INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

Manual de Procedimientos de la Unidad de Transparencia del Instituto Electoral de la Ciudad de México.

ÍNDICE.

1. Objetivo 3

2. Definiciones 3

3. Interpretación. 7

4. Unidad de Transparencia del Instituto Electoral de la Ciudad de México. 8

5. Procedimiento para la atención de solicitudes de información pública. 9

6. Procedimiento para la atención de solicitudes de acceso, rectificación, cancelación u oposición de datos personales (Derechos ARCO). 10

7. Atención y seguimiento de los recursos de revisión interpuestos en contra de las respuestas del Instituto Electoral a las solicitudes de información pública y de datos personales. 12

8. Avisos de Privacidad. 14

9 Sistemas de Datos Personales. 15

10. Elaboración y/o actualización de los Documentos de Seguridad. 17

11. Publicación y actualización de las obligaciones de transparencia, en el Sitio institucional de Internet y en la Plataforma Nacional de Transparencia. 18

12. Elaboración y presentación de los informes. 18

ANEXOS

Anexo 1 Cédula para la Atención de Solicitudes de Información Pública (Código: SE/OTAIPDPyA/PR01) ……..……. 20

Anexo 2 Cédula Atención a solicitudes para el ejercicio de los derechos ARCO, (Código: SE/OTAIPDPyA/PR02) …… ……. 45

Anexo 3 Cédula Elaboración y/o actualización de los Avisos de Privacidad, Código: SE/OTAIPDPyA/PR03) ……..… 73

Anexo 4 Cédula Creación, modificación o supresión de los Sistemas de Datos Personales, Código: SE/OTAIPDPyA/PR04) ……..…… 94

Anexo 5 Cédula Elaboración y/o actualización de los Documentos de Seguridad, Código: SE/OTAIPDPyA/PR05) ……..…… 129

Anexo 6 Actualización de las obligaciones de transparencia en el Portal Institucional de Transparencia y en la Plataforma Nacional de Transparencia, Código: SE/OTAIPDPyA/PR06)…….……... 174

1. Objetivo.

El presente Manual tiene como finalidad establecer los procedimientos mediante los cuales la Unidad de Transparencia, orgánicamente denominada, Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo, del Instituto Electoral de la Ciudad de México, dará cumplimiento a las disposiciones establecidas en la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas, así como en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley de Archivos, todas de la Ciudad de México.

Lo anterior, a efecto de transparentar el ejercicio de la función pública y establecer criterios y procedimientos tendentes a garantizar el pleno ejercicio del derecho de acceso a la información generada o en posesión de este órgano autónomo, resguardando toda aquella información de acceso restringido, ya sea en su modalidad de reservada o confidencial; y propiciar la debida rendición de cuentas de los recursos públicos, y regular el ejercicio de las funciones y atribuciones de las personas servidoras públicas que integran la misma.

2. Definiciones.

2.1. Ordenamientos jurídicos.

a). Código: Código de Instituciones y Procedimientos Electorales de la Ciudad de México;

b). Ley General de Transparencia: Ley General de Transparencia y Acceso a la Información Pública;

c). Ley General de Protección de Datos: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

d). Ley de Transparencia: Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México;

e). Ley de Datos: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;

f). Reglamento de Transparencia: Reglamento del Instituto Electoral de la Ciudad de México en Materia de Transparencia, Acceso a la Información Pública y Rendición de Cuentas.

g). Reglamento de Datos. Reglamento del Instituto Electoral de la Ciudad de México en materia de Protección de Datos Personales.

h). Reglamento de Funcionamiento: Reglamento de Funcionamiento del Comité de Transparencia del Instituto Electoral de la Ciudad de México;

i). Lineamientos de Clasificación: Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas;

j). Lineamientos de Datos Personales: Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;

k). Lineamientos para la gestión de solicitudes: Lineamientos para la gestión de solicitudes de información pública y de datos personales en la Ciudad de México;

l). Lineamientos para la portabilidad: Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales;

m). Lineamientos Técnicos: Lineamientos Técnicos Generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el Título Quinto y en la fracción IV y artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portarles de Internet y en la Plataforma Nacional de Transparencia.

n). Lineamientos del INFO: Lineamientos Técnicos para Publicar, Homologar y Estandarizar la Información de las Obligaciones establecidas en el Título Quinto de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

ñ). Lineamientos de Funcionamiento de los Comités: Lineamientos Técnicos para la Instalación y Funcionamiento de los Comités de Transparencia de los Sujetos Obligados de la Ciudad de México.

o) Manual: El presente Manual de Procedimientos de la Unidad de Transparencia del Instituto Electoral de la Ciudad de México.

p) Criterios: Criterios para regular el bloqueo de la información, verificación y supresión de los sistemas de datos personales del Instituto Electoral de la Ciudad de México.

2.2. Órganos e instancias.

a). AR´s: Cada una de las áreas administrativas del Instituto Electoral de la Ciudad de México: Presidencia del Consejo General, Oficinas de las y los Consejeros Electorales, Secretaría Ejecutiva, Secretaría Administrativa, Contraloría Interna, Direcciones Ejecutivas, Unidades Técnicas y Órganos Desconcentrados.

b). Comité: Comité de Transparencia del Instituto Electoral de la Ciudad de México.

c). Enlace: Persona designada por la persona titular del área administrativa, para atender los temas relacionados con acceso a la información pública, datos personales, actualización de las obligaciones de transparencia y transparencia proactiva, la cual fungirá como vínculo entre la Unidad de Transparencia y las personas Titulares de las distintas áreas que conforman el Instituto Electoral de la Ciudad de México.

d). Instituto Electoral: Instituto Electoral de la Ciudad de México.

e). INFO: Instituto de Transparencia, Acceso a la Información Pública; Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

f). Oficial de Protección de Datos Personales: Persona servidora pública especialista en materia de datos personales, designada por el responsable del Instituto Electoral, adscrita a la Unidad de Transparencia; quien coordina las actividades para atender los asuntos relacionados con la protección de datos personales.

g). Responsable del Sistema de Datos Personales: Persona servidora pública del Instituto Electoral, con el cargo de Titular del área que administra el Sistema de Datos Personales; que decide y determina la finalidad, fines, medios, medidas de seguridad y todo aquello relacionado con el tratamiento de datos personales.

h). Unidad Jurídica: Unidad Técnica de Asuntos Jurídicos del Instituto Electoral

i). Unidad de Transparencia: Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral de la Ciudad de México.

2.3. Glosario.

2.3.1. Clasificación de información: Acto formal a través del cual las AR's someten a consideración del Comité de Transparencia, la propuesta para determinar que la información solicitada es de carácter restringido en su modalidad de confidencial o reservada.

a). Información clasificada: La información en posesión del Instituto Electoral, bajo las figuras de reservada o confidencial.

b). Información confidencial: Información que contiene datos personales y se encuentra en posesión del Instituto Electoral, susceptible de ser tutelada por el derecho fundamental a la privacidad, intimidad, honor, dignidad y toda aquella que la Ley prevea como tal.

c). Información reservada: Información pública que se encuentra temporalmente sujeta a alguna de las excepciones previstas en la Ley de Transparencia;

d) Versión pública: Información a la que se da acceso, eliminando u omitiendo partes o secciones clasificadas.

2.3.2. Datos Personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información como puede ser nombre, número de identificación, datos de localización, identificador en línea o uno o varios elementos de la identidad física, fisiológica, genética, psíquica, patrimonial, económica, cultural o social de la persona.

2.3.2.1. Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

2.3.3. Información pública: A la señalada en el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos;

a) Derecho de acceso a la información pública: Prerrogativa que tiene toda persona para acceder a la información generada o en poder del Instituto Electoral, en los términos de la Ley de Transparencia;

b) Información de interés público: información que resulta relevante **o beneficiosa** para la sociedad **y no simplemente de interés individual, cuya divulgación resulta útil para que el público comprenda las actividades que llevan a cabo el Instituto Electoral**;

c) Persona solicitante: Toda persona que pide información pública, así como el acceso, cancelación, rectificación, u oposición de datos personales al Instituto Electoral;

d) Solicitud: Escrito libre o formatos impresos o electrónicos mediante los cuales la persona solicitante presenta su requerimiento de información pública o de acceso, rectificación, cancelación, oposición y portabilidad de datos personales, al Instituto Electoral;

e) Consulta Directa: Prerrogativa que tiene toda persona de allegarse de información pública, sin intermediarios;

2.3.4. PNT: Plataforma Nacional de Transparencia;

2.3.5. Portal de Internet: Sitio web oficial del IECM, al que se puede acceder desde www.iecm.mx; y

2.3.6. Estrados de la Unidad de Transparencia: lugar donde se colocan para efectos de la notificación y para el conocimiento público, los escritos y documentos, relacionados con las solicitudes de información pública y de datos personales.

3. Interpretación.

La interpretación de las disposiciones del presente Manual, se realizará conforme a los criterios establecidos por los artículos 4 y 10 de la Ley de Transparencia, 7 de la Ley de Datos; así como lo correspondiente a la Ley de Archivos, aplicable en la Ciudad de México.

4. Unidad de Transparencia del Instituto Electoral de la Ciudad de México.

4.1. Definición, horario de atención, ubicación y contacto.

Definición: La Unidad de Transparencia es la unidad administrativa del Instituto Electoral receptora de las peticiones ciudadanas de información pública, y de las solicitudes de acceso, rectificación, cancelación, oposición y de portabilidad de datos personales, a cuya tutela estará el trámite de las mismas conforme a lo establecido en la Ley de Transparencia, Ley de Datos, los Lineamientos para la gestión de solicitudes, Lineamientos de Datos Personales, Lineamientos de Funcionamiento de los Comités, los Reglamentos de Transparencia y Funcionamiento del Comité, y en términos de este Manual.

La Unidad de Transparencia tendrá un horario de atención al público: De 9:00 a 16:00 horas, de lunes a viernes (días hábiles);

Ubicación:
Calle Huizaches No. 25, Planta baja, Entrada Principal, Colonia Rancho Los Colorines, Demarcación territorial Tlalpan, C. P. 14386, en la Ciudad de México;

Teléfono: Conmutador: 54 83 38 00, extensión 4727;

Sitio de Internet: www.iecm.mx; y

Dirección de correo electrónico:
unidad.transparencia@iecm.mx

4.2. Atribuciones.

Las establecidas en los artículos 93 de la Ley de Transparencia, 76 de la Ley de Datos; así como lo correspondiente a la Ley de Archivos, aplicable en la Ciudad de México.

5. Procedimiento para la atención de solicitudes de información pública.

La Unidad de Transparencia llevará a cabo su actuación de conformidad con la Ley de Transparencia, Ley de Datos; así como a lo dispuesto en el Reglamento de Transparencia, Reglamento de Datos, Reglamento de Funcionamiento, el Manual y demás normativa atinente.

5.1. La orientación a las personas solicitantes.

El personal de la Unidad de Transparencia se encargará de orientar en forma sencilla, comprensible y accesible a las personas solicitantes, cuando así se requiera, ya sea por vía telefónica, correo electrónico o personalmente.

De ser necesario, la Unidad de Transparencia brindará apoyo y orientación a los particulares en la elaboración de sus solicitudes, especialmente cuando la información solicitada no sea precisa o los detalles proporcionados para localizar los documentos resulten insuficientes, o no contenga todos los datos requeridos.

5.2. La información que se encuentra para consulta directa en la Unidad de Transparencia.

La información relacionada con las obligaciones de transparencia, también llamada información pública de oficio, prevista en la Ley de Transparencia, estará disponible para su consulta.

5.3. La recepción de solicitudes y su registro.

En términos de lo establecido por la Ley de Transparencia y el Reglamento de Transparencia, la Unidad de Transparencia recibirá las solicitudes de información por las vías siguientes:

I. Por escrito;

II. "Formato de solicitud de acceso a la información pública", que se encuentra en el Sitio de Internet para su impresión, y en las instalaciones de la Unidad de Transparencia;
III. Correo electrónico;
IV. Correo postal y telégrafo;
V. Manera verbal, de forma presencial o telefónica;
VI. PNT; y
VII. Medios electrónicos.

Tratándose de solicitudes de información presentadas por cualquiera de los medios señalados en las fracciones I, II, III, IV, y V la Unidad de Transparencia las registrará en la PNT, a más tardar, al día hábil siguiente en que tenga conocimiento de las mismas.

5.4. Trámite de las solicitudes de información pública.

Toda persona por sí o por medio de representante, tiene derecho a presentar una solicitud de acceso a la información pública, sin necesidad de sustentar justificación o motivación alguna.

Para conocer el trámite que se dará a una solicitud de información pública presentada ante el Instituto Electoral, la persona solicitante podrá consultar la **cédula para la Atención de Solicitudes de Información Pública** (Código: SE/OTAIPDPyA/PR01), en la que se describe el procedimiento y términos para su atención, misma que forma parte del presente Manual, (**Anexo 1).**

6. Procedimiento para la atención de solicitudes de acceso, rectificación, cancelación, oposición (Derechos ARCO) y portabilidad de datos personales;

Para la tramitación de las solicitudes en ejercicio de los derechos ARCO y portabilidad dirigidas al Instituto Electoral; la Unidad de Transparencia, se apegará

a lo establecido en la: Ley General de Transparencia, Ley General de Protección de Datos, Ley de Transparencia, Ley de Datos, Lineamientos de Datos, Reglamento de Datos y demás normativa en la materia.

El personal de la Unidad de Transparencia orientará a las personas titulares respecto al ejercicio de los derechos ARCO y de portabilidad de sus datos personales, que se administren en los sistemas de datos personales en posesión del Instituto Electoral.

6.1. Requisitos para atención de solicitudes en ejercicio de los derechos ARCO y portabilidad de datos personales.

Las solicitudes relacionadas con los datos personales se tramitarán en los términos siguientes:

Sólo la persona interesada o su representante legal, previa acreditación de su personalidad, podrá solicitar al Instituto Electoral el acceso, rectificación, cancelación u oposición de sus datos personales.

