PROGRAMA DE CAPACITACIÓN

EN MATERIA DE

PROTECCIÓN DE DATOS PERSONALES

Comité de Transparencia

abril2025

INTRODUCCIÓN

Los partidos políticos, en el ejercicio de sus funciones, poseen una gran cantidad de datos personales de la ciudadanía, los cuales se encuentran protegidos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados -Ley de Datos Personales- y demás normatividad aplicable, la cual, establece una serie de obligaciones a cargo de los sujetos obligados para su cumplimiento, y en el caso concreto del Partido del Trabajo -PT-, representa un reto importante al ser un Partido Político Nacional. En ese sentido, existe la obligación y la necesidad de generar un Programa de Capacitación en Protección de Datos Personales, específico para el PT, con la finalidad de que todas y cada una de las personas militantes y colaboradoras administrativas involucradas en el tratamiento de datos personales al interior de este Instituto Político Nacional, cuenten con cierto grado de especialización que les permita garantizar la observancia de los principios rectores de la protección de los datos personales a los cuales dan tratamiento en el ejercicio de sus funciones.

OBJETIVOS

- Explicar, los conceptos clave para comprender el derecho a la protección de datos personales, entre ellos, la definición de datos personales, la importancia de su protección, en qué consiste el derecho a la protección de los datos personales y cómo se pueden ejercer los derechos ARCOP.

- Conocer los controles de seguridad para cumplir con las obligaciones en materia de protección de datos personales resultado del análisis de riesgo del Documento de Seguridad de Datos Personales del Partido del Trabajo.

- Comprender la importancia del sistema de gestión de datos personales dentro del Partido del Trabajo.

- Que las personas colaboradoras administrativas de todos los niveles en el Partido del Trabajo dimensionen la importancia que tiene el derecho a la protección de datos personales; a través de herramientas que permitan prevenir, identificar y en su caso, saber cómo actuar ante un mal uso de los datos personales; asimismo, que el tratamiento de datos personales llevado a cabo en el ejercicio de sus atribuciones garantice de manera efectiva a la población el correcto uso de su información.

- En cumplimiento de los artículos 24 fracción III, 27 fracción VIII y 29 fracción VII de la Ley de Datos Personales y los Lineamientos Generales, el Partido del Trabajo ha formulado el presente Programa de Capacitación en la materia, con una visión para el corto, mediano y largo plazo.

SOBRE EL PROGRAMA

Corto plazo

Sensibilización

Una de las primeras acciones a realizar en esta etapa, es la de sensibilizar a las personas colaboradoras administrativas en el Partido del Trabajo sobre el derecho humano consagrado en el artículo 16, párrafos primero y segundo de la Constitución Política de los Estados Unidos Mexicanos, que establece:

> *"…Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.*
>
> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros…".*

Es importante hacer del conocimiento de las personas colaboradoras administrativas en el Partido del Trabajo, sobre la importancia de este derecho concerniente a cada persona, que debe serle reconocido no solamente como una prerrogativa, sino como un derecho fundamental garantizado por el Estado, a través de mecanismos de protección idóneos.

Para lo anterior, es necesario impartir un curso de sensibilización en protección de datos personales para el Partido del Trabajo con el propósito de difundir el conocimiento sobre la protección de datos personales desde su carácter fundamental asentado en la Constitución, su alcance y contenido, de conformidad con los aspectos relevantes de la normatividad emitida en la materia.

Mediano plazo
Entrenamiento

Esta etapa tiene como objetivo principal proporcionar a las personas colaboradoras administrativas en el Partido del Trabajo las herramientas normativas y técnicas para el cumplimiento de lo establecido en la Ley de Datos Personales, haciendo énfasis en el desarrollo de las capacidades que las mismas requieren para el desempeño eficiente de sus diferentes roles y responsabilidades relacionadas con el tratamiento y seguridad de los datos personales inherentes a sus procesos de trabajo.

Para la impartición de la capacitación, se tomarán en cuenta los inventarios de datos personales realizados por las personas colaboradoras administrativas en el Partido del Trabajo, en el que se identificaron los tratamientos de datos personales que servirán de base para conformar los perfiles a capacitar en las

diferentes actividades que se tienen contempladas para esta segunda etapa.

En ese sentido, el curso de entrenamiento otorgará las personas colaboradoras administrativas en el Partido del Trabajo que realizan el tratamiento de datos personales, los conocimientos necesarios para que:

1) Identifiquen los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
2) Distingan el contenido y alcance de los derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad -ARCOP-.
3) Conozcan los objetivos y alcances en materia de medidas de seguridad para la protección de los datos personales

Largo plazo
Fortalecimiento

En una visión de largo plazo, es necesario que los esquemas y sistemas de trabajo del Partido del Trabajo, incorporen desde su diseño la protección de los datos personales y la autodeterminación informativa, como principios fundamentales, así como, que las prácticas y conductas de las personas colaboradoras administrativas, reflejen en su gestión cotidiana los valores que este derecho humano protege.

