MOVIMIENTO
CIUDADANO

COMPENDIO DE LINEAMIENTOS EN MATERIA DE TRANSPARENCIA, DATOS PERSONALES Y GESTIÓN ARCHIVÍSTICA

ÍNDICE

LINEAMIENTOS PARA LA REDACCION DE REGLAMENTOS, LINEAMIENTOS CRITERIOS Y MANUALES

CAPITULO PRIMERO

Disposiciones generales

PRIMERO. Estos lineamientos tienen como objeto el proveer reglas generales de estilo y formato para garantizar coherencia y unidad en los diferentes materiales aprobados por la Comisión Nacional de Transparencia, a propuesta de las Unidades Técnicas de Control. Se tratan de accesorios a las disposiciones del Reglamento General de Transparencia, Datos Personales, Archivos y Acceso a la Información de Movimiento Ciudadano.

SEGUNDO. Los lineamientos serán de observancia obligatoria para la Comisión Nacional de Transparencia y sus Unidades Técnicas de Control. Por excepción, las Comisiones Estatales de Transparencia podrán usar este manual para redactar cambios a su reglamento o para generar uno nuevo.

TERCERO. Se entienden como materiales de transparencia, datos personales, archivos y acceso a la información a los reglamentos, manuales, lineamientos y criterios, los cuales son contemplados y explicados por el Reglamento General de Transparencia, Datos Personales, Archivos y Acceso a la Información de Movimiento Ciudadano.

CAPITULO SEGUNDO

Del formato en general

CUARTO. Todos los materiales, excepto los criterios individuales, deberán de tener una portada, con el logo de Movimiento Ciudadano al centro. En medio de la portada, en letra Arial 20 y con mayúsculas, deberá venir el título del documento.

Los criterios podrán compilarse semestral o anualmente y deberán contar con el formato general de los materiales.

QUINTO. Los reglamentos, lineamientos y manuales deberán de ser antecedidos por una sección de consideraciones y una de acuerdos, cuyas secciones irán con un separador en mayúsculas, negritas y al centro.

SEXTO. En las consideraciones deben listarse, por medio de un número arábigo en negrita, cada párrafo donde se señalen los hechos y razones que dan lugar al material tratado. Ejemplo:

CONSIDERANDOS

1. Que en fecha…
2. Que por motivo de…

SÉPTIMO. Las consideraciones deben concluir con un párrafo solemne en el que, habiéndose expuesto los motivos y razones, se fundamenta cómo la Comisión Nacional de Transparencia puede proclamar su orden. En la sección de acuerdos, se listarán en lenguaje imperativo las disposiciones de la Comisión Nacional de Transparencia sobre la creación de dichos materiales. Cada elemento tendrá un numeral ordinal en negritas y mayúscula. Ejemplo:

Por lo anteriormente expuesto y con fundamento en… la Comisión Nacional de Transparencia emite el siguiente:

ACUERDO

PRIMERO. Se aprueba…
SEGUNDO. Se instruye…

OCTAVO. Salvo indicación de lo contrario, los materiales serán escritos en letra Arial tamaño 12, justificado y con un espaciado de 1.

CAPITULO TERCERO

De los Reglamentos

NOVENO. Los reglamentos deberán escribirse en un lenguaje mayormente imperativo, estableciendo normas ónticas, deónticas y técnicas. El título del reglamento deberá estar en la parte superior del documento, al centro y en negrillas.

Ejemplo:

REGLAMENTO GENERAL DE TRANSPARENCIA, DATOS PERSONALES, ARCHIVOS Y ACCESO A LA INFORMACION

DÉCIMO. Los reglamentos podrán dividirse en Libros, Títulos y Capítulos; cada división deberá tener un título debajo, ambos deberán plasmarse en mayúsculas.

Ejemplos:

LIBRO I

ORGANIZACIÓN GENERAL

TITULO I

DISPOSICIONES GENERALES

…

CAPÍTULO I

COMISION NACIONAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN

DÉCIMO PRIMERO. El articulado deberá ir en negritas de la forma siguiente: "**Artículo (Número)**". Cada artículo de los reglamentos deberá tener una descripción en negritas antecediéndole. Dicha descripción podrá usarse en párrafos donde esto sea relevante.

Ejemplo:

Objeto del Reglamento

Artículo 1. El presente reglamento tiene por objeto regular los procedimientos internos de Movimiento Ciudadano…

DÉCIMO SEGUNDO. Las numeraciones hechas en cada artículo deberán ir en numerales romanos.

DÉCIMO TERCERO. En caso de referirse a una enumeración de conceptos, ésta deberá de ir de la siguiente forma: "(numeral romano). **Título del concepto:** (Definición)".

Ejemplo:

Principios de la transparencia

Artículo 5. Son principios rectores de la transparencia:

I. **Eficacia:** se deberá tutelar de forma efectiva el derecho de acceso a la información. Se debe dar publicidad a las deliberaciones y actos relacionados con sus atribuciones, así como otorgar acceso a la información que generen.

…

DÉCIMO CUARTO. La sección de normas transitorias debe contar con una separación que así lo indique; deberá ir en mayúsculas y negrillas; los elementos de esta sección deberán ir en números ordinales, en mayúsculas y negrillas.

Ejemplo:

TRANSITORIOS

PRIMERO. Este reglamento entrará en vigor el día…

DÉCIMO QUINTO. En los reglamentos modelo, la metanorma deberá anteceder al cuerpo del articulado, su sección deberá distinguirse de misma forma que con los transitorios; podrá crearse una explicación sobre la misma antes de proceder a su elaboración. Los elementos de la metanorma tendrán el mismo formato que el articulado general.

Ejemplo:

METANORMA

Se entiende por metanorma a la regla que hace cumplir otra...

Propósitos del reglamento

Artículo 1. Este reglamento tiene como propósito cumplir con el procedimiento que se establece en el artículo 41 del Reglamento General de Transparencia, que a su vez aplica los artículos 68, 69 y 70 de los Estatutos de Movimiento Ciudadano.

CAPITULO CUARTO

De los lineamientos

DÉCIMO SEXTO. Los lineamientos deben escribirse en un lenguaje mayormente imperativo, estableciendo normas técnicas. El título de los lineamientos deberá estar en la parte superior del documento, al centro y en negrillas.

DÉCIMO SÉPTIMO. Los reglamentos podrán dividirse en capítulos cuyas divisiones se plasmarán en mayúsculas; éstas deberán tener debajo un título en minúsculas. Cada elemento del reglamento deberá ir en números ordinales en mayúsculas y negrillas.

Ejemplo:

CAPITULO PRIMERO
Disposiciones generales

PRIMERO. Estos lineamientos tienen como objeto…

DÉCIMO OCTAVO. Las numeraciones hechas por cada elemento deberán ir en numerales romanos.

DÉCIMO NOVENO. Los ejemplos deberán ir en letra Arial 10, con justificación.

VIGÉSIMO. La sección de normas transitorias debe tener una separación que así lo indique, en mayúsculas y negrillas; los elementos de esta sección deberán ir en números ordinales, en mayúsculas y negrillas.

CAPITULO QUINTO

De los manuales

VIGÉSIMO PRIMERO. Los manuales deben escribirse en un lenguaje descriptivo, estableciendo procedimientos a seguir para el cumplimiento de objetivos concretos. Su título deberá encontrarse en la parte superior del documento, al centro y en negrillas.

VIGÉSIMO SEGUNDO. Los manuales podrán dividirse en secciones, éstas deberán tener un numeral arábigo y podrán tener subsecciones marcadas con letras. Cada manual deberá contar con los siguientes elementos:

I. Objetivos;
II. Alcance;
III. Responsables de la aplicación del manual;
IV. Políticas;
V. Procedimientos;
VI. Glosario, y
VII. Formatos.

VIGÉSIMO TERCERO. Cada procedimiento podrá tener sub-procedimientos y deberán especificar:

I. Objetivo;
II. Descripción, y
III. Actividades secuenciales por responsable.

VIGÉSIMO CUARTO. Las actividades secuenciales por responsable deberán tener los elementos siguientes:

I. Responsable;
II. Número de acción;
III. Actividades, y
IV. Método o herramienta.

Estos elementos podrán manifestarse en un cuadro con las características siguientes:

Responsable	No.	Actividades	Método o herramienta
Oficialía de partes/Unidad de correspondencia	1	Recibe correspondencia y paquetería oficial externa. ¿La correspondencia se recibe sin envase? a) Sí: continúa actividad 2. b) No: continúa actividad 3.	Correspondencia con acuse de recibido

VIGÉSIMO CUARTO. Las actividades secuenciales podrán seguir una causalidad lineal, circular o con ramificaciones. Al finalizar cada cuadro, deberá indicarse poniendo debajo del mismo la frase **"Fin del procedimiento"**. Ejemplo:

Oficialía de partes/Unidad de correspondencia	23	Elabora reporte de gestión y resolución de asuntos con fines de seguimiento.	Reporte diario de correspondencia (anexo 2)

Fin del procedimiento

CAPITULO SEXTO

De los criterios

VIGÉSIMO QUINTO. Los criterios deberán escribirse en lenguaje imperativo establecer interpretaciones de la Ley ylos materiales de transparencia, datos personales, archivo y acceso a la información que resuelvan problemas sobre su sentido o hagan integraciones ante asuntos imprevistos.

VIGÉSIMO SEXTO. Los criterios deberán tener un encabezado y un cuerpo. El primero es un resumen de la interpretación y deberá estar en negrita, el segundo es la interpretación que se realiza. Lo anterior debe ser análogo a los criterios del INAI.

Ejemplo:

Las dependencias y entidades no están obligadas a generar documentos ad hoc para responder una solicitud de acceso a la información. Tomando en consideración lo establecido por el artículo 42 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que establece que las dependencias y entidades sólo estarán obligadas a entregar documentos que se encuentren en sus archivos, las dependencias y entidades no están obligadas a elaborar documentos ad hoc para atender las solicitudes de información, sino que deben garantizar el acceso a la información con la que cuentan en el formato que la misma así lo permita o se encuentre, en aras de dar satisfacción a la solicitud presentada.

VIGÉSIMO SÉPTIMO. Si el criterio nace de una o varias solicitudes donde surge la problemática, debajo del mismo deben listarse los expedientes.

LINEAMIENTOS PARA PUBLICAR Y ACTUALIZAR INFORMACIÓN EN LOS PORTALES DE TRANSPARENCIA (MICROSITIO y SIPOT)

CAPITULO PRIMERO

Disposiciones generales

PRIMERO. El presente lineamiento tiene como finalidad reglamentar el cumplimiento de las obligaciones de transparencia que debe realizar Movimiento Ciudadano en su carácter de Sujeto Obligado, de acuerdo con los artículos 70 y 76 de la Ley General de Transparencia y Acceso a la Información Pública y a su equivalente en las respectivas legislaciones locales de cada unidad.

SEGUNDO. Las obligaciones de transparencia mencionadas por el artículo anterior se cumplen mediante la carga de información en el Sistema de Portales de Transparencia (en lo sucesivo SIPOT) y en el sitio de transparencia de Movimiento Ciudadano (en lo sucesivo Micro sitio).

La información se actualizará por las Unidades Administrativas Responsables en los tiempos señalados por la Ley.

TERCERO. Dichas obligaciones se llevarán a cabo por la Comisión Nacional de Transparencia y las Unidades de Transparencia de los respectivos estados y el Nacional.

CUARTO. El procedimiento de carga de información tiene las siguientes fases:

Para el Micro sitio:

I. Identificación de obligaciones de Transparencia a nivel nacional y por estados, mediante la tabla de aplicabilidad proporcionada por los Órganos Garantes.
II. El Comité de Transparencia Nacional y de cada Estado, junto con las Unidades Administrativas responsables de la información, deberán sesionar para asignar los Artículos y Fracciones correspondientes a cada Unidad Administrativa o responsable de la información.
III. Registro de Unidades Administrativas y responsables para su seguimiento.
IV. Carga preliminar de la información
V. Revisión de la información.
VI. Publicación.

Para el SIPOT: una vez validada y cargada la información para dar cumplimiento en el Micro sitio nacional o de los Estados, se podrá migrar dicha información a los formatos de la Plataforma Nacional de Transparencia (PNT).

VII. La unidad de Transparencia, una vez dada de alta ante el órgano garante local o federal, podrá administrar el SIPOT y dar de alta a usuarios y sus contraseñas, asignándoles las fracciones y formatos correspondientes.
VIII. Dadas de alta las Unidades Administrativas con sus respectivas fracciones, los responsables por unidad administrativa podrán descargar los formatos asignados.
IX. Una vez descargados dichos formatos, deberán ser requisados con la información previamente validada y actualizada en el Micro sitio del partido.
X. Por ultimo deberá cargar los formatos debidamente llenados dándolos de alta para consulta pública en la PNT y SIPOT.

CAPITULO SEGUNDO

De la identificación de obligaciones y registro de Unidades Administrativas Responsables

QUINTO. La Comisión Nacional de Transparencia del Partido Movimiento Ciudadano, por medio de las Unidades de Transparencia, deberá registrar cuáles son las Unidades Administrativas Responsables que tienen obligaciones de transparencia y formatos asignados.

SEXTO. Las Unidades de Transparencia deberán revisar las obligaciones aplicables contenidas en la Ley General de Transparencia y en la normatividad ajustable de conformidad con la tabla de aplicabilidad generada por los órganos garantes. Deberán analizar también la carga de trabajo correspondiente a cada Unidad Administrativa Responsable, para generar un proyecto de reparto de obligaciones y carga que después someterá a consideración de la Comisión Nacional de Transparencia para generar el acuerdo correspondiente.

SÉPTIMO. Hecho el acuerdo correspondiente, la Comisión Nacional de Transparencia deberá repartir las listas, los formatos y las contraseñas correspondientes, así como el tratamiento de la información obligada a cargar.