En la solicitud de acceso, rectificación, cancelación u oposición de los datos personales no podrán imponerse mayores requisitos que los siguientes:

I. El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones;
II. Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante;
III. De ser posible, el área responsable del tratamiento de los datos personales;
IV. La descripción clara y precisa de los datos personales respecto de los cuales desea ejercer los derechos ARCO, o bien, lo que solicita el titular; y
V. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

6.2. Recepción de las solicitudes de derechos ARCO.

La solicitud de acceso, rectificación, cancelación u oposición de datos personales, se deberá presentar ante la Unidad de Transparencia del Instituto Electoral, en cualquiera de las siguientes modalidades:

I. Escrito material, presentado personalmente por la persona titular de los datos o su representante legal;

II. En forma verbal, realizada por la persona titular de los datos o su representante legal, en cuyo supuesto deberá ser capturada por el personal de la Unidad de Transparencia en el formato respectivo;

III. Por correo electrónico, la persona interesada formula su solicitud a través de una dirección electrónica, dirigida a la dirección de correo electrónico asignada a la Unidad de Transparencia;

IV. Por la Plataforma Nacional de Transparencia, y

V. Por vía telefónica, en términos de los lineamientos que expida el INFO.

6.3. Trámite para la Atención a solicitudes para el ejercicio de los derechos ARCO y de portabilidad.

Para conocer las directrices que habrá de seguir el trámite de las Solicitudes para el ejercicio de los derechos de Acceso, Rectificación, Cancelación, Oposición y portabilidad de Datos Personales; así como el procedimiento, términos de atención y responsabilidades por cada una de las áreas involucradas, la persona titular podrá consultar la **Cédula *Atención a solicitudes para el ejercicio de los derechos ARCO,*** (Código: SE/OTAIPDPyA/PR02), (**Anexo 2).**

7. Atención y seguimiento de los recursos de revisión interpuestos en contra de las respuestas del Instituto Electoral a las solicitudes de información pública y de datos personales.

Para el caso de inconformidad con la respuesta a una solicitud de información o de protección de datos personales, la Unidad de Transparencia orientará a la persona solicitante sobre su derecho de interponer recurso de revisión, así como el modo de

hacerlo; en términos de lo establecido en la Ley de Transparencia o la Ley de Datos, atendiendo el caso específico; bien sea, ante la propia Unidad de Transparencia del Instituto Electoral o directamente ante el INFO.

En caso de que se interponga un recurso de revisión en contra de la respuesta a una solicitud de información ante la Unidad de Transparencia, ésta deberá remitirlo al INFO a más tardar al día hábil siguiente de haberlo recibido.

Asimismo, cuando la Unidad de Transparencia reciba la notificación de la interposición de un recurso de revisión, lo hará del conocimiento del área que propuso el contenido de la respuesta, a más tardar al día hábil siguiente, para que elabore el proyecto de informe.

El área deberá enviar a la Unidad de Transparencia el proyecto de informe, dentro de los dos días hábiles siguientes a la notificación, para cumplir con el plazo establecido en la Ley de Transparencia y el Reglamento de Transparencia, junto con las pruebas que sustenten lo manifestado en el informe.

Para la realización del informe, la Unidad de Transparencia solicitará la asesoría de la Unidad Jurídica debiendo remitir el proyecto de informe con los documentos respectivos, por lo menos con tres días de anticipación a la fecha del vencimiento del plazo para su presentación ante el INFO, por lo que dicha Unidad deberá remitir el proyecto de informe con las observaciones que considere pertinentes, dentro de las 48 horas de haberlo recibido. En caso de urgencia, se remitirá por lo menos con dos días de anticipación a la fecha del vencimiento de plazo para su presentación ante el INFO, debiendo adjuntar el escrito en el que se justifique la urgencia, en cuyo caso, la Unidad Jurídica tendrá 24 horas para remitir observaciones al proyecto de informe.

La Unidad de Transparencia presentará ante el INFO, el informe, así como las pruebas para su desahogo, dentro de los siete días hábiles siguientes contados a partir de la recepción de la respectiva notificación.

La Unidad de Transparencia dará seguimiento a los recursos de revisión interpuestos en contra de las decisiones del Instituto Electoral, e informará al Comité el sentido de la resolución emitida por el INFO.
La Unidad de Transparencia informará al INFO del cumplimiento de sus resoluciones en términos de la Ley de Transparencia y del Reglamento de Transparencia.

8. Avisos de Privacidad.

El Aviso de privacidad, también conocido como el deber de informar, es el primer documento que debe ser puesto a disposición de la persona titular de los datos personales, ya sea de forma física o electrónica, previo a recabar datos personales.

En este sentido, el Responsable del Sistema de Datos Personales deberá informar a la persona titular de los datos sobre las características principales del tratamiento, la finalidad y cualquier cambio relacionado con sus datos personales, previo al tratamiento de los mismos, a fin de que pueda tomar decisiones informadas al respecto.

Por regla general, el aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que cuente el responsable.

Para que el aviso de privacidad cumpla de manera eficiente con su función de informar, deberá estar redactado y estructurado de manera clara, sencilla y comprensible.

El aviso de privacidad, en sus modalidades de integral y simplificado, deberán cumplir con los formatos previstos en los Lineamientos de Datos Personales vigentes.

8.1. Elaboración y/o actualización de los Avisos de Privacidad.

El aviso debe comprender, cuando menos: la identificación del responsable y la ubicación de su domicilio; fundamento legal que faculta al responsable para llevar a cabo el tratamiento; los datos personales que serán sometidos a tratamiento, así como de la existencia de un sistema de datos personales; las finalidades del tratamiento para las cuales se recaban los datos personales, el ciclo de vida de los mismos, la revocación del consentimiento y los derechos de la persona titular sobre éstos, la Oficina en donde podrá ejercer sus derechos ARCO y la ubicación de la Unidad de Transparencia.

En este sentido, para llevar a cabo la elaboración y/o actualización de los Avisos de privacidad de los Sistemas de Datos Personales en posesión del Instituto Electoral, se deberá consultar la **cédula *Elaboración y/o actualización de los Avisos de Privacidad*,** (Código: SE/OTAIPDPyA/PR03), en la que se describe de manera detallada como llevar a cabo la elaboración de un aviso de privacidad ya sea simplificado o integral, características, políticas de operación, términos, procedimiento y formatos.(**Anexo 3).**

9. Sistemas de Datos Personales.

Para el debido tratamiento de datos personales, es de suma importancia contar con Sistemas de Datos Personales, para su debido resguardo y protección, por lo que un Sistema de Datos Personales, se considera como el conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión del Instituto Electoral, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

9.1. Creación, modificación o supresión de los Sistemas de Datos Personales.

Como regla general para llevar a cabo la creación, modificación o supresión de un Sistema de Datos Personales, se requiere de su publicación en Gaceta Oficial de la Ciudad de México, y como mínimo deberá inscribirse la información siguiente:

a) La finalidad o finalidades de los sistemas de datos personales; así como los usos y transferencias previstos;
b) Las personas físicas o grupos de personas sobre las que se recaben o traten datos personales;
c) La estructura básica del sistema de datos personales y la descripción de los tipos de datos incluidos;
d) Las instancias responsables del tratamiento del sistema de datos personales: titular del sujeto obligado, usuarios y encargados, si los hubiera;
e) Las áreas ante las que se podrán ejercer los derechos de acceso, rectificación, cancelación y oposición;
f) El procedimiento a través del cual se podrán ejercer los derechos de acceso, rectificación, cancelación y oposición; y
g) El nivel de seguridad y los mecanismos de protección exigibles.

En la supresión de los sistemas de datos personales, se considerará además el ciclo vital del dato personal, la finalidad, y los destinos de los datos contenidos en el mismo o, en su caso, las previsiones adoptadas para su destrucción.

Derivado de lo anterior, deberán observarse las acciones establecidas en los Criterios, a efecto de resguardar durante el proceso de supresión el debido tratamiento de la información contenida en los sistemas de datos personales.

Asimismo, todos los Sistemas de Datos Personales que sean creados por el Instituto Electoral, deberán quedar debidamente registrados ante la PNT; en el caso de las modificaciones y supresiones, de igual forma, serán notificadas al órgano garante.

Bajo esta tesitura, para la creación, modificación o supresión de alguno de los Sistemas de Datos Personales con que cuenta el Instituto Electoral, se deberá llevar a cabo de conformidad con el procedimiento establecido en la **Cédula *Creación, modificación o supresión de los Sistemas de Datos Personales,*** (Código: SE/OTAIPDPyA/PR04), en la que se describe cómo realizar cada uno de los

documentos, los plazos y términos, forma de su registro y los formatos para su realización **(Anexo 4).**

10. Elaboración y/o actualización de los Documentos de Seguridad.

Para que el tratamiento de datos personales sea lícito, transparente y responsable, se deberán adoptar las medidas de seguridad necesarias para su protección, de manera tal que permitan protegerlos contra daño, pérdida, alteración, destrucción o del uso, acceso o tratamiento no autorizados, por lo que las acciones relacionadas con dichas medidas deberán estar documentadas y contenidas en un sistema de gestión denominado documento de seguridad.

Todos los Sistemas de Datos Personales del Instituto Electoral, deberán contar con su documento de seguridad, entendiendo éste, cómo: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por las áreas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

El documento de seguridad deberá ser considerado confidencial y sólo podrá otorgarse, en su caso, versión pública del mismo, ante la presentación de una solicitud de acceso a la información pública.

En este contexto, para la elaboración de los documentos de seguridad deberá consultarse la **Cédula *Elaboración y/o actualización de los Documentos de Seguridad,*** (Código: SE/OTAIPDPyA/PR05), en la que se describe paso a paso cómo realizar un documento de seguridad, los apartados a considerar y cómo desarrollar cada uno, los plazos y términos de actualización, políticas de operación, responsabilidades y formato para su integración. **(Anexo 5).**

11. Publicación y actualización de las obligaciones de transparencia, en el Sitio institucional de Internet y en la PNT.

Con la finalidad de que la información en poder del Instituto Electoral se encuentre debidamente actualizada, las Áreas deberán revisar de manera trimestral la información pública de oficio que les competa, conforme a lo siguiente:

I. Respecto a la actualización de la información que les corresponda, las áreas responsables observarán lo previsto en los Lineamientos Técnicos y los Lineamientos del INFO;
II. En cuanto al índice de la información que previamente haya sido clasificada como reservada por las áreas responsables, se observará lo previsto en los Lineamientos de clasificación.

La Secretaría Ejecutiva a través de la Unidad de Transparencia, solicitará mediante oficio a las personas titulares de las áreas responsables de generar y administrar las obligaciones de transparencia, la actualización correspondiente. Para tal efecto, se deberá consultar la **Cédula Actualización de las obligaciones de transparencia en el Portal Institucional de Transparencia y en la PNT,** (Código: SE/OTAIPDPyA/PR06), en el que se describe los pasos a seguir tanto para la actualización del apartado de transparencia del Sitio institucional de Internet como en la PNT, políticas de operación, plazos, términos y responsabilidades por cada una de las áreas. **(Anexo 6).**

12. Elaboración y presentación de los informes.

La Unidad de Transparencia elaborará los informes siguientes:

I. Estadístico de la tramitación de Solicitudes de Información Pública y de Datos Personales;
II. De las Actividades del Comité de Transparencia;
III. Del seguimiento de Acuerdos del Comité de Transparencia;

IV. Sobre la actualización de la sección de Transparencia en el Sitio de Internet y en la Plataforma Nacional de Transparencia, y
V. Sobre las obligaciones y actualización de los Sistemas de Datos Personales.
Dichos informes serán presentados trimestralmente ante el Comité.

Además, integrará los informes que deben ser enviados al INFO, de conformidad con los lineamientos y criterios que expida y en términos de las disposiciones normativas en materia de Transparencia, ejercicio del Derecho de Acceso a la Información Pública y de Datos Personales.

Contenido

1. Objetivo 2
2. Alcance 2
3. Marco normativo 2
4. Definiciones y Abreviaturas 3
5. Responsabilidades 5
6. Políticas de operación para la tramitación de las solicitudes de información 6
7. Diagrama de flujo 7
8. Descripción de las actividades 9
9. Formatos 24

Control de Cambios

Revisión	Fecha	Descripción del Cambio
00	09 febrero 2023	Emisión del documento

1. Objetivo

Establecer las directrices para la atención de las Solicitudes de Acceso a la Información Pública formuladas al Instituto Electoral de la Ciudad de México, a través de los diversos instrumentos de gestión, a fin de cumplir con las disposiciones normativas en materia de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

2. Alcance

El presente Procedimiento es aplicable a todas las áreas que integran el Instituto Electoral de la Ciudad de México:

- Presidencia;
- Oficinas de Consejeras y Consejeros Electorales;
- Secretaría Ejecutiva;
- Secretaría Administrativa;
- Contraloría Interna;
- Direcciones Ejecutivas;
- Unidades Técnicas; y
- Órganos Desconcentrados.