Para lograr lo anterior es necesario consolidar en el Partido del Trabajo una gestión institucional fincada en una cultura de protección de datos personales, para lo cual la capacitación es uno de los factores más influyentes en la generación de nuevos valores y perfiles de actuación en las personas colaboradoras administrativas.

Por lo anterior, se gestionará la incorporación permanente del curso de sensibilización en protección de datos personales como parte de los Cursos de Formación de las Bases de la Estructura petista, con el propósito de que la militancia lo curse obligatoriamente, a efecto de ir conformando una cultura organizacional consciente de la protección de este derecho.

Sabemos que este Programa será de gran utilidad ya que dotará de la información y las herramientas necesarias para seguir fortaleciendo la protección de los datos personales dentro del Partido del Trabajo, evitando así incumplimientos futuros o situaciones de riesgo que pudieran resultar.

ALCANCE

Aplicable a todas las personas que colaboran en el Partido del Trabajo, sea cual fuere su nivel jerárquico y

su situación en la institución; así como para las personas externas que debido a la prestación de un servicio, tengan acceso a los sistemas de protección de datos personales, que para términos del presente documento, desempeñan la función de encargadas, y quienes en la misma medida deben tener conocimiento mínimo de los conceptos de protección de datos personales que aseguren las políticas que en la materia ha implementado este instituto político para el debido resguardo de los datos personales recabados.

LA PROTECCIÓN DE LOS DATOS PERSONALES EN POSESIÓN DEL PARTIDO DEL TRABAJO

Desde la publicación de la derogada Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en el Diario Oficial de la Federación, el día 26 de enero de 2017, y de la vigente, el 20 de marzo d e2025, el Partido del Trabajo ha realizado diferentes acciones con la finalidad de garantizar el derecho de toda persona a la protección de sus datos personales que este instituto político resguarda.

De entre ellas destaca un primer acercamiento con las áreas, lo que permitió generar un inventario inicial de los datos personales recabados, así como la identificación de los activos que intervienen en su tratamiento, dando como resultado la existencia de un Documento de Seguridad de Datos Personales, el cual permite estandarizar la organización, resguardo, conservación y destrucción, procesos que en conjunto, el Comité de Transparencia, el Oficial de Protección de Datos Personales, las personas responsables de los sistemas de datos personales y el Equipo jurídico del Partido, definieron al implementar las medidas de seguridad administrativas, físicas y tecnológicas necesarias para la protección de los sistemas de datos personales, observando siempre los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, acorde con lo establecido por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, a fin de garantizar su protección y debido tratamiento.

Además, con el objetivo de establecer un método de trabajo que permita un mejor tratamiento de los datos personales, se ha implementado un modelo de mejora continua, que aporta beneficios en la gestión de la seguridad de la información denominado Sistema de Gestión de Seguridad de Datos Personales -SGSDP-, basado en el modelo -PHVA- "Planificar-Hacer-Verificar- Actuar", de tal manera que a través de su metodología se logre un nivel aceptable del riesgo en el tratamiento de la información personal.

I. CAPACITACIÓN BÁSICA

¿QUÉ ES UN DATO PERSONAL?