CAPITULO TERCERO

De la carga y publicación de la información

OCTAVO. Al recibir los formatos previamente asignados, las Unidades Administrativas Responsables deberán llenarlos con la información solicitada y cargarlos en el portal de transparencia de Movimiento Ciudadano (Micro sitio).

NOVENO. La Comisión Nacional de Transparencia deberá supervisar la carga de la información y, al estar desprovista de errores, habilitarla a disposición del público.

DÉCIMO. La información habilitada deberá cargarse de la misma forma al SIPOT, guardando los acuses y corrigiendo la información donde así lo observe el garante después de una evaluación vinculatoria.

DÉCIMO PRIMERO. En el caso de información provista por el Instituto Nacional Electoral, la Comisión Nacional de Transparencia hará el reparto de la misma a las Unidades de Transparencia de los estados y éstas a su vez a la Unidad Administrativa correspondiente para que ésta realice su carga.

LINEAMIENTOS PARA LA ATENCIÓN DE SOLICITUDES DE ACCESO A LA INFORMACIÓN

CAPITULO PRIMERO

Disposiciones generales

PRIMERO. El presente lineamiento tiene como propósito establecer las reglas por las cuales Movimiento Ciudadano debe recibir, canalizar, tramitar y responder las solicitudes de acceso a la información que le lleguen.

SEGUNDO. La Unidad de Transparencia es la responsable de llevar a cabo todas las gestiones y notificaciones necesarias a fin de garantizar la efectividad del procedimiento administrativo y, en sí, facilitar el acceso a la información a todo público que lo solicite.

TERCERO. El procedimiento administrativo de acceso a la información sigue las siguientes etapas:

I. Recepción de la solicitud a través del sistema INFOMEX, correo a la Unidad de Transparencia, correo postal, llamada telefónica a la UT.
II. Se analiza si procede o no dicha solicitud.
III. En caso de no proceder por ajustarse a algún supuesto descrito por la norma aplicable, el sistema deshabilitara dicha solicitud eliminándola.
IV. En caso de ser procedente dicha solicitud, el sistema INFOMEX le asigna un número de folio para su identificación.
V. Turno a la Unidad Administrativa Responsable.
VI. Generación de la información por parte de la Unidad Responsable;
VII. Entrega de la información a la Unidad de Transparencia.
VIII. En caso de no poder enviar la información a través del sistema INFOMEX, la Unidad de Transparencia deberá ofrecer al peticionario las demás formas de entrega de la información.

CUARTO. La respuesta a la solicitud de la información debe darse en un plazo no mayor a veinte días; éste puede encontrarse sujeto a una prórroga de hasta diez días cuando exista motivo para ello y se emita una resolución debidamente fundada y motivada por parte del Comité de Transparencia, ya sea Nacional o del estado; debe notificarse por parte de la unidad administrativa antes del vencimiento del plazo de Ley.

QUINTO. La información debe ser entregada en la modalidad de entrega seleccionada por el solicitante; de no ser posible, se le podrán ofrecer otras opciones, siempre y cuando se funden y motiven las razones para esto, por ejemplo: puesta a disposición de la información al particular (previa acreditación de la personalidad), envío de la información por correo postal, copias simples y copias certificadas en su cuestión. En el caso de que la información solicitada

consista en bases de datos, se deberá privilegiar la entrega de la misma en Formatos Abiertos.

CAPITULO SEGUNDO

De la recepción y turno de las solicitudes

SEXTO. La Unidad de Transparencia tiene la obligación de actuar como receptor de solicitudes presenciales de acceso a la información, de turnar toda solicitud recibida en la Unidad Administrativa Responsable que tenga o pueda tener la información requerida y dar control y seguimiento de las mismas hasta su respuesta.

CAPITULO TERCERO

De la generación de información

SÉPTIMO. Si la información existe y puede ser entregada tal y como se encuentra, la Unidad Administrativa Responsable informará a la Unidad de Transparencia y señalará el día de entrega de la información.

Si la solicitud no es clara, la Unidad Administrativa Responsable solicitará a Unidad de Transparencia información adicional al solicitante.

Si se requiere de una prórroga, la Unidad Administrativa Responsable pedirá a la Unidad de Transparencia sesionar y realizar la solicitud de prórroga a través de la plataforma dentro del plazo de los primeros 5 días a su recepción.

OCTAVO. Si después de una búsqueda exhaustiva y razonable, en los archivos físicos y electrónicos del sujeto obligado, no se localiza la información solicitada, la Unidad Administrativa Responsable deberá emitir un oficio fundado y motivado para solicitar a la Unidad de Transparencia que sesione el Comité de Transparencia y declare la inexistencia de la información a través de un acuerdo y resolutivo, declarando la Inexistencia de la Información.

CAPITULO CUARTO

De la entrega de la información a la Unidad de Transparencia;

NOVENO. Al recibir la información suministrada por la Unidad Administrativa Responsable, la Unidad de Transparencia verificará la pertinencia de la respuesta,

para que, en caso de no cumplir con los requerimientos de Ley, se requiera su modificación.

DÉCIMO. Teniendo la información requerida, la Unidad de Transparencia preparará la respuesta formal, por oficio, al requirente. Ésta se cargará en el Sistema Nacional de Transparencia con todos sus anexos.

CAPITULO QUINTO

De la clasificación de la información

La clasificación de la información, por parte de las Unidades Administrativas Responsables, se llevará a cabo al momento de recibir una solicitud de información, determinar mediante resolución de autoridad competente y generar versiones públicas para dar cumplimiento a las obligaciones de ley.

DÉCIMO PRIMERO. En caso de que la Unidad Administrativa Responsable considere que la información solicitada es sujeta de clasificarse como información confidencial, deberá enviar un oficio en el que pida a la Unidad de Transparencia apruebe su clasificación total o parcial según el caso, dicho oficio deberá ir acompañado de una prueba de daño, en términos del artículo 114 de la Ley General de Transparencia y Acceso a la Información Pública.

DÉCIMO SEGUNDO. El razonamiento hecho en la prueba de daño deberá contener:

I. La definición del interés público que se afecta;
II. La definición del interés particular de Movimiento Ciudadano en relación al principio general utilizado para justificar la causal de reserva y el interés particular.
III. El contraste de intereses tomando como eje el principio general.
IV. La explicación de por qué el interés particular, conjuntado al principio general constituyen una excepción válida al principio de máxima publicidad contenido en el artículo 6º de la Constitución Federal.

DÉCIMO TERCERO. Al recibir el oficio de la Unidad Administrativa Responsable, la Unidad de Transparencia pedirá la versión pública de los documentos solicitados y los remitirá al Comité de Transparencia para que resuelva el caso.

La información clasificada como *Reservada* se ajustara a los supuestos previstos en el artículo 113, 114 y 115 de la LGTAIP.

LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE LAS OBLIGACIONES DE TRANSPARENCIA POLÍTICA

CAPITULO PRIMERO

Disposiciones generales

PRIMERO. Estos lineamientos tienen como finalidad establecer los elementos necesarios para efectuar el contenido de la fracción II del artículo 50 del Reglamento General de Transparencia, Datos Personales, Archivos y Acceso a la Información de Movimiento Ciudadano. También se buscan implementar los artículos 52 a 56 de dicho Reglamento.

SEGUNDO. La política de trasparencia proactiva, contenida en la fracción II del artículo 50 del Reglamento General de Transparencia, implica la publicación de información más allá de lo que exige la Ley General de Transparencia y Acceso a la Información Pública.

Esto debe llevarse a cabo por medio del llenado de formatos por parte de los sujetos obligados de la transparencia proactiva, de acuerdo con su categoría, con la información que se les requiera.

TERCERO. Para efecto de recabar la información proactiva, se puede hacer uso de las bases de datos que Movimiento Ciudadano posee de los integrantes de sus órganos de decisión, siempre y cuando se sigan las medidas de protección de datos necesarias y determinadas por la Comisión Nacional de Transparencia a propuesta de la Unidad de Datos Personales.

CUARTO. Las categorías de sujetos obligados de la transparencia proactiva de Movimiento Ciudadano, en su representación nacional y estatal, son las siguientes:

I. **Dirigentes:** comprende a los dirigentes y funcionarios que realicen tareas políticas de Movimiento Ciudadano a nivel nacional, estatal y municipal. Esto incluye a los miembros de las comisiones de control y a los titulares de las secretarías y comisiones diversas de la Comisión Operativa Nacional.

II. **Personal administrativo:** sistematiza a todos los que participen en la estructura administrativa de Movimiento Ciudadano a nivel nacional, estatal y municipal, en lo que respecta al uso de los fondos públicos recibidos por dicho instituto político y por la toma de decisiones de trascendencia pública.

III. **Candidatos:** se conforma por todos aquellos que sean candidatos por Movimiento Ciudadano a cualquier puesto de representación popular, sin importar el nivel de gobierno ni su afiliación o militancia.

IV. **Padrón de representantes populares en funciones:** integrado por los diputados locales y federales, senadores, gobernadores, presidentes municipales, síndicos y regidores que tienen afiliación o afinidad con Movimiento Ciudadano.

QUINTO. La información de transparencia proactiva deberá recabarse por medio de formatos y publicarse en Internet.

Los militantes y simpatizantes del partido que se encuentren dentro de las categorías de sujetos obligados de transparencia proactiva deberán también llenar y firmar una carta compromiso con el decálogo identitario de Movimiento Ciudadano. Este documento será escaneado y deberá hacerse público en la página de Internet correspondiente.

Para hacer pública la información relativa a la declaración de impuestos, patrimonial y de interés, militantes y simpatizantes del partido que se encuentren dentro de las categorías de sujetos obligados de transparencia proactiva, deberán firmar una carta donde den permiso expreso para ello.

SEXTO. Las Comisiones Nacional de Transparencia y Acceso a la Información Pública y de Seguimiento de los Órganos de Dirección en Redes Sociales son las encargadas de crear los formatos, coordinar a las categorías de sujetos para que provean la información requerida, coadyuvar en la actualización de la información y publicar la información de transparencia proactiva en línea.

CAPÍTULO SEGUNDO

Del llenado de formatos y entrega de cartas y declaraciones

SÉPTIMO. Todo dirigente tiene la obligación de llenar el formato de transparencia proactiva en línea y de entregarlo a la Comisión de Seguimiento de los Órganos de Dirección en Redes Sociales, al momento de tomar posesión de su cargo; la información deberá ser verificada por la Comisión Nacional de Transparencia.

Una vez que se dé cuenta de que se ha llenado el formato correctamente, la Comisión Nacional de Transparencia ordenará a la Comisión de Seguimiento de los Órganos de Dirección en Redes Sociales que publique dicha información en línea.

OCTAVO. La página de Internet con la información recabada de transparencia política deberá tener un espacio para que los ciudadanos y organizaciones de la sociedad civil manifiesten su opinión de la coherencia de las acciones de los dirigentes con respecto a la definición ideológica del partido.

NOVENO. Todo funcionario administrativo tiene la obligación de llenar el formato y entregarlo a la Comisión de Seguimiento de los Órganos de Dirección en Redes

Sociales al momento de asumir su puesto; la información deberá ser verificada por la Comisión Nacional de Transparencia.

Una vez llenado el formato correctamente, la Comisión Nacional de Transparencia ordenará a la Comisión de Seguimiento de los Órganos de Dirección en Redes Sociales que publique dicha información en línea.

DÉCIMO. El cumplimiento de las obligaciones de transparencia política es un requisito esencial para el registro de las candidaturas. La Comisión Nacional de Transparencia verificará su cumplimiento e implementará dicha sanción.

DÉCIMO PRIMERA. Todo candidato tiene la obligación de llenar el formato correspondiente en línea y de entregarlo a la Comisión de Seguimiento de los Órganos de Dirección en Redes Sociales antes de registrar su candidatura; la información deberá ser verificada por la Comisión Nacional de Transparencia.

DÉCIMO SEGUNDA. La página de Internet donde se contengan los formatos que constituyen las obligaciones de transparencia política deberá tener también un espacio para que los ciudadanos y organizaciones de la sociedad civil manifiesten su opinión de la coherencia de las acciones de los candidatos con respecto a la definición ideológica del partido.

DÉCIMO TERCERA. Todo funcionario de elección popular tiene la obligación de llenar el formato correspondiente en línea y de entregarlo a la Comisión de Seguimiento de los Órganos de Dirección en Redes Sociales al momento de tomar posesión de su cargo; la información deberá ser verificada por la Comisión Nacional de Transparencia.

Una vez que se dé cuenta de que se ha llenado el formato correctamente, la Comisión Nacional de Transparencia ordenará a la Comisión de Seguimiento de los Órganos de Dirección en Redes Sociales que publique dicha información en línea.

DÉCIMO CUARTA. La página de Internet con la información recabada de transparencia política deberá tener también un espacio para que los ciudadanos y organizaciones de la sociedad civil manifiesten su opinión sobre la coherencia de las acciones de los funcionarios populares electos con respecto a la definición ideológica del partido.

DÉCIMO QUINTA. Todas las categorías de sujetos obligados deberán tener sus declaraciones patrimoniales, de impuestos e intereses, así como una carta compromiso con el decálogo del partido y una carta donde se autorice la publicación de los datos personales que contienen dichas declaraciones al momento de iniciar su cargo o encomienda o cuando se lo requiera la Comisión Nacional de Transparencia.

LINEAMIENTOS PARA LA ADMINISTRACIÓN DEL SISTEMA DE RESGUARDO DE DATOS PERSONALES

CAPÍTULO PRIMERO

Disposiciones generales

PRIMERO. El Sistema de Resguardo de Datos Personales de Movimiento Ciudadano tiene el propósito de cumplir con las disposiciones del artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, respecto a los datos personales. La supervisión de su buen funcionamiento corre a cargo de la Comisión Nacional de Transparencia a través de la Unidad de Datos Personales.