3. Marco normativo

- Constitución Política de los Estados Unidos Mexicanos;
- Constitución Política de la Ciudad de México;
- Código de Instituciones y Procedimientos Electorales de la Ciudad de México;
- Ley General de Transparencia y Acceso a la Información Pública;
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Ley General de Archivos;
- Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México;
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;
- Ley de Archivos Local. Ley de Archivos, aplicable en la Ciudad de México;
- Reglamento Interior del Instituto Electoral de la Ciudad de México;
- Reglamento del Instituto Electoral de la Ciudad de México, en materia de Transparencia, Acceso a la Información Pública y Rendición de Cuentas;
- Reglamento de Funcionamiento del Comité de Transparencia del Instituto Electoral de la Ciudad de México;
- Lineamientos para la gestión de solicitudes de información pública y de datos personales en la Ciudad de México.
- Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, aprobados por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales;

- Lineamientos Técnicos para Publicar, Homologar y Estandarizar la Información de las Obligaciones establecidas en el Título Quinto de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.
- Aviso por el que se da a conocer de manera íntegra el Acuerdo mediante el cual se aprueba el Criterio que deberán aplicar los Sujetos Obligados, respecto a la clasificación de información en la modalidad de confidencial, Acuerdo del INFO 1072/SO/03-08/2016 aprobado por el Pleno del INFODF el 3 de agosto de 2016, y publicado en la Gaceta Oficial de la Ciudad de México el 15 de agosto de 2016.

4. Definiciones y Abreviaturas

AR´s.- Cada una de las unidades o áreas administrativas del Instituto Electoral de la Ciudad de México que genere, obtenga o posea información en términos de la legislación aplicable.

Aviso del INFO en materia de Datos Personales: Comunicado por el que se da a conocer de manera íntegra el Acuerdo INFO 1072/SO/03-08/2016, mediante el cual se aprueba el *Criterio que deberán aplicar los Sujetos Obligados, respecto a la clasificación de información en la modalidad de confidencial.*

Clasificación de información.- Acto formal a través del cual las áreas del Instituto Electoral de la Ciudad de México someten a consideración del Comité de Transparencia, la propuesta para determinar que la información solicitada es de carácter restringido en su modalidad de confidencial o reservada.

Comité.- Comité de Transparencia del Instituto Electoral de la Ciudad de México.

Declaratoria de inexistencia.- Documento a través del cual se hace constar que la información motivo de una solicitud de acceso a la información pública, no obra en los archivos del Instituto Electoral de la Ciudad de México.

Instituto Electoral.- Instituto Electoral de la Ciudad de México.

JDDPyAJ.- Jefatura de Departamento de Datos Personales y Apoyo Jurídico adscrita a la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo.

JDSI.- Jefatura de Departamento de solicitudes de información, adscrita a la Oficina de Transparencia, Acceso a la Información Pública, datos Personales y Archivo.

Instrumentos de gestión, son los medios a través de los cuales, las personas formulan solicitudes de acceso a la información pública, de manera: a) Verbal, por comparecencia o vía telefónica; b) Escrita, escrito libre, formato, correo electrónico, correo postal o telégrafo; c) Sistema de solicitudes de acceso a la información (SISAI2.0) de la Plataforma Nacional de Transparencia.

Oficio de ampliación.- Documento a través del cual se hace del conocimiento de la persona solicitante, que el término de respuesta a su solicitud de información será prorrogado hasta por 7 días hábiles más.

Oficio de no presentación de la solicitud.- Documento por el cual se notifica a la persona solicitante que, ante la falta de respuesta a la prevención, o bien, porque la solicitud de información se considera ofensiva, se tiene por no presentada.

Oficio de orientación.- Documento por el cual se comunica a la persona solicitante que, considerando el contenido de su solicitud de información, el Instituto Electoral no cuenta con las atribuciones y/o facultades para atenderla y en su caso, que ha sido canalizada al Sujeto Obligado correspondiente; notificándole la instancia ante la cual se puede dirigir o dar seguimiento a dicha solicitud.

Oficio de prevención.- Documento en el cual se requiere a la persona solicitante para que aclare o precise algún aspecto de su solicitud, por ejemplo: información solicitada; periodo de la información; datos de identificación de la información (en caso de ser necesario), domicilio o medio señalado para recibir notificaciones; modalidad en la que prefiere se otorgue el acceso a la información; aclaración respecto de la información solicitada; lo anterior, para estar en posibilidad de atender su solicitud de información.

Oficio de remisión.- Documento mediante el cual se envía al Sujeto Obligado correspondiente una solicitud de información, para su atención.

Oficio de respuesta.- Documento a través del cual las AR's comunican a la Unidad de Transparencia la respuesta a la solicitud de información para que sea notificada a la persona solicitante.

Oficio de colaboración: Documento mediante el cual el Instituto Electoral, solicita a la Secretaría de Pueblos y Barrios Originarios y Comunidades Indígenas Residentes (SEPI) su colaboración para la traducción de una Solicitud de Acceso a la Información Pública o para dar respuesta a la misma.

Oficio de trámite.- Documento mediante el cual la OTAIPDPyA pide a las AR's del Instituto Electoral atiendan la solicitud de información formulada por la persona solicitante.

Registro electrónico.- Archivo generado con motivo de las solicitudes de información promovidas, en el cual se describen los elementos básicos de identificación, así como el trámite otorgado a cada una.

Sistema de solicitudes de acceso a la información de la Plataforma Nacional de Transparencia. (SISAI 2.0): Es el medio electrónico a través del cual las personas podrán presentar sus solicitudes de acceso a la información pública, considerándose el único medio para el registro, captura y seguimiento de todas las solicitudes formuladas a los Sujetos Obligados, independientemente del instrumento de gestión utilizado (Verbal, por comparecencia o vía telefónica; Escrito, mediante formato, correo electrónico, correo postal o telégrafo; Sistema Electrónico habilitado para tal efecto); asimismo, para la interposición de los recursos de revisión, se llevará a cabo a través de la Plataforma Nacional de Transparencia

STyDP.- Subdirección de Transparencia y Datos Personales, adscrita a la Oficina de Acceso a la Información Pública y Protección de Datos Personales del Instituto Electoral de la Ciudad de México.

Titular de la Oficina.- Titular de la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral de la Ciudad de México, también denominada Unidad de Transparencia.

OTAIPDPyA.- Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral de la Ciudad de México, a la cual también se le denominará indistintamente como Unidad de Transparencia.

Unidad de Transparencia.- Unidad administrativa receptora de las solicitudes de acceso a la información, responsable de su atención, trámite y respuesta, también denominada orgánicamente Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral.

UTAJ.- Unidad Técnica de Asuntos Jurídicos del Instituto Electoral.

5. Responsabilidades

La OTAIPDPyA es el área responsable de recibir, y registrar las solicitudes de acceso a la información pública en el sistema electrónico SISAI 2.0, así como de turnarlas mediante oficio de trámite y a través del sistema electrónico a las AR´s, que de acuerdo con sus atribuciones y/o facultades, generen, obtengan o posean la información motivo de la solicitud, a más tardar **dentro de las 24 horas posteriores a su recepción.**

La OTAIPDPyA será responsable de notificar las respuestas de las solicitudes de información a las personas solicitantes en un **término no mayor a 9 días hábiles**, a partir de su recepción, a través del sistema electrónico SISAI 2.0, así como del medio que para tal efecto señalen en la solicitud de información (correo electrónico, domicilio o el propio SISAI 2.0).

La OTAIPDPyA, notificará a los integrantes e invitados del Comité, la convocatoria y documentos que al efecto emita la Presidencia de dicho órgano colegiado.

La OTAIPDPyA es el área responsable de asesorar y orientar a las AR´s del Instituto Electoral en materia de transparencia, acceso a la información, protección de datos personales y archivos, en la atención de las solicitudes de información.

Las AR´s que generen, obtengan o posean la información son responsables de atender las solicitudes de información **en el término de 6 días hábiles**, contados a partir de la recepción de la solicitud de información. Cuando se trate de **información pública de oficio**, la OTAIPDPyA atenderá las solicitudes de información en **un plazo no mayor a 4 días hábiles.**

Las AR´s, al momento de emitir respuesta a una solicitud de información, serán las responsables de proponer la clasificación o declaración de inexistencia de la información, lo anterior de conformidad con la información que generen, obtengan o posean en términos de la legislación aplicable.

La Unidad de Transparencia, será la responsable de determinar si la información solicitada se encuentra o no, dentro de las atribuciones del Instituto Electoral, para la subsecuente atención de la misma.

6. Políticas de operación para la tramitación de las solicitudes de información

La **JDSI**, a partir de la recepción de la solicitud de información por cualquiera de los instrumentos de gestión, realiza de manera inmediata, la captura de los datos de identificación de la solicitud en el sistema electrónico SISAI 2.0.

Si la Información solicitada tiene el carácter de **reservada o confidencial**, las AR´s lo comunicarán a la OTAIPDPyA, en **un plazo no mayor a 3 días hábiles** a partir de que tengan conocimiento de la solicitud y solicitarán a la misma, convocar al Comité.

Si la información es de carácter reservada, las AR´s deberán precisar de manera fundada y motivada la información que se reserva, así como aplicar la prueba de daño, fijar el plazo de reserva y, en su caso, acompañar la propuesta de versión pública.

Si la información es catalogada como confidencial, las AR´s, tendrán que señalar los datos personales o información confidencial que clasifican; la legislación específica que la regula, o bien, que corresponde a información que previamente ha sido clasificada por el Comité de Transparencia.

En el supuesto de información previamente clasificada por el Comité como confidencial, la OTAIPDPyA deberá precisar los datos de la Sesión y Acuerdo del Comité en que se aprobó dicha clasificación; a fin de dar cumplimiento al Acuerdo del INFO 1072/SO/03-08/2016, así como a las demás disposiciones adoptadas por el Órgano Garante.

Para los casos en que las AR´s consideren que la información debe ser entregada en versión pública, observarán lo dispuesto en los *Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas*, testando las partes o secciones clasificadas e indicarán los datos que se testan, precisando el fundamento y motivación en cada caso concreto.

Todas las **respuestas emitidas por la OTAIPDPyA,** invariablemente se notificarán a las personas solicitantes a través del Sistema SISAI 2.0 y por el medio elegido para tal fin.

La OTAIPDPyA dispondrá de 3 días hábiles, contados a partir de la recepción de la solicitud de acceso a la información, **para comunicar que la información solicitada no se encuentra dentro de las atribuciones y/o facultades del Instituto Electoral**, a fin de que proceda a remitir la solicitud al Sujeto Obligado correspondiente y oriente a la persona solicitante.

Para emitir un Oficio de prevención, las AR´s dispondrán de **2 días hábiles**, contados a partir de la recepción del oficio de trámite para remitirlo a la OTAIPDPyA, quien notificará el motivo de la aclaración a la persona solicitante.

Para emitir un Oficio de ampliación, las AR´s dispondrán de un **plazo de 6 días hábiles**, contados a partir de la recepción de la solicitud de información, para informar de manera fundada y motivada a la OTAIPDPyA, las razones para postergar el plazo de atención a la solicitud de acceso a la información, a fin de que lo notifique a la persona solicitante.

La orientación de una solicitud de información pública a los Sujetos Obligados de la Ciudad de México será procedente cuando de su lectura se desprenda que la información requerida no corresponde con las atribuciones y/o facultades del Instituto Electoral, lo cual se hará del conocimiento de la persona solicitante **en el término de 3 días hábiles**, posteriores a la formulación de su solicitud.

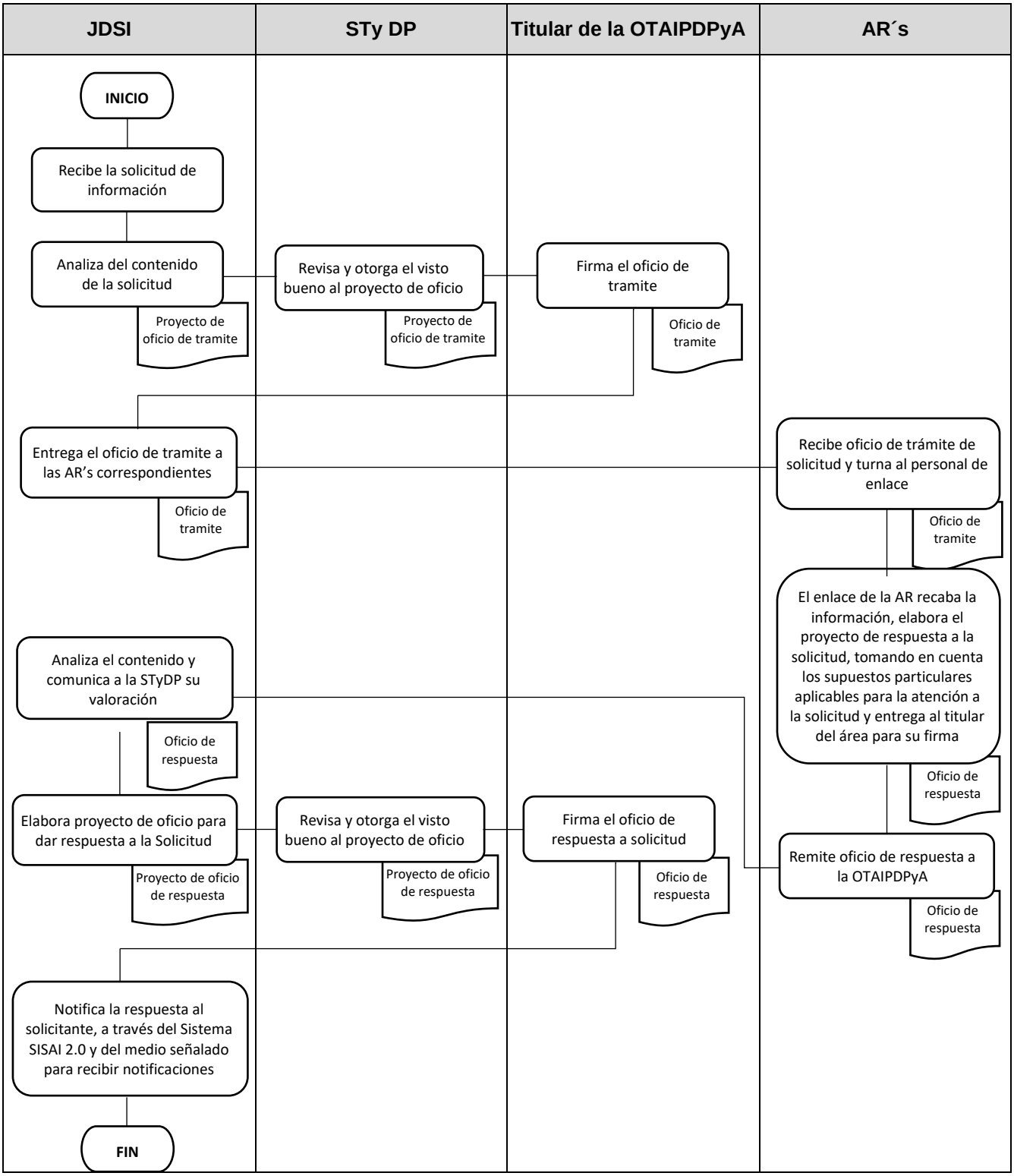
En los casos que la información requerida corresponda parcialmente al Instituto Electoral y a diverso Sujeto Obligado, la respuesta deberá otorgarse en un **término no mayor de 9 días hábiles**, posteriores a su recepción, utilizando para ello el sistema electrónico SISAI 2.0, de conformidad con los Lineamientos para la gestión de solicitudes.