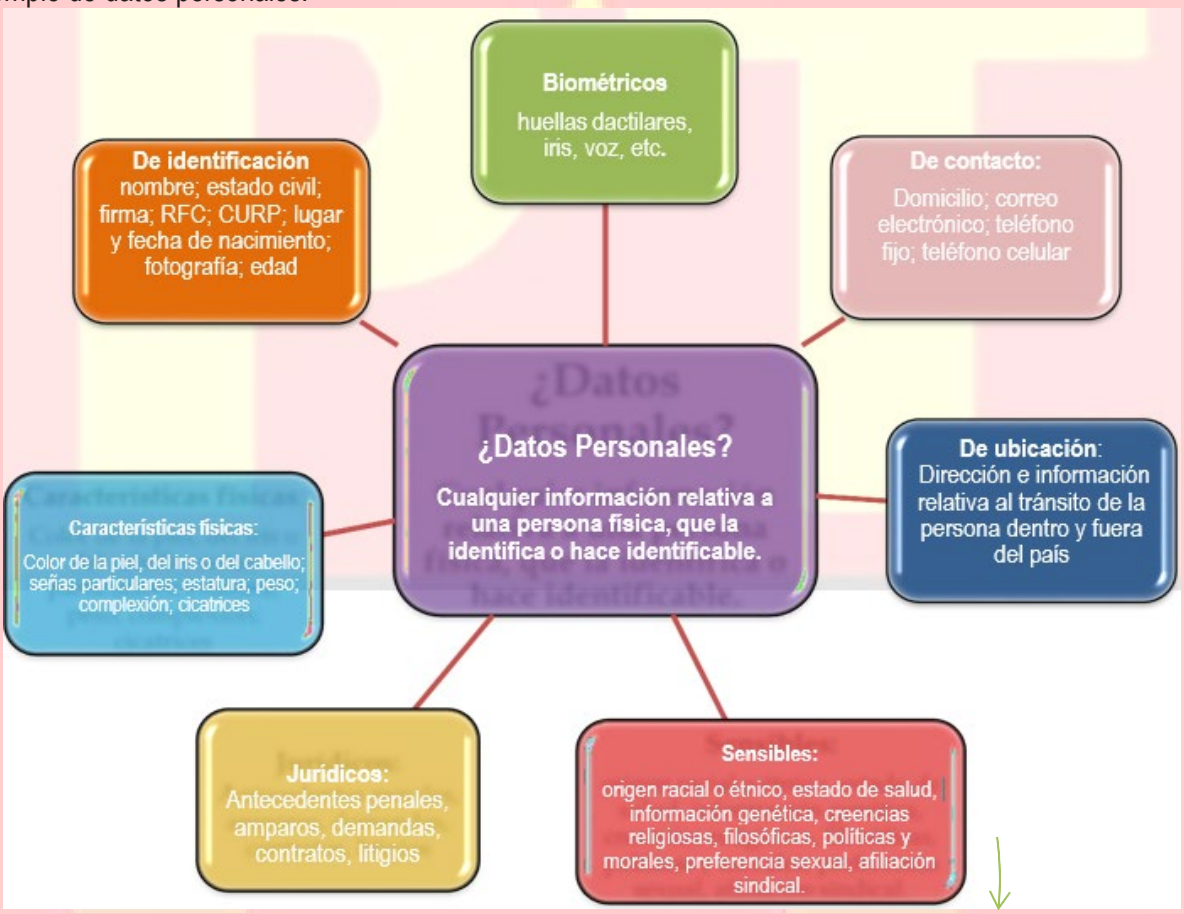
Los datos personales son toda información relativa a una persona física, que la identifica o hace identificable. Es la información que nos describe y nos distingue de las demás personas, como nombre, edad, sexo, estado civil, nacionalidad, patrimonio, etc. El artículo 3º fracción IX de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados -Ley de Datos Personales- define los datos personales como:

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

Existen además, datos personales que requieren de especial protección y cuidado por ser sensibles y la Ley de Datos Personales los refiere como:

"Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para ésta…"

Ejemplo de datos personales:



¿POR QUÉ ES IMPORTANTE PROTEGER LOS DATOS PERSONALES?

La información personal dice quién somos; qué nos gusta; cuáles son nuestras habilidades o deficiencias; con quién nos relacionamos, es decir, dicen todo sobre nuestra persona, por ello, sin importar quién posea esa información, su manejo inadecuado puede causar riesgos o daños, por lo que esa información es valiosa y debemos cuidarla como cualquier otro bien con valor e importancia.

El uso de las tecnologías de la información implica todo un reto para la privacidad, el uso intensivo de la

información personal en las redes sociales, internet, teléfonos celulares, entre otros, ponen en riesgo nuestra privacidad, por ello debemos tener presente el daño que puede causar que alguien haga un uso indebido de nuestra información personal.

Un mal uso de la información personal puede afectar la relación con la familia o amigos. Imaginemos que alguien roba la identidad y publica fotos o mensajes no autorizados o hace mal uso de nuestra credencial para votar, robe nuestra identidad o compre productos con nuestra tarjeta de crédito.

¿QUÉ ES EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES?

La protección de datos personales es un derecho humano que tiene toda persona para decidir de manera libre e informada sobre el uso, divulgación y todo tratamiento de su información personal.

En 2009 se reformó el segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos para darle al derecho a la protección de los datos personales un estatus constitucional, reconociéndose además los derechos de acceso, rectificación y cancelación de los datos personales, así como el derecho a manifestar su oposición al tratamiento de los mismos y la solicitud de la portabilidad de

los datos proporcionados de manera libre y voluntaria al sujeto obligado. Impone obligaciones a los particulares y a las instituciones públicas que utilizan datos personales, y otorga derechos a las personas titulares de los datos.

