



**DOCUMENTO DE SEGURIDAD
EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES EN
POSESIÓN DEL PARTIDO VERDE ECOLOGISTA DE MÉXICO**



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

CONTENIDO

- 1. INTRODUCCIÓN**
- 2. OBJETIVO**
- 3. ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD**
- 4. MARCO JURÍDICO**
- 5. ÁMBITO DE APLICACIÓN**
- 6. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD**
- 7. SANCIONES POR INCUMPLIMIENTO**
- 8. INVENTARIO DE DATOS PERSONALES**
- 9. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES**
- 10. ANÁLISIS DE RIESGOS**
- 11. ANÁLISIS DE BRECHAS**
- 12. PLAN DE TRABAJO**
- 13. MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD**
- 14. CAPACITACIÓN**
- 15. ANEXOS**
 - 1. INVENTARIO DE TRATAMIENTO DE DATOS PERSONALES**
 - 2. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES**
 - 3. ANÁLISIS DE RIESGOS POR ÁREA**
 - 4. MEDIDAS DE SEGURIDAD IMPLEMENTADAS**
 - 5. SUPRESIÓN DE DATOS PERSONALES**



DOCUMENTO DE SEGURIDAD VERSIÓN PÚBLICA

1. INTRODUCCIÓN

En el Partido Verde Ecologista de México la información es un activo que debe protegerse a través de un conjunto de procesos y sistemas diseñados, administrados y mantenidos por este Instituto Político. De esta manera, mediante la gestión de la seguridad de la información, se busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas de la información, aplicando un enfoque basado en los riesgos que el partido podría llegar a afrontar.

A partir de la publicación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (LGDPSP), todas las dependencias y entidades –incluidos partidos políticos- al llevar a cabo el tratamiento de los datos personales de personas físicas, adquieren el carácter de “responsable” y deberán tratar dichos datos conforme a los principios de: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad y responsabilidad; adoptar medidas de seguridad con base en los sistemas de datos que traten; plasmar en un documento de seguridad dichas medidas; garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) y demás obligaciones previstas en las disposiciones jurídicas vigentes.

Este documento contiene las medidas de seguridad de carácter administrativo, físico y técnico, implementadas por el partido, que permiten proteger los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado.

El presente Documento de Seguridad en Materia de Tratamiento de Datos Personales en Posesión del Partido Verde Ecologista de México (Documento de Seguridad) se elabora en cumplimiento de las disposiciones jurídicas vigentes



DOCUMENTO DE SEGURIDAD

VERSIÓN PÚBLICA

contenidas en la Constitución Política de los Estados Unidos Mexicanos (CPEUM), en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), Lineamientos que establecen los Parámetros, Modalidades y Procedimientos para la Portabilidad de Datos Personales (Lineamientos de Portabilidad) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales), con el fin de garantizar la integridad, confidencialidad y disponibilidad de los datos personales que este Partido Político guarda, e impedir que cualquier tratamiento contravenga las disposiciones del marco normativo en la materia.

Por lo tanto, la integridad reside en garantizar la exactitud y confiabilidad de la información y los sistemas del Partido, de manera que éstos no puedan ser modificados sin autorización, ya sea accidental o intencionadamente.

A su vez, la confidencialidad consiste en asegurar que la información no sea accedida o divulgada a personas o procesos no autorizados.

Por último, la disponibilidad radica en que las personas o procesos autorizados del partido accedan a los activos de información cuando así lo requieran.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

2. OBJETIVO

Entre los deberes previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se encuentra el de elaborar un documento de seguridad (artículo 29 de la LGPDPPSO) en el cual se describan y de cuenta de manera general sobre las medidas de seguridad administrativas, físicas y técnicas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que poseen las distintas áreas de este instituto político para la protección de los datos personales contra daño, pérdida, alteración, destrucción, o su uso, acceso o tratamiento no autorizado en posesión del Partido Verde Ecologista de México. La elaboración de este documento fue coordinada por la Unidad de Transparencia del Partido Verde Ecologista de México.