SEGUNDO. Este Sistema se dividirá en las siguientes bases de datos:

I. Afiliados, militantes y simpatizantes.

II. Empleados.

III. Precandidatos.

IV. Consejo Ciudadano Nacional.

V. Círculos ciudadanos.

VI. Comisión operativa musical.

VII. Fundación México con Valores.

VIII. Participantes en eventos.

TERCERO. Son sujetos del Sistema de Resguardo de Datos Personales, los siguientes:

I. Responsables: persona o personas de la estructura de Movimiento Ciudadano, decide sobre el tratamiento de los datos personales.

II. Encargados: tratan los datos personales por cuenta del responsable, como consecuencia de la existencia de una relación que le vincula con el mismo y delimita el ámbito de su actuación a las instrucciones del responsable.

III. Usuarios: personas pertenecientes a Movimiento Ciudadano, por su actividad requieren consultar las bases de datos de dicho instituto político y se encuentran autorizadas para ello.

IV. Comisión Nacional de Transparencia: órgano de control de Movimiento Ciudadano para instituir y mantener el resguardo de datos personales.

V. Unidad de Datos Personales: unidad técnica de control por medio de la cual opera la Comisión Nacional de Transparencia para el cumplimiento de su propósito.

CUARTO. El resguardo de datos personales es aquella actividad inclinada a evitar que personas no autorizadas tengan acceso a la información personal recabada y tratada por Movimiento Ciudadano, con el consentimiento de aquellos a quienes les atiene.

Se entiende por resguardo físico al almacenaje y protección de datos personales plasmados en medios mecánicos y electromecánicos o electrónicos, evitando el acceso no autorizado del lugar donde se encuentren los mismos. Dichos medios permiten un acceso directo del usuario al medio donde se encuentra la información.

El resguardo electrónico es aquel en el que el almacenaje y protección de las bases de datos se da a través de un sistema electrónico que compila la información en un servidor. Este medio no permite un acceso directo del usuario al medio donde se encuentra la información, pues ésta se encuentra fuera de dicho espacio físico.

QUINTO. Los responsables, encargados y usuarios del Sistema de Resguardo de Datos Personales deben tener consciencia de las medidas de seguridad necesarias para garantizar el almacenamiento, protección y tratamiento adecuado de datos personales. Para ello, la Unidad de Datos Personales deberá implementar procedimientos de concienciación.

CAPÍTULO SEGUNDO

De las obligaciones de los sujetos del sistema de resguardo de datos personales

SEXTO. Son obligaciones del responsable de una base de datos del Sistema de Resguardo de Datos Personales:

I. Cumplir con las políticas de seguridad y procedimientos estipulados en el documento de seguridad y en la política de seguridad de datos personales generada por la Unidad de Datos Personales: debe autorizar la Comisión Nacional de Transparencia.
II. Adoptar los mecanismos idóneos para conservar la información a su resguardo bajo las condiciones de seguridad necesarias en aras de impedir su alteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
III. Garantizar que los datos tratados de carácter personal sean los adecuados, pertinentes y no excesivos para la finalidad que justifica su tratamiento, deben

mantenerse exactos y cancelarse cuando ya no respondan a la finalidad para la que se recabaron.
IV. Garantizar a los titulares, a través de los canales de atención establecidos por el partido, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento, a fin de que pueda tomar decisiones informadas al respecto.
V. Solicitar al encargado el resguardo correcto de las autorizaciones otorgadas por los titulares de datos.
VI. Informar a los titulares de los datos personales sobre la finalidad de la recolección y los derechos que le asisten en virtud de ello, en el texto utilizado—para obtener la autorización—o en el Aviso de Privacidad.
V. Garantizar que la información suministrada al encargado del tratamiento sea veraz, completa, exacta, comprobable y comprensible.
VI. Exigir al encargado del tratamiento, en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.
VII. Informar al responsable de la Unidad de Datos Personales cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración y resguardo de la información de datos personales.
VIII. Las que se señalen en el documento de seguridad y política de seguridad aprobadas por la Comisión Nacional de Transparencia.
IX. Las que deriven del Reglamento General de Transparencia, de los lineamientos y criterios aprobados por la Comisión Nacional de Transparencia.

SÉPTIMO. Son obligaciones del encargado de una base de datos del Sistema de Resguardo de Datos Personales:

I. Resguardar las autorizaciones otorgadas por los titulares de datos.
II. Verificar que se informe a los titulares de los datos personales sobre la finalidad de la recolección y los derechos que le asisten en virtud de ello, en el texto utilizado—para obtener la autorización—o en el Aviso de Privacidad.
IV. Adoptar los mecanismos idóneos para conservar la información bajo las condiciones de seguridad necesarias en aras de impedir su alteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
V. Verificar que la información sea veraz, completa, exacta, comprobable y comprensible.
VI. Exigir a los usuarios que el tratamiento de la información cumpla en todo momento con las condiciones de seguridad y privacidad de la información del titular.
VII. Supervisar que sólo las personas autorizadas tengan acceso a la información, previa autorización del responsable.
VIII. Informar al responsable cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración y resguardo de la información de datos personales.
IX. Cumplir con las políticas de seguridad y procedimientos contenidos en el presente documento de seguridad de datos personales.

X. Las que se señalen en el documento de seguridad y política de seguridad aprobadas por la Comisión Nacional de Transparencia.
XI. Las que deriven del Reglamento General de Transparencia, de los lineamientos y criterios aprobados por la Comisión Nacional de Transparencia.

OCTAVO. Son obligaciones de los usuarios del Sistema de Resguardo de Datos Personales, en lo que les resulte aplicable, las siguientes:

I. Entregar al responsable la autorización otorgada por el titular de los datos personales.
II. Informar a los titulares de los datos personales sobre la finalidad de la recolección y los derechos que le asisten en virtud de ello, en el texto utilizado—para obtener la autorización—o en el Aviso de Privacidad.
III. Adoptar los mecanismos establecidos para conservar la información bajo las condiciones de seguridad necesarias en aras de impedir su alteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
IV. Verificar que la información sea veraz, completa, exacta, comprobable y comprensible.
V. Cumplir en todo momento con las condiciones de seguridad y privacidad en el tratamiento de los datos personales manejado.
VI. Informar al encargado cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración y resguardo de la información de datos personales.
VII. Cumplir con las políticas de seguridad y procedimientos contenidos en el presente documento de seguridad de datos personales.
VIII. Las que se señalen en el documento de seguridad y política de seguridad aprobadas por la Comisión Nacional de Transparencia.
IX. Las que deriven del Reglamento General de Transparencia, de los lineamientos y criterios aprobados por la Comisión Nacional de Transparencia.

NOVENO. Son obligaciones de la Comisión Nacional de Transparencia en lo que refiere al Sistema de Resguardo de Datos Personales:
I. Aprobar el documento de seguridad que someta a su consideración la Unidad de Datos Personales;
II. Aprobar la política de seguridad de datos personales que someta a su consideración la Unidad de Datos Personales.
III. Generar los lineamientos y criterios necesarios para que se implementen de forma plena el documento de seguridad y la política de seguridad.
IV. Supervisar la implementación del documento de seguridad y la política de seguridad que lleve a cabo la Unidad de Datos Personales.
V. Las que se señalen en el documento de seguridad y política de seguridad aprobadas por la Comisión Nacional de Transparencia.
VI. Las que deriven del Reglamento General de Transparencia y de sus lineamientos y criterios.

DÉCIMO. Son obligaciones de la Unidad de Datos Personales:

I. Poner a consideración de la Comisión Nacional de Transparencia un proyecto de documento de seguridad para su aprobación.
II. Poner a consideración de la Comisión Nacional de Transparencia un proyecto de política de seguridad de datos personales para su aprobación.
III. Capacitar a usuarios, responsables y encargados que lo requieran.
IV. Dar consultas a usuarios, responsables y encargados que se lo pidan.
V. Atender el ejercicio de los derechos ARCO formulados por los titulares dentro de los términos establecidos.
VI. Implementar el contenido del documento de seguridad y la política de seguridad que apruebe la Comisión Nacional de Transparencia.
VII. Las que se señalen en el documento de seguridad y política de seguridad aprobadas por la Comisión Nacional de Transparencia.
VIII. Las que deriven del Reglamento General de Transparencia, de los lineamientos y criterios aprobados por la Comisión Nacional de Transparencia.

CAPÍTULO TERCERO

De los proveedores de servicio de tratamiento de datos personales

DÉCIMO PRIMERO. En caso de que Movimiento Ciudadano contrate servicios para el tratamiento de datos personales, el subcontratado deberá asumir el carácter de encargado en términos de los lineamientos de datos personales y cualquier otro que resulte aplicable.
Asimismo, deberá existir autorización expresa de Movimiento Ciudadano para el tratamiento de datos personales con el subcontratado a través de un contrato o cualquier otro instrumento jurídico que se decida. El tratamiento de los datos personales por parte del subcontratado se deberá limitar a través de cláusulas contractuales u otros instrumentos jurídicos de conformidad con la normatividad que le resulte aplicable.

DÉCIMO SEGUNDO. El instrumento de subcontratación debe ser firmado por el representante jurídico de Movimiento Ciudadano. Son partes del mismo:

I. Encabezado;

II. Declaraciones;

III. Clausulado;

IV. Fundamentación y motivación, y

VI. Firmas de titulares y testigos.

DÉCIMO TERCERO. En el caso de la contratación o adhesión de servicios, aplicaciones e infraestructura en el cómputo en la nube que implique el tratamiento de datos personales, el subcontratado deberá garantizar políticas de protección de

datos personales equivalentes a las establecidas en la normativa interna de Movimiento Ciudadano.

DÉCIMO CUARTO. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube, en los que Movimiento Ciudadano se adhiera a los mismos, mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla al menos con lo siguiente:

- Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la normativa interna de Movimiento Ciudadano.
- Transparentar las subcontrataciones donde se involucre la información sobre la que se presta el servicio.
- Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio.
- Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

DÉCIMO QUINTO. El proveedor deberá contar con mecanismos que:

- Den a conocer cambios en sus políticas de privacidad o condiciones del servicio prestado.
- Permitan a Movimiento Ciudadano limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio.
- Establezcan y mantengan medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio.
- Garanticen la supresión de los datos personales una vez concluido el servicio prestado al responsable y este último haya podido recuperarlos.
- Impidan el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar acerca de ese hecho al responsable.

DÉCIMO SEXTO. Movimiento Ciudadano no podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme al presente documento de seguridad y demás disposiciones que resulten aplicables.

CAPÍTULO CUARTO

Del resguardo electrónico

DÉCIMO SÉPTIMO. Serán medidas mínimas de resguardo electrónico las siguientes:

I. Los controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos.
II. La creación de copias de respaldo de la información y aplicaciones.

III. El respaldo seguro de datos personales, garantizando que el mismo tenga el mismo nivel de protección que la base de datos.

IV. La gestión y control de las redes necesarias para mantener la seguridad de las bases de datos.

V. El uso de contraseñas de acuerdo con las buenas prácticas de seguridad.

VI. Los registros de auditoría relacionados a las actividades de los usuarios, las excepciones y eventos de seguridad. Se debe registrar la fecha de acceso, el usuario y los cambios a realizar.

VII. La administración de la asignación y uso de privilegios.
VIII. Bloqueos automáticos de equipos desatendidos.
IX. Identificación y autenticación de usuarios.
X. Control de vulnerabilidades técnicas de los sistemas de información que se utilizan.

CAPÍTULO CUARTO

Del resguardo físico

DÉCIMO OCTAVO. Serán medidas mínimas de resguardo electrónico las siguientes:

I. Los perímetros de seguridad física tales como cerrojos, candados, paredes, tarjetas que controlan entradas, recepciones entre otros.
II. Los controles de entrada para asegurar que únicamente personal autorizado tenga permitido el acceso.
III. La protección y seguridad del equipo de cómputo.
IV. La autorización de salida del equipo, información y software de las instalaciones.

V. Eliminación segura de los medios de almacenamiento cuando no sean necesarios.
VI. La protección de medios físicos de almacenamiento en tránsito.

LINEAMIENTOS PARA LA CREACIÓN DEL DOCUEMENTO DE SEGURIDAD INICIAL DE DATOS PERSONALES

CAPÍTULO PRIMERO

Disposiciones generales

PRIMERO. Estos lineamientos tienen como finalidad establecer los elementos del documento de seguridad para sistematizar la información obtenida en la Evaluación de Impacto de Datos Personales.

SEGUNDO. La estructura del documento de seguridad debe seguir lo dispuesto por el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y deberá contener lo siguiente:

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.
VII. El programa general de capacitación.

TERCERO. La responsable de recopilar la información obtenida de la Evaluación de Impacto de Datos Personales y de redactar el documento de seguridad es la Unidad de Datos Personales.

CUARTO. La Unidad de Datos Personales podrá llevar a cabo la redacción del documento de seguridad por medio de su responsable o de quien o quienes se designen para tal efecto. En el caso de dirigencias estatales, la Unidad de Transparencia deberá de realizar el documento por medio de su oficial de datos personales.

QUINTO. En casos de dirigencias estatales sin registro, la Unidad de Datos Personales de Movimiento Ciudadano Nacional podrá redactar el documento de seguridad por acuerdo de la Comisión Nacional de Transparencia.

SEXTO. El documento de seguridad deberá tener un formato previo que señale el perfil del o los redactores. Dicho perfil deberá señalar:

I. Nombre.

II. Posición dentro de la Unidad de Datos Personales.

III. Grados profesionales (listar los tres más recientes).

IV. Experiencia (no más de tres renglones).

CAPITULO SEGUNDO

Del inventario de datos personales y de los sistemas de tratamiento

SÉPTIMO. El documento de seguridad deberá listar cada Unidad Administrativa Responsable que maneje datos personales y los sistemas bajo su responsabilidad, en el caso de ser dos o más, deberán listarse por separado. Deberán incluirse también los datos que se incluyen en el sistema, el tipo de soporte de los mismos y una descripción del lugar donde se encuentran resguardados.

