encargados. Actividades de control: 208. Especificaciones de las causas de incumplimiento 209. La normativa aplicable 210. Tipos de sanciones
D7.5	Auditorías de debida diligencia sobre prácticas de protección de datos con encargados	*Control* Objetivo: 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: 211. Plan de auditorías internas y/o externas que integre: o Personas responsables de la ejecución de la auditoría o Temporalidad de las auditorías o Cualificaciones de los auditores en materia de protección de datos personales o Presentación del informe de la auditoría 212. Seguimiento al cumplimiento de las no conformidades. 213. 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 Ley para dar cumplimiento al principio de información.		
D8.1	Procedimientos para generar avisos de privacidad	*Control* Disponer de procedimientos para que la organización elabore sus avisos de

Tabla 1. Dominios y objetivos de control

		privacidad con los requisitos de la normatividad aplicable. Actividades de control: 214. Señalar qué datos requieren la obtención del consentimiento de manera previa 215. Señalar qué datos requieren la obtención del consentimiento de forma expresa o tácita, incluidos los datos personales que son obtenidos indirectamente 216. En caso de requerirse consentimiento, este de ser solicitado de forma concisa y redactado con claridad. 217. Informar: o las características del tratamiento de los datos personales, o los alcances y condiciones generales del tratamiento a que serán sometidos los datos personales, o los mecanismos, medios y procedimientos habilitados para atender las solicitudes para el ejercicio de los derechos ARCO. o el o los medios a través de los cuales se hará del conocimiento del titular el aviso de privacidad simplificado o integral.
D8.2	Avisos de privacidad con el detalle sobre el manejo de los datos personales (integral)	*Control* Los avisos de privacidad integrales deben incluir todos los elementos que detalla la normativa aplicable. Actividades de control: 218. El sitio, lugar o mecanismo implementado para conocer el aviso de privacidad integral. 219. Información al titular de las transferencias nacionales e

Tabla 1. Dominios y objetivos de control

		internacionales que no requieran de su consentimiento indicando: ○ los destinatarios o terceros receptores, ○ finalidades de las transferencias y ○ el fundamento legal. 220. El domicilio completo, que incluya: la calle, numero, colonia, ciudad, municipio o delegación, código postal y entidad federativa (es posible incluir otros datos de contacto). 221. Los tipos de datos personales que se recaban, distinguiéndolos expresamente de los datos personales de carácter sensible. 222. 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. 223. Información sobre los mecanismos, medios y procedimientos habilitados para atender las solicitudes de los derechos ARCO.
D8.3	Aviso de privacidad con el resumen sobre el manejo de los datos personales (simplificado)	*Control* Los avisos de privacidad simplificados deben incluir todos los elementos que detalla la normativa aplicable. Actividades de control: 224. Denominación completa del responsable 225. 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,

Tabla 1. Dominios y objetivos de control

		○ ser específicas y redactadas con claridad ○ identificación de las finalidades que requieran el consentimiento del titular y las que no. 226. Identificación de las transferencias que requieran el consentimiento del titular. 227. Incluir o informar sobre mecanismos y medios para manifestar la negativa del tratamiento por parte del titular.
D8.4	Disposición del aviso de privacidad en todos los puntos de recolección de datos personales	*Control* Poner a disposición los avisos de privacidad en todos los puntos a través de los cuales se lleva a cabo la recolección de los datos. Actividades de control: 228. Evidencia de la disposición al titular del aviso de privacidad simplificado 229. Evidencia de la publicación del aviso de privacidad de manera permanente. 230. Evidencia de la disposición al titular del nuevo aviso de privacidad cuando: cambie su identidad, requiera recabar datos personales sensibles adicionales, cambie las finalidades, modifique las condiciones o realice trasferencias no previstas. 231. Disposición del aviso de privacidad en diferentes formatos: • físicos • electrónicos • sonoros • audiovisuales • braille • otra tecnología que permita su comunicación eficaz 232. Disposición del aviso de privacidad en lenguas indígenas • náhuatl

Tabla 1. Dominios y objetivos de control

		• mixteco • otomí • mazateco • zapoteco • mazahua
D8.5	Disposición de los avisos de privacidad en medios visibles	*Control* Los avisos de privacidad deben colocarse en todos los puntos a través en los cuales se lleva a cabo la recolección de los datos personales. Actividades de control: Para medios electrónicos: 233. Aviso de privacidad integrales en páginas web, chats, redes sociales con ligas accesibles y visibles y/o ventanas emergentes 234. Aviso de privacidad simplificado en espacios visibles en páginas web, chats, redes sociales, ventanas emergentes Para medios físicos: 235. Carteles con letra legible 236. Ubicación del aviso de privacidad en lugares accesibles para personas en sillas de ruedas o de baja estatura. Para ambos casos (integrales o simplificados), considerar: 237. Evidencia que demuestre el cumplimiento, como: • manuales de procedimientos, • grabaciones telefónicas, • fotografías, • fe de hechos o • firmas de los titulares, otros.