El documento de seguridad del Partido Verde Ecologista de México ha sido generado conjuntamente por la Unidad y la Comisión Nacional de Transparencia y Acceso a la Información, en el ámbito de sus facultades y atribuciones, así como con los instrumentos que cada área de este Instituto Político generó.

Este documento de seguridad tiene como propósito identificar el sistema de datos personales que posee cada área del partido, así como los responsables, encargados y usuarios de cada sistema.

Asimismo, el presente documento de seguridad deberá mantenerse siempre actualizado y ser de observancia obligatoria para todo el personal de este ente político que trabaja con datos personales.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

3. ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD

Se consultó con todas las áreas del partido con la finalidad de recabar información útil para la elaboración de este Documento.

Se concentraron los elementos relacionados con el cumplimiento de los requisitos establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

A través de la Unidad y la Comisión Nacional de Transparencia y Acceso a la Información, se platicó con diversas áreas del partido, para conocer las medidas de seguridad que deben prevalecer en los sistemas de soporte físico y electrónico.

Así, las distintas áreas del Partido Verde Ecologista de México que cuentan con sistemas de datos personales aportaron elementos para la integración del Documento de Seguridad.

Se les dio a conocer a las diversas áreas de este instituto político, el borrador del Documento de Seguridad del Partido Verde Ecologista de México.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

4. MARCO JURÍDICO

- **Constitución Política de los Estados Unidos Mexicanos.**
- **Ley General de Transparencia y Acceso a la Información Pública.**
- **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.**
- **Lineamientos Generales de Protección de Datos Personales para el Sector Público.**
- **Lineamientos que establecen los Parámetros, Modalidades y Procedimientos para la Portabilidad de Datos Personales.**
- **Estatutos del Partido Verde Ecologista de México.**

El artículo 1º de la Constitución Política de los Estados Unidos Mexicanos dispone que: “En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece.”

El derecho a la protección de datos personales para el sector público, en México, se remonta a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental artículos 3 fracción II y 18 fracción II, publicada en 2002.

En atención a que el Partido Verde Ecologista de México, conforme al artículo 41 de la Constitución Política de los Estados Unidos Mexicanos, es: una “*entidad de interés público que tiene como finalidad promover la participación del pueblo en la vida democrática, contribuir a la integración de los órganos de representación política y como organizaciones de ciudadanos, hacer posible el acceso de éstos al ejercicio del poder público, de acuerdo con los programas, principios e ideas que postulan y mediante el sufragio universal, libre, secreto y directo, así como las*



DOCUMENTO DE SEGURIDAD VERSIÓN PÚBLICA

reglas para garantizar la paridad entre los géneros, en candidaturas a legisladores federales y legales". Además de lo dispuesto por el artículo 1º de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, este ente político, es un sujeto obligado en materia de protección de datos personales y, por ende, responsable del tratamiento de los datos personales que resguarda para el ejercicio de sus atribuciones.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público, establecen un conjunto mínimo de medidas de seguridad que el Partido Verde Ecologista de México deberá considerar al perfilar su estrategia de seguridad para la protección de los datos personales bajo su custodia, según el tipo de soportes —físicos, electrónicos o ambos— en los que residen dichos datos.

En este mismo sentido, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece que los partidos políticos deberán expedir un documento de seguridad que contenga las medidas administrativas, físicas y técnicas aplicables a los sistemas de datos personales y que dicho documento será de observancia obligatoria.

De conformidad con el artículo 29 de la LGPDPPSO, el documento de seguridad deberá contener, al menos, la siguiente información:

- I. El inventario de datos personales y de los sistemas de tratamiento;
- II. Las funciones y obligaciones de las personas que traten datos personales;
- III. El análisis de riesgos;
- IV. El análisis de brecha;
- V. El plan de trabajo;
- VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

VII. El programa general de capacitación.

El artículo 111 de los Estatutos del Partido Verde Ecologista de México establece lo siguiente:

Los datos personales recabados serán protegidos, incorporados y tratados en el Sistema de Datos Personales “Padrón de Afiliados (simpatizantes, adherentes y militantes) del Partido Verde Ecologista de México” y cuya finalidad es crear el banco de datos de afiliados a este Instituto Político y serán resguardados por Consejo Político Nacional del Partido Verde Ecologista de México, para su custodia, administración, actualización y ejecución de todo lo relativo al padrón de afiliados, la instancia donde se podrá ejercer los derechos de acceso, rectificación, cancelación y oposición, así como la revocación del consentimiento lo es el Consejo Político Nacional en las oficinas del Comité Ejecutivo Nacional.