OCTAVO. El contenido del párrafo anterior deberá manifestarse en el siguiente formato:

UNIDAD ADMINISTRATIVA RESPONSABLE

Denominación:

Nombre del Sistema de Datos Personales:

Datos personales contenidos en el sistema:

Soporte del sistema de datos personales

- Tipo de soporte:
- Descripción:

Características del lugar donde se resguardan los soportes:

NOVENO. En lo que respecta a los datos personales contenidos en el sistema, se debe de dar una descripción de los mismos y listar cada uno de los tipos de datos recabados. Pueden incluirse datos de identificación como los son nombres, apellido paterno, apellido materno, domicilio y estado civil, además de datos laborales tales como correo electrónico institucional y teléfono institucional, entre otros.

DÉCIMO. Respecto al tipo de soporte, se debe especificar si el sistema de datos personales se encuentra en soportes físicos, electrónicos, ambos o si a futuro se va a realizar una transición de un formato a otro o si se piensa ir de uno a ambos.

DÉCIMO PRIMERO. La descripción del soporte debe especificar el tipo de formato del archivo. De esta forma, aquellos datos en soporte físico deben explicar si están en listas, documentos, expedientes u otros, mientras que los datos en soporte electrónico, pudieran quedar contenidos en hojas de cálculo o bases de datos.

DÉCIMO SEGUNDO. Las reseñas de los lugares donde se resguardan los soportes deberán ceñirse a las siguientes reglas:

I. En el caso de soportes físicos, debe describirse por escrito las características físicas de la oficina o lugar donde se resguarde; pueden anexarse fotografías.

II. Para soportes electrónicos, la descripción debe contener un diagrama de la arquitectura de seguridad, en ella se debe ver el flujo de datos a través de la o las redes electrónicas que interconectan los equipos del sistema; también deben describirse las medidas de seguridad física implementadas para la protección del centro de datos.

III. De estar los datos personales soportados en ambas formas, deben de realizarse las descripciones de forma conjunta.

IV. Asimismo, si dos o más sistemas se resguardan en el mismo lugar, se puede hacer una descripción común donde se especifique a qué sistemas aplica.

CAPÍTULO TERCERO

Funciones y obligaciones del personal involucrado en datos personales

DÉCIMO TERCERO. En el documento de seguridad, deberán enumerarse también los sujetos involucrados en el almacenamiento y uso de los sistemas de datos personales, los cuales podrán ser de tres tipos:

I. Responsables: la persona o personas de la estructura de Movimiento Ciudadano que decide sobre el tratamiento de los datos personales.

II. Encargados: personas que tratan los datos personales por cuenta del responsable, como consecuencia de la existencia de una relación con el mismo y delimita el ámbito de su actuación a las instrucciones del Responsable.

III. Usuarios: personas pertenecientes a Movimiento Ciudadano que por su actividad requieren consultar las bases de datos de dicho instituto político y se encuentran autorizadas para ello.

DÉCIMO CUARTO. Los titulares de los derechos ARCO no son involucrados en los sistemas de datos personales, más bien son la materia de los mismos.

DÉCIMO QUINTO. El formato en el que se deben plasmar las funciones y obligaciones del personal es el siguiente:

Responsable:

- Nombre:
- Cargo:
- Funciones:
- Obligaciones:

Encargado:

E1

- Nombre:
- Cargo:
- Funciones:
- Obligaciones:

E2

- Nombre:
- Cargo:
- Funciones:
- Obligaciones:

Usuarios:

U1

- Nombre:
- Cargo:
- Funciones:
- Obligaciones:

U2

- Nombre:
- Cargo:
- Funciones:
- Obligaciones:

DÉCIMO SEXTO. En el caso de sistemas de datos personales operados por diversas unidades administrativas y que repercuten sobre las dirigencias estatales de Movimiento Ciudadano, se debe listar como responsable a la unidad administrativa con la última palabra sobre dicho sistema.

DÉCIMO SÉPTIMO. La descripción de las funciones debe versar exclusivamente sobre las atribuciones del tratamiento de datos personales. De igual manera, las responsabilidades descritas deben circunscribirse al tratamiento de datos personales.

DÉCIMO OCTAVO. Se deberán reportar los datos de todos los usuarios que tienen acceso u operan el sistema. En caso de ser muchos, dicha información deberá agregarse como anexo al documento de seguridad.

CAPÍTULO CUARTO

Análisis de riesgos y brecha

DÉCIMO NOVENO. En el documento de seguridad, deberán listarse los resultados del análisis de brecha y riesgo, llenados en el formato de Evaluación de Impacto de Datos Personales, anexando al documento los formatos llenados.

VIGÉSIMO. Al compilarse todos los análisis de riesgo, deberán de anexarse los formatos llenados y poner solamente la lista de los sistemas de datos, con la unidad administrativa que los trata y el nivel de seguridad resultante. Para este efecto, se usará el formato siguiente:

Unidad administrativa responsable	Sistema de datos personales	Nivel de seguridad

VIGÉSIMO PRIMERO. El análisis básico de brecha deberá manifestarse en una lista simple de las cosas requeridas por la Ley en materia de resguardo de datos personales.

Estado ideal	Estado real (Poner “si” o “no”)
Políticas internas para la gestión y tratamiento de los datos personales	
Funciones y obligaciones del personal involucrado	
Inventario de datos personales	
Análisis de riesgo de los datos personales	
Análisis de brecha	
Plan de trabajo	
Monitoreo y revisión periódica de las medidas de seguridad implementadas	
Capacitación del personal	
Sistema de gestión de medidas de seguridad	
Documento de seguridad	
Bitácora de vulneraciones a la seguridad	
Informe de vulneración al titular de los datos	
Aviso de privacidad	
Control de confidencialidad	

VIGÉSIMO SEGUNDO. Análisis avanzados de brecha podrán incluir un contraste entre las medidas implementadas y las mejores prácticas internacionales.

CAPÍTULO QUINTO

Plan de trabajo

VIGÉSIMO TERCERO. Deberá incluirse, para el documento de seguridad, un resumen ejecutivo, con extensión máxima de tres cuartillas, del plan de trabajo propuesto para subsanar la brecha existente en materia de seguridad. El desarrollo completo de dicho plan deberá anexarse al documento de seguridad.

CAPÍTULO SEXTO

Mecanismos de monitoreo y revisión de medidas de seguridad

VIGÉSIMO CUARTO. La información recolectada de las Unidades Administrativas Responsables en lo referente a seguridad deberá compilarse en el formato siguiente:

Estado ideal	Estado real (Poner "en ninguna, en pocas, en la mitad, en muchas o en todas")
Procedimientos para los traslados de datos personales.	
Medidas para el resguardo de los soportes físicos de sistemas de datos.	
Bitácoras para accesos y operación cotidiana del sistema de datos.	
Medidas para garantizar la seguridad de las oficinas que guardan datos personales	
Mecanismo para la actualización de la información personal contenida en el sistema.	
Sistema de perfiles de usuario y contraseñas en los sistemas electrónicos de datos personales.	
Bitácora de vulneraciones.	
Procedimientos de respaldo y recuperación de datos.	
Plan de contingencia.	

CAPÍTULO SÉPTIMO

Programa de capacitación

VIGÉSIMO QUINTO. El o los redactores del documento de seguridad, así como quien o quienes compilaron la información de las evaluaciones de impacto, si fueran diferentes al primer grupo, podrán hacer una propuesta de capacitación.

VIGÉSIMO SEXTO. Dicha propuesta deberá hacerse con base en los siguientes criterios:

I. Cantidad de unidades involucradas.
II. Número de usuarios en cada uno de los sistemas de datos.
III. Número de responsables y gestores.
IV. Existencia de datos personales sensibles.
V Tamaño de la brecha.
VI. Medidas de seguridad existentes.

VIGÉSIMO SÉPTIMO. En el documento de seguridad, deberá incluirse un resumen de ejecutivo, no más de 3 páginas, de la propuesta de capacitación, anexando al documento el estudio que sea mayor a dicha cantidad.

LINEAMIENTOS PARA LA EVALUACIÓN INICIAL DE DATOS PERSONALES

CAPÍTULO PRIMERO

Disposiciones generales

PRIMERO. Estos lineamientos tienen como finalidad señalar los elementos mínimos para toda evaluación inicial de datos personales y cómo habrá de implementarse.

SEGUNDO. Son sujetos de este lineamiento los órganos nacionales de Movimiento Ciudadano y sus dirigencias estatales, cuando se requiera determinar la existencia de los sistemas de datos personales, quiénes los resguardan y sus alcances.

TERCERO. La evaluación inicial se dividirá en dos partes, una llevada a cabo por las Unidades Administrativas Responsables y otra implementada por la Unidad de Datos Personales.

CUARTO. Será la Unidad de Datos Personales, a través de su responsable o a quien él designe, la encargada de recopilar las evaluaciones de cada Unidad Administrativa y la propia para después unificarlas en un solo documento. En el caso de dirigencias estatales, quien lleve la evaluación deberá ser la Unidad de Transparencia por medio de su oficial de datos personales.

QUINTO. En casos de dirigencias estatales sin registro, podrá la Unidad de Datos Personales de Movimiento Ciudadano Nacional llevar a cabo la evaluación inicial por acuerdo de la Comisión Nacional de Transparencia.

SEXTO. Toda evaluación inicial deberá contar con un formato previo que señale el perfil del recopilador y la justificación para la Evaluación Inicial de Impacto de Datos Personales.

SÉPTIMO. El perfil del recopilador deberá señalar:

I. Nombre.

II. Posición dentro de la Unidad de Datos Personales.

III. Grados profesionales (listar los tres más recientes).

IV. Experiencia (no más de tres renglones).

OCTAVO. La justificación de la evaluación inicial deberá contener:

I. Hechos que la motivan.

II. Razonamiento aplicable.

III. Legislación que lo respalda.

IV. Entrelazamiento entre hechos, razones y leyes.

CAPÍTULO SEGUNDO

De la evaluación que realicen las Unidades Administrativas Responsables

NOVENO. La evaluación inicial deberá llevarse a cabo por medio de un cuestionario que permita determinar cuánto conocimiento tiene el responsable del área administrativa de los datos personales y si su actividad inherentemente tiene que ver con datos personales.

DÉCIMO. El cuestionario deberá contener exclusivamente preguntas que se respondan de forma afirmativa o negativa e incluir una sección donde quien lo responda plasme su perfil.

DÉCIMO PRIMERO. El cuestionario deberá abarcar los siguientes temas:

I. Contacto con datos personales, inventario de datos personales y sistemas de tratamiento.

II. Análisis de riesgo.

DÉCIMO SEGUNDO. De la primera parte del cuestionario, el recopilador deberá elaborar también una lista de unidades administrativas, determinando su prioridad con base en la frecuencia del tratamiento de datos y la sensibilidad de los mismos. Dicha lista debe expresarse de la forma siguiente:

I. Datos sensibles, tratamiento frecuente.

II. Datos sensibles, tratamiento medianamente frecuente.

III. Tratamiento frecuente.

IV. Tratamiento medianamente frecuente.

V. Datos sensibles, tratamiento infrecuente.

En el caso de las fracciones IV y V, el recopilador deberá justificar su inclusión aplicando de forma análoga los criterios del numeral octavo de estos lineamientos.

DÉCIMO TERCERO. El análisis de riesgo tiene como propósito determinar qué aspectos de la estructura y recursos destinados a resguardar datos personales están en riesgo de ser vulnerados. Para tal efecto, el cuestionario debe de comprender los aspectos siguientes:

I. Medidas existentes.

II Riesgos en el manejo de datos.

III. Sensibilidad de los datos personales.

DÉCIMO CUARTO. La sección del cuestionario relativa a las medidas de seguridad existentes para el manejo de datos personales deberá tocar la existencia de lo siguiente:

I. Procedimientos para el traslado de datos personales.

II. Medidas de seguridad para el resguardo de los soportes físicos de sistemas de datos.

III. Bitácoras para accesos y operación cotidiana del sistema de datos.

IV. Medidas para garantizar la seguridad de las oficinas que guardan datos personales.

V. Sistema de perfiles de usuario y contraseñas en los sistemas electrónicos de datos personales.

VI. Bitácora de vulneraciones.

VII. Procedimientos de respaldo y recuperación de datos.

VIII. Plan de contingencia.

DÉCIMO QUINTO. En lo relativo a los riesgos inherentes en el manejo de datos personales, el cuestionario debe tocar:

I. Obligaciones de confidencialidad de parte de las personas que tratan datos personales.

II. Medidas para garantizar el ejercicio personal de los derechos ARCO.

DÉCMO SEXTO. En cuanto al nivel de sensibilidad de los datos personales, debe incluirse lo siguiente:

I. Posesión de datos especialmente protegidos.

II. Consentimiento expreso y por escrito para ello.

III. Acreditación del consentimiento expreso obtenido.

IV. Existencia de procedimientos para gestionar la revocación del consentimiento expreso del afectado.

DÉCIMO SÉPTIMO. Fuera de las preguntas de respuesta afirmativa o negativa, el cuestionario que se trate deberá también preguntar la cantidad de titulares de derechos arco para el o los sistemas de datos personales bajo responsabilidad de la Unidad Administrativa Responsable.

DÉCIMO OCTAVO. Habiendo recibido las evaluaciones de las Unidades Administrativas Responsables, el recopilador deberá sistematizar su contenido para que las mismas puedan usarse en el documento de seguridad. Asimismo, deberá obtener el parámetro de seguridad por cada Unidad Administrativa.

DÉCIMO NOVENO. El parámetro de seguridad se obtiene de la suma genérica de las afirmativas obtenidas en cada cuestionario. El procedimiento para obtener el nivel de seguridad de cada cuestionario deberá determinarse en el Manual de Datos Personales, pero el mismo deberá incluir cuatro niveles:

I. Bajo.

II. Medio-bajo.

III. Medio-alto.

IV. Alto.

VIGÉSIMO. El recopilador tomará la información resultante y la expresará en el siguiente cuadro:

Unidad administrativa responsable	**Sistema de datos personales**	**Nivel de seguridad**

CAPÍTULO TERCERO

De la evaluación de la Unidad de Datos Personales

VIGÉSIMO PRIMERO. La evaluación inicial deberá llevarse a cabo por medio de un cuestionario que permita determinar si la Unidad de Datos Personales da buen trato a los datos personales. Quien realice la evaluación no deberá tener conexión directa con la unidad evaluada.