Tabla 1. Dominios y objetivos de control

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: 238. 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: 239. Integración en las capacitaciones/sensibilizaciones del personal de nuevo ingreso información referente a los avisos de privacidad 240. Capacitación especializada sobre la conformación del aviso de privacidad al personal que por sus funciones tiene contacto directo con los titulares de los datos. 241. Inclusión en los scripts de la información referente al aviso de privacidad 242. Disponer de material de reforzamiento: • Manuales • infografías • cursos virtuales • folletos

Tabla 1. Dominios y objetivos de control

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: 243. Motivos por los cuales el responsable hará uso de medidas compensatorias de comunicación masiva u otros mecanismos de amplio alcance 244. Las modalidades para la aplicación de medidas compensatorias y sus procedimientos de instrumentación 245. 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, o • Cualquier otro medio alterno de comunicación masivo 246. Criterios para seleccionar el medio para difundir el aviso de privacidad 247. Los criterios para la publicación del aviso de privacidad en los diferentes medios de comunicación
Dominio 9. Solicitudes ARCO		
Objetivo: Verificar que la organización dispone de procedimientos que provean eficiencia al proceso de atención a solicitudes ARCO.		
D9.1	Procedimientos o guías para atender solicitudes o proveer	*Control*

Tabla 1. Dominios y objetivos de control

	mecanismos para que los titulares ejerzan sus derechos de acceso, rectificación, cancelación y oposición de datos personales	Contar con procedimientos conocidos y accesibles para la atención de las solicitudes ARCO. Actividades de control: 248. Requisitos para la presentación de una solicitud de ejercicio de derechos ARCO. 249. Plazos y procedimientos para la atención de las solicitudes. 250. Medios de entrega de información a los titulares. 251. Instancias responsables de garantizar el ejercicio de los derechos ARCO. 252. En qué consisten los derechos ARCO. 253. Causales de no procedencia. 254. Modalidades y costos. 255. Medios de defensa. 256. Atención de dudas respecto al ejercicio de los derechos por parte del responsable.
D9.2	Procedimientos para responder solicitudes relacionadas con el derecho al olvido	*Control* Contar con procedimientos conocidos y accesibles que den respuesta a las solicitudes relacionadas con el derecho al olvido. Actividades de control: 257. Requisitos para la presentación de una solicitud de derecho al olvido 258. Plazos y procedimientos 259. En qué consiste el derecho al olvido 260. Condiciones para ejercer el derecho 261. Causales de no procedencia 262. Atención de dudas respecto al ejercicio del derecho al olvido

Tabla 1. Dominios y objetivos de control

D9.3	Procedimientos para responder solicitudes sobre portabilidad de datos personales	*Control* Contar con procedimientos conocidos y accesibles que den respuesta a las solicitudes sobre la portabilidad de datos personales. Actividades de control: 263. En qué consiste la portabilidad de datos personales 264. Causales de no procedencia 265. Atención de dudas respecto al ejercicio del derecho al olvido 266. Requisitos para la presentación de una solicitud de portabilidad de datos personales 267. Plazos 268. Pasos a seguir de forma detallada 269. Medios de entrega de la información y formato (audio, imagen, texto base de datos, video, etc).
D9.4	Procedimientos para la revocación de los datos personales	*Control* Contar con procedimientos que den respuesta a las solicitudes de los titulares sobre la revocación del consentimiento para el tratamiento de los datos personales. Actividades de control: 270. Personas facultadas para solicitar la revocación del consentimiento al tratamiento de los datos personales. 271. Pasos a seguir de forma detallada. 272. Tiempo de atención a la solicitud. 273. Tiempo para aplicar la revocación. 274. Causas por las cuales puede negarse la revocación. 275. Medio usado para la revocación sencillo y gratuito. 276. Formato de solicitud o ejemplo.