DOCUMENTO DE SEGURIDAD

VERSIÓN PÚBLICA

5. ÁMBITO DE APLICACIÓN

El documento de seguridad es aplicable y de observancia obligatoria para todas las áreas del Partido Verde Ecologista de México que en el ejercicio de sus funciones o atribuciones traten con sistemas de datos personales, sin importar si los recaban de manera directa o indirecta de las personas titulares de los datos personales.

Asimismo, serán aplicables al tratamiento de datos personales que obren en soportes físicos y/o electrónicos, independientemente de la forma o modalidad en que fueron creados, procesados, almacenados y organizados. Los datos personales podrán ser guardados en forma numérica, alfabética, gráfica, alfanumérica, fotográfica o en cualquier otro formato.

Por lo tanto, se deberán tratar los datos personales con responsabilidad y de conformidad a las medidas de seguridad que se hayan establecido para tal fin.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

6. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

El presente documento de seguridad se actualizará, en caso de que ocurra alguno de los supuestos del artículo 30 de la LGPDPPSO:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

7. SANCIONES POR INCUMPLIMIENTO

Cuando la Unidad de Transparencia tenga conocimiento del incumplimiento de alguna obligación prevista en este documento, deberá realizar al área correspondiente un exhorto con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

Cuando la persona encargada del tratamiento de datos personales incumpla las instrucciones del responsable y decida por sí misma sobre el tratamiento de los datos personales, asumirá el carácter de responsable y las consecuencias legales correspondientes conforme a la legislación en la materia que le resulte aplicable de conformidad con el artículo 54 de la LGPDPPSO.



DOCUMENTO DE SEGURIDAD VERSIÓN PÚBLICA

8. INVENTARIO DE DATOS PERSONALES

Cada área deberá elaborar un inventario de datos personales y de los sistemas de tratamiento, en el que se incluyan los siguientes elementos:

- Los medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
- Las finalidades de cada tratamiento de datos personales;
- Los tipos de datos personales que se traten, indicando si son sensibles o no;
- La descripción general de la ubicación física y/o electrónica de los datos personales;
- La lista de encargados que tienen acceso a los sistemas de tratamiento con nombres completos;
- En su caso, los destinatarios de las transferencias que se efectúen, así como las finalidades que las justifican.

Se deberá considerar en el inventario el ciclo de vida de los datos personales, conforme a lo siguiente:

- La obtención de los datos personales;
- El almacenamiento de los datos personales;
- El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
- La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
- La cancelación, supresión o destrucción de los datos personales.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

9. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES

Todos los integrantes del partido que tengan acceso a los datos personales tienen la obligación de conocer y aplicar las medidas de seguridad de cada Sistema en el que se concentren los datos y es aplicable en todas y cada una de las fases del tratamiento de los datos personales, iniciando con la obtención de estos y finalizando con su eliminación.

Cada área deberá definir las funciones, obligaciones y responsabilidades específicas de los encargados de los tratamientos de datos personales que se efectúen dentro del partido.

Además, se deberán establecer mecanismos para asegurar que los encargados involucrados en el tratamiento conozcan sus funciones para el cumplimiento de los objetivos, así como las consecuencias de su incumplimiento.

Cabe mencionar que, la obligación de confidencialidad debe subsistir aún después de que los involucrados hayan finalizado su participación en el tratamiento de los datos personales porque hayan cambiado de funciones y aun cuando la relación laboral con el partido haya finalizado.