Asimismo, deberá realizar un análisis de brecha y un plan de trabajo.

VIGÉSIMO SEGUNDO. Si la persona de la Unidad de Datos Personales que llena el cuestionario es diferente del encargado de recopilar la información, deberá redactar su perfil y agregarlo al cuestionario como anexo.

VIGÉSIMO TERCERO. El contenido del cuestionario deberá tocar los siguientes aspectos sobre la atención a titulares de derechos ARCO:

I. Medios para el ejercicio de los derechos ARCO.

II. Medidas y procedimientos para garantizar el ejercicio de los derechos ARCO.

III. Información que se ofrece.

IV. Formatos en que se ofrece la información.

V. Mecanismos y procedimientos para informar a los posibles cesionarios de datos personales de las rectificaciones o cancelaciones realizadas.

VIGÉSIMO CUARTO. El parámetro de buen trato de datos personales se obtiene de la suma genérica de las afirmativas que tenga cada cuestionario. El procedimiento para obtenerlo deberá determinarse en el Manual de Datos Personales, pero el mismo deberá incluir tres niveles:

I. Bajo.

II. Medio.

III. Alto.

CAPÍTULO CUARTO

Del análisis de brecha y el plan de trabajo

VIGÉSIMO QUINTO. La Unidad de Datos Personales deberá también llevar a cabo un análisis de brecha en el que se contraste lo que la ley exige en medidas de seguridad y lo implementado. A Movimiento Ciudadano le es aplicable la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en su título segundo marca principios y deberes, estando éstos últimos señalados en los numerales 32 a 42.

VIGÉSIMO SEXTO. Las exigencias de Ley en materia de datos personales pueden plasmarse en la siguiente lista:

Estado ideal	Estado real (Poner “si” o “no”)
Políticas internas para la gestión y tratamiento de los datos personales.	
Funciones y obligaciones del personal involucrado.	
Inventario de datos personales.	
Análisis de riesgo de los datos personales.	
Análisis de brecha.	
Plan de trabajo.	
Monitoreo y revisión periódica de las medidas de seguridad implementadas.	
Capacitación del personal.	
Sistema de gestión de medidas de seguridad.	
Documento de seguridad.	
Bitácora de vulneraciones a la seguridad.	
Informe de vulneración al titular de los datos.	
Aviso de privacidad.	
Control de confidencialidad.	

VIGÉSIMO SÉPTIMO. Una vez determinada la brecha en materia de medidas de seguridad de datos personales, la Unidad de Datos Personales deberá elaborar un plan de trabajo para colmarla.

VIGÉSIMO OCTAVO. El plan de trabajo deberá establecer una problemática general y dividirse en otras de corte particular. Deberá seguirse el siguiente esquema:

I. Problemática.
II. Medida.

III. Consecuencias previsibles.

IV. Seguimiento.

V. Metas a corto, mediano y largo plazo.
VI. Estudio de costos aproximados de la implementación de medidas.

LINEAMIENTOS PARA REALIZAR AUDITORIAS SOBRE EL MANEJO DE DATOS PERSONALES

CAPÍTULO PRIMERO

Disposiciones generales

PRIMERO. La Comisión Nacional de Transparencia y Acceso a la Información deberá revisar, por medio de la Unidad de Datos Personales, la implementación, en forma adecuada, de las medidas de seguridad necesarias para el debido resguardo de los datos personales a cargo de Movimiento Ciudadano.

SEGUNDO. Para cumplir con lo anterior, la Unidad de Datos Personales podrá realizar auditorías de seguridad. Éstas deberán **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

TERCERO. Las auditorías podrán ser técnicas o de gestión.

CUARTO. Las auditorías técnicas consideran revisiones tales como evaluaciones de vulnerabilidades o pruebas de penetración; las de gestión permiten conocer el estado del cumplimiento con relación a estándares, normas o requisitos legales. Serán internas cuando se hacen por el personal de Movimiento Ciudadano y externas cuando se lleven a cabo por personal ajeno.

QUINTO. Las auditorías deberán ser periódicas y todas las actividades relacionadas con las mismas estarán documentadas.

CAPÍTULO SEGUNDO

Del programa de auditoría

SEXTO. La Unidad de Datos Personales propondrá a la Comisión Nacional de Transparencia un programa de auditoría donde se considere un conjunto de auditorías planeadas para un alcance específico.

SÉPTIMO. Se deberá contar con un plan por cada auditoría considerada dentro del programa. En éste se realizará una descripción de las actividades a realizar, los procesos y áreas sujetas a la revisión y los resultados obtenidos en evaluaciones previas. Se deberán incluir los criterios, alcance, responsables y métodos de auditoría, entre otros aspectos.

OCTAVO. Cada auditoría realizada deberá generar un informe que muestre los resultados y permita priorizar las inconformidades. La Comisión Nacional de Transparencia deberá atender los incumplimientos y desviaciones de lo

establecido en los estándares, normas o requisitos legales que sirven como referencia para la evaluación.

CAPÍTULO TERCERO

Del proceso de una auditoria

NOVENO. Las auditorías deberán seguir el siguiente proceso:

I. Planeación.
II. Revisión documental.
III. Preparación de auditoría en sitio.
IV. Auditoría en sitio.
V. Conclusiones.
VI. Seguimiento.

CAPÍTULO CUARTO

De la planeación de la auditoría

DÉCIMO. La Comisión Nacional de Transparencia autorizará, rechazará o realizará observaciones al calendario de auditorías y al equipo de auditoría que someta a su consideración la Unidad de Datos Personales.

DÉCIMO PRIMERO. El equipo de auditoría que proponga la Unidad de Datos Personales podrá estar conformado por personal de diversas áreas y éste se deberá seleccionar con la intención de mantener la imparcialidad del proceso de auditoría, considerando la idea de no revisar el propio trabajo.

DÉCIMO SEGUNDO. El grupo de trabajo propuesto deberá tener:

I. Auditores técnicos.
II. Auditor líder.
III. Auditores adjuntos.
IV. Observadores.

DÉCIMO TERCERO. Una vez aprobado, el grupo de trabajo deberá definir los objetivos y alcances y criterios de las auditorías.

CAPÍTULO QUINTO

De la revisión documental y la preparación de auditoría en sitio

DÉCIMO CUARTO. Antes de dar inicio a la auditoría, se llevará a cabo una revisión de la documentación del sistema de gestión, a partir de los criterios de

auditoría, con el propósito de ampliar el panorama e identificar elementos de interés que podrán ser revisados con mayor detalle. Asimismo, se deberán considerar todas las actividades que el equipo auditor crea necesarias para la revisión en sitio.

CAPÍTULO SEXTO

De la auditoría en sitio

DÉCIMO QUINTO. En la auditoría deberá seguirse el protocolo. Éste deberá contener lo siguiente:

I. Junta de apertura.
II. Conducción de auditoría en sitio.
III. Comunicación de hallazgos.
IV. Junta de cierre.
V. Distribución del informe con los resultados de la auditoría.

DÉCIMO SEXTO. Al tenerse las condiciones para iniciar la junta de apertura, se dará seguimiento al plan de auditoría. Una vez finalizadas las revisiones en sitio, el equipo auditor deberá generar el informe de auditoría.

DÉCIMO SÉPTIMO. El informe deberá ser aprobado por el auditor líder y presentado a la Comisión Nacional de Transparencia--o a su Presidente—durante la junta de cierre, donde además se resolverán las dudas y controversias del proceso.

DÉCIMO OCTAVO. La auditoría concluye una vez que el auditado firma la conformidad de los resultados. La Unidad de Datos Personales deberá presentar al equipo auditor un plan para resolver las inconformidades y observaciones encontradas.

DÉCIMO NOVENO. El auditor debe entregar copia del informe a la Comisión Nacional de Transparencia, a la Unidad de Datos Personales y al auditado.

CAPÍTULO SÉPTIMO

Seguimiento de la auditoría

VIGÉSIMO. Concluido el proceso de auditoría, deben aplicarse actividades de seguimiento sobre las acciones correctivas, encaminadas a satisfacer las desviaciones identificadas en los hallazgos que fueron identificados y clasificados (inconformidades u observaciones).

LINEAMIENTOS PARA LA RESPUESTA A SOLICITUDES DE DERECHOS ARCO

CAPÍTULO PRIMERO

Disposiciones generales

PRIMERO. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición de datos personales, por parte del titular de los mismos, es un derecho contemplado en el artículo 16 de la Constitución Política de los Estados Unidos Mexicano. El ejercicio de este derecho es gratuito y sólo se podrá cobrar a quien ejerza el costo de reproducción, cuando la documentación provista sea mayor a veinte hojas simples.

Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente.

SEGUNDO. La Unidad de Transparencia es el órgano técnico encargado de la recepción de solicitudes de derechos ARCO, mientras que la Unidad de Datos Personales es el órgano técnico da trámite y desahogo a las mismas. Ambas unidades son independientes una de la otra y están supeditadas a la autoridad de la Comisión Nacional de Transparencia.

TERCERO. Las solicitudes de ejercicio de derechos ARCO podrán realizarse de forma electrónica, por medio de la Plataforma Nacional de Transparencia, o de presencial ante la Unidad de Transparencia, la cual registrará la petición en esta Plataforma Nacional y llevará al solicitante ante la Unidad de Datos Personales.

CUARTO. La Unidad de Datos Personales deberá auxiliar y orientar al titular que lo requiera en lo relativo al ejercicio de sus derechos ARCO. Para tal efecto, en sus oficinas deberá tener un equipo de cómputo dedicado exclusivamente al uso de la ciudadanía.

CAPÍTULO SEGUNDO

Del procedimiento de recepción de solicitudes de ejercicio de derechos ARCO

QUINTO. Dentro del procedimiento de atención a solicitudes de derechos ARCO, la Unidad de Transparencia o en su caso la Unidad de Transparencia local, es la encargada de recibirlas de forma presencial o a través de la Plataforma Nacional de Transparencia y deberá hacerlas llegar a la Unidad de Datos Personales para su trámite y desahogo.

SEXTO. La solicitud para el ejercicio de los derechos ARCO deberá contar con la información siguiente:

- Nombre y domicilio del titular o cualquier otro medio para recibir notificaciones.
- Documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.
- Descripción clara y precisa de los datos personales que se quieran rectificar, cancelar u oponerse a su tratamiento.
- Descripción del derecho que se quiere ejercer o de lo que solicita el titular.
- En su caso, documentos o información que faciliten la localización de los datos personales, entre ella, el área responsable del tratamiento.

Dependiendo del derecho que se desee ejercer, la solicitud deberá incluir:

- **Derecho de acceso:** modalidad en la que prefiere reproducir los datos personales solicitados.
- **Derecho de rectificación:** modificaciones solicitadas para los datos personales, así como la aportación de documentos que sustenten la solicitud.
- **Derecho de cancelación:** motiva la petición para eliminar los datos de los archivos, registros o bases de datos.
- **Derecho de oposición:** causas o situación que lo llevan a solicitar la finalización del tratamiento de sus datos personales, así como el daño o perjuicio que le causaría la prolongación de dicho tratamiento; o bien, deberá indicar las finalidades específicas respecto de las cuales desea ejercer este derecho.

SÉPTIMO. Todo solicitante deberá acreditar ante la Unidad de Datos Personales la titularidad del dato personal para la procedencia de su solicitud. Para tal efecto, son documentos de identidad los siguientes:

- Credencial del Instituto Nacional Electoral vigente.
- Pasaporte vigente.
- Cartilla del Servicio Militar Nacional.
- Cédula profesional.
- Cartilla de identidad postal (expedida por SEPOMEX).
- Licencia de manejo vigente.
- Constancia de residencia.
- Credencial de afiliación del IMSS.
- Credencial de afiliación al ISSSTE.
- Documento migratorio que constate la legal estancia del extranjero en el país

En las solicitudes presenciales, realizadas ante la Unidad de Transparencia, la acreditación se llevará ante la misma y no se necesitará repetirse ante la Unidad de Datos Personales.

La acreditación de la identidad del titular de datos personales podrá ser constatada mediante la presentación de copia del documento de identificación, éste deberá cotejarse con el original y, de esta forma, se acreditará la identidad de manera fehaciente.

También son admisibles los instrumentos electrónicos por medio de los cuales sea posible identificar fehacientemente al titular, como lo son la Clave Única del Registro de Población, la Firma Electrónica Avanzada o la Cédula de Identificación Fiscal.

OCTAVO. En caso de que el titular haga efectivos sus derechos a través de un representante, aparte de la acreditación de la identidad de ambos, en los términos del numeral sexto, la Unidad de Datos Personales o la Unidad de Transparencia, en el caso de solicitudes presenciales, deberá verificar la representación a través de los siguientes medios:

- Instrumento público en el que conste la representación.
- Carta poder firmada ante notario.
- Declaración en comparecencia del titular

NOVENO. Para el ejercicio de derechos ARCO de menores de edad, si los padres ejercen la patria potestad y son los que presenten la solicitud, se deberán aportar los siguientes documentos:

- Documento que acredite la identidad de menor.
- Acta de nacimiento del menor.
- Identificación oficial del padre o de la madre que pretenda ejercer el derecho.
- Carta en la que se manifieste, bajo protesta de decir verdad, que el padre o la madre es quien ejerce la patria potestad del menor y no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.

Si una persona distinta a los padres es quien ejerce la patria potestad y es quien presenta la solicitud:

- Documento que acredite la identidad del menor.
- Acta de nacimiento del menor.
- Documento legal que acredite la posesión de la patria potestad.
- Identificación oficial de quien presenta la solicitud y posee la patria potestad.

- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la patria potestad del menor y no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.

Cuando un tutor es quien ejerce la patria potestad:

- Documento que acredite la identidad de menor.
- Acta de nacimiento del menor.
- Documento legal que acredite la tutela.
- Identificación oficial del tutor.
- Carta en la que se manifieste, bajo protesta de decir verdad, la tutela del menor y éste no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la tutela.

DÉCIMO. Para solicitudes de derechos ARCO de personas en estado de interdicción o incapacidad legal:

- Documento que acredite la identidad del titular de los datos personales.
- Instrumento legal de designación del tutor.
- Identificación oficial del tutor.
- Carta donde se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y no se encuentra dentro de lo alguno de los supuestos legales de suspensión o limitación de la misma.

DÉCIMO PRIMERO. La acreditación deberá realizarse por medio del llenado de un formato que contenga los elementos siguientes:

- Nombre.
- Fecha de nacimiento.
- Domicilio.
- Teléfono de contacto.
- Vertiente del derecho que se ejerce.

El formato deberá resguardarse por la Unidad de Datos Personales aplicando los protocolos de protección de datos pertinentes.

DÉCIMO SEGUNDO. Si el titular del dato personal que hizo su solicitud por medio de la Plataforma Nacional de Transparencia residiera en otra entidad federativa, puede acudir a la Unidad de Transparencia local de Movimiento Ciudadano más próxima a realizar su acreditación.

CAPÍTULO TERCERO

Del procedimiento de trámite y desahogo de solicitudes de ejercicio de derechos ARCO

DÉCIMO TERCERO. Al proceder la acreditación de la titularidad del dato personal, la Unidad de Datos Personales deberá definir el sistema de información de Movimiento Ciudadano que pueda contener el dato personal referido en la solicitud, para de ahí turnar la solicitud a su responsable.

DÉCIMO CUARTO. El responsable de la base de datos determinará si el dato personal de la solicitud se encuentra en su banco de información. Si no se cuenta con la información suficiente para determinar la ubicación del dato personal, se podrá pedir a la Unidad de Datos Personales para solicitar mayor información al titular del dato personal.

DÉCIMO QUINTO. Una vez encontrado el dato personal, se dará trámite al ejercicio del derecho ARCO.

DÉCIMO SEXTO. Si el dato personal no se encontrara, la Unidad de Datos Personales ordenará una búsqueda generalizada en las bases de datos de Movimiento Ciudadano. Si hecha la pesquisa correspondiente el dato no se encontrara, se declarará la inexistencia del mismo.

DÉCIMO SÉPTIMO. El ejercicio de los derechos ARCO puede negarse bajo los siguientes supuestos:

- Cuando el titular del dato personal o su representante no se acrediten.
- Al no encontrarse los datos personales en la base de datos del responsable.
- Al lesionarse derechos de terceros.
- Cuando la rectificación, cancelación u oposición haya sido realizada previamente.
- Al existir impedimento legal o resolución de una autoridad que restrinja o nulifique el ejercicio de estos derechos.

CAPÍTULO CUARTO

De los derechos ARCO

DÉCIMO OCTAVO. El derecho de acceso consiste en que el titular del dato personal sepa si el mismo es objeto de tratamiento, además de los alcances, condiciones y parámetros del mismo. Este derecho se garantiza:

- Al conocer la existencia del tratamiento al que son sometidos sus datos personales.
- Con el acceso a los datos personales en posesión de Movimiento Ciudadano.
- Con el conocimiento de las circunstancias esenciales del tratamiento consistentes en las finalidades que justifican el tratamiento, en las personas que intervienen en el mismo.

En el caso de la transferencia de datos, el derecho de acceso implica proporcionar conocimiento a los destinatarios de dicho acto, las finalidades del mismo y el dato personal transferido.

Se dará por cumplido el derecho de acceso cuando, habiendo acreditado al titular o su representante, se ponga a disposición del mismo los datos personales de forma presencial o a través de copias simples, medios magnéticos, ópticos, sonoros, visuales u holográficos o cualquier otro que permita la Ley.

DÉCIMO NOVENO. El derecho de rectificar consiste en corregir la información del titular que resulte ser incompleta o inexacta en la forma en que él lo indique en su petición.

En el supuesto de que los datos personales a corregir hayan sido transferidos a terceros, el derecho de rectificación ejercido ante Movimiento Ciudadano queda exhausto cuando este instituto político le informe al titular de la situación para que acuda ante quien posea sus datos y ejerza el derecho correspondiente.

VIGÉSIMO. El derecho de cancelación implica la supresión total o parcial de los datos personales en los registros, archivos, bases de datos o tratamientos realizados por el responsable, previo bloqueo. El titular de los datos personales—o su representante—deberá ejercer la solicitud de eliminación de datos personales cuando considere que los mismos no están siendo tratados conforme a los principios, deberes y obligaciones previstas en la Ley.

El periodo de bloqueo consiste en el resguardo de los datos por un tiempo razonable que comprenda un posible surgimiento de responsabilidades relacionadas con el tratamiento de los mismos. Durante el transcurso de este periodo deberán implementarse medidas de seguridad que permitan conservar los datos personales, deshabilitando cualquier tratamiento de la información.

VIGÉSIMO PRIMERO. El derecho de cancelación puede negarse bajo los siguientes supuestos:

- Cuando los datos personales que se buscan eliminar refieran a las partes de un contrato privado, social o administrativo y los mismos sean necesarios para su desarrollo y cumplimiento.
- Cuando los datos deban ser tratados por disposición de Ley.

- Al obstaculizar la eliminación de datos actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
- Al ser los datos necesarios para proteger los intereses jurídicamente tutelados del titular.
- Cuando los datos se requieran para realizar una acción en función del interés público o para cumplir con una obligación legalmente adquirida por el titular.
- Cuando los datos sean objeto de tratamiento para la prevención, el diagnóstico médico o la gestión de servicios de salud, al ser dicho tratamiento realizado por un profesional de la salud sujeto a un deber de secreto.

VIGÉSIMO SEGUNDO. El derecho de oposición consiste en solicitar el cese del tratamiento de datos personales. Éste puede ocurrir sobre propósitos específicos del tratamiento y, al ser así, se deja a salvo cualquier otra finalidad que no esté contemplada en el ejercicio de este derecho.

En la solicitud de ejercicio de este derecho, el titular debe manifestar si se opone a un tratamiento o tratamientos específicos y explicar las razones legítimas que dimanan de su situación personal para oponerse a que sus datos personales sigan siendo tratados para fines específicos, a fin de evitar un perjuicio que derive de la persistencia en el tratamiento de su información.

El derecho de oposición al tratamiento de datos personales puede negarse por las mismas causales que operan hacia la eliminación en términos del numeral décimo octavo de los presentes lineamientos.

CAPÍTULO QUINTO

De la cancelación de datos personales

VIGÉSIMO TERCERO. Al proceder la solicitud de cancelación del dato personal, el responsable del sistema de datos personales al que pertenece el dato deberá realizar una revisión exhaustiva en los archivos, registros, expedientes y bases de datos donde se reguardan copias o reproducciones del dato, verificando si el mismo tiene valores históricos, estadísticos o contables.

VIGÉSIMO CUARTO. En caso de contener dichos valores, éstos serán sujetos a lo dispuesto por el manual de políticas y procedimientos de archivos de trámite.
VIGÉSIMO QUINTO. Se procederá al bloqueo lógico inmediato de los datos, con el fin de impedir su utilización, cuando se encuentren almacenados en aplicaciones o bases de datos ubicadas en los sistemas de información de Movimiento Ciudadano. Éstos serán sujetos a lo dispuesto por el Manual de Archivos.

VIGÉSIMO SEXTO. Se procederá al bloqueo físico inmediato de los datos, con el fin de impedir su utilización, cuando los datos estén almacenados en soportes físicos o documentos. Se almacenarán los soportes en un lugar de acceso restringido y estarán sujetos a lo dispuesto por el Manual de Archivos.

LINEAMIENTOS PARA LA CREACIÓN DE LA POLITICA DE GESTIÓN DE DATOS PERSONALES

CAPÍTULO PRIMERO

Disposiciones generales

PRIMERO. Estos lineamientos tienen como finalidad establecer los elementos para la política de gestión de datos personales de Movimiento Ciudadano.

SEGUNDO. La política de seguridad de datos personales deberá tener los siguientes elementos:

I. Parte introductoria.

II. Definiciones.

III. Principios rectores de la gestión de datos personales.

IV. Encargados de la gestión de datos personales.

V. Forma en cómo se obtienen los datos personales.

VI. Forma en cómo se resguardan los datos personales.

VII. Sanciones.

TERCERO. La parte introductoria deberá contener todo lo relativo a la forma en cómo Movimiento Ciudadano se relaciona con los datos personales y los aspectos básicos de su política en la materia. Son elementos mínimos de la parte introductoria los siguientes:

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

II. Objetivos de Movimiento Ciudadano con respecto a los datos personales.

III. Alcances de la política de gestión de datos personales de Movimiento Ciudadano.

CAPÍTULO SEGUNDO

Definiciones y principios rectores

CUARTO. La política de gestión de datos personales de Movimiento Ciudadano deberá recoger 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.

QUINTO. Podrán también incorporarse principios de datos personales reconocidos por la comunidad internacional, consolidados en las mejores prácticas existentes, siempre y cuando constituyan una expansión de lo señalado por la Ley o amplíen derechos constitucionales relacionados con los datos personales.

SEXTO. Las definiciones deberán tomar como mínimo las establecidas en el artículo 3º de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, pudiéndose agregar otras contenidas en lineamientos o criterios del garante.

CAPÍTULO TERCERO

Encargados de la gestión de datos personales

SÉPTIMO. La política de gestión de datos debe explicar cuál es el rol de la Comisión Nacional de Transparencia en la materia, así como el papel de la Unidad Técnica de Datos Personales.

OCTAVO. Se deberá incluir también la dirección e información de contacto de la Comisión Nacional de Transparencia y la Unidad Técnica de Datos Personales.

CAPÍTULO CUARTO

Obtención y resguardo de datos

NOVENO. La política de gestión de datos personales de Movimiento Ciudadano debe explicar cómo se obtienen los datos personales, las diferentes formas en que se recaban y el tipo de información manejada. Deben también establecerse las razones por las que se realiza dicha actividad de recolección.

DÉCIMO. En la política de datos personales, se debe establecer la presunción siguiente: quien otorga los datos lo hace porque le pertenecen o está autorizado, siendo dicha información correcta, completa, veraz, exacta y actual.

DÉCIMO PRIMERO. Se deben establecer de forma clara los derechos de los titulares de datos personales respecto a los mismos.

DÉCIMO SEGUNDO. Se deben establecer los estándares de calidad de Movimiento Ciudadano en el cuidado de datos personales, así como el deber de este instituto político de guardar respeto y confidencialidad.

DÉCIMO TERCERO. Se debe establecer que los datos personales obtenidos lo serán por vías lícitas, mediando la buena fe y el cuidado de los mismos.

DÉCIMO CUARTO. Movimiento Ciudadano tiene el deber de obtener datos personales sólo para el cumplimiento de su propósito como partido político, esta información debe relacionarse sólo con la identidad y la escolaridad.

DÉCIMO QUINTO. Debe establecerse en la política de gestión la forma en cómo se resguardan los datos personales y cómo se investigarán internamente posibles violaciones, además de la notificación respectiva al garante.

DÉCIMO SEXTO. Se debe de explicar cómo se procesarán y resolverán las solicitudes de ejercicio de derechos ARCO que presenten los titulares de datos personales; serán procesadas por la Unidad Técnica de Datos Personales y resueltas de forma definitiva por la Comisión Nacional de Transparencia de Movimiento Ciudadano.

CAPÍTULO QUINTO

Sanciones

DÉCIMO SÉPTIMO. Deben explicarse las sanciones posibles a quienes infrinjan y vulneren los sistemas de datos personales bajo el resguardo y administración de Movimiento Ciudadano. Para ello, deberá hacerse cita del precepto aplicable de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y de cualquier otra norma que resultara viable.

LINEAMIENTOS PARA PARA LA POLÍTICA DE SEGURIDAD DE DATOS PERSONALES

CAPÍTULO PRIMERO

Disposiciones generales

PRIMERO. La política de seguridad de datos personales es un documento donde se reúnen los requerimientos mínimos para el Sistema de Resguardo de Datos Personales en el almacenaje, resguardo y tratamiento de datos personales. Éstos se manifiestan en lo que está permitido y prohibido durante la operación general del sistema.

SEGUNDO. La política de gestión de datos personales deberá tener los elementos siguientes:

I. Parte introductoria.

II. Características de la política de seguridad.

III. Sujetos del Sistema de Resguardo de Datos Personales.

IV. Principios rectores del resguardo de datos personales.

V. Forma en cómo se resguardan los datos personales.

TERCERO. La parte introductoria deberá contener todo lo relativo a la forma en cómo Movimiento Ciudadano se relaciona con los datos personales y los aspectos básicos de su política en la materia. Son elementos mínimos de la parte introductoria:

I. Naturaleza jurídica de Movimiento Ciudadano con respecto a los datos personales-

II. Objetivos de Movimiento Ciudadano con respecto a los datos personales.

III. Alcances de la política de seguridad de datos personales de Movimiento Ciudadano.

CAPÍTULO SEGUNDO

Características de la política de seguridad

CUARTO. 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 los usuarios del Sistema de Resguardo de Datos

Personales, haciendo desde su rol lo necesario para garantizar que los datos personales cedidos a Movimiento Ciudadano no sean accedidos por quien no tenga autorización.