Respecto de las solicitudes de información pública que sean competencia de un **Sujeto Obligado del ámbito Federal**, ante la imposibilidad técnica para canalizarla de manera directa a través del sistema electrónico SISAI 2.0; la OTAIPDPyA, **en el término de 3 días hábiles** contados a partir de la recepción de la solicitud, orientará a la persona solicitante, para que acuda ante la Unidad de Transparencia del Sujeto Obligado responsable de atenderla, proporcionándole los datos del registro de su solicitud.

La OTAIPDPyA no dará trámite a las solicitudes de acceso a la información que sean ofensivas o denostativas para el Instituto Electoral o su personal, así como aquellas que contengan lenguaje soez, y se tendrán por no presentadas, notificándolo a la persona solicitante.

7. Diagrama de flujo

Actividades generales para la atención y respuesta a solicitudes de acceso a la información


JDSI
STy DP
Titular de la OTAIPDPyA
AR´s
INICIO
Recibe la solicitud de información
Analiza del contenido de la solicitud
Proyecto de oficio de tramite
Revisa y otorga el visto bueno al proyecto de oficio
Proyecto de oficio de tramite
Firma el oficio de tramite
Oficio de tramite
Entrega el oficio de tramite a las AR's correspondientes
Oficio de tramite
Recibe oficio de trámite de solicitud y turna al personal de enlace
Oficio de tramite
El enlace de la AR recaba la información, elabora el proyecto de respuesta a la solicitud, tomando en cuenta los supuestos particulares aplicables para la atención a la solicitud y entrega al titular del área para su firma
Oficio de respuesta
Analiza el contenido y comunica a la STyDP su valoración
Oficio de respuesta
Elabora proyecto de oficio para dar respuesta a la Solicitud
Proyecto de oficio de respuesta
Revisa y otorga el visto bueno al proyecto de oficio
Proyecto de oficio de respuesta
Firma el oficio de respuesta a solicitud
Oficio de respuesta
Remite oficio de respuesta a la OTAIPDPyA
Oficio de respuesta
Notifica la respuesta al solicitante, a través del Sistema SISAI 2.0 y del medio señalado para recibir notificaciones
FIN

8. Descripción de las actividades

A. Actividades generales para la atención y respuesta a solicitudes de acceso a la información			
#	**Actividad**	**Área responsable**	**Documento empleado**
A1	Recibe la Solicitud de acceso a la información presentada por escrito, de manera verbal o medio electrónico y la registra en el SISAI 2.0.	**JDSI.**	Solicitud de Acceso a la Información. Registro en sistema electrónico SISAI 2.0.
A2	Analiza el contenido de la solicitud, prepara el proyecto de oficio de trámite para remitirla a las AR´s que generen, obtengan o posean la información solicitada.	**JDSI.**	Proyecto de oficio de trámite acompañado de la Solicitud de Acceso a la Información.
A3	Revisa y, en su caso, otorga el Visto bueno al proyecto de oficio de trámite para turnar la Solicitud de Acceso a la Información a las AR´s.	**ST y DP.**	Proyecto de Oficio de trámite.
A4	Firma el oficio de trámite y lo devuelve a la JDSI para su entrega al AR correspondiente.	**Titular de la OTAIPDPyA.**	Oficio de trámite.
A5	Entrega el oficio de trámite a las AR´s correspondientes, el mismo día que se recibe la Solicitud de Acceso a la Información Pública.	**JDSI.**	Oficio de trámite.
A6	Recibe oficio de trámite de solicitud y turna al personal de enlace para atender la Solicitud de Acceso a la Información. Pública.	**AR´s.**	Oficio de trámite, Solicitud de Acceso a la Información.
A7	Recaba la información, elabora proyecto de respuesta a la solicitud de acceso a la información y entrega a la persona Titular del área para firma.	**Enlace de AR´s.**	Proyecto de oficio de respuesta; en su caso, anexos.
A8	Remite a la OTAIPDPyA el oficio de respuesta a la Solicitud de acceso a la información, en el término de 6 días hábiles, contados a partir de la fecha de su recepción.	**AR´s.**	Oficio de respuesta; en su caso, anexos.
A9	Recibe el oficio de respuesta de las AR´s, analiza el contenido, verifica que sean atendidos todos los puntos requeridos y comunica a la STyDP su valoración.	**JDSI.**	Oficio de respuesta a la solicitud de acceso a la información.

A10	Elabora proyecto de oficio para dar respuesta a la Solicitud de Acceso a la Información y lo remite para Vo.Bo.de la STy DP.	**JDSI.**	Proyecto de oficio de respuesta.
A11	Revisa la respuesta a la solicitud de información formulada por las AR´s, así como el proyecto de oficio, en su caso, otorga el visto bueno al proyecto de oficio de respuesta y remite al Titular de la OTAIPDPyA.	**STyDP.**	Proyecto de Oficio de respuesta.
A12	Firma el oficio de respuesta y devuelve a la JDSI, para continuar con el trámite.	**Titular de la** OTAIPDPyA.	Oficio de respuesta.
A13	Notifica la respuesta a la persona solicitante, a través del sistema electrónico SISAI 2.0 y por el medio señalado para recibir notificaciones.	**JDSI.**	Notificación.
Fin de las actividades generales para la atención y respuesta a solicitudes de acceso a la información pública			

.

B. Atención a solicitudes de acceso a información pública de oficio			
#	**Actividad**	**Área responsable**	**Documento empleado**
B1	Recibe la Solicitud de información presentada por escrito, de manera verbal o medio electrónico y la registra en el Sistema Electrónico SISAI 2.0.	**JDSI.**	Solicitud de Acceso a la Información. Registro en el sistema SISAI 2.0.
B2	Analiza el contenido de la Solicitud; determina que la información corresponde a las Obligaciones de Transparencia (información pública de oficio) publicadas en la página de Internet, y comunica a la STy DP	**JDSI.**	Solicitud de Acceso a la Información.
B3	Verifica que la información solicitada corresponda a las Obligaciones de Transparencia publicadas en la página de Internet.	**STy DP.**	Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México; Sección de transparencia del sitio Institucional de Internet del IECM.

B4	Elabora el proyecto de oficio para dar respuesta a la Solicitud de Acceso a la Información, la cual deberá emitirse en un plazo no mayor a 4 días posteriores a la presentación de la solicitud.	**JDSI.**	Proyecto de oficio de respuesta.
B5	Revisa y, en su caso, otorga el visto bueno al proyecto de oficio de respuesta.	**STy DP.**	Proyecto de oficio de respuesta.
B6	Firma el oficio de respuesta y devuelve al Departamento de Solicitudes de Información para continuar con el trámite.	**Titular de la OTAIPDPyA.**	Oficio de respuesta.
B7	Notifica la respuesta a través del Sistema electrónico SISAI 2.0 y del medio señalado por la persona solicitante para recibir notificaciones.	**JDSI.**	Notificación.
Fin de la actividad de atención a una solicitud de acceso a la información pública de oficio.			

C. Actividades para la atención y respuesta a solicitudes de acceso a la información cuando se realiza prevención al solicitante			
#	**Actividad**	**Área responsable**	**Documento empleado**
C1	Procede de la Actividad **A6**.	**JDSI, STyDP, Titular de la OTAIPDPyA, Enlace de AR.**	Solicitud de Acceso a la Información, registro en sistema electrónico SISAI 2.0, proyecto de oficio de trámite acompañado de la solicitud de acceso a la información.
C2	Revisa si la solicitud de información pública es clara. ¿La solicitud de información es clara? **No** Continúa en la actividad **C3.** **Sí** Continúa conforme a las actividades **A7** al **B7**.	**Enlace de AR´s.**	Solicitud de Acceso a la Información

C3	Elabora, proyecto de oficio en el que informa a la OTAIPDPyA, en un término de 2 días hábiles posteriores a la recepción de la solicitud de información, que no es clara ni precisa, a fin de la que persona solicitante sea prevenida.	**Enlace de AR´s.**	Proyecto de oficio de prevención.
C4	Firma el oficio de prevención y solicita se entregue a la Unidad de Transparencia.	**Titular de las AR´s.**	Oficio de prevención.
C5	Recibe oficio de las AR´s, en el que señalan que la solicitud no es clara ni precisa.	**JDSI.**	Oficio de prevención.
C6	Elabora proyecto de oficio de prevención dirigido a la persona solicitante y lo remite a la STyDP para su revisión y validación.	**JDSI.**	Proyecto de Oficio de prevención a la persona solicitante.
C7	Revisa y en su caso, emite el visto bueno al proyecto de oficio de prevención para la persona solicitante.	**STyDP.**	Proyecto de Oficio de prevención.
C8	Firma oficio de prevención y devuelve a la JDSI para su envío.	**Titular de la OTAIPDPyA.**	Oficio de prevención.
C9	Notifica a la persona solicitante la prevención a través del Sistema electrónico SISAI 2.0 y por el medio de notificación señalado. ¿La persona solicitante desahoga la prevención? **No.** Se tiene por no presentada la solicitud de información y realiza la anotación correspondiente en el sistema SISAI 2.0. **Sí.** Continúa en la actividad **C10.**	**JDSI.**	Notificación Constancia de no desahogo de prevención en el sistema electrónico SISAI 2.0.
C10	Elabora proyecto de oficio de trámite dirigido al AR, enviando la solicitud de información **y adjunta la aclaración o precisión** contenida en el desahogo de la prevención presentado por la persona solicitante.	**JDSI.**	Proyecto de Oficio de trámite.
C11	Revisa y, en su caso, otorga el visto bueno al proyecto de oficio con el que se enviará la solicitud de acceso a la información, así como la aclaración o precisión formulada por la persona solicitante.	**STyDP.**	Proyecto de Oficio de trámite de la Solicitud de Acceso a la Información.

C12	Firma el oficio y remite la solicitud de acceso a la información con la aclaración o precisión formulada por la persona solicitante y lo devuelve a la JDSI para su entrega a las AR´s.	**Titular de la OTAIPDPyA**	Oficio de trámite de la Solicitud de Acceso a la Información.
C13	Procede conforme a las actividades descritas en los numerales **A7** al **B7**.	**JDSI, STyDP, AR´s, Titular de la OTAIPDPyA.**	Solicitud de acceso a la información pública, oficio de trámite, oficio de respuesta.
Fin de actividades relacionadas con la Atención a solicitudes de acceso a la Información, cuando se realiza prevención al solicitante.			

D. Atención a solicitudes de acceso a la Información, en los casos en que el IECM cuenta o no con las atribuciones para dar atención a la solicitud de acceso a la información			
#	**Actividad**	**Área responsable**	**Documento empleado**
D1	Procede de la Actividad **A6**.	**JDSI**.	Solicitud de Acceso a la Información, Registro en el sistema electrónico SISAI 2.0.
D2	Analiza si la información solicitada se encuentra o no, dentro de las atribuciones del Instituto Electoral y lo comunica a la STyDP.	**JDSI**.	Solicitud de Acceso a la Información, Reglamento Interior del IECM.
D3	Asesora a la persona solicitante si la información solicitada se encuentra o no, dentro de las atribuciones del Instituto Electoral para atenderla.	**JDSI.**	Registro electrónico SISAI 2.0, Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.
D4	Verifica la información solicitada. ¿La información se encuentra o no, dentro de las atribuciones del Instituto Electoral? **No.** Continúa en la actividad **D9.**	**STyDP.**	Reglamento Interior del IECM, Ley de Transparencia, Acceso a la Información Pública y Rendición de

	Sí. Realizan las actividades atinentes descritas en los apartados **A7** al **B7**.		Cuentas de la Ciudad de México.
D5	Elabora el proyecto de oficio de orientación, fundando y motivando los casos en los no se encuentra dentro de las atribuciones del Instituto Electoral para dar respuesta a una solicitud de información, o en su caso, aquellas que serán remitidas al Sujeto Obligado con las atribuciones para su atención.	**JDSI**.	Proyecto de Oficio de remisión.
D6	Revisa y otorga el visto bueno al proyecto de oficio por el que se remitirá la solicitud de acceso a la información a diverso Sujeto Obligado.	**STyDP.**	Proyecto de Oficio de remisión.
D7	Firma el oficio para remitir la solicitud de información al Sujeto Obligado facultado para atender la solicitud de información y lo devuelve a la JDSI para su envío.	**Titular de la OTAIPDPyA**	Oficio de remisión.
D8	Notifica a través del sistema electrónico SISAI 2.0 y del medio señalado por la persona solicitante para recibir notificaciones, el oficio de remisión al Sujeto Obligado con las atribuciones legales para atender la Solicitud de Acceso a la Información.	**JDSI.**	Notificación.
Fin de la Actividad de orientación de una Solicitud de Acceso a la Información, por no encontrarse dentro de las atribuciones del Instituto para atenderla.			
D9	Determina que el Instituto Electoral cuenta con las atribuciones parciales para conocer y dar respuesta a una Solicitud de Acceso a la Información Pública: Elabora proyecto de oficio dirigido a los titulares de las AR´s del Instituto Electoral que de acuerdo con sus facultades generen, obtengan o posean la información requerida, con la finalidad de que atiendan la solicitud de acceso a la información y en su caso, comunique si es incompetente para atenderla.	**JDSI.**	Proyecto de oficio
D10	El proceso se realiza conforme a las actividades **A7** al **B7**.	**ÁR´S, JDSI, STyDP, Titular de la OTAIPDPyA.**	Oficio de trámite.