DOCUMENTO DE SEGURIDAD VERSIÓN PÚBLICA

10. ANALISIS DE RIESGOS

El riesgo deviene de la exposición a amenazas, por lo tanto, es fundamental entender qué es una amenaza para el partido y cómo se pueden identificar escenarios de riesgo para los datos personales. Además, se deberá hacer una evaluación del riesgo y establecer las medidas para su reducción o mitigación, con el fin de proteger los datos personales.

La evaluación del riesgo se hará conforme a lo siguiente:

- El valor de los datos personales de acuerdo a su clasificación y ciclo de vida;
- La exposición de los activos involucrados en el tratamiento de los datos personales;
- Las consecuencias negativas para los responsables que pudieran derivar de una vulneración de seguridad ocurrida;
- El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las amenazas y vulnerabilidades existentes para los datos personales y los recursos o activos involucrados en su tratamiento, como pueden ser: hardware, software, personal o cualquier otro recurso humano o material, entre otros;
- La sensibilidad de los datos personales tratados;
- Las vulneraciones previas ocurridas en los sistemas de tratamiento.

Ecuación: Analizar la probabilidad de que se materialice el riesgo y establecer un valor. Asignar valores a la probabilidad y asignar valores al impacto.



DOCUMENTO DE SEGURIDAD VERSIÓN PÚBLICA

11. ANALISIS DE BRECHA

Es el análisis entre las medidas de seguridad existentes y aquellas faltantes, que resultan necesarias para la protección de los datos personales en posesión de este Partido Político, teniendo en cuenta el cumplimiento legal, la clasificación y acceso de los activos, el control de acceso, las posibles vulneraciones a la seguridad de la información, entre otros.

Para llevar a cabo el análisis de brecha, se debe considerar los siguientes:

- Las medidas de seguridad existentes y efectivas;
- Las medidas de seguridad faltantes, y
- La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

12. PLAN DE TRABAJO

Es el proceso mediante el cual cada área decidirá e implementará las medidas de seguridad y el tratamiento adecuado para un riesgo en el contexto de sus funciones, atribuciones y el sistema de datos personales que tratan. Se hará con base en el resultado del análisis de riesgos y del análisis de brecha.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

13. MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales de este instituto político.

Las medidas de seguridad implementadas deberán considerar de conformidad con el artículo 26 de la LGPDPPSO, lo siguiente:

- El riesgo inherente a los datos personales tratados;
- La sensibilidad de los datos personales tratados;
- El desarrollo tecnológico;
- Las posibles consecuencias de una vulneración para los titulares;
- Las transferencias de datos personales que se realicen;
- El número de titulares;
- Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
- El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

Tipos de medidas de seguridad

a) Las **medidas de seguridad administrativas** son las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel institucional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

b) Las **medidas de seguridad físicas** son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. Algunas de las actividades que se deben considerar son las siguientes:

- Prevenir el acceso no autorizado a las instalaciones físicas del partido;
Para lo anterior se cuenta con un contrato de prestación de servicios de seguridad y vigilancia privado, así como con el Gobierno de la Ciudad de México que tiene por objeto la vigilancia, protección a instalaciones, bienes y personas en el inmueble que ocupa el partido, es decir, resguardan las instalaciones, recursos e información las 24 horas los 365 días del año.
- Proteger cualquier soporte físico o electrónico que pueda salir del partido;
Se tiene un control en el uso de aparatos eléctricos y electrónicos, un control en el ingreso y egreso de aparatos, así como de documentos y materiales.
- Proveer a los equipos que almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.
Los equipos de cómputo cuentan con un programa de mantenimiento periódico.

c) Las **medidas de seguridad técnicas** abarcan el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. Se deben considerar algunas de sus actividades:



DOCUMENTO DE SEGURIDAD

VERSIÓN PÚBLICA

- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
El acceso a la base de datos es exclusivo para el personal adscrito al partido.
- Revisar la configuración de seguridad en la operación, desarrollo y mantenimiento del software y hardware;
Se realizan constantemente respaldos de la información.
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.
Se cuenta con protección Firewall y los antivirus propios de cada marca.

