



# **MOVIMIENTO CIUDADANO**

## **POLITICA DE SEGURIDAD DE DATOS PERSONALES**

Abril/2018

## **1. INTRODUCCION**

### **a. Naturaleza jurídica de Movimiento Ciudadano con respecto a los datos personales**

Movimiento Ciudadano es una entidad de interés público cuya finalidad consiste en ser vehículo de la población general para el acceso a la función pública y fungir como promotor de la democracia, tal y como lo señala el artículo 41 constitucional. En este carácter y por ser sujeto obligado por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, tiene como obligación primordial el proteger los datos personales, los cuales en sí son un derecho humano. Esto hace que, para efecto de la transparencia y los datos personales, Movimiento Ciudadano sea equiparable a una autoridad y por ende, se encuentra obligada a respetar y garantizar derechos humanos en términos del artículo 1º de la Constitución Política de los Estados Unidos Mexicanos.

### **b. Objetivos de Movimiento Ciudadano con respecto a los datos personales**

Este instituto político tiene como meta el tratar los datos personales que recabe y resguardarlos de acuerdo a la Ley y a las mejores prácticas existentes, durante el tiempo que se permita. Llevar a cabo esta actividad con rigor técnico protege los derechos humanos de datos personales y ARCO, consagrados en el artículo 16 constitucional. Esto se logra tanto por los procedimientos, estándares y lineamientos que se establezcan, así como por la normativa interna que al efecto tiene Movimiento Ciudadano para regirse en la materia, integrados en el Compendio de Reglamentos, Manuales y Lineamientos de Movimiento Ciudadano publicado en la página <https://transparencia.movimientociudadano.mx/organos-de-transparencia>.

### **c. Alcances de la política de seguridad de datos personales de Movimiento Ciudadano**

La política de seguridad de datos personales de Movimiento Ciudadano se da en cumplimiento del mandato que realiza el artículo 31 de la Ley General de Datos Personales en Posesión de los Sujetos Obligados que al efecto dice:

**Artículo 31.** Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Esta política es de observancia general para todos aquellos responsables, encargados, gestores y usuarios del Sistema de Resguardo de Datos Personales de Movimiento Ciudadano y para aquellos encargados de verificar el buen funcionamiento de dicho sistema. La entrada en vigor de estas políticas se da en el momento en que se hace pública.

## **2. CARACTERÍSTICAS DE LA POLÍTICA DE SEGURIDAD**

La política de seguridad de datos personales es complementaria a la política de gestión de datos personales. Ésta debe tener en su eje el respeto a los derechos humanos, con todos los participantes en el tratamiento de los datos haciendo desde su rol lo necesario para garantizar que los datos personales cedidos a Movimiento Ciudadano no sean accedidos por quien no tenga autorización.

Esta política debe ser el punto de referencia de los procedimientos y herramientas que existan para resguardar datos personales y debe servir para coordinar a los sujetos del Sistema de Resguardo de Datos Personales de Movimiento Ciudadano. Por ello deberá tener las siguientes características:

- **Holística.** Debe cubrir todos los aspectos posibles de la seguridad de datos personales.
- **Proporcional.** Debe adecuarse a las necesidades y recursos de Movimiento Ciudadano.
- **Pro persona.** Tomando en cuenta lo anterior, debe a la vez proveer la protección más amplia posible.
- **Atemporal.** El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- **Amplia.** Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

### **3. SUJETOS DEL SISTEMA DE RESGUARDO DE DATOS PERSONALES**

La política de seguridad de datos personales es responsabilidad de todos aquellos sujetos que forman parte del Sistema de Resguardo de Datos Personales: La Comisión Nacional de Transparencia de Movimiento Ciudadano es la instancia interna final en lo relativo a datos personales y su resguardo; ésta aprueba lo relativo a los procedimientos y políticas en la materia, a propuesta de la Unidad Técnica de Datos Personales, que se encarga de la supervisión de las mismas.

Los responsables de las bases de datos que conforman los sistemas de datos personales son personas física o moral de carácter privado que deciden sobre el tratamiento de los datos personales, para fines de éste documento de seguridad el responsable además de Movimiento Ciudadano, también es el sujeto que tiene a su cargo la supervisión del sistema de datos personales que se trate y sus decisiones son la última palabra respecto del mismo. Los encargados son persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que los vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Los gestores son aquellas personas que tratan datos personales por cuenta del responsable que pertenece a la estructura de Movimiento Ciudadano. Los usuarios son aquellas personas pertenecientes a Movimiento Ciudadano que por su actividad requieren consultar las bases de datos o recabar los datos personales y que se encuentran autorizadas para ello.

La Comisión Nacional de Transparencia y la Unidad Técnica de Datos Personales tienen su dirección en Calle Providencia número 807, esquina Concepción Beistegui, 2do. Piso, Colonia del Valle Centro, Alcaldía Benito Juárez, C.P. 03100, Ciudad de México y cuenta con el siguiente correo electrónico [rramirez@gmail.com](mailto:r Ramirez@gmail.com).