Tabla 1. Dominios y objetivos de control

		277. Instrucciones de llenado del formato o solicitud de ejemplo. 278. 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.
D9.5	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: 279. Personas facultadas para solicitar el recurso de revisión 280. Documentos de acreditación 281. Tiempo de atención a la solicitud 282. Proceso de cumplimiento y plazos 283. Causales de procedencia 284. Requisitos del escrito de recurso de revisión 285. Medios de presentación 286. Formato de solicitud o ejemplo 287. Instrucciones de llenado del formato o solicitud de ejemplo 288. Medios de impugnación
Dominio 10. Evaluaciones de impacto en la protección de datos personales		
Objetivo: Verificar que los riesgos a los que están expuestos los datos personales cuentan con una estrategia de tratamiento de riesgos.		
D10.1	Evaluaciones de Impacto en la Protección de Datos (EIPDs) para nuevos programas, sistemas y procesos	*Control* Para llevar a cabo las evaluaciones de impacto, se debe contar con un instrumento mediante el cual se valoren los impactos reales respecto de determinado tratamiento, a efecto de identificar y mitigar posibles riesgos relacionados con los principios,

Tabla 1. Dominios y objetivos de control

		deberes y derechos de los titulares previstos en la normativa aplicable. Actividades de control: 289. Integración de una cláusula de ejecución de EIPDs dentro de la política de protección de datos personales organizacional. 290. Evidencia de la ejecución de EIPDs. 291. Contar con un procedimiento o guía para llevar a cabo EIPDs.
D10.2	Procedimientos o guías para llevar a cabo EIPDs	*Control* Disponer de un procedimiento que permita homologar el proceso y presentación de las EIPDs. Actividades de control: 292. Qué es un tratamiento intensivo o relevante de datos personales. 293. Casos en los que se debe realizar una EIPD. 294. Elementos mínimos que debe incluir una EIPD establecidos por la normatividad aplicable. 295. Descripción de la metodología 296. Formatos o guías de apoyo.
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: 297. Inclusión en cláusulas contractuales de la cooperación del encargado en la ejecución de EIPDs.
Dominio 11. Gestión de vulneraciones		

Tabla 1. Dominios y objetivos de control

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 de la seguridad de datos personales	*Control* Para la atención de las vulneraciones a la seguridad de los datos personales se debe disponer de planes de respuesta a estos incidentes. Actividades de control: 298. Un Plan de respuesta separado o integrado a los planes de respuesta de atención de incidentes de seguridad de la información. 299. Procedimientos para identificar, escalar las vulneraciones de seguridad de datos personales a la unidad administrativa correspondiente. 300. Identificación de las vulneraciones a las que están expuestas los datos personales. 301. Roles y responsabilidades para la atención de las vulneraciones. 302. Recolección y preservación de evidencia. 303. Descripción de las actividades de atención de la vulneración (análisis, contención, erradicación, recuperación). 304. Protocolo de notificación de una vulneración a órganos en materia de transparencia, al Órgano Garante y a los titulares, cuando corresponda.
D11.2	Verificación, revisión y evaluación del Plan de Respuesta a vulneraciones de	*Control* Establecer los periodos de verificación, revisión y evaluación de los planes de respuesta a incidentes de datos personales,

Tabla 1. Dominios y objetivos de control

	la seguridad de datos personales	así como la evidencia para demostrar las actividades realizadas. Actividades de control: 305. Documento que acredite las verificaciones, revisiones y evaluaciones por parte de órganos en materia de transparencia, que contenga: 306. Fecha de la verificación, revisión y evaluación. 307. Responsable (nombre y cargo) 308. Firmas 309. Descripción del resultado de las verificaciones, revisiones y evaluaciones.
D11.30	Protocolo de notificación (a los titulares afectados) y de reportes (a las autoridades de protección de datos) sobre vulneraciones	*Control* Contar con un protocolo que defina la forma, medios e información a difundir como parte de la notificación de incidentes a los titulares afectados y las autoridades correspondientes. Actividades de control: 310. Establecimiento de tiempos para la notificación. 311. Medios oficiales para la notificación. 312. Asignación del responsable de las notificaciones y reportes de las vulneraciones (contacto único de comunicación). 313. Información requerida en la notificación.
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:

Tabla 1. Dominios y objetivos de control

		314. Fecha en que ocurrió la vulneración. 315. El motivo. 316. Las acciones correctivas implementadas de forma inmediata. 317. Las acciones correctivas implementadas de forma definitiva. 318. Las acciones preventivas que, en su caso, puedan ser implementadas para vulneraciones posteriores. 319. Las consecuencias de la vulneración.
Dominio 12. Monitoreo de la protección de los datos personales		
Objetivo: Verificar la adecuada gestión en la protección de los datos personales con base en lo establecido en el sistema de gestión.		
D12.1	Revisiones internas y autoevaluaciones del sistema de gestión de datos personales	*Control* Generar un calendario que indique las fechas de las revisiones del sistema de gestión de datos personales, considerando las autoevaluaciones que permitan identificar el cumplimiento de la protección de los datos personales. Actividades de control: 320. Un plan de auditorías de verificación del sistema de gestión. 321. Plan de trabajo para la atención de las no conformidades. 322. Revisiones por parte del CT del cumplimiento de las no conformidades.
D12.2	Mecanismos de verificaciones y revisión integrales (monitoreo y supervisión) de las políticas, planes, procesos, y procedimientos para la protección de los datos personales	*Control* Revisar los procesos actuales, al menos una vez al año, o cuando exista un cambio en la normatividad aplicable, para asegurar que reflejan los nuevos requerimientos. Actividades de control:

Tabla 1. Dominios y objetivos de control

		323. Un plan de auditorías para las políticas, planes, procesos, y procedimientos para la protección de los datos personales. 324. Plan de trabajo para la atención de las no conformidades. 325. Revisiones por parte del CT.
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: 326. Documentos probatorios de revisiones independientes de la protección de datos personales. 327. Plan de trabajo para atención de las recomendaciones. 328. Revisiones al proceso de atención de las recomendaciones por parte del CT.
D12.4	Atención de dudas y quejas de los titulares	*Control* Definir procedimientos para recibir y responder dudas y quejas de los titulares para cumplir con el principio de responsabilidad. Actividades de control: 329. Procedimientos para recibir y responder las dudas y quejas de los titulares. 330. Preguntas y respuestas frecuentes para los titulares.
Dominio 13. Cumplimiento normativo		
Objetivo: Verificar y generar evidencia del cumplimiento de la normatividad en la materia con base en el principio de responsabilidad.		

Tabla 1. Dominios y objetivos de control

D13.1	Identificación de cambios regulatorios y de cumplimiento	*Control* Impactar los cambios en la normatividad aplicable en los procedimientos, procesos y evidencia generada para demostrar el cumplimiento de la protección de datos personales. Actividades de control: 331. La normatividad aplicable para tratar los datos personales de acuerdo con las atribuciones o facultades. 332. Investigaciones continuas sobre cambios regulatorios 333. Suscripciones a asociaciones nacionales e internacionales sobre protección de datos personales.

BIBLIOGRAFÍA

(26 de enero de 2017). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. Ciudad de México, México.

Acosta, D. (15 de May de 2017). *ISO/IEC 29100:2011 – Una introducción al marco de trabajo de privacidad para la protección de información de identificación personal (PII)*. Recuperado el 17 de enero de 2019, de David E. Acosta2017: https://www.deacosta.com/isoiec-291002011-una-introduccion-al-marco-de-trabajo-de-privacidad-para-la-proteccion-de-informacion-de-identificacion-personal-pii/

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.

Article 29 Working Party. (July 2010). *Opinion 3/2010 on the principle of accountability. 00062/10/EN WP 173.* Article 29 Data Protection Working Party.

Asamblea Geneal de la ONU. (14 de diciembre de 1990). *Principios rectores para la reglamentación de los ficheros computarizados de datos personales. Resolución 45/95.* Recuperado el 11 de octubre de 2018, de Orden Jurídico: http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf

BSI Group. (s.f.). *Introducción al Anexo SL. La nueva estructura de alto nivel para todas las futuras normas de sistemas de gestión.* Recuperado el 8 de novimbre de 2017, de BSI Group: https://www.bsigroup.com/LocalFiles/es-ES/Documentos%20tecnicos/Revisiones%20ISO/ISO%209001/BSI-Anexo%20SL-ISO-9001-2015.pdf

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

de la Peña Santillán, M. (2010). *Gestión del Conocimiento. El Modelo de Gestión de Empresas del Siglo XXI.* eSPAÑA: Netbiblio.

Deming, E. (2010). *PDSA Cycle*. Recuperado el 20 de febrero de 2019, de The W. Edwards Deming Institute: https://deming.org/explore/p-d-s-a

EDPS. (2016). *Opinión 9/2016. Opinion on Personal Information Management System.* Marrakesh: European Data Protection Supervisor (EDPS).

EDPS. (s.f.). *Personal Information Management System*. Recuperado el 18 de agosto de 2019, de European Data Protection Supervisor: https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en

Giraldo Giraldo, R. A. (2017). *Mejoramiento del proceso de compras de la constructura 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

Heras Saizarbitoria, I., Bernardo, M., & Casadesús Fa, M. (diciembre de 2008). La integración de Sistemas de Gestión basados estándares internacionales: resultado de un estudio empírico realizado en la CAPV. *Rvista de Dirección y Administración de Empresas*(14), 155-174.