* Esto deberá observarse durante todo el ciclo de vida de los datos personales, desde su obtención hasta su eliminación.

Se deberán monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, tomando en cuenta lo siguiente:

- Los nuevos activos que se incluyan en la gestión de riesgos;
- Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;
- Las nuevas amenazas dentro y fuera del partido que no han sido valoradas;
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- El cambio en el impacto o consecuencias de amenazas valoradas y vulnerabilidades que resulten en un nivel inaceptable de riesgo, y
- Los incidentes y vulneraciones de seguridad ocurridas.



DOCUMENTO DE SEGURIDAD VERSIÓN PÚBLICA

14. CAPACITACIÓN

La capacitación del personal se hará dependiendo de sus funciones y obligaciones respecto del tratamiento de los datos personales a su cargo, seguridad de los datos personales y el perfil de los puestos, entre otros.

Por lo anterior, se impartirá una capacitación para los Enlaces de Datos Personales, los responsables y operadores del tratamiento de estos, que incluirá los siguientes temas de manera enunciativa más no limitativa:

- *Teoría y normatividad en materia de datos personales*
- *Principios, deberes y derechos*
- *Responsabilidades de los operadores*
- *Medidas de seguridad a observar*
- *Medidas de apremio y sanciones*



DOCUMENTO DE SEGURIDAD
VERSION PUBLICA

15. ANEXOS



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

1. INVENTARIO DE TRATAMIENTO DE DATOS PERSONALES

El inventario que se detalla en el presente documento es aquel que contiene datos personales, que se encuentran tanto en soporte electrónico como físico:

AREA: SECRETARIA DE FINANZAS	
Cómo se obtienen los datos personales:	<ul style="list-style-type: none">• Directamente del titular<ul style="list-style-type: none">○ De manera personal, con la presencia física del titular de los datos personales.○ Por internet o sistema informático.
Qué tipo de datos personales se tratan: ¿son sensibles?	Todos aquellos requeridos para la elaboración de los contratos. No son datos sensibles.
Dónde se almacena y realiza el tratamiento de datos personales:	<ul style="list-style-type: none">• Se almacena en una base de datos digital. La base de datos se encuentra en las oficinas del CEN del PVEM.• Se almacena de manera física en el Archivo del área.
Para qué finalidades se utilizan los datos personales:	Para contratación del personal.
Quién tiene acceso a la base de datos y a quién se comunican los datos personales al interior del área:	Todo el personal del área tiene acceso a la base de datos y se lo comunican a la Secretaría de Finanzas.
Qué transferencias se realizan o se podrían realizar de los datos personales:	La transferencia de los datos personales se hace al Instituto Nacional Electoral. No se requiere el consentimiento para la transferencia de conformidad con el artículo 16 de la LGPDPPSO.
Se difunden los datos personales:	No se difunden los datos personales.
Cuál es el plazo de conservación de los datos personales:	El plazo es por cinco años de conformidad con los instrumentos de clasificación archivística del partido.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

ÁREA: Consejo Político Nacional	
Cómo se obtienen los datos personales:	De manera personal, con la presencia física del titular de los datos personales. Por escrito presentado directamente en las oficinas del sujeto obligado.
Qué tipo de datos personales se tratan: ¿son sensibles?	Todos los requeridos por el formato de afiliación del Partido. No son datos sensibles.
Dónde se almacena y realiza el tratamiento de datos personales:	<ul style="list-style-type: none">Se almacena en una base de datos digital.La base de datos se encuentra en las oficinas del CEN del PVEM.
Para qué finalidades se utilizan los datos personales:	Para crear el padrón de afiliados.
Quién tiene acceso a la base de datos y a quién se comunican los datos personales al interior del área:	A la base de datos tienen acceso todas las áreas del Partido que intervienen con el padrón. Se comunican a los responsables por cada área de los datos personales y solo se le comunican al titular de cada área.
Qué transferencias se realizan o se podrían realizar de los datos personales:	La transferencia de los datos personales se hace al Instituto Nacional Electoral del padrón de afiliados. No se requiere el consentimiento para la transferencia de conformidad con el artículo 16 de la LGPDPPSO.
Se difunden los datos personales:	Si a través de Portal de Transparencia y la página web del Partido.
Cuál es el plazo de conservación de los datos personales:	El plazo es por cinco años de conformidad con los instrumentos de clasificación archivística del partido.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