Atención de las Solicitudes de Información Pública

Fin de la Actividad de atención a una solicitud de acceso a la información en los casos en que el IECM cuenta de manera parcial o total, con las atribuciones para dar atención a la solicitud.

E. Atención a solicitudes de acceso a la Información, con ampliación de plazo para emitir la respuesta			
#	**Actividad**	**Área responsable**	**Documento empleado**
E1	Procede de la Actividad **A6**.	**AR´S.**	Solicitud de Acceso a la Información pública, Registro en Sistema SISAI 2.0, oficio de trámite.
E2	Analiza si requiere ampliación en el plazo para contestar la solicitud de información. ¿Requiere ampliación de plazo? **No.** Continúa en la actividad **E3**. **Sí.** Continúa en la actividad **E4**.	**AR´s.**	Solicitud de Acceso a la Información pública en trámite.
E3	Realizan las actividades atinentes descritas en los apartados **A7** al **B7**.	**Enlace de AR´s, JDSI, STyDP, Titular de la OTAIPDPyA.**	Solicitud de Acceso a la Información pública en trámite, oficio de respuesta y en su caso los anexos correspondientes.
E4	En un plazo no mayor a 6 días hábiles, elabora proyecto de oficio dirigido a la UT, exponiendo los fundamentos legales y motivos por los cuales, por única vez, pretende la ampliación del plazo para atender la solicitud de acceso a la información pública, y somete a consideración del titular de su área.	**Enlace de AR´s.**	Proyecto de oficio de ampliación de plazo.
E5	Firma oficio de ampliación de plazo, para su posterior remisión a la OTAIPDPyA.	**AR´s.**	Oficio de ampliación de plazo.
E6	Remite a la OTAIPDPyA, el oficio en que requiere la ampliación del plazo para atender la solicitud de acceso a la información.	**AR´s.**	Oficio de solicitud de ampliación de plazo.

E7	Recibe respuesta del AR, por la que se notifica a la persona solicitante la ampliación del plazo para la atención a su solicitud de acceso a la información; lo anterior en un periodo máximo de 5 días hábiles.	**JDSI.**	Proyecto de oficio de ampliación de plazo.
E8	Revisa y, en su caso, emite visto bueno al proyecto de oficio para la ampliación del plazo, por única vez, para dar respuesta a la solicitud de información.	**STyDP.**	Proyecto de Oficio de ampliación de plazo.
E9	Firma oficio y lo devuelve a la JDSI para que notifique a la persona solicitante la ampliación del plazo, hasta 7 días hábiles adicionales, posteriores al vencimiento del término inicial, para atender la solicitud de información.	**Titular de la OTAIPDPyA.**	Oficio de ampliación de plazo.
E10	Notifica a la persona solicitante, a través del medio señalado para recibir notificaciones, sobre la ampliación del plazo para la atención de su solicitud de acceso a la información.	**JDSI**.	Notifica el oficio de ampliación de plazo.
E11	Realizan las actividades descritas en los apartados **A7** al **A13**, una vez concluida la ampliación del plazo.	**Enlace de AR, JDSI, STyDP, Titular de la OTAIPDPyA.**	Solicitud de Acceso a la Información en trámite, oficio de respuesta y en su caso los anexos correspondientes.
E12	**Fin de la actividad de atención a solicitudes de acceso a la Información pública, con ampliación del plazo para emitir la respuesta.**	**JDSI.**	Respuesta a la solicitud.
Fin de la Atención a solicitudes de acceso a la Información, con ampliación de plazo para emitir la respuesta			

F. Atención a solicitudes cuando la Información, se considera clasificada			
#	**Actividad**	**Área responsable**	**Documento empleado**
F1	Procede de la Actividad **A6**.	**JDSI, STyDP, AR,**	Solicitud de Acceso a la Información, Registro en Sistema

		Titular de la OTAIPDPyA.	SISAI 2.0, oficio de trámite.
F2	Comunica, mediante oficio, al Titular de la OTAIPDPyA que: ¿La información es reservada? **Sí.** Continúa en la actividad **F3**. **No.** Continúa en la actividad **F17.**	**AR´s**	Oficio de respuesta y, en su caso, anexos.
F3	Determina que la información solicitada es clasificada en su modalidad de reservada o confidencial.	**AR´s**	Oficio de clasificación.
F4	Elabora y adjunta la prueba de daño, tratándose de información reservada y solicita se convoque al Comité.	**AR´s**	Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, oficio de respuesta.
F5	Señala los datos personales o información confidencial que se pretende tutelar en estricto apego a la legislación aplicable y solicita se convoque al Comité.	**AR´s**	Normatividad en materia de Datos Personales aplicable, y disposiciones complementarias que protejan la información confidencial, oficio de respuesta.
F6	Precisa en cada supuesto, la legislación específica que la protege, o bien, que corresponde a información que previamente ha sido clasificada como confidencial por el Comité.	**JDDPyAJ**	Normatividad en materia de Datos Personales aplicable, y disposiciones complementarias que protejan la información confidencial.

F7	Precisa, en su caso, la fecha y número de Acuerdo del Comité, cuando la información solicitada, haya sido clasificada previamente por el Comité como información confidencial.	**JDDPyAJ**	Normatividad en materia de Datos Personales aplicable, y disposiciones complementarias que protejan la información confidencial.
F8	Refiere el Acuerdo 1072/SO/03-08/2016 del INFO, vigente, así como a las demás disposiciones adoptadas por el Órgano Garante.	**JDDPyAJ**	Normatividad en materia de Datos Personales aplicable, y disposiciones complementarias que protejan la información confidencial.
F9	Elabora, en su caso, Versión Pública, de la documentación conforme a las Políticas de Operación y elabora oficio de respuesta.	**Enlace de AR´S, JDDPyAJ.**	Normatividad en materia de Datos Personales aplicable, y disposiciones complementarias que protejan la información confidencial; versión púbica, de ser el caso.
F10	Analiza la clasificación formulada por las AR's; de resultar procedente, propone a la STyDP se someta el asunto al Comité, en atención a la petición formulada por las AR´s.	**JDDPyAJ.**	Oficio de respuesta y, en su caso, anexos.
F11	Elabora proyecto de oficio de convocatoria al Comité y entrega para revisión a la STyDP, junto con el oficio de respuesta y, en su caso los anexos.	**JDDPyAJ**	Proyecto de convocatoria, Proyecto de Orden del Día, Oficio de respuesta y, en su caso, anexos.
F12	Revisa el proyecto de oficio de convocatoria y entrega a la persona titular de la OTAIPDPyA.	**STyDP.**	Proyecto de convocatoria, Proyecto de Orden del Día, Oficio de

			respuesta y, en su caso los anexos correspondientes.
F13	Propone a la Presidencia del Comité, el proyecto de oficio de convocatoria.	**Titular de la OTAIPDPyA.**	Proyecto de convocatoria, Proyecto de Orden del Día, Oficio de respuesta y, en su caso, anexos.
F14	Firma la convocatoria e insta al Comité para que se reúna en sesión ordinaria o extraordinaria, para analizar y resolver el asunto en cuestión.	**Presidencia del Comité**	Convocatoria al Comité, Orden del Día y documentos de análisis.
F15	Analiza la propuesta de clasificación de la información formulada por las AR´s.	**Integrantes del Comité**	Constancias que integran el expediente, proyecto de versión pública y proyecto de Resolución.
F16	Confirma, revoca o modifica la clasificación de la información propuesta por las AR´s, e instruye a la **OTAIPDPyA** para que notifique a la persona solicitante la resolución emitida.	**Integrantes del Comité**	Resoluciones adoptadas por el Comité Minutas de las sesiones del Comité.
F17	Realiza con las AR´s las observaciones y aclaraciones respecto de la información solicitada, cuando ésta no tiene el carácter de reservada a efecto de remitir la respuesta a la persona solicitante.	**JDSI, JDDPyAJ, AR´S.**	Información solicitada y en su caso, anexos
F18	Elabora y envía la respuesta a la solicitud de información, una vez determinado que la información no es clasificada.	**AR´s**	Oficio de respuesta y anexos.
F19	Elabora proyecto de oficio de respuesta y entrega a la STyDP, para revisión y validación.	**JDSI.**	Proyecto de Oficio de respuesta y anexos de ser el caso.
F20	Revisa y da el Visto Bueno al oficio de respuesta.	**STyDP.**	Oficio de respuesta.

F21	Firma el oficio de respuesta y lo devuelve a la JDSI para continuar con las gestiones correspondientes.	**Titular de la OTAIPDPyA.**	Oficio de respuesta.
F22	Envía por el Sistema electrónico SISAI 2.0 y medio de notificación, la respuesta a la persona solicitante.	**JDSI.**	Respuesta a la solicitud de acceso a la información.
Fin de las actividades para la atención de solicitudes de acceso a la información pública cuando la Información solicitada se clasifica.			

G. Atención a solicitudes de acceso a la Información, cuando se propone declaración de inexistencia de información			
#	**Actividad**	**Área responsable**	**Documento empleado**
G1	Procede de la Actividad **A6**.	**ÁR´S, JDSI, STyDP, Titular de la OTAIPDPyA.**	Solicitud de Acceso a la Información, Registro en sistema electrónico SISAI 2.0, oficio de trámite.
G2	Propone la inexistencia de la información solicitada y comunica a la **OTAIPDPyA**. ¿Es inexistente la información? **No.** Continúa en la actividad **G13**. **Sí.** Continúa en la actividad **G3**.	**AR´s.**	Oficio y anexos, de ser el caso.
G3	Prepara el asunto para someterlo al Comité de Transparencia, con ayuda del personal del área correspondiente.	**JDDPyA.**	Oficio de respuesta y anexos si es el caso.
G4	Elabora oficio de convocatoria al Comité y entrega para revisión a la STyDP, junto con el oficio de respuesta y, en su caso, los anexos.	**JDDPyAJ.**	Proyecto de convocatoria, Oficio de respuesta y anexos, si es el caso.
G5	Revisa el proyecto de oficio de convocatoria y entrega a la persona titular de la OTAIPDPyA	**STyDP.**	Proyecto de Convocatoria, Proyecto de Orden del Día, Oficio de

			respuesta y anexos, de ser el caso.
G6	Propone a la Presidencia del Comité el proyecto de oficio de convocatoria.	**Titular de la OTAIPDPyA.**	Proyecto de convocatoria al Comité: Proyecto de Oficio de convocatoria, Proyecto de Orden del Día, Oficio de respuesta y anexos, de ser el caso.
G7	Firma la convocatoria e insta al Comité para que se reúna en sesión Extraordinaria o Urgente, según sea el caso, para analizar y resolver el asunto.	**Presidencia del Comité**	Convocatoria al Comité: Oficio de convocatoria, Orden del Día.
G8	Analizan propuesta de declaratoria de inexistencia de la información. ¿Confirma la inexistencia de la información? **Sí.** Continúa en la actividad **G9**. **No.** Continúa en la actividad **G10**.	**Integrantes del Comité**	Documentales de la información solicitada.
G9	Emiten el Acuerdo respectivo para su suscripción por parte de la Presidencia y Secretaría del Comité, Titular de las Ar´s que proponen la inexistencia de la información y la persona titular de la Contraloría Interna del Instituto Electoral.	**Integrantes del Comité**	Documentales de la información solicitada. Declaratoria de inexistencia de la información. Minutas generadas en las sesiones del Comité.
G10	Revocan o modifican la propuesta de inexistencia de la información.	**Integrantes del Comité**	Documentales de la información solicitada. Declaratoria de inexistencia de la información.

			Minutas generadas en las sesiones del Comité.
G11	Acuerdan plazos y términos para la entrega de información.	**Integrantes del Comité**	Documentales de la información solicitada. Declaratoria de inexistencia de la información.
G12	Analiza la respuesta por parte del área. ¿Es correcta la respuesta? **Sí.** Continúa con las actividades descritas en los numerales **A10** al **A13.** **No.** Continúa en la actividad **G13.**	**JDSI.**	Oficio de respuesta y anexos.
G13	Acuerda con el personal del AR sobre las discrepancias para remitir la respuesta a la persona solicitante.	**JDSI.**	Oficio de respuesta y anexos.
G14	Continúa con las actividades descritas de la **A10** a la **A13**.	**JDSI, STyDP, Titular de la OTAIPDPyA.**	Solicitud de Acceso a la Información, Registro en sistema Electrónico SISAI 2.0, oficio de respuesta y anexos.
	Fin de las actividades para la atención de solicitudes de acceso a la información pública cuando la información es declarada inexistente por el Comité.		