El artículo 16 párrafo segundo constitucional señala textualmente lo siguiente:

> *"Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".*

El Partido del Trabajo es regulado por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y por los Lineamientos Generales de Protección de Datos Personales para el Sector Público. De acuerdo con éstos, los sujetos obligados deben observar ocho principios y dos deberes para la protección de los datos personales:

PRINCIPIOS PARA LA PROTECCIÓN DE LOS DATOS PERSONALES

Principio de Licitud -Art. 11 LGPDPDSO-: Implica identificar en la ley las competencias que autorizan a tratar datos personales. Nadie debe utilizar los datos personales para actividades ilícitas, ni que viole la legislación de datos personales, o ninguna otra ley o normatividad aplicable en nuestro país.

Principio de Finalidad -Art. 12 LGPDPDSO-: Implica que se defina el uso concreto, lícito, explícito y legítimo que se le va a dar a los datos personales. Cualquier cambio en el uso de los datos personales requiere el consentimiento de la persona titular de la información. Los o las responsables solo podrán tratar los datos personales para objetivo distintos cuando cuenten con el consentimiento de la persona titular y de acuerdo con la ley. En el Aviso de Privacidad deben estar contenidas las finalidades por las cuales son recabados los datos personales, mismo que es generado por el sujeto obligado que recaba los datos personales.

Principio de Consentimiento -Arts. 14, 15 y 16 LGPDPDSO-: Implica guardar la información personal sólo con la autorización, expresa o tácita, de la persona. Previo a tratar los datos personales, el o la responsable debe obtener el consentimiento del titular, de manera libre e informada, por lo que es importante que se muestre el Aviso de privacidad en el momento de recabar cualquier dato personal.

Principio de Lealtad -Art. 13 LGPDPDSO-: Implica no actuar de manera engañosa o fraudulenta: sin dolo, error o mala fe o negligencia, que él o la responsable beneficie los intereses de la persona titular para que el manejo de sus datos personales no dé lugar a discriminación o trato injusto. Es importante tratar los datos únicamente para las finalidades para las cuales fueron recabados, éstas deben coincidir con las contenidas en el Aviso de Privacidad.

Principio de Calidad -Arts. 17 y 18 LGPDPDSO-: Implica asegurar que los datos personales se mantengan

exactos, completos y actualizados para los fines que persigue del manejo de datos personales. Implica definir y documentar procedimientos para conservar y, en su caso, bloquear y quitar los datos personales; también implica borrar los datos personales una vez cumplida la finalidad que motivó su tratamiento.

Principio de Proporcionalidad -Art. 19 LGPDPDSO-: Implica recolectar y utilizar sólo los datos que son estrictamente necesarios para el objetivo propuesto procurando pedir el menor número posible de datos personales. Recordemos que entre mayor cantidad de datos personales se recaben, el nivel de seguridad requerido para resguardarlos será proporcional.

Principio de Responsabilidad -Arts. 23 y 24 LGPDPDSO-: Implica implementar políticas, programas y mecanismos obligatorios y exigibles al interior de la organización del responsable que acrediten el cumplimiento de los principios, deberes y obligaciones previstos en la Ley. El o la responsable está obligado a la rendición de cuentas ante la persona titular y la Autoridad Garante.

Principio de Información -Arts. 20, 21 y 22 LGPDPDSO-: Implica informar a las personas titulares la existencia y características principales del manejo al que serán sometidos sus datos personales, mediante un "Aviso de Privacidad".

Es un derecho conocer el Aviso de Privacidad antes de proporcionar cualquier información personal. Si no se muestra, se debe solicitar, éste puede ser electrónico, físico e incluso una grabación o video. Solo así se estará en posibilidad de tomar una decisión informada respecto de la entrega o no de los datos personales.

DEBERES PARA LA PROTECCIÓN DE LOS DATOS PERSONALES

Deber de Confidencialidad: Garantiza a las personas titulares de los datos personales que sus datos personales no se difundan o compartan con otras personas, salvo que lo autoricen o alguna obligación legal lo requiera.

En el Partido del Trabajo se protege la información de los sistemas de datos personales mediante acuerdos de confidencialidad o de no revelación de información, donde individualmente las personas involucradas en el tratamiento de los datos personales se comprometen a no divulgar, usar o explotar la información de datos personales a la que tengan acceso, respetando los lineamientos definidos en la materia, así como las obligaciones y responsabilidades asumidas por las partes, incluyendo las que debe cumplir una vez finalizada la relación contractual.

Deber de Seguridad: Se debe garantizar a las personas titulares de los datos personales el derecho a que su información personal proporcionada sea protegida bajo medidas de seguridad adecuadas, que eviten su pérdida, uso, acceso o tratamiento no autorizado. Las medidas deben ser físicas, administrativas y técnicas, para garantizar a las personas titulares a que su información personal proporcionada estará protegida bajo medidas de seguridad adecuadas, que eviten su pérdida, uso, acceso o tratamiento no autorizado.