AREA: Comisión Nacional de Honor y Justicia	
Cómo se obtienen los datos personales:	A través de los instrumentos legales en los que intervienen tanto el sujeto obligado como el quejoso según sea el caso.
Qué tipo de datos personales se tratan: ¿son sensibles?	Todos aquellos requeridos para la elaboración del instrumento legal. No son datos sensibles.
Dónde se almacena y realiza el tratamiento de datos personales:	<ul style="list-style-type: none">• Se almacena de manera digital en las oficinas del CEN del PVEM.• Se almacena de manera física en el Archivo del área.
Para qué finalidades se utilizan los datos personales:	Para la elaboración y resolución de los expedientes.
Quién tiene acceso a la base de datos y a quién se comunican los datos personales al interior del área:	Todo el personal del área tiene acceso a la base de datos.
Qué transferencias se realizan o se podrían realizar de los datos personales:	La transferencia de los datos personales se realiza a la autoridad competente según sea el caso. No se requiere el consentimiento para la transferencia de conformidad con el artículo 16 de la LGPDPPSO.
Se difunden los datos personales:	No se difunden los datos personales.
Cuál es el plazo de conservación de los datos personales:	El plazo es por cinco años de conformidad con los instrumentos de clasificación archivística del partido.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

2. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES

AREA: Secretaría de Finanzas	
Nombre del sistema:	Finanzas
Responsable:	
Nombre:	Elisa Uribe Anaya
Cargo:	Secretaria de Finanzas
Funciones:	Supervisar el sistema de datos personales del área. Descripción de las funciones en relación con el tratamiento de datos personales Instruir a los encargados de resguardar los datos personales, de no proporcionar información a personas no autorizadas. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.
Obligaciones: Descripción de las responsabilidades en cuanto al tratamiento de datos personales	Vigilar que se lleve a cabo el resguardo de datos personales conforme a lo establecido en la LGPDPPSO. Difundir las medidas de seguridad para sistemas de datos personales contenidas en el presente documento. Autorizar cambios al documento de seguridad respecto al sistema de datos personales del área a su cargo. Informar ocurría una vulneración a los datos personales. Guardar confidencialidad respecto de los datos personales tratados. Mantener la integridad, disponibilidad y confidencialidad de la información.
Datos personales contenido en el sistema:	Nombres, apellido paterno, apellido materno, edad, nacionalidad, género, RFC, CURP, nivel de estudios, acta de nacimiento, domicilio, teléfono, correo electrónico, firma.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

AREA: Consejo Político Nacional	
Nombre del sistema:	Padrón de Afiliados
Responsable:	
Cargo:	Consejeros
Funciones:	Supervisar el sistema de datos personales del área.
Descripción de las funciones en relación con el tratamiento de datos personales	Integrar y actualizar el padrón. Instruir a los encargados de resguardar los datos personales, de no proporcionar información a personas no autorizadas. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.
Obligaciones:	Vigilar que se lleve a cabo el resguardo del padrón conforme a lo establecido en la LGPDPPSO. Llevar a cabo la transferencia de datos a la autoridad electoral. Difundir las medidas de seguridad para sistemas de datos personales contenidas en el presente documento. Autorizar cambios al documento de seguridad respecto al sistema de datos personales del área. Informar cuando ocurra una vulneración a los datos personales.
Datos personales contenido en el sistema:	Nombres, apellido paterno, apellido materno, edad, género, clave de elector, sección electoral, escolaridad, domicilio, teléfono, correo electrónico, firma.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