H. Atención a solicitudes de acceso a la Información, cuyo trámite implica su traducción a una lengua indígena o al castellano			
#	**Actividad**	**Área responsable**	**Documento empleado**
H1	Recibe la Solicitud de información presentada a través de alguno de los instrumentos de gestión, se percata que requiere la intervención de un intérprete en lenguas indígenas para su traducción al castellano, a fin de proceder a su registro en el	**JDSI.**	Solicitud de Acceso a la Información

	sistema electrónico SISAI 2.0, lo comunica a la STyDP.		
H2	Informa a la persona Titular de la OTAIPDPyA.	**STyDP.**	Solicitud de Acceso a la Información.
H3	Instruye a la STyDP realizar las gestiones ante las instancias correspondientes para atender la solicitud de información.	**Titular de la OTAIPDPyA.**	Instrucción de trabajo.
H4	Elabora proyecto de oficio dirigido a la Secretaría de Pueblos y Barrios Originarios y Comunidades Indígenas Residentes (**SEPI**) del Gobierno de la Ciudad de México, para solicitar su colaboración para que en el plazo máximo de 3 días hábiles a partir de la recepción de la misma, se traduzca el documento, a fin de registrar la solicitud en el Sistema SISAI 2.0.	**JDSI.**	Convenio de Colaboración IECM-SEPI, Solicitud de Acceso a la Información.
H5	Firma el oficio y lo devuelve a la JDSI, para que sea presentado a la SEPI.	**Titular de la OTAIPDPyA.**	Oficio, solicitud de Acceso a la Información, Oficio de colaboración.
H6	Devuelve al Instituto Electoral el documento traducido al castellano, en un plazo no mayor a 4 días hábiles.	**SEPI.**	Oficio, Documento traducido.
H7	Registra la solicitud de información de acuerdo a la traducción realizada por la SEPI y la turna a las AR´s..	**JDSI.**	Solicitud de acceso a la información y anexos, traducidos al castellano.
H8	Recaba la información solicitada y elabora el proyecto de oficio para dar respuesta a la solicitud de acceso a la información y lo turna para firma de la/el Titular del AR.	**Enlace de las AR´s.**	Proyecto de oficio de respuesta.
H9	Firma el oficio de respuesta y lo remiten a la OTAIPDPyA, en su caso, con información anexa para dar respuesta a la Solicitud presentada.	**Titular de AR´s.**	Oficio de Respuesta, en su caso, anexos.
H10	Elabora proyecto de oficio de respuesta a la solicitud de acceso a la información pública, así como el proyecto de oficio para solicitar a la SEPI la	**JDSI.**	Proyecto de oficio de respuesta.

	traducción de la respuesta a la lengua indígena correspondiente.		
H11	Revisa y, en su caso, otorga el Visto bueno a los proyectos de oficio y los presenta a la persona Titular de la OTAIPDPyA	**STyDP.**	Oficio de respuesta.
H12	Firma los oficios e instruye al JDSI para que sea presentado a la SEPI, a fin de que realice la traducción a la lengua indígena correspondiente.	**Titular de la OTAIPDPyA**	Oficio de respuesta, Oficio de Colaboración, Oficio de respuesta de las AR´s.
H13	Devuelve al Instituto Electoral el documento traducido en la lengua indígena.	**SEPI.**	Oficio, Documento traducido.
H14	Notifica la respuesta a la persona solicitante a través del Sistema Electrónico SISAI 2.0 y del medio señalado para tal fin.	**JDSI.**	Oficio de respuesta.
Fin de la Actividad de atención a una solicitud de acceso a la información pública cuyo registro se debe hacer en una lengua indígena.			

9. Formatos

9.1.- Formato de Solicitud de Información Pública

9.1.1.-Instructivo de llenado

1. Se anotará el número de folio que corresponda al registro en el sistema SISAI 2.0

2. Se anotará el día de la fecha en que se recibe la solicitud en la Unidad de Transparencia.

3. Se anotará el mes de la fecha en que se recibe la solicitud en la Unidad de Transparencia.

4. Se anotará el año de la fecha en que se recibe la solicitud en la Unidad de Transparencia.

5. Se anotará la hora en que se recibe la solicitud en la Unidad de Transparencia.

6. Se anotará el nombre del Instituto Electoral de la Ciudad de México, por ser el sujeto obligado ante el cual se ejercerá el derecho de acceso a la información.

7. Se anotará el nombre de la o el solicitante que acude a la Unidad de Transparencia.

8. para presentar su solicitud de acceso a la información.

9. Se anotará el apellido paterno de la o el solicitante que acude a la Unidad de Transparencia, para presentar su solicitud de acceso a la información.

10. Se anotará el apellido materno de la o el solicitante que acude a la Unidad de Transparencia, para presentar su solicitud de acceso a la información.

11. Se anotará el nombre, denominación o razón social en caso de que la o el interesado sea una persona moral que acude a la Unidad de Transparencia, a través de su representante para presentar su solicitud de acceso a la información.

12. Se anotará el nombre de la o el representante y/o autorizado/a para recoger la información requerida en nombre de la persona solicitante.

13. Se anotará el nombre del representante legal o mandatario/a para el caso de que la o el solicitante sea una persona moral y se anexará los documentos que lo acrediten

14. Se anotará el nombre de las y los autorizados para oír y recibir notificaciones y documentos relacionados con su solicitud de acceso a la información.

15. Se anotará el lugar o medio por el cual la persona solicitante desea recibir notificaciones, puede seleccionar: correo electrónico, tendrá que anotar una dirección de correo electrónico; acudir a la Unidad de Transparencia; o domicilio, tendrá que anotar la Calle, Número exterior, Número interior, Colonia, Delegación o Municipio, Código Postal, Estado y País. De manera opcional podrá anotar su número telefónico.

16. Se anotará la modalidad en que desea la entrega de la información solicitada, puede seleccionar: Consulta directa, acudiendo a las oficinas de la Unidad de Transparencia, copia simple de los documentos o copia certificada, medio electrónico, CD, disquete.

17. Se anotará de forma clara y precisa la información que solicita.

18. En caso de que la persona solicitante requiera más espacio para hacer su solicitud, podrá anexar un documento especificando el número de hojas.

19. Sólo de manera opcional y para fines estadísticos la persona solicitante anotará: Sexo (Femenino o Masculino), Edad y Nacionalidad.

20. Se anotará de manera opcional la ocupación actual de la persona solicitante: Empresario/a, persona servidora pública, Empleado/a u Obrero/a, Medios de Comunicación, Asociación Política, Organización no Gubernamental, Comerciante, Académico/a o Estudiante u Otro. Y de forma opcional señalará el último grado de estudios de la o el solicitante: Sin estudios, Primaria, Secundaria, Bachillerato, Licenciatura, Maestría o Doctorado.

Contenido

1. Objetivo 2
2. Alcance 2
3. Marco normativo 2
4. Definiciones 3
5. Responsabilidades 5
6. Políticas de operación 7
7. Diagrama de flujo 10
8. Descripción de las actividades 11
9. Formatos 20

Control de Cambios

Revisión	Fecha	Descripción del Cambio
00	09 febrero 2023	Emisión del documento

1. Objetivo

Establecer las directrices para la atención de las Solicitudes para el ejercicio de los derechos de Acceso, Rectificación, Cancelación, Oposición y de portabilidad de Datos Personales (solicitudes de datos personales), formuladas al Instituto Electoral de la Ciudad de México, a través de los diversos instrumentos de gestión, a fin de cumplir con las disposiciones normativas en materia de Datos Personales.

2. Alcance

El presente manual aplica a todas las áreas del Instituto Electoral de la Ciudad de México, que administren datos personales:

- Presidencia;
- Oficinas de Consejeras y Consejeros Electorales;
- Secretaría Ejecutiva;
- Secretaría Administrativa;
- Contraloría Interna;
- Direcciones Ejecutivas;
- Unidades Técnicas y
- Órganos Desconcentrados.

3. Marco normativo

- Constitución Política de los Estados Unidos Mexicanos;
- Constitución Política de la Ciudad de México;
- Código de Instituciones y Procedimientos Electorales de la Ciudad de México;
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Ley General de Archivos;
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;
- Ley de Archivos Local. Ley de Archivos, aplicable en la Ciudad de México;
- Reglamento Interior del Instituto Electoral de la Ciudad de México;
- Reglamento del Instituto Electoral de la Ciudad de México, en materia de Protección de Datos Personales;
- Reglamento de Funcionamiento del Comité de Transparencia del Instituto Electoral de la Ciudad de México;
- Lineamientos para la Gestión de Solicitudes de Información Pública y de Datos Personales en la Ciudad de México, aprobados por el otrora Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal;
- Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;

- Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, aprobados por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales;
- Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales;
- Criterios para regular el bloqueo de la información, verificación y supresión de los Sistemas de Datos Personales del Instituto Electoral, y
- Aviso por el que se da a conocer de manera íntegra el Acuerdo mediante el cual se aprueba el Criterio que deberán aplicar los Sujetos Obligados, respecto a la clasificación de información en la modalidad de confidencial, Acuerdo del INFO Número 1072/SO/03-08/2016 aprobado por el Pleno del INFODF el 3 de agosto de 2016, y publicado en la Gaceta Oficial de la Ciudad de México el 15 de agosto de 2016.

4. Definiciones

AR´s: Cada una de las áreas administrativas del Instituto Electoral de la Ciudad de México que administren bases de datos o sistemas de datos personales, en términos de la legislación aplicable.

Constancia de acreditación de identidad: Documento a través del cual la Unidad de Transparencia hace constar que el titular de los datos personales ha acreditado su identidad a través de documento oficial original y vigente.

Comité: Comité de Transparencia del Instituto Electoral de la Ciudad de México.

Declaratoria de inexistencia de datos personales: Determinación del Comité por el cual se hace constar que los datos personales no obran en los archivos, registros, expedientes, base de datos o sistemas de datos personales del Instituto Electoral.

Derechos ARCO: Derechos de Acceso, Rectificación, Cancelación, Oposición y portabilidad de Datos Personales.

Enlace: Persona designada en cada AR´s para la gestión de solicitudes de datos personales.

Instituto Electoral: Instituto Electoral de la Ciudad de México.

Instrumentos de gestión: Son los medios a través de los cuales, las personas formulan solicitudes de datos personales de manera: a) Verbal, por comparecencia o vía telefónica; b) Escrita, mediante escrito libre, formato, correo electrónico, correo postal o telégrafo; c) PNT.

JDDPyAJ: Jefatura de Departamento Datos Personales y Apoyo Jurídico, adscrita a la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo.

JDSI: Jefatura de Departamento de Solicitudes de Información, adscrito a la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo.

Ley de Datos: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Lineamientos Generales de Datos: Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

OTAIPDPyA: Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral de la Ciudad de México, a la cual también se le denominará indistintamente como Unidad de Transparencia.

Oficio de ampliación: Documento a través del cual se hace del conocimiento de la persona titular, que el término de respuesta a su solicitud de datos personales, será prorrogado hasta por 15 días hábiles más.

Oficio de colaboración: Documento mediante el cual el Instituto Electoral, solicita a la Secretaría de Pueblos y Barrios Originarios y Comunidades Indígenas Residentes (SEPI) su apoyo para la traducción de una Solicitud de datos personales; así como cualquier oficio de notificación de trámite o respuesta a la misma.

Oficio de notificación de procedencia: Documento a través del cual se hace del conocimiento de la persona titular de manera fundada y motivada, que es procedente el ejercicio del derecho solicitado.

Oficio de orientación por incompetencia: Documento a través del cual, dentro de los 3 días siguientes a la presentación de la solicitud; de manera fundada y motivada, se hace del conocimiento de la persona titular, que el Instituto Electoral no es competente para atender la solicitud de datos personales, y que se orientará al sujeto obligado competente.

Oficio de prevención: Documento con el cual se requiere a la persona titular, para que dentro del término de 5 días hábiles aclare o precise algún aspecto de su solicitud, por ejemplo: información solicitada; periodo de la información; datos de identificación de la información (de ser necesario), domicilio o medio señalado para recibir notificaciones; aclaración respecto del derecho ARCO o al derecho de portabilidad que desea ejercer; lo anterior, para estar en posibilidad de atender su solicitud.

Oficio de reconducción: Documento por el cual, dentro de los tres días hábiles siguientes a la presentación de la solicitud, comunica a la persona titular que, considerando el contenido de la misma, no corresponde al ejercicio de los derechos ARCO o al derecho de portabilidad, por lo que se reconducirá a la vía correcta; sin menoscabo de cumplir los requisitos, y plazos establecidos en la normativa aplicable.

Oficio de respuesta: Documento a través del cual las AR's comunican a la Unidad de Transparencia la respuesta a la solicitud de datos personales para que sea notificada a la o el titular.

Oficio de trámite: Documento mediante el cual la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo pide a las AR's atiendan la solicitud de datos personales.

PNT: Plataforma Nacional de Transparencia

Portabilidad de datos personales: Prerrogativa de la persona titular para obtener del Instituto Electoral una copia de los datos personales objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado, que le permita seguir utilizándolos.

Registro electrónico: Archivo generado con motivo de las solicitudes de derechos ARCO promovidas, en el cual se describen los elementos básicos de identificación, así como el trámite otorgado a cada una.

Sistema de solicitudes de acceso a la información de la Plataforma Nacional de Transparencia. (SISAI 2.0): Es el medio electrónico a través del cual las personas podrán presentar sus solicitudes de acceso a la información pública, considerándose el único medio para el registro, captura y seguimiento de todas las solicitudes formuladas a los Sujetos Obligados, independientemente del instrumento de gestión utilizado (Verbal, por comparecencia o vía telefónica; Escrito, mediante formato, correo electrónico, correo postal o telégrafo; Sistema Electrónico habilitado para tal efecto); asimismo, para la interposición de los recursos de revisión, se llevará a cabo a través de la Plataforma Nacional de Transparencia

Solicitud ARCO: Solicitudes de Acceso, Rectificación, Cancelación u Oposición de Datos Personales (solicitudes de datos personales), formuladas al Instituto Electoral. También denominada solicitud de datos personales.

STyDP: Subdirección de Transparencia y Datos Personales, adscrita a la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral.

Titular: Persona física a quien corresponden los datos personales.

Titular de la Oficina: Titular de la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral, también denominada Unidad de Transparencia.

Unidad de Transparencia: Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral.

UTAJ: Unidad Técnica de Asuntos Jurídicos del Instituto Electoral.