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

I. Holística: cubrir todos los aspectos posibles de la seguridad de datos personales.

II. Proporcional: adecuarse a las necesidades y recursos de Movimiento Ciudadano.

III. Pro persona: proveer la protección más amplia posible.

IV. Atemporal: el tiempo en el que se aplica no debe influir en su eficacia y eficiencia.

IV. Amplia: definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

CAPÍTULO TERCERO

Sujetos del Sistema de Resguardo de Datos Personales

SEXTO. La política de seguridad de datos personales debe explicar el papel que poseen los sujetos del Sistema de Resguardo de Datos Personales.

SÉPTIMO. Se deberá incluir también la dirección e información de contacto de la Comisión Nacional de Transparencia y la Unidad Técnica de Datos Personales.

CAPÍTULO CUARTO

Principios rectores del resguardo de datos personales

OCTAVO. La política de seguridad de datos personales de Movimiento Ciudadano 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. El Sistema de Resguardo de Datos Personales debe contar con flujos de información libres y abiertos, y deben garantizarse los principios básicos de protección de datos personales.

NOVENO. Son principios rectores de la política de seguridad de Movimiento Ciudadano:

I. Congruencia: esfuerzos para fortalecer la seguridad de los sistemas de información de Movimiento Ciudadano deben ser consistentes con sus valores y principios.

II. 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. Éstos deben comprender que los fallos en la seguridad pueden dañar significativamente los sistemas bajo su control y vulnerar los derechos humanos de terceros.

III. Responsabilidad: todos los participantes son responsables de la seguridad de los sistemas de datos y deben actuar de una manera apropiada para su papel individual. La responsabilidad de los mismos varía de acuerdo con los papeles que desempeñen.

IV. 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.

V. Respuesta: los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.

VI. Ética: los participantes deben realizar esfuerzos para desarrollar y adoptar buenas prácticas y promover conductas que reconozcan la necesidad de salvaguardar la seguridad y respetar los intereses legítimos de terceros.

VII. Democracia: la seguridad de los sistemas de información debe ser compatible con los valores esenciales de una sociedad democrática y garante de derechos humanos.

VIII. Evaluación del riesgo: los participantes deben llevar a cabo evaluaciones de riesgo.

IX. Diseño y realización de la seguridad: los participantes deben incorporar la seguridad como un elemento esencial de los sistemas de información.

X. 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.

XI. 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.

Estos principios son complementarios entre sí y deben interpretarse como un todo; éstos son de interés general para todos los participantes y en todos los niveles.

DÉCIMO. Podrán también incorporarse principios de datos personales reconocidos por la comunidad internacional, consolidados en las mejores prácticas existentes, siempre y cuando constituyan una expansión de lo señalado por la Ley o amplíen derechos constitucionales relacionados con los datos personales.

CAPÍTULO QUINTO

Forma en cómo se resguardan los datos personales

DÉCIMO PRIMERO. La política de seguridad de datos personales de Movimiento Ciudadano debe mencionar los soportes de datos personales manejados y explicar las medidas mínimas que poseen para el resguardo de los mismos. Asimismo, debe establecer los estándares de calidad aplicados en las medidas de seguridad.

LINEAMIENTOS PARA LA CREACIÓN DEL AVISO DE PRIVACIDAD

CAPÍTULO ÚNICO

Disposiciones generales

PRIMERO. Estos lineamientos tienen como finalidad establecer los elementos mínimos que debe tener el aviso de privacidad establecido en los artículos 3, 26 y 27 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

SEGUNDO. El aviso de privacidad es el documento que Movimiento Ciudadano debe poner a disposición del titular de datos personales, 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.

TERCERO. El aviso de privacidad tiene los elementos siguientes:

I. Sujetos consistentes en Movimiento Ciudadano como sujeto obligado de la Ley y el titular de datos personales.

II: Propósito: informar al titular del uso que se le dará a los datos personales proporcionados al obligado, a fin de que pueda tomar decisiones informadas sobre los mismos.

III. Forma en que deben presentarse (física, electrónica u otra).

CUARTO. La información tratada por Movimiento Ciudadano debe ser adecuada, relevante y estrictamente necesaria; si esto no es así, el obligado tiene derecho a ejercer a rectificar o cancelar sus datos.

QUINTO. El aviso de privacidad tiene dos modalidades: el simplificado y el integral.

SEXTO. El aviso simplificado debe tener lo siguiente:

I. La denominación del responsable.
II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo las que requieran el consentimiento del titular.
III. Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa por el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular.

IV. El sitio donde se podrá consultar el aviso de privacidad integral.

Los mecanismos y medios a los de la fracción III deberán estar disponibles para que el titular pueda manifestar su negativa al tratamiento de sus datos personales para las finalidades o transferencias que requieran el consentimiento del titular, previo a dicho tratamiento.

SÉPTIMO. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar sobre:

I. 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.
II. Las finalidades de estas transferencias.

OCTAVO. La puesta a disposición del aviso simplificado no exime al responsable de su obligación de proveer los mecanismos para que el titular pueda conocer el contenido del aviso integral.

NOVENO. El aviso de privacidad integral deberá contener:

I. El domicilio del responsable.
II. Los datos personales sometidos a tratamiento, identificando los 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 del titular.
V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO.
VI. El domicilio de la Unidad de Transparencia.
VII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

LINEAMIENTOS PARA LA BITÁCORA DE VULNERACIONES Y EL INFORME DE VULNERACIONES

CAPÍTULO PRIMERO

Disposiciones generales

PRIMERO. Estos lineamientos tienen como finalidad establecer las reglas necesarias para garantizar el registro y aviso de vulneraciones exigidos por los artículos 39 y 40 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

SEGUNDO. Los lineamientos en materia de vulneraciones deben responder a la descentralización geográfica con la que opera la estructura política de Movimiento Ciudadano, tomando en cuenta las actividades que generan su representación nacional y sus dirigencias estatales.

TERCERO. Toda vulneración en materia de datos personales debe quedar registrada en la bitácora respectiva y ser avisada a los titulares de la información vulnerada.

CAPÍTULO SEGUNDO

De las bitácoras de vulneraciones

CUARTO. La bitácora de vulneraciones es el registro donde se lleva la cuenta de las vulneraciones a la seguridad de los sistemas de datos personales de Movimiento Ciudadano. Los procedimientos de registro y notificación de vulneraciones deberán plasmarse en el Manual de Datos Personales.
QUINTO. Movimiento Ciudadano deberá tener tres formatos de bitácora:

I. **Nacional:** lo mantienen las Unidades Administrativas Responsables de la representación nacional de Movimiento Ciudadano.
II. **Estatal:** lo mantienen las dirigencias estatales de Movimiento Ciudadano a través de los órganos correspondientes.
III. **General:** lo debe mantener la Comisión Nacional de Transparencia por conducto de su Unidad de Datos Personales y debe llevar registro de todas las vulneraciones acontecidas, independientemente de que sean locales o nacionales.

SEXTO. El formato nacional de la bitácora de vulneraciones deberá ser el siguiente:

Unidad administrativa responsable

- Sistema de datos personales vulnerado:
- Tipo de soporte:
- Responsable:
- Encargados:
- Descripción de la vulneración:
- Fecha en que ocurrió:
- Motivo:
- Acciones correctivas implementadas:
- Tipo de dato personal:
- Titular (es) afectado(s)[1]:

SÉPTIMO. En el caso de las entidades federativas, el formato de registro es el siguiente:

Movimiento Ciudadano (entidad federativa)

- Titular de la unidad de la transparencia local:
- Sistema de datos personales vulnerado:
- Tipo de soporte:
- Autoridad administrativa responsable:
- Responsable:
- Encargados:
- Descripción de la vulneración:
- Fecha en que ocurrió:
- Motivo:
- Acciones correctivas implementadas:
- Tipo de dato personal:
- Titular (es) afectado(s):

OCTAVO. En la bitácora general, el formato debe quedar como sigue a continuación:

Bitácora general

- Sistema de datos personales vulnerado:
- Tipo de soporte:
- Autoridad administrativa o entidad federativa responsable:
- Responsable:
- Encargados:
- Descripción de la vulneración:
- Fecha en que ocurrió:
- Motivo:
- Acciones correctivas implementadas:
- Acciones correctivas adicionales:
- Tipo de dato personal:

[1] De ser una gran cantidad, se pondrá el número y la lista de cada uno, además de agregarse como anexo.

- Titular (es) afectado(s):

CAPÍTULO TERCERO

Del informe de vulneración

NOVENO. Movimiento Ciudadano deberá informar sin dilación alguna al titular o titulares de los datos personales sobre las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que tuvieron lugar. También deberá dar aviso al garante correspondiente.

DÉCIMO. Dicho informe deberá realizarse por escrito y variar de acuerdo con el sujeto a quien se dirige. La notificación a los titulares de datos debe ser personal, mientras que el funcionario competente del órgano garante es aquel con la titularidad sobre la dirección de partidos políticos, siendo en segundo lugar la presidencia del órgano la que debe ser notificada si se considera relevante por la Comisión Nacional de Transparencia.

DÉCIMO PRIMERO. Al momento de redactar el informe de vulneración, se deben de expresar:

I. Los hechos que dan lugar a la vulneración.

II La forma en cómo se vulneraron los datos.

III. La legislación emite el informe.

IV. La forma en que los hechos se relacionan con el marco jurídico.

V. Las medidas tomadas.

VI. En el caso de los titulares de datos, se debe agregar las posibles consecuencias de las vulneraciones a sus derechos.

VII. Para los órganos garantes, se deberá justificar que las medidas tomadas para el resguardo antes de la vulneración eran acordes a la Ley y las mejores prácticas.

DÉCIMO SEGUNDO. Junto al escrito de informe de vulneración, debe anexarse la entrada correspondiente de la bitácora.

LINEAMIENTOS PARA LA CREACIÓN DEL CONTROL DE CONFIDENCIALIDAD

CAPÍTULO ÚNICO

Disposiciones generales

PRIMERO. Estos lineamientos tienen como finalidad establecer los elementos mínimos que debe tener el control de confidencialidad establecido en el artículo 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

SEGUNDO. Para Movimiento Ciudadano, el mecanismo idóneo para ejercer el control antes mencionado es el contrato de confidencialidad, es decir, un acto jurídico por medio del cual se reitera la obligación de guardar confidencialidad respecto de los datos personales que se trataron para el sujeto obligado de datos personales.

TERCERO. Son sujetos de la obtención y resguardo de datos personales:

I. **Responsables:** persona física que forma parte de Movimiento Ciudadano y decide sobre el tratamiento de los datos personales. Posee una relación laboral con este instituto político.
II. **Gestores:** personas físicas que se encuentran bajo la dirección del responsable del sistema de datos personales, tienen como función implementar sus órdenes, además de llevar el mantenimiento y seguimiento de dicho sistema.

III. **Usuarios:** integrantes de Movimiento Ciudadano o terceros autorizados, pueden tener acceso a sus sistemas de datos personales. Se da en el contexto de una relación laboral o civil.
IV. **Compiladores de datos:** obtienen información de encuestas o recaban de forma directa datos personales. Estos sujetos pueden tener una relación laboral con Movimiento Ciudadano.
Los contratos de confidencialidad deben de variar de acuerdo con el sujeto que deba de firmarlo.

CUARTO. Son partes del contrato de confidencialidad:

I. Encabezado.

II. Declaraciones.

III. Clausulado.

IV. Fundamentación y motivación.

V. Firmas de titulares y testigos.

QUINTO. El contrato de confidencialidad debe ser firmado por el representante jurídico de Movimiento Ciudadano.

SEXTO. El encabezado es la parte del contrato donde se señala su tipo, quiénes lo celebran y el carácter que guardan respecto de uno y otro y de Movimiento Ciudadano.

SÉPTIMO. En las declaraciones, las partes acreditan que tienen la capacidad para suscribir el contrato.

OCTAVO. El clausulado es el conjunto de condiciones que las partes establecen para llevar a cabo el contrato; en el caso de un contrato de confidencialidad, se debe cumplir con la obligación establecida en el artículo 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

NOVENO. En la fundamentación y motivación, se establecen los hechos que propician la celebración del contrato y la legislación aplicable al mismo.

LINEAMIENTOS PARA REALIZAR UN PLAN DE CONTINGENCIA

CAPÍTULO PRIMERO

Disposiciones generales

PRIMERO. El presente lineamiento busca normar las medidas técnicas, humanas y organizativas necesarias para garantizar el resguardo de datos personales ante emergencias o amenazas que lo puedan impedir.

SEGUNDO. El plan de contingencia es el conjunto de procedimientos para describir los pasos a seguir en caso de una emergencia que ponga en peligro la capacidad de Movimiento Ciudadano de resguardar datos personales.

TERCERO. El plan de contingencias deberá seguir un ciclo *planificar-hacer-comprobar-actuar* y estará sujeto a una revisión periódica. La Unidad de Datos Personales será la encargada de elaborar y revisar este plan, deberá ser aprobado por la Comisión Nacional de Transparencia y Acceso a la Información.

CUARTO. El plan de contingencia comprenderá tres sub-planes:

I. Plan de respaldo: contempla las contramedidas preventivas antes de materializarse una amenaza.

II. Plan de emergencia: contempla las contramedidas necesarias durante la materialización de una amenaza o inmediatamente después.

III. Plan de recuperación: contempla las medidas necesarias después de materializada y controlada la amenaza.

CAPÍTULO SEGUNDO

De los parámetros del plan de contingencia

QUINTO. Al materializarse una emergencia o amenaza, debe realizarse una valoración de la efectividad del plan de contingencia.

SEXTO. Si la emergencia o amenaza estaba prevista, y si las medidas para hacerle frente fueron eficaces, se deberán llevar a cabo correcciones que mejoren la eficiencia del plan.

SÉPTIMO. Si la emergencia o amenaza estaba prevista, pero las medidas fueron ineficaces, se deberán analizar las causas del fallo y proponer nuevas medidas.

OCTAVO. Si la amenaza no estaba prevista, deberá promoverse un nuevo análisis de riesgos y realizar los cambios pertinentes al plan.