AREA: Comisión Nacional de Honor y Justicia	
Nombre del sistema:	Expedientes legales
Responsable:	
Nombre:	Roberta Fernanda Blásquez Martínez
Cargo:	Presidenta
Funciones:	Supervisar el sistema de datos personales del área.
Descripción de las funciones en relación con el tratamiento de datos personales	Resguardar los datos personales y no proporcionar información a personas no autorizadas. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.
Obligaciones:	Vigilar que se lleve a cabo el resguardo de datos personales conforme a lo establecido en la LGPDPPSO.
Descripción de las responsabilidades en cuanto al tratamiento de datos personales	Difundir las medidas de seguridad para sistemas de datos personales contenidas en el presente documento. Autorizar cambios al documento de seguridad respecto al sistema de datos personales del área a su cargo. Informar cuando ocurra una vulneración a los datos personales. Realizar el tratamiento de los datos personales conforme a las instrucciones del titular.
Datos personales contenido en el sistema:	Nombres, apellido paterno, apellido materno, género, domicilio, teléfono, correo electrónico, firma.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

3. ANÁLISIS DE RIESGOS POR ÁREA

ÁREA: Secretaría de Finanzas	
Activos:	Es todo aquello que interviene en la protección de datos, como el servidor del CEN, los trabajadores del partido, las copias de seguridad.
Riesgos que pueden atacar los activos:	Un virus, que los trabajadores revelen información, robo de información.
Medidas de seguridad implementadas:	Antivirus, copias de seguridad periódicas, acceso restringido al lugar donde se resguardan los datos personales.

ÁREA: Consejo Político Nacional	
Activos:	Es todo aquello que interviene en la protección de datos, como el servidor del CEN, los trabajadores del partido, las copias de seguridad.
Riesgos que pueden atacar los activos:	Un virus, que los trabajadores revelen información, robo de información.
Medidas de seguridad implementadas:	Antivirus, copias de seguridad periódicas, acceso restringido al lugar donde se resguarda el Padrón.

ÁREA: Comisión Nacional de Honor y Justicia	
Activos:	Es todo aquello que interviene en la protección de datos, como el servidor del CEN, los trabajadores del partido, las copias de seguridad.
Riesgos que pueden atacar los activos:	Un virus, que los trabajadores revelen información, robo de información.
Medidas de seguridad implementadas:	Antivirus, copias de seguridad periódicas, acceso restringido al lugar donde se resguardan los expedientes que contienen los datos personales.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

4. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

ÁREA: Secretaría de Finanzas	
Nombre del sistema:	Finanzas
Registro de incidentes:	
Los datos que registra:	Fecha, hora y lugar del incidente: Descripción del incidente: Los datos personales comprometidos: Acciones correctivas implementadas de forma inmediata: Nombre y firma de los involucrados:
Si el registro está en soporte físico o soporte electrónico:	Soporte físico y electrónico
Cómo asegura la integridad de dicho registro:	Únicamente el Titular del área podrá tener acceso a dicho registro.
Actualización de la información contenida en el sistema	
La actualización se realiza de forma periódica y cada vez que se cuenta con nueva información.	
Procedimientos de Respaldo y Recuperación de Datos	
Señalar si realiza respaldos completos, diferenciales o incrementales:	El respaldo se realiza cada vez que se tiene información nueva.
El tipo de medios que utiliza para almacenar las copias de seguridad:	Discos duros, CD-ROM.
Cómo y dónde archiva esos medios:	En equipos de cómputo ubicados en los espacios de labores cotidianas en las oficinas del CEN.
Quién es el responsable de realizar estas operaciones:	El enlace por área de los datos personales.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

ÁREA: Consejo Político Nacional	
Nombre del sistema:	Padrón de Afiliados
Registro de incidentes:	
Los datos que registra:	Fecha, hora y lugar del incidente: Descripción del incidente: Los datos personales comprometidos: Acciones correctivas implementadas de forma inmediata: Nombre y firma de los involucrados:
Si el registro está en soporte físico o soporte electrónico:	Soporte físico y electrónico
Cómo asegura la integridad de dicho registro:	Únicamente el Titular del área podrá tener acceso a dicho registro.
Actualización de la información contenida en el sistema	
La actualización se realiza de forma periódica y cada vez que se cuenta con nueva información.	
Procedimientos de Respaldo y Recuperación de Datos	
Señalar si realiza respaldos completos, diferenciales o incrementales:	El respaldo se realiza cada vez que se tiene información nueva.
El tipo de medios que utiliza para almacenar las copias de seguridad:	Discos duros, CD-ROM.
Cómo y dónde archiva esos medios:	En equipos de cómputo ubicados en los espacios de labores cotidianas en las oficinas del CEN.
Quién es el responsable de realizar estas operaciones:	El enlace por área de los datos personales.