#### 4. PRINCIPIOS RECTORES DEL RESGUARDO DE DATOS PERSONALES

Al ser complemento de la política de gestión de datos personales, la política de seguridad tiene como punto de partida los principios de datos contenidos en el Capítulo I del Título Segundo de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Los principios rectores de la política de seguridad de Movimiento Ciudadano son:

- **Congruencia.** Los esfuerzos para fortalecer la seguridad de los sistemas de información de Movimiento Ciudadano deben ser consistentes con sus valores y principios.
- **Concientización.** Los participantes deberán ser conscientes de la necesidad de contar con sistemas de datos seguros y tener conocimiento de los medios para ampliar dicha seguridad. Estos deben comprender que los fallos en la seguridad pueden dañar significativamente los sistemas bajo su control y vulnerar los derechos humanos de terceros.
- **Responsabilidad.** Todos los participantes son responsables de la seguridad de los sistemas de datos y deben actuar de una manera apropiada a su papel individual. La responsabilidad de los mismos varía de acuerdo con los papeles que desempeñen.
- **Actualización constante.** Los participantes deben igualmente revisar sus propias políticas, prácticas, medidas y procedimientos de manera regular y evaluar si éstos son apropiados en relación con su propio entorno.
- **Respuesta.** Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.
- **Ética.** Los participantes deben hacer esfuerzos por desarrollar y adoptar buenas prácticas y promover conductas que reconozcan la necesidad de salvaguardar la seguridad y respetar los intereses legítimos de terceros.
- **Democracia.** La seguridad de los sistemas de información debe ser compatible con los valores esenciales de una sociedad democrática y garante de derechos humanos.
- **Evaluación del riesgo.** Los participantes deben llevar a cabo evaluaciones de riesgo.
- **Diseño y realización de la seguridad.** Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas de información.
- **Gestión de la Seguridad.** Los participantes deben adoptar una visión integral de la administración de la seguridad. Las políticas de seguridad de los sistemas de información,

así como las prácticas, medidas y procedimientos deben estar coordinadas e integradas para crear un sistema coherente de seguridad.

- **Reevaluación.** Los participantes deben revisar y reevaluar la seguridad de sus sistemas de información, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.

## 5. FORMA EN CÓMO SE RESGUARDAN LOS DATOS PERSONALES

Movimiento Ciudadano obtiene, almacena y trata sus datos personales en virtud de la relación de participación política que existe entre este instituto y ciudadanos afines a su ideología. Movimiento Ciudadano también es responsable de resguardar los datos personales que dimanen de sus actividades administrativas, los cuales se consolidan en un Sistema de Resguardo de Datos Personales consistentes en ocho bases de datos, que tienen un responsable y uno o más encargados.

Movimiento Ciudadano resguarda su información en medios físicos y electrónicos. La infraestructura de almacenamiento que resguarda los sistemas de datos personales son:

- Almacenamiento en equipo de cómputo local.
- Almacenamiento en la red corporativa.
- Almacenamiento en dispositivos externos.
- Almacenamiento en equipos de cómputo portátiles.
- Almacenamiento en expediente físico
- Almacenamiento bajo prestador de servicio
- Almacenamiento de copias de seguridad.

En lo que respecta al resguardo físico, se toman las siguientes medidas:

- Asignación de roles y responsabilidades del personal;
- Administración y uso de medios de almacenamiento físico, mediante la implementación de procedimientos formales de protección contra acceso no autorizado y mal uso de medios de almacenamiento, así como su eliminación segura cuando ya no se necesiten, de tal forma que no sea posible reconstruirlos;

- Registro de usuarios y eliminación de los derechos de acceso mediante bitácoras de registro;
- Mecanismos de seguridad perimetral y control físico de entrada;
- Administración y entrega de los activos y copias de la información una vez terminada la relación laboral;
- Protección de la información al ser transferida o intercambiada con terceros, estableciendo acuerdos y procedimientos. Movimiento Ciudadano no realiza transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados;
- Implementación de acuerdos de confidencialidad;

En cuanto al resguardo electrónico:

- Gestión de uso aceptable de los activos involucrados en el tratamiento de los datos personales para que estos sean utilizados exclusivamente para los fines propuestos.
- Establecimiento de procedimientos de control de cambios.
- Implementación de controles contra código malicioso para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso.
- Establecimiento de procedimientos para la realización de los respaldos de información digital de los sistemas de datos personales, en medios de almacenamiento removibles, en el equipo de cómputo, en la red corporativa y en la nube.
- Gestión de privilegios de acceso lógico para la asignación, modificación y revocación de privilegios de accesos al sistema o aplicaciones de datos personales.
- Administración de usuarios y contraseñas.
- Procedimiento para administrar y controlar la disponibilidad y uso de equipo informático que intervienen en el tratamiento de datos personales dentro y fuera de las instalaciones.
- Registro de auditorías relacionadas a las actividades de los usuarios de los sistemas de datos personales, considerando el registro de cualquier acceso desde cualquier entorno a datos personales, fecha de acceso, usuario y cambios realizados, incluyendo IP origen e IP destino para cada conexión.

- Asegurar la protección de la información de los sistemas de datos personales en el momento de ser transferida o intercambiada con terceros, estableciendo acuerdos y procedimientos necesarios para el intercambio de información (Protocolos Seguros, Cifrado del medio, Autenticación). Movimiento Ciudadano no realiza transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
- Acuerdos de Confidencialidad.
- Administración del uso de la Red y servicios de datos.

La Unidad de Datos Personales tiene los siguientes protocolos para revisar que se implementen las medidas de seguridad:

- Programar de manera periódica auditorías a la unidad responsable del sistema de datos personales, para evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar su cumplimiento y en su caso, implementar mejoras de manera continua, ésta debe mostrar el estado en el que se encuentra la protección de la información por medio de la identificación, análisis y evaluación de debilidades en los activos y en los controles de seguridad aplicados, dicho mecanismo podrá ser técnico o de gestión, interno o externo.
- Asegurar que en todo momento, los empleados conocen, entienden y cumplen con las políticas y procedimientos adoptados por Movimiento Ciudadano en materia de seguridad de datos personales, concientizándolos de los riesgos que puede suponer un mal uso de los dispositivos y soluciones tecnológicas a su alcance.