NOVENO. De darse el caso en el que se hayan aplicado medidas a una emergencia o amenaza no prevista y las mismas hayan resultado efectivas, se deberá realizar un nuevo análisis de riesgos y cambiar el plan de contingencia.

DÉCIMO. El plan de contingencias deberá tener los elementos siguientes:

I. Los recursos materiales necesarios para crearlo e implementarlo.

II. Las personas implicadas en el cumplimiento del plan.

III. Las responsabilidades concretas de las personas involucradas.

IV. Los protocolos a seguir.

LINEAMIENTOS PARA LA SUPRESIÓN DE BASES DE DATOS DEL SISTEMAS DE RESGUARDO DE DATOS PERSONALES

CAPÍTULO PRIMERO

Disposiciones generales

PRIMERO. Los presentes lineamientos tienen el propósito de normar la baja de bases de datos personales del Sistema de Resguardo de Datos Personales de Movimiento Ciudadano.

SEGUNDO. La base de datos personales sólo podrá ser cancelada cuando haya dejado de ser necesaria o pertinente para la finalidad con la cual fue recabada.

TERCERO. En la eliminación de bases de datos personales, deberán tomarse en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Deberán considerarse también los plazos de conservación, la vigencia documental, la clasificación de reserva o confidencialidad y el destino final de los documentos previstos en el Manual de Archivo.

CAPÍTULO SEGUNDO

Del plazo de conservación

CUARTO. El plazo de conservación es el periodo de tiempo necesario para llevar a cabo las finalidades del tratamiento de datos personales. Al vencimiento de su plazo de conservación, se debe cancelar la base de datos personales que se trate.
QUINTO. El plazo de conservación estará a los tiempos que señale la ley y a los periodos de bloqueo que se requieren para cancelar los datos personales.

CAPÍTULO TERCERO

Del mecanismo de destrucción

SEXTO. Una vez concluido el periodo máximo de tratamiento de una base de datos personales, su destrucción debe llevarse a cabo bajo procedimientos seguros para garantizar que la información fue borrada en su totalidad, tanto en sus soportes físicos como electrónicos, y no puedan recuperarse.

SÉPTIMO. La destrucción de la base de datos personales debe llevarse a cabo por el responsable de la misma, contando con la asesoría y supervisión de la Unidad de Datos Personales.

OCTAVO. El responsable del sistema deberá seleccionar una herramienta de borrado que permita obtener un documento para identificar claramente la realización de dicho proceso, detallando cuándo y cómo fue llevado a cabo.

NOVENO. La técnica de destrucción elegida deberá tener las siguientes características: irreversibilidad, seguridad, confidencialidad y ser favorable al medio ambiente.

LINEAMIENTOS PARA LA ORGANIZACIÓN DE LA GESTIÓN ARCHIVÍSTICA

CAPÍTULO PRIMERO

Disposiciones generales

PRIMERO. Los presentes lineamientos establecen las reglas para regular la forma de coordinación de los sujetos que comprenden el Sistema Institucional de Archivos.

SEGUNDO. Son sujetos del Sistema Institucional de Archivos de Movimiento Ciudadano:

I. El Coordinador Nacional de Archivo.

II. Las Unidades Administrativas Responsables.

III. El Archivo de Trámite.

IV. El Archivo de Concentración.

V. El Archivo Histórico.

VI. La Oficialía de Partes.

CAPÍTULO SEGUNDO

Del Control de Gestión Documental.

TERCERO. Las Unidades Administrativas determinarán al funcionario responsable de realizar las siguientes funciones:

I. Recibir y distribuir la correspondencia de entrada.
II. Registrar y controlar la correspondencia de entrada y salida.
III. Recibir y despachar la correspondencia de salida de sus áreas.

CUARTO. Los funcionarios responsables del control de gestión documental elaborarán una ficha de control para el seguimiento administrativo de la gestión a la que dé lugar el documento ingresado a la Unidad Administrativa responsable. Ésta deberá contener como elementos mínimos de descripción los siguientes:

I. El número identificador (folio consecutivo de ingreso renovable anualmente).
II. El asunto (breve descripción del contenido del documento).
III. Fecha y hora de recepción.
IV. Generador y receptor del documento (nombre y cargo).

CAPÍTULO TERCERO

De los Archivos de Trámite.

QUINTO. La organización de los archivos deberá asegurar la disponibilidad, localización expedita, integridad y conservación de los documentos de archivo que poseen las Unidades Administrativas. En cada Unidad Administrativa, existirá un archivo de trámite.

SEXTO. Los responsables de las Unidades Administrativas designarán a un responsable encargado de coordinar el archivo de trámite, el cual tendrá las siguientes funciones:

I. Integrar los expedientes de archivo.
II. Conservar la documentación activa y aquella clasificada como reservada o confidencial, conforme al catálogo de disposición documental.
III. Elaborar los inventarios de transferencia primaria.
IV. Valorar y seleccionar los documentos y expedientes de las series documentales, con el objeto de realizar las transferencias primarias al archivo de concentración, conforme al catálogo de disposición documental.
V. Aplicar los criterios de organización, manejo y administración del archivo de trámite, así como los procedimientos archivísticos para el acceso a la información.
VI. Elaborar el inventario general de la Unidad Administrativa por lo que hace al archivo de trámite.

SÉPTIMO. Los responsables de los archivos de trámite elaborarán, por lo que hace a dicho archivo, la parte correspondiente de la guía simple con base en el cuadro general de clasificación archivística, éste deberá contener la descripción básica de sus series documentales, la relación de documentos y expedientes del archivo de trámite, así como el nombre, cargo, dirección, teléfono y correo electrónico del propio responsable.

CAPÍTULO CUARTO

Del archivo de concentración

OCTAVO. El archivo de concentración estará adscrito al área coordinadora de archivos. El responsable del archivo de concentración fungirá como enlace con los responsables de los archivos de trámite y deberá:

I. Recibir de los archivos de trámite la documentación semiactiva.

II. Conservar precautoriamente la documentación semiactiva hasta cumplir su vigencia documental conforme al catálogo de disposición documental, o al cumplir su periodo de reserva.

III. Valorar los documentos y expedientes de las series resguardadas conforme al catálogo de disposición documental, tomando en cuenta sus valores administrativos, legales, fiscales y/o contables.

IV. Elaborar los inventarios de transferencia secundaria y de baja documental, según sea el caso.

V. Solicitar a los responsables de archivo de trámite el visto bueno del área generadora de los documentos, la liberación de los expedientes para determinar su destino final.

VI. Realizar, en su caso, las transferencias secundarias al archivo histórico Institucional.

CAPÍTULO QUINTO

Del Archivo Histórico

NOVENO. El Archivo Histórico estará adscrito al área coordinadora de archivos. El responsable del archivo histórico fungirá como enlace con el responsable del archivo de concentración y deberá:

I. Recibir los documentos con valor histórico enviados por el archivo de concentración.
II. Validar la documentación que deba conservarse permanentemente por tener valor histórico.
III. Organizar, conservar, describir y difundir la documentación con valor histórico.
IV. Establecer un programa que permita respaldar los documentos históricos a través de sistemas ópticos y electrónicos.
V. Establecer el uso y aprovechamiento social de la documentación histórica, difundiendo el acervo y sus instrumentos de consulta.

LINEAMIENTOS PARA EL DESARROLLO DE LA GESTIÓN ARCHIVÍSTICA

CAPÍTULO PRIMERO
Disposiciones generales

PRIMERO. Los presentes lineamientos establecen las reglas que habrán de regular la forma de llevar a cabo las actividades propias del Sistema Institucional de Archivos de Movimiento Ciudadano.

CAPÍTULO SEGUNDO

Del préstamo de expedientes

SEGUNDO. El acceso y uso de la información documental deberá realizarse por medio de los controles establecidos y a través de un vale de préstamo de expediente.

TERCERO. Los expedientes facilitados en calidad de préstamo, por medio de vale, deberán estar previamente cosidos o sujetos con broches. Se deberá identificar el número de clave de clasificación y el número del expediente o legajo del mismo que se solicita en préstamo y el total de fojas que integran el expediente.

CUARTO. El responsable del resguardo documental, en el archivo de trámite al que se solicita el préstamo, deberá de manera inmediata localizar el legajo y/o expediente para facilitarlo al solicitante autorizado.

A todo expediente prestado, se deberá indicar en el inventario general de expediente en dónde se encuentra en préstamo, por medio del “Vale de Préstamo”, “Petición por Oficio” u otro medio.

QUINTO. Cuando el documental prestado sea devuelto, éste deberá integrarse a su lugar físico que le corresponde, exactamente en el sitio donde le corresponde.

CAPÍTULO TERCERO

De los Instrumentos de Consulta y de Control Archivístico

SEXTO. El responsable de la coordinación nacional de archivos deberá elaborar y actualizar los instrumentos de consulta y control para propiciar la organización, conservación y localización expedita de los archivos del instituto, por lo que deberá contar al menos con los siguientes:

I. El cuadro general de clasificación archivística.
II. El catálogo de disposición documental.
III. Los inventarios documentales.
    a. General.
    b. De transferencia.
    c. De baja.
IV. La guía simple.

El responsable de la coordinación nacional de archivos proporcionará la asesoría técnica a los responsables para la elaboración de los instrumentos de consulta y de control archivístico para los archivos de trámite.

SÉPTIMO. La estructura del cuadro general de clasificación será atendiendo a los siguientes niveles:

I. Primero: (fondo) conjunto de documentos producidos orgánicamente por el instituto, se identifica por su nombre.
II. Segundo: (sección) cada una de las divisiones del fondo, basada en las atribuciones de cada órgano responsable de conformidad con las disposiciones legales aplicables.
III. Tercero: (serie) división de una sección que corresponde al conjunto de documentos producidos en el desarrollo de una misma atribución general y versan sobre una materia o asunto específico.

Lo anterior, sin perjuicio de que existan niveles intermedios, según los requerimientos de las Unidades Administrativas. Los niveles podrán identificarse mediante una clave alfabética, numérica o alfanumérica, según sea el caso, mismos que serán establecidos y uniformados por la coordinación de archivos.

CAPÍTULO CUARTO

De los Expedientes de Archivo

OCTAVO. Además de contener documentos, los expedientes deben formarse con la portada o guarda exterior, ésta debe incluir datos de identificación del mismo, considerando el cuadro general de clasificación archivística. El marcado de identificación del expediente debe contener como mínimo lo siguiente:

I. Unidad Administrativa responsable.
II. Fondo.
III. Sección.
IV. Serie.
V. Número de expediente o clasificador: el número consecutivo que dentro de la serie documental identifica a cada uno de sus expedientes.
VI. Fecha de apertura y, en su caso, de cierre del expediente.

VII. Asunto (resumen o descripción del expediente).
VIII. Valores documentales.
IX. Vigencia documental.
X. Número de fojas útiles al cierre del expediente: es el número total de hojas contenidas en los documentos del expediente.

En la ceja de la portada o guarda exterior del expediente, deberá señalarse la nomenclatura asignada a los incisos III, IV y V. Cuando se trate de expedientes y documentos clasificados como reservados o confidenciales, deberán contener la leyenda de clasificación conforme a lo establecido la Ley General de Transparencia y Acceso a la Información Pública.

CAPÍTULO QUINTO

De la Conservación de Archivos

NOVENO. El catálogo de disposición documental se actualizará periódicamente cada año de calendario y será responsabilidad de las Unidades Administrativas. En el catálogo de disposición documental, se establecerán los periodos de vigencia de las series documentales, sus plazos de conservación, así como su carácter de reserva o confidencialidad.

En los plazos de conservación de los archivos, se tomará en cuenta la vigencia documental, así, como en su caso, el periodo de reserva correspondiente.

DÉCIMO. A partir de la desclasificación de los expedientes reservados, el plazo de conservación adicionará un periodo igual al de reserva o al establecido por el catálogo de disposición documental, si éste fuera mayor al primero.

Aquellos documentos que hayan sido objeto de solicitudes de acceso a la información, se conservarán por dos años más desde la conclusión de su vigencia documental.

DÉCIMO PRIMERA. Al concluir los plazos establecidos en el lineamiento anterior, el área coordinadora de archivos emitirá un dictamen de valoración para determinar el destino final de los documentos.

DÉCIMO SEGUNDA. Los inventarios de baja documental autorizados por el Comité Nacional de Transparencia deberán conservarse en el archivo de concentración por un plazo de cinco años, contados a partir de la fecha en que se haya autorizado la baja correspondiente. Este plazo se incluirá en el catálogo de disposición documental.

DÉCIMO TERCERA. Las Unidades Administrativas y la Coordinación Nacional de Archivos adoptarán medidas y procedimientos técnicos que garanticen la conservación de la información y la seguridad de sus soportes, entre otros:

I. Contar con espacios diseñados y destinados exclusivamente a la recepción, organización y resguardo temporal o definitivo de los documentos.
II. Contar con sistemas de control ambiental y de seguridad para conservar los documentos.

CAPÍTULO SEXTO

De los documentos electrónicos.

DÉCIMO CUARTA. Los titulares de las Unidades Administrativas y el responsable de la coordinación de archivos tomarán las medidas necesarias para administrar y conservar los documentos electrónicos, generados o recibidos, cuyo contenido y estructura permitan identificarlos como documentos de archivo que aseguren la identidad e integridad de su información.

DÉCIMO QUINTA. Los titulares de las Unidades Administrativas y el responsable de la coordinación nacional de archivos aplicarán las medidas técnicas de administración y conservación para asegurar la validez, autenticidad, confidencialidad, integridad y disponibilidad de los documentos electrónicos de acuerdo con las especificaciones de soportes, medios y aplicaciones de conformidad con las normas nacionales e internacionales.

DÉCIMO SEXTA. Los titulares de las Unidades Administrativas y el responsable de la coordinación nacional de archivos realizarán programas de respaldo y migración de los documentos electrónicos, de acuerdo con sus recursos.

LINEAMIENTOS DE ENTREGA-RECEPCIÓN