ÁREA: Comisión Nacional de Honor y Justicia	
Nombre del sistema:	Expedientes Legales
Registro de incidentes:	
Los datos que registra:	Fecha, hora y lugar del incidente: Descripción del incidente: Los datos personales comprometidos: Acciones correctivas implementadas de forma inmediata: Nombre y firma de los involucrados:
Si el registro está en soporte físico o soporte electrónico:	Soporte físico y electrónico
Cómo asegura la integridad de dicho registro:	Únicamente el Titular del área podrá tener acceso a dicho registro.
Actualización de la información contenida en el sistema	
La actualización se realiza de forma periódica y cada vez que se cuenta con nueva información.	
Procedimientos de Respaldo y Recuperación de Datos	



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

Señalar si realiza respaldos completos, diferenciales o incrementales:	El respaldo se realiza cada vez que se tiene información nueva.
El tipo de medios que utiliza para almacenar las copias de seguridad:	Discos duros, CD-ROM.
Cómo y dónde archiva esos medios:	En equipos de cómputo ubicados en los espacios de labores cotidianas en las oficinas del CEN.
Quién es el responsable de realizar estas operaciones:	El enlace por área de los datos personales.



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

5. SUPRESIÓN DE DATOS PERSONALES

AREA: Secretaría de Finanzas	
Nombre del sistema:	Finanzas
Motivo de la supresión:	Se suprimen los datos personales cuando han dejado de ser necesarios para el cumplimiento de las finalidades correspondientes y una vez que concluya su plazo de conservación.
Plazos y condiciones para el bloqueo del sistema:	5 años
Procedimiento para la supresión del sistema:	Para la supresión definitiva de los datos personales, se considera lo siguiente: <ul style="list-style-type: none">• Irreversibilidad: que el proceso utilizado no permita recuperar los datos personales;• Seguridad y confidencialidad: que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la LGPDPPSO y los Lineamientos Generales, y• Favorable al medio ambiente: que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.
AREA: Consejo Político Nacional	
Nombre del sistema:	Padrón de Afiliados
Motivo de la supresión:	Se suprimen los datos personales cuando han dejado de ser necesarios para el cumplimiento de las finalidades correspondientes y una vez que concluya su plazo de conservación.
Plazos y condiciones para el bloqueo del sistema:	5 años
Procedimiento para la supresión del sistema:	Para la supresión definitiva de los datos personales, se considera lo siguiente: <ul style="list-style-type: none">• Irreversibilidad: que el proceso utilizado no permita recuperar los datos personales;• Seguridad y confidencialidad: que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la LGPDPPSO y los Lineamientos Generales, y• Favorable al medio ambiente: que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.
AREA: Comisión Nacional de Honor y Justicia	
Nombre del sistema:	Expedientes Legales



DOCUMENTO DE SEGURIDAD
VERSIÓN PÚBLICA

Motivo de la supresión:	Se suprimen los datos personales cuando han dejado de ser necesarios para el cumplimiento de las finalidades correspondientes y una vez que concluya su plazo de conservación.
Plazos y condiciones para el bloqueo del sistema:	5 años
Procedimiento para la supresión del sistema:	<p>Para la supresión definitiva de los datos personales, se considera lo siguiente:</p> <ul style="list-style-type: none">• Irreversibilidad: que el proceso utilizado no permita recuperar los datos personales;• Seguridad y confidencialidad: que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la LGPDPPSO y los Lineamientos Generales, y• Favorable al medio ambiente: que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.