En ese sentido, la Ley sugiere que todo sujeto obligado debe tener un Documento de Seguridad de Datos

Personales que tenga al menos los siguientes elementos:

- ✓ El inventario de datos personales y de los sistemas de tratamiento;
- ✓ Las funciones y obligaciones de las personas que traten datos personales;
- ✓ El análisis de riesgos;
- ✓ El análisis de brecha;
- ✓ El plan de trabajo;
- ✓ Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
- ✓ El programa general de capacitación.

En el Partido del Trabajo es la Metodología BAA la utilizada para evaluar las medidas de seguridad necesarias para proteger los sistemas de datos personales identificados, la cual se enfoca en tres variables que afectan la percepción del valor de los datos personales para un atacante:

- ➢ **Factor Beneficio,** deriva en el nivel de riesgo por tipo de dato, determinado por el riesgo inherente del y el volumen de titulares de las que se tratan datos.
- ➢ **Factor Accesibilidad,** determina el nivel de riesgo por tipo de acceso, es decir, el número de accesos potenciales a los datos.
- ➢ **Factor Anonimidad,** determina el nivel de riesgo por tipo de entorno desde el que se tiene acceso a los datos.

El objetivo es realizar una clasificación de los datos personales en función de las variables anteriores, a fin de ponderar el riesgo e identificar la información que por orden de prioridad requiera tener más protección, para ello se consideran las tablas matriciales existentes basadas en la norma internacional ISO/IEC 27002 que brinda orientación a las organizaciones que desean establecer, implantar y mejorar un sistema de gestión de seguridad de la información (SGSI) centrado en la ciberseguridad**,** dando como resultado la lista de controles de seguridad aplicables: administrativos, físicos y técnicos que deben ser implementados en cada uno de los sistemas.

Algunos sistemas de protección de datos personales son:

¿QUÉ ES UN AVISO DE PRIVACIDAD?

Es un documento que se debe poner a disposición de la persona titular de forma física, electrónica o en cualquier formato generado, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Existen dos modalidades de Aviso de Privacidad: el Aviso de Privacidad simplificado y Aviso de Privacidad integral. Los elementos que integran el Aviso de Privacidad simplificado son:

I. La denominación y el domicilio del responsable;
II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento de la persona titular;
III. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:
   a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y
   b) las personas físicas o morales a las que se transfieren los datos personales;
IV. Los mecanismos y medios disponibles para que la persona titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento de la persona titular, y
V. El sitio donde se podrá consultar el aviso de privacidad integral.

El Aviso de Privacidad integral, deberá contener, al menos, la siguiente información los siguientes**:**

I. La denominación y el domicilio del responsable;
II. Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;
III. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;
IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento de la persona titular;
V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCOP;
VI. El domicilio de la Unidad de Transparencia;
VII. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:
   a. Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y
   b. Las finalidades de estas transferencias;
VIII. Los mecanismos y medios disponibles para que la persona titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento de la persona titular, y
IX. Los medios a través de los cuales el responsable comunicará a las personas titulares los cambios al aviso de privacidad.

¿QUÉ ES LA BITÁCORA DE VULNERACIONES?

Importancia de la notificación de una vulneración

La notificación de vulneraciones de seguridad es considerada una medida de seguridad, por lo que la Ley de Datos Personales la considera una obligación del responsable del sistema de datos personales para que las personas titulares puedan tomar medidas para la protección de sus derechos morales y patrimoniales, por lo que es obligación notificar a la persona titular del dato y a la Autoridad Garante correspondiente en un plazo no mayor a 72 horas una vez identificado el incidente.

Proceso de notificación de vulneraciones en el Partido del Trabajo

La notificación de vulneraciones se debe realizar lo antes posible al jefe superior inmediato, con la información suficiente mediante correo electrónico o en persona.

En el Partido del Trabajo existen tres formatos de bitácora, dichos formatos se encuentran en la Guía para el uso de la bitácora de vulneraciones:

- ✓ **Bitácora Nacional:** Realizada por el Órgano Interno responsable del Partido del Trabajo a nivel nacional.
- ✓ **Bitácora Estatal:** Realizada por el Órgano Interno responsable del Partido del Trabajo en cada una de las entidades federativas.
- ✓ **Bitácora General:** Realizada por la Unidad de Transparencia, en la que se concentra las vulneraciones ocurridas, la cual reside en el Oficial de Protección de Datos Personales.