5. Responsabilidades

OTAIPDPyA	• Recibir, tramitar y registrar las solicitudes de datos personales a través del SISAI 2.0, así como turnarlas mediante oficio de trámite y sistema electrónico a las AR´s, que de acuerdo con sus atribuciones y/o facultades, competencias o funciones puedan o deban poseer los datos personales sobre los que versen las solicitudes, dentro de las 24 horas posteriores a su recepción. • Notificar a la persona titular respecto de la procedencia de su solicitud de datos personales, así como, requerir la acreditación de la personalidad de la persona titular o su Representante, una vez que haya recibido la respuesta a la solicitud por parte de las AR´s, a través del SISAI 2.0, y del medio que para tal efecto se señale (correo electrónico, domicilio o el SISAI 2.0). • Entregar la respuesta a la solicitud de datos personales a la persona titular o su Representante, en un **término máximo de 15 días hábiles**, a partir de su recepción, directamente en la Unidad de Transparencia, o bien, en el medio que para tal efecto señalen en la solicitud de datos personales (domicilio o correo electrónico). • Notificar a los integrantes e invitados del Comité, la convocatoria y documentos que al efecto ordene la Presidencia de dicho órgano colegiado. • Asesorar y orientar a las AR´s del Instituto Electoral en materia de protección de datos personales y archivos, para la atención de las solicitudes de datos personales. • Determinar si los datos personales respecto de los cuales se desea ejercer alguno de los derechos ARCO y el derecho de portabilidad se encuentra, dentro de las atribuciones del Instituto Electoral, para la subsecuente atención de la misma.
AR´s	• Atender las solicitudes de datos personales **en el término de 9 días hábiles**, contados a partir de la fecha en que reciban la solicitud. • Requerir a la Unidad de Transparencia, para que **en el término de 3 días hábiles** contados a partir de la fecha en que reciban la solicitud, prevenga a la persona titular de los datos personales, a fin de que aclare algún aspecto de su petición. • Solicitar a la Unidad de Transparencia, **en el término de 9 días hábiles** contados a partir de la fecha en que reciban la solicitud, que notifique a la o el

titular, la ampliación del término para dar respuesta a la solicitud de datos personales.

- Serán las responsables de declarar la inexistencia de los datos personales, al momento de emitir respuesta a la solicitud, lo anterior de conformidad con los archivos, registros, expedientes, base de datos o sistemas de datos personales que generen, obtengan o posean en términos de la legislación aplicable.

6. Políticas de operación

La JDSI, a partir de la recepción de la solicitud de datos personales por cualquiera de los instrumentos de gestión, realizará de manera inmediata, la captura de los datos de identificación de la solicitud en el SISAI 2.0.

En caso de que la solicitud para el ejercicio de los derechos ARCO se presente directamente ante una AR´s distinta a la Unidad de Transparencia, ésta deberá remitirla a la Unidad de Transparencia **dentro de las 24 horas** siguientes de su presentación.

Con relación a los Órganos Desconcentrados, en materia de solicitudes ARCO, por excepción, la OTAIPDPyA, será la encargada de turnar directamente las solicitudes de datos que sean de su competencia o se encuentren dentro de las facultades de las oficinas de las Direcciones Distritales.

En este sentido, las respuestas de las Direcciones Distritales a las solicitudes ARCO deberán ser remitidas, mediante oficio a la Secretaría Ejecutiva con atención a la Dirección de Apoyo a Órganos Desconcentrados y con copia de conocimiento a la OTAIPDPyA.

Para dar trámite a las solicitudes de datos personales, invariablemente deberá contar con la acreditación de identidad de la persona titular o, en su caso, de su representante, el cual deberá acreditar su identidad mediante documento oficial, y quedará constancia en los archivos de la OTAIPDPyA.

Para el caso del ejercicio de los derechos ARCO de menores de edad será a través del padre, madre o tutor y en el caso de personas que se encuentren en estado de interdicción o incapacidad declarada por Ley o por autoridad judicial, se estará a las reglas de representación dispuestas en el Código Civil para el Distrito Federal y demás disposiciones que resulten aplicables en la materia, privilegiando en todo momento el interés superior del menor.

Tratándose de datos personales concernientes a personas fallecidas, podrá ejercer los derechos ARCO, la persona que acredite tener un interés jurídico o legítimo, el heredero o el albacea de la persona fallecida, de conformidad con las leyes aplicables, o bien cuando exista un mandamiento judicial para dicho efecto.

Para acreditar la identidad para el ejercicio de los derechos ARCO, ya sea por la persona Titular, su Representante, o en caso de menores de edad o personas fallecidas, la Unidad de

Transparencia deberá atender a lo dispuesto en los artículos del 72 a 78 de los Lineamientos Generales de Datos.

En la respuesta a las solicitudes para el ejercicio de los derechos ARCO, se deberán señalar los costos de reproducción, plazos y procedimiento para realizar el pago, en su caso las constancias que acrediten el efectivo ejercicio de los derechos ARCO, así como el derecho que asiste al solicitante para interponer recurso de revisión ante el órgano garante.

Los costos de reproducción de la información relacionada con el ejercicio de derechos ARCO, será gratuita hasta 60 hojas; en su caso, se exceptuará el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas de la persona titular, siempre que así lo manifieste en la solicitud de datos personales.

Para emitir un Oficio de prevención, las AR´s dispondrán de **3 días hábiles** contados a partir de la recepción del oficio de trámite, a fin de que la **OTAIPDPyA**, notifique a la persona titular el motivo de la aclaración.

Para emitir un Oficio de ampliación, las AR´s dispondrán de un **plazo máximo de 9 días hábiles** contados a partir de la recepción de la solicitud ARCO, para informar de manera fundada y motivada a la **OTAIPDPyA**, las razones para postergar el plazo de atención a la solicitud, a fin de que lo notifique a la persona titular.

La orientación de una solicitud ARCO a los Sujetos Obligados de la Ciudad de México será procedente cuando de su lectura se desprenda que el ejercicio de los derechos ARCO no corresponde a las atribuciones y/o facultades del Instituto Electoral, lo cual se hará del conocimiento de la persona titular de los datos **en el término de 3 días hábiles**, posteriores a la formulación de su solicitud.

En los casos en que el ejercicio de los derechos ARCO corresponda parcialmente al Instituto Electoral y a diverso Sujeto Obligado, la respuesta deberá otorgarse en un **término máximo de 15 días hábiles**, posteriores a su recepción, utilizando el SISAI 2.0, de conformidad con los *Lineamientos para la Gestión de Solicitudes de Información Pública y de Datos Personales.*

Respecto del ejercicio de los derechos ARCO que sean competencia de un **Sujeto Obligado del ámbito Federal**, ante la imposibilidad técnica para canalizarla de manera directa a través del SISAI 2.0; la OTAIPDPyA, **en el término de 3 días hábiles** contados a partir de la recepción de la solicitud ARCO, orientará a la persona solicitante, para que acuda ante la Unidad de Transparencia del Sujeto Obligado responsable de atenderla.

Todas las respuestas relacionadas con el ejercicio de los derechos ARCO**,** invariablemente deberán ser notificadas a la persona titular de los datos personales, previa acreditación de su identidad, dentro del **plazo de 15 días hábiles,** contados a partir de la recepción de la solicitud que para tal efecto se reciba en la **Unidad de Transparencia**.

Las solicitudes de **acceso a datos personales** se tendrán por cumplidas cuando, previa acreditación de su identidad, se ponga a disposición de la persona titular los datos personales solicitados, a través de consulta directa en el sitio en donde se encuentren; mediante la expedición de copias simples o certificadas o medio electrónico que determine la persona titular.

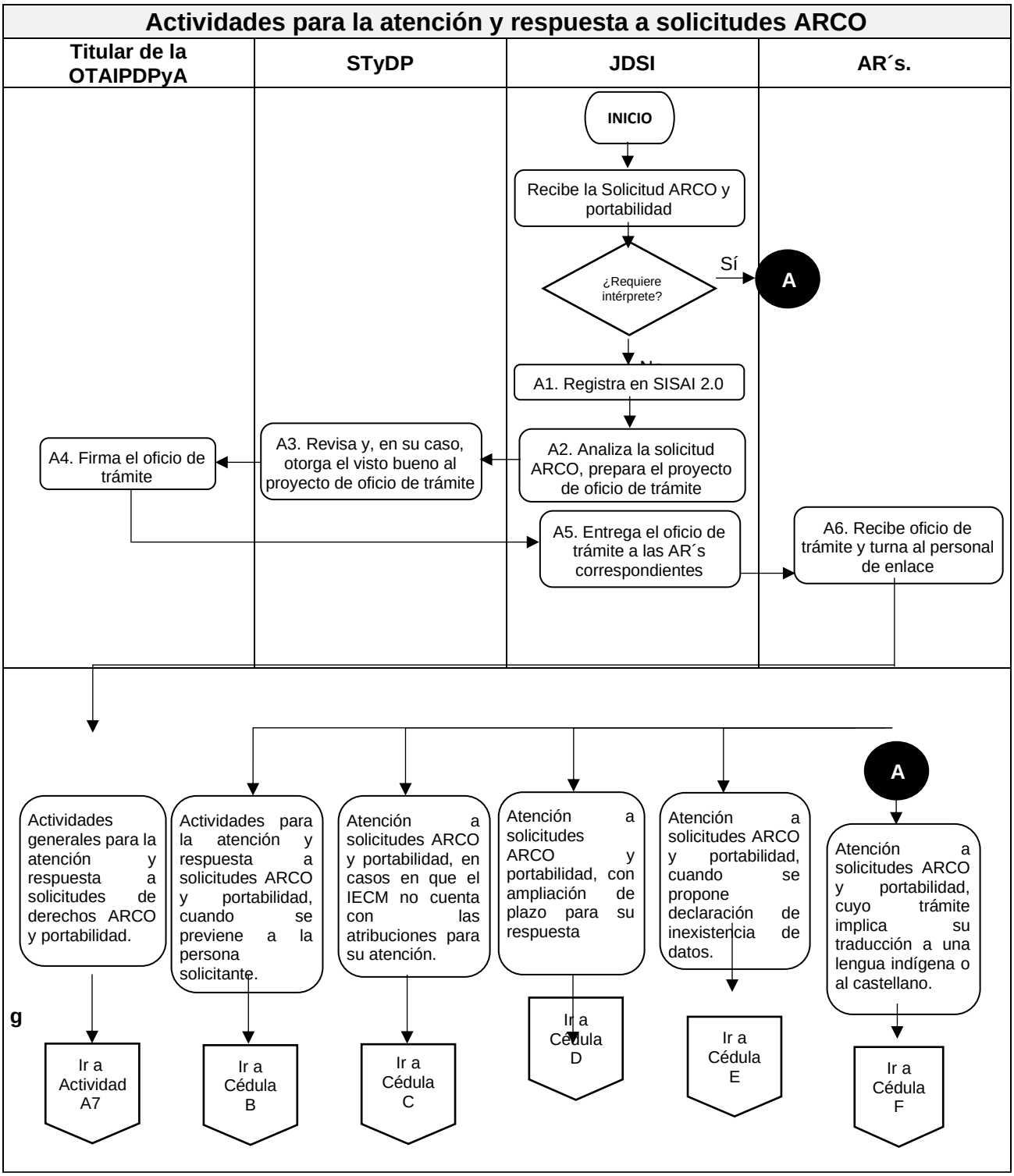
Para el caso de las solicitudes de **rectificación de datos personales** se darán por cumplidas cuando, previa acreditación de su identidad, se notifique a la persona titular de los datos, el documento en el que consten los datos personales rectificados y la fecha a partir de la cual fueron rectificados en los registros de los archivos, expedientes, sistemas de información, bases de datos y sistemas de datos personales**.**

Las solicitudes de **cancelación de datos personales** se darán por cumplidas, cuando previa acreditación de su identidad, se notifique a la persona titular de los datos personales, la constancia en la que se indique los documentos, archivos, expedientes y/o sistemas donde se encuentren los datos personales objeto de la cancelación, el periodo de bloqueo, las medidas de seguridad durante el bloqueo y las políticas o métodos para la supresión definitiva de los datos personales**.**

Al respecto, el responsable del sistema de datos personales que inicie la cancelación de los datos personales solicitados por la persona titular de los mismos, deberá observar los Criterios respectivos.

Para el caso de las solicitudes de **oposición de datos personales,** se dará por cumplida cuando, previa acreditación de su identidad, se notifique a la persona titular de los datos personales, la constancia del Instituto Electoral de cesar el tratamiento de los datos personales**.**

7. Diagrama de flujo



8. Descripción de las actividades

A. Actividades generales para la atención y respuesta a solicitudes ARCO			
#	Actividad	Área responsable	Documento empleado
A1	Recibe la solicitud ARCO presentada por escrito, de manera verbal o medio electrónico y la registra en el **SISAI 2.0**.	**JDSI.**	Solicitud ARCO. Registro en **SISAI 2.0**.
A2	Analiza el contenido de la solicitud ARCO, prepara el proyecto de oficio de trámite para remitirla a las AR´s que **administren** los datos personales solicitados.	**JDSI.**	Proyecto de oficio de trámite acompañado de la Solicitud ARCO.
A3	Revisa y, en su caso, otorga el Visto bueno al proyecto de oficio de trámite para turnar la solicitud ARCO a las AR´s.	**STyDP.**	Proyecto de Oficio de trámite.
A4	Firma el oficio de trámite y devuelve a la **JDSI** para su entrega al AR´s correspondiente.	**Titular de la OTAIPDPyA.**	Oficio de trámite.
A5	Entrega el oficio de trámite a las AR´s correspondientes, el mismo día que se recibe la solicitud ARCO.	**JDSI.**	Oficio de trámite. Solicitud ARCO
A6	Recibe oficio de trámite y turna al personal de enlace para atender la solicitud ARCO.	**AR´s.**	Oficio de trámite, Solicitud ARCO.
A7	Elabora proyecto de oficio de procedencia respecto de la solicitud ARCO y entrega a la persona Titular del área para firma.	**Enlace de AR´s.**	Proyecto de oficio de procedencia.
A8	Remite a la **OTAIPDPyA** en el término de 9 días hábiles contados a partir de la fecha de recepción el oficio de procedencia de la solicitud ARCO.	**AR´s.**	Oficio de procedencia.
A9	Recibe el oficio de procedencia de las AR´s, analiza el contenido, y comunica a la **STyDP** su valoración.	**JDSI.**	Oficio de procedencia para el ejercicio de derechos ARCO.
A10	Elabora proyecto de oficio de respuesta mediante el cual comunica a la **persona** titular de los datos personales, la procedencia a su solicitud ARCO y lo remite a la **STyDP** para Vo.Bo.	**JDSI.**	Proyecto de oficio de respuesta.