ICTEA. (s.f.). *¿Qué es una Infraestructura Digital o 'Framework'?* Recuperado el 2 de septiembre de 2019, de W-ictea: http://www.ictea.com/cs/index.php?rp=/knowledgebase/8991/Que-es-una-Infraestructura-Digital-o-andsharp039Frameworkandsharp039.html

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

INAI. (2019). Parámetros de mejores prácticas en materia de protección de datos personales del sector público. México.

ISACA. (2017). *Implementing a Privacy Protection Program: Using COBIT 5 Enablers wirh the ISACA Privacy Principles.* Ilinois.

ISO. (15 de 01 de 2014). International Standard ISO/IEC 27000. *Information technology-Security techniques - Information scurity management systems - Overview and vocabulary*. Switzerland.

ISO. (s.f.). *ISO/IEC 27000 family - Information security management systems.* Recuperado el 24 de octubre de 2018, de ISO International Organization for Standardization: https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC 11179-1:2004 (e). (2004). *Information technology-Metadata registries (MDR). Part 1: Framework*. Switzerland.

ISO/IEC. (15 de diciembre de 2011). Information technology - Security techniques - Privacy frameworks. *Internatoinal Standard ISO/IEC 29100*. Suiza.

ISO/IEC. (2015). ISO/IEC Directives, Part 1. . *Consolidated ISO Supplement - Procedires specific to ISO*. Recuperado el 3 de diciembre de 207, de DV BENCHMARK.

ISO/IEC 27001. (1 de octubre de 2013). *Information technology -Security techniques - Information security management sistems - Requirements*. Switzerland.

ISO/IEC 27002. (1 de octubre de 2013). *Information technology - Security techniques - Code of practice for information security controls*. Switzerland.

ISO/IEC 27701. (agosto de 2019). *Security techiques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*. Switzerland.

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

ISO27000.ES. (s.f.). *Portal del ISO 27001 en Español*. Recuperado el 28 de marzo de 2019, de http://iso27000.es/iso27000.html

Kaplan, R., & Norton, D. (January de 2008). *Mastering the Management System*. Recuperado el 24 de marzo de 2018, de Harvard Business Review: https://hbr.org/2008/01/mastering-the-management-system

Lamas Abreu, E., & Ramos Pérez, M. (mayo de 2011). Procedimiento para el diseño de un sistema de gestión de calidad basado en un enfoque de procesos. *Contribuciones a la Economía*. Recuperado el 16 de junio de 2018, de Enciclopedia Virtual: http://www.eumed.net/ce/2011a/larp.htm

McCallister, E., Grance, T., & Scarfone, K. (April de 2010). Guide to Protecting the Confidentiality of Personally Identifiable Informatio (PII). . *NIST SP 800-122*. Recuperado el 22 de febrero de 2018, de NIST: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

Naranjo, F. (15 de 01 de 2015). *Sistemas de Gestión: Valor Estratégico de las Organizaciones*. Recuperado el 21 de octubre de 2018, de Consultoría de Gestión: http://blog.seidor.com/infraestructura/sistemas-de-gestion-valor-estrategico-de-las-organizaciones/

NYMITY. (2016). *Una aproximación estructurada a la gestión de datos personales: Manual introductorio.* Recuperado el 12 de febrero de 2018, de NYMITY: https://latam.nymity.com/~/media/NymityAura/Resources/LATAM%20Website/Una%20aproximaci%C3%B3n%20estructurada%20a%20la%20gesti%C3%B3n%20de%20datos%20personales%20%20-%20Manual.pdf

NYMITY. (s.f.). *Recursos NYMITY*. Recuperado el 12 de febrero de 2018, de NYMITY. Innovating compliance: https://latam.nymity.com/recursos.aspx

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

Red Iberoamericana de Protección de Datos. (2007). *Directrices para la armonización de la Protección de Datos en la Comunidad Iberoamericana.*

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

Szarfman, J. (Abril de 2019). *Normas ISO de Sistemas de Gestión ISO-MSS.* Recuperado el 15 de febrero de 2019, de https://www.slideshare.net/JoseSzarfman/iso-normas-de-sistemas-de-gestion

Van Lieshout, M., & Emmert, S. (2018). RESPECT4 - Privacy as Innovatn Oportunity. En M. Medina, A. Mitrakas, K. Rannenberg, E. Schweighofer, N. Tsouroulas, & (Eds.), *Privcy Technologies and Policy. 6th Annual Privacy Forum, APF* (págs. 43-60). Barcelona, Spain: Springer.