Cada el Órgano Interno Responsable debe llevar una Bitácora y la Unidad de Transparencia debe llevar una Bitácora general, la cual reside en el Oficial de Protección de Datos Personales. De ocurrir una vulneración, el responsable del sistema de datos personales debe registrarla en su bitácora y notificar al Oficial de Protección de Datos Personales para que ésta se inscriba en la Bitácora general, se informe de lo ocurrido al Comité de Transparencia y se notifique a las personas titulares de los datos personales y al INAI.

IMPORTANTE: Si ocurrida una vulneración de seguridad, se identifica un posible delito, se debe dar parte al Ministerio Público.

BORRADO SEGURO DE LOS DATOS PERSONALES

Una vez que la información tratada ha llegado al final de su vida útil, previa consideración de los plazos de conservación de los mismos, debe ser eliminada o destruida bajo técnicas seguras de borrado que garanticen que los datos son eliminados de los sistemas de datos personales en su totalidad y que los mismos no pueden ser recuperados ni utilizados de manera indebida.

Es importante considerar que existen métodos de borrado no seguro, ya que es posible invertir el proceso para recuperar de manera parcial o total los datos personales, por ejemplo:

- Romper archivos y documentos a mano, con tijeras o rasgarlos, permite que una persona pueda recuperarlos y extraer información importante.
- Utilizarlos como papel de reciclaje o arrojarlos íntegros a la basura es una conducta aún más riesgosa.
- Utilizar comandos como “borrar”, “eliminar” o “formatear”, permite que los archivos puedan ser recuperados con la utilización de software que en su mayoría puede ser gratuito.

Técnicas de destrucción y borrado seguro	
Destrucción de medios de almacenamiento físico	Trituración Incineración Químicos
Destrucción de los medios de almacenamiento electrónicos	Desintegración. Pulverización Incineración. Abrasión
Métodos lógicos de borrado	Desmagnetización. Sobre-escritura Cifrado de medios

Importante: Se debe comprobar y documentar cuándo y cómo el proceso de borrado se ha realizado a fin de demostrar que los datos personales fueron eliminados. -Actas, fotografías y bitácoras de destrucción-. En el Partido del Trabajo se cuenta con un formato denominado “Reporte de operación de borrado”.

LOS DERECHOS ARCOP

Las personas titulares de los datos personales tienen derecho a acceder a ellos, rectificarlos, o solicitar que se eliminen o cancelen, así como a oponerte a su uso y solicitar una copia electrónica para su portabilidad. A estos derechos se les conoce como ARCOP, por sus siglas, y están reconocidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

Derecho de Acceso: Es el derecho que tiene la persona titular de solicitar el acceso sus datos personales que están en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacena o utiliza, así como de conocer información relacionada con el uso que se da a su información personal.

Derecho de Rectificación: Es el derecho que tiene la persona titular de solicitar la revisión para hacer una rectificación o corrección de sus datos personales, cuando éstos sean inexactos o incompletos o no se encuentren actualizados.

Derecho de Cancelación: Es el derecho que tiene la persona titular de solicitar que uno ovarios datos personales se eliminen del sistema o base de datos, archivos, registros, expedientes, sistemas del responsable que los posee a fin de evitar un daño a su persona.
Derecho de Oposición: Es el derecho que tiene la persona titular de solicitar que uno o varios de sus datos personales no se utilicen para ciertos fines o no sean sometidos al tratamiento de los mismos.
***Derecho de Portabilidad*:** El derecho a la portabilidad de datos permite a la persona titular, obtener de forma segura del Partido del Trabajo como responsable de la posesión de los datos personales, una copia electrónica de los datos objeto de tratamiento, en un formato estructurado, comúnmente utilizado y sin afectar su uso, para sus propios fines.

IMPORTANTE: En el caso de los derechos de Cancelación y Oposición debemos tomar en cuenta que no siempre se podrán eliminar sus datos personales, principalmente cuando sean necesarios por alguna cuestión administrativa, legal o para el cumplimiento de obligaciones.

¿Cómo se pueden ejercer los Derechos ARCOP?

Recepción de solicitud ARCOP

La solicitud debe ser presentada ante la Unidad de Transparencia del Partido del Trabajo a través del formato correspondiente o en la Plataforma Nacional de Transparencia en la siguiente dirección electrónica: *http://www.plataformadetransparencia.org.mx* con la siguiente información:

a) Nombre de la persona titular de los datos personales.
b) Documentos que acrediten la identidad de la persona titular y, en su caso, la personalidad e identidad de su representante;
c) De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud;
d) La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCOP, salvo que se trate del derecho de acceso;
e) La descripción del derecho ARCOP que se pretende ejercer, o bien, lo que solicita la persona titular;
f) Domicilio o cualquier medio para recibir notificaciones
g) En su caso, documentos o información que faciliten la localización de los datos personales, en su caso.

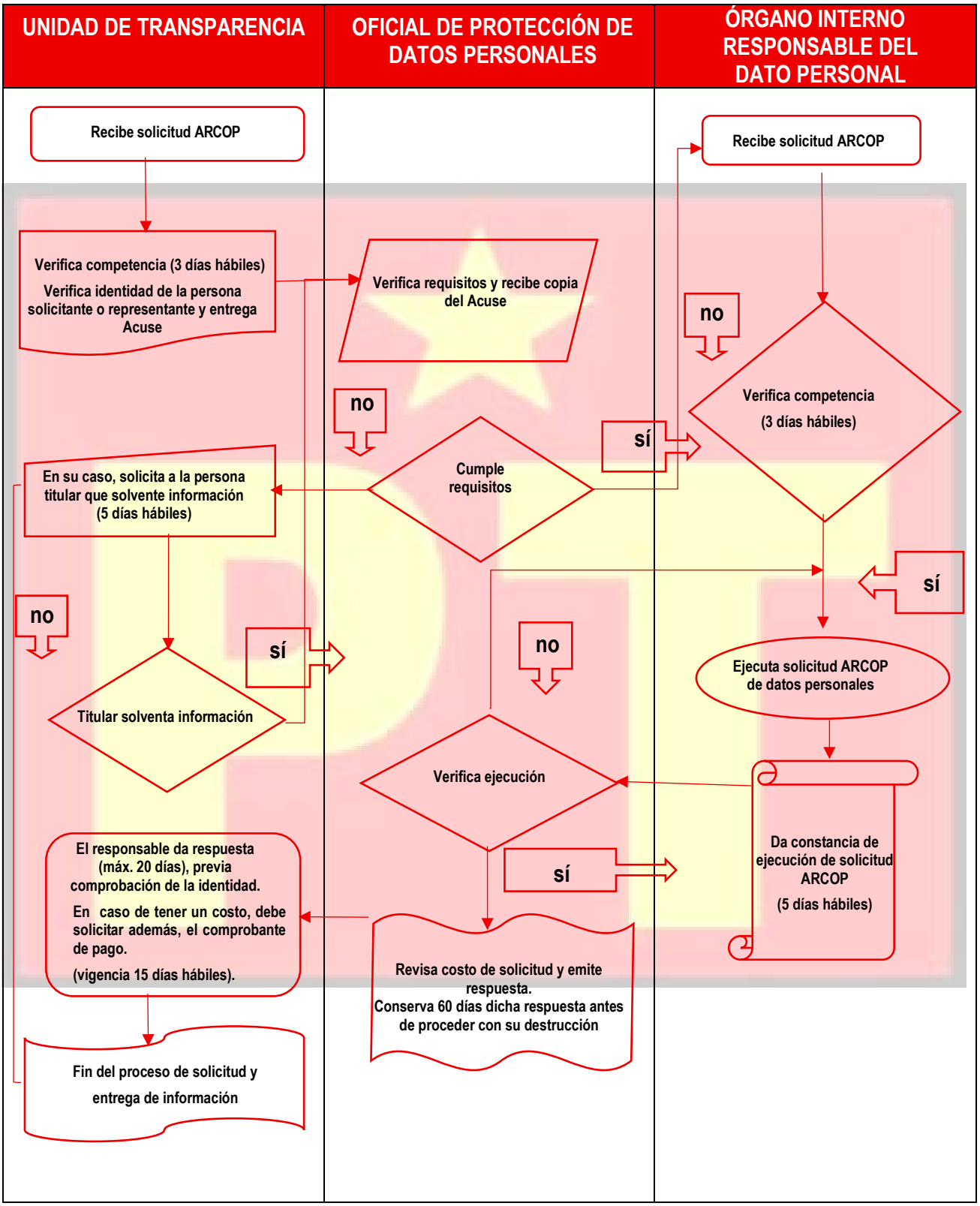
Acreditación de la identidad

Toda persona solicitante deberá acreditar la titularidad del dato personal para la procedencia de su solicitud, acreditando la identidad de la persona titular y, en su caso, la identidad y personalidad con la que actúe la persona representante; entre las identificaciones oficiales válidas se encuentran: credencial para votar, pasaporte, cartilla militar, cédula profesional, licencia para conducir y documento migratorio, Credencial para Votar expedida por el Instituto Nacional Electoral.

Trámite y desahogo de solicitudes ARCOP

Una vez acreditada la titularidad del dato personal y verificada la competencia, la solicitud es turnada por la Unidad de Transparencia al Órgano Interno responsable del sistema de datos personales para dar respuesta a la solicitud en un plazo máximo de 20 días. El ejercicio de los derechos ARCOP es gratuito, sólo se podrá realizar el cobro para recuperar los costos se reproducción, certificación o envío.

Diagrama de flujo para el trámite de solicitudes ARCOP



EJERCICIO DE REFLEXIÓN

Responda las siguientes preguntas a modo de reflexión:

1. ¿Qué es un dato personal?
2. ¿Cuáles son los datos personales sensibles?
3. ¿Qué son los derechos ARCO?
4. ¿Para qué sirve el Aviso de Privacidad?

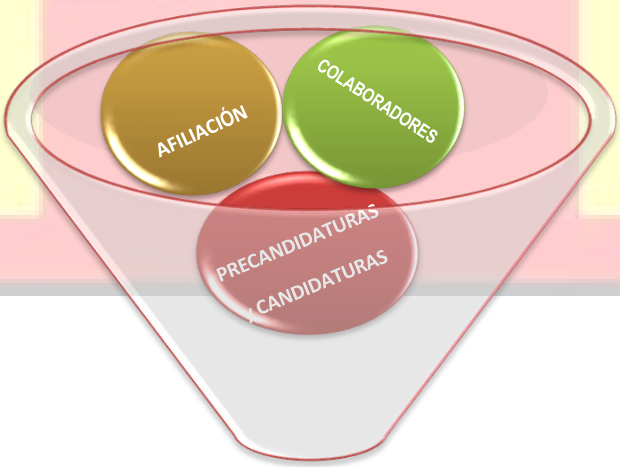
II. CAPACITACIÓN PRÁCTICA

DOCUMENTO DE SEGURIDAD

El Partido del Trabajo debe garantizar a las personas titulares que su información personal proporcionada estará protegida bajo medidas de seguridad adecuadas, que eviten su pérdida, uso, acceso o tratamiento no autorizado.

Las medidas deben ser físicas, administrativas y técnicas. En este sentido, la Ley sugiere que se debe tener un Documento de Seguridad de Datos Personales que tenga al menos los siguientes elementos:

- El inventario de datos personales y de los sistemas de tratamiento;
- Las funciones y obligaciones de las personas que traten DP;
- El análisis de riesgos;
- El análisis de brecha;
- El plan de trabajo;
- Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
- El programa general de capacitación.



El Documento de Seguridad, proporciona a los Órganos Internos responsables un marco de referencia general unificado que estandariza el tratamiento, la organización y conservación de los datos personales.

Figuras que intervienen

Debemos identificar los roles de las personas que intervienen en el resguardo de nuestra información

Responsable:	Encargado:	Gestor:	Usuario:
Toma las decisiones sobre el tratamiento de los Datos Personales bajo su resguardo.	Trata los Datos Personales a nombre del Órgano Interno responsable. Existe una relación jurídica que delimita el ámbito de su actuación. (Prestador de Servicio)	Trata los Datos Personales por indicaciones del responsable, pertenece a la estructura estatutaria del Partido del Trabajo.	Personas autorizadas para consultar o recabar los Datos Personales, forman parte de la estructura estatutaria del Partido del Trabajo en los Estados y la Ciudad de México

Principales obligaciones de los sujetos obligados Responsables, Gestores y Usuarios

Medidas de seguridad básicas

EJERCICIO DE REFLEXIÓN

Responda las siguientes preguntas a modo de reflexión:

1. ¿Qué es el DSDP?
2. ¿Cuáles son las figuras que intervienen en el resguardo de la información en MC?
3. ¿Menciona 3 obligaciones de los responsables?

GLOSARIO

Activo. La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para el instituto político.

Aviso de privacidad: Documento a disposición de la persona titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Base(s) de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Consentimiento: Manifestación de la voluntad libre, específica e informada de la persona titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

Confidencialidad. Propiedad de la información para no estar a disposición o ser revelada a personas, entidades o procesos no autorizados.

Datos personales. Cualquier información concerniente a una persona física identificada o identificable.

Derechos ARCOP: Los derechos de acceso, rectificación, cancelación, oposición y portabilidad al tratamiento de datos personales -*ARCOP por sus siglas*- señalados en la Ley General de Protección de Datos Personales en Poder de los Sujetos Obligados;

Disponibilidad. Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.

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

Encargado. La persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Incidente. Escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades.

Integridad. La propiedad de salvaguardar la exactitud y completitud de los activos.

Responsable. Persona física o moral de carácter privado que decide sobre el tratamiento de los datos personales.

Sistema de Gestión de Seguridad de Datos Personales -SGSDP-. Sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley de Datos Personales.

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

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

Tratamiento. La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Transferencia. Toda comunicación de datos realizada a persona distinta de la persona titular, responsable o encargado del tratamiento, dentro o fuera del territorio nacional.

Vulnerabilidad. Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.