A11	Revisa el oficio de procedencia de la solicitud ARCO formulada por las AR´s, así como el proyecto de oficio de respuesta, en su caso, otorga el visto bueno al proyecto de oficio de respuesta y remite al Titular de la **OTAIPDPyA**.	**STyDP.**	Proyecto de Oficio de respuesta.
A12	Firma el oficio de respuesta y devuelve a la **JDSI**, para continuar con el trámite.	**Titular de la OTAIPDPyA.**	Oficio de respuesta.
A13	Notifica la respuesta de procedencia al ejercicio de los derechos ARCO a la **persona** Titular, a través del **SISAI 2.0** y por el medio señalado para recibir notificaciones.	**JDSI.**	Notificación.
Fin de las actividades generales para la atención y respuesta a solicitudes ARCO.			

B. Actividades para la atención y respuesta a solicitudes ARCO, cuando se previene a la persona solicitante			
#	**Actividad**	**Área responsable**	**Documento empleado**
B1	Procede de la Actividad **A6**.	**JDSI, STyDP, Titular de la OTAIPDPyA, Enlace de AR.**	Documentación empleada en numerales 1 al 6 del apartado A
B2	Revisa si la solicitud ARCO es clara. ¿La solicitud ARCO es clara? **No** Continúa en la actividad **B3** **Sí** Continúa conforme a las actividades **A7** a **A13.**	**Enlace de AR´s.**	Solicitud ARCO
B3	Elabora en el término de 3 días hábiles posteriores a la recepción de la solicitud ARCO, proyecto de oficio en el que informa a la **OTAIPDPyA** que la solicitud no es clara o precisa, o bien, que no cumple los requisitos de procedencia establecidos por el artículo 50 de la Ley de Datos, a fin de prevenir a la persona solicitante.	**Enlace de AR´s.**	Proyecto de oficio de prevención.
B4	Firma el oficio de prevención y solicita se entregue a la **Unidad de Transparencia**.	**Titular de las AR´s.**	Oficio de prevención.
B5	Recibe oficio de las AR´s, en el que señalan que la solicitud no es clara o precisa o bien que no cumple con los requisitos de procedencia establecidos en la Ley de Datos.	**JDSI.**	Oficio de prevención.

B6	Elabora proyecto de oficio de prevención dirigido a la persona solicitante y lo remite a la **STyDP** para revisión y en su caso, validación.	**JDSI.**	Proyecto de Oficio de prevención a la persona solicitante.
B7	Revisa y en su caso, emite el visto bueno al proyecto de oficio de prevención para la persona solicitante.	**STyDP.**	Proyecto de Oficio de prevención.
B8	Firma oficio de prevención y devuelve a la **JDSI** para su notificación.	**Titular de la OTAIPDPyA.**	Oficio de prevención.
B9	Notifica a la persona solicitante la prevención a través del **SISAI 2.0** y por el medio de notificación señalado. ¿La persona solicitante desahoga la prevención? **No.** Se tiene por no presentada la solicitud ARCO. **Sí.** Continúa en la actividad **B10**.	**JDSI**.	Notificación Constancia de que la persona solicitante no desahogó la prevención en el **SISAI 2.0**.
B10	Elabora proyecto de oficio de trámite dirigido a las AR´s, enviando la solicitud ARCO y **adjunta la aclaración o precisión** formulada por la persona solicitante en desahogo de la prevención.	**JDSI**.	Proyecto de Oficio de trámite.
B11	Revisa y, en su caso, otorga el visto bueno al proyecto de oficio con el que se enviará la aclaración o precisión formulada por la persona solicitante a la solicitud ARCO.	**STyDP.**	Proyecto de Oficio de trámite de la solicitud ARCO.
B12	Firma el oficio y remite la aclaración o precisión formulada por la persona solicitante y devuelve a la **JDSI** para su entrega a las AR´s.	**Titular de la OTAIPDPyA.**	Oficio de trámite de la solicitud ARCO.
B13	Procede conforme a las actividades descritas en los numerales **A7** a **A13**.	**JDSI, STyDP, AR´s, Titular de la OTAIPDPyA.**	Solicitud ARCO, oficio de trámite, oficio de respuesta.
Fin de actividades relacionadas para la Atención de solicitudes ARCO, cuando se previene a la persona solicitante.			

C. Atención a solicitudes ARCO, en casos en que el IECM no cuenta con las atribuciones.			
#	**Actividad**	**Área responsable**	**Documento empleado**
C1	Procede de la Actividad **A6**.	**JDSI**.	Documentación empleada en numerales 1 al 6 del apartado A
C2	Analiza si los datos personales corresponden a las atribuciones del Instituto Electoral y lo comunica a la ST.	**JDSI**..	Solicitud ARCO, Reglamento Interior del Instituto Electoral
C3	Asesora a la persona solicitante, sobre las atribuciones, del Instituto Electoral para atender la solicitud ARCO.	**JDSI..**	Registro **SISAI 2.0**, Ley de Datos Personales y Lineamientos Generales de Datos.
C4	Verifica el ejercicio de los derechos ARCO solicitados. ¿Los datos personales sobre los que se desea ejercer alguno de los derechos ARCO se encuentra o no, dentro de las atribuciones del Instituto Electoral? **No.** Continúa en la actividad **C5.** **Sí.** Continúa conforme a las actividades **A7** a **A13.**	**STyDP.**	Reglamento Interior del Instituto Electoral, Ley de Datos Personales y Lineamientos Generales de Datos.
C5	Elabora el proyecto de oficio de orientación, fundando y exponiendo las razones por las cuales no está dentro de las atribuciones del Instituto Electoral el atender la solicitud ARCO, y proporciona los datos del sujeto obligado que puede ser competente.	**JDSI**..	Proyecto de Oficio de orientación.
C6	Revisa y otorga el visto bueno al proyecto de oficio de orientación.	**STyDP.**	Proyecto de Oficio de orientación.
C7	Firma el oficio de orientación y lo devuelve a la **JDSI** para su notificación.	**Titular de la OTAIPDPyA.**	Oficio de orientación.
C8	Notifica a través del **SISAI 2.0** y del medio señalado por la persona solicitante para recibir notificaciones, el oficio de orientación y comunica el nombre del Sujeto Obligado con atribuciones para atender la solicitud ARCO.	**JDSI**.	Notificación.
Fin de la Actividad en casos en que el IECM no cuenta con las atribuciones.			

C9	Determina que el Instituto Electoral cuenta con las atribuciones parciales para conocer y dar respuesta a una solicitud ARCO: Elabora proyecto de oficio dirigido a los titulares de las AR´s del Instituto Electoral que de acuerdo con sus facultades obtengan, posean o administren los datos personales solicitados, con la finalidad de que atiendan la solicitud ARCO y en su caso, comunique si es incompetente para atenderla.	**JDSI**.	Proyecto de oficio
C10	El proceso se realiza conforme a las actividades A7 a la A13.	**ÁR´S, JDSI, STyDP, Titular de la OTAIPDPyA.**	Oficio de trámite.
Fin de la Actividad de atención a una solicitud ARCO en casos en que el IECM cuenta con atribuciones para dar atención parcial a la solicitud.			

D. Atención a solicitudes ARCO, con ampliación de plazo para su respuesta			
#	**Actividad**	**Área responsable**	**Documento empleado**
D1	Procede de la Actividad **A6**.	**AR´S.**	Documentación empleada en numerales 1 al 6 del apartado A
D2	Analiza si requiere ampliación en el plazo para atender el ejercicio de derechos ARCO. ¿Requiere ampliación de plazo? **No.** Continúa en la actividad D3. **Sí.** Continúa en la actividad D4.	**AR´s.**	Solicitud ARCO en trámite.
D3	Realizan las actividades descritas en los apartados A7 a A13.	**Enlace de AR´s, JDSI, STyDP, Titular de la OTAIPDPyA.**	Solicitud ARCO en trámite, y en su caso oficio de respuesta
D4	En un plazo máximo de 9 días hábiles, elabora proyecto de oficio dirigido a la **Unidad de Transparencia**, exponiendo los fundamentos legales y motivos por los cuales, por única vez, se pretende la ampliación del plazo para atender la solicitud ARCO, y somete a consideración del titular de su área.	**Enlace de AR´s.**	Proyecto de oficio de ampliación de plazo.

D5	En su caso, emite el visto bueno y firma oficio de ampliación de plazo, para su inmediata remisión a la OAIPyPDP.	**AR´s.**	Oficio de ampliación de plazo.
D6	Remite a la **OTAIPDPyA**, el oficio en que requiere la ampliación del plazo para atender la solicitud ARCO.	**AR´s.**	Oficio de solicitud de ampliación de plazo.
D7	Recibe dentro del plazo de 9 días hábiles, respuesta de las AR's, para que se notifique a la persona solicitante la ampliación del plazo para la atención a su solicitud ARCO.	**JDSI..**	Proyecto de oficio de ampliación de plazo.
D8	Revisa y, en su caso, emite visto bueno al proyecto de oficio para la ampliación del plazo, por única vez, para dar respuesta a la solicitud ARCO.	**STyDP.**	Proyecto de Oficio de ampliación de plazo.
D9	Firma oficio y lo devuelve a la **JDSI** para que notifique a la persona solicitante la ampliación del plazo, por única vez, hasta por 15 días hábiles adicionales; posteriores al vencimiento del término inicial, para atender la solicitud ARCO.	**Titular de la OTAIPDPyA.**	Oficio de ampliación de plazo.
D10	Notifica a la persona solicitante, a través del **SISAI 2.0** y del medio señalado para recibir notificaciones, la ampliación del plazo para la atención de su solicitud ARCO.	**JDSI**.	Oficio de ampliación de plazo.
Fin de la Actividad de atención a solicitudes ARCO, con ampliación de plazo para su respuesta.			

E. Atención a solicitudes ARCO, cuando se propone declaración de inexistencia de datos.			
#	**Actividad**	**Área responsable**	**Documento empleado**
E1	Procede de la Actividad A**6**.	**ÁR´S, JDSI, STyDP, Titular de la OTAIPDPyA.**	Documentación empleada en numerales 1 al 6 del apartado A
E2	Propone a la **OTAIPDPyA** la declaratoria de inexistencia de los datos personales motivo de la solicitud. ¿Son inexistentes los datos personales? **No.** Continúa en la actividad **E13.** **Sí.** Continúa en la actividad **E3.**	**AR´s.**	Proyecto de Declaratoria de inexistencia de datos.

E3	Prepara los antecedentes del asunto para someterlo a consideración del Comité de Transparencia, con apoyo del personal de las AR's.	**JDAJ.**	Proyecto de Declaratoria de inexistencia de datos
E4	Elabora oficio de Convocatoria para los integrantes del CT y entrega a la **STyDP**, para su revisión, adjunta el oficio de las AR's que proponen la declaratoria de inexistencia de los datos personales, y en su caso, los anexos.	**JDAJ.**	Proyecto de Convocatoria, Proyecto de Declaratoria de inexistencia de datos y anexos, si es el caso.
E5	Revisa el proyecto de oficio de Convocatoria y entrega a la persona titular de la **OTAIPDPyA** para firma de la Presidencia del CT.	**STDP.**	Proyecto de Convocatoria, Proyecto de Orden del Día, Proyecto de Declaratoria de inexistencia de datos y anexos, de ser el caso.
E6	Propone a la Presidencia del **Comité** el proyecto de oficio de Convocatoria.	**Titular de la OTAIPDPyA.**	Proyecto de Oficio de Convocatoria, Proyecto de Orden del Día, Proyecto de Acuerdo para la Declaratoria de inexistencia de datos y anexos, en su caso.
E7	Firma la convocatoria para sesión del **Comité**, a fin de analizar, discutir y resolver el asunto.	**Presidencia del Comité.**	Oficio de Convocatoria, Orden del Día.
E8	Analizan propuesta de declaratoria de inexistencia de datos personales. ¿Confirma la inexistencia de datos personales? **Sí.** Continúa en la actividad **E9**. **No.** Continúa en la actividad **E10**.	**Integrantes del Comité.**	Propuesta de Declaratoria de inexistencia y anexos.
E9	Analizan la respuesta de las AR's. y emiten resolución que confirma la propuesta que declara la inexistencia de datos personales y se elabora el documento respectivo para su suscripción por parte de la Presidencia, Vocales y Secretaría del **Comité**, Titular de las AR´s que proponen la inexistencia y la persona titular de la Contraloría Interna del Instituto Electoral o quien asista en su representación.	**Integrantes del Comité.**	Propuesta de Declaratoria de inexistencia y anexos. Acuerdo de Declaratoria de inexistencia de datos. Minuta de la sesión del Comité.
E10	Revocan o modifican la propuesta de inexistencia de datos personales.	**Integrantes del Comité.**	Minuta de la sesión del Comité.

E11	Establecen plazos y términos para la atención de la solicitud ARCO.	**Integrantes del Comité.**	Minuta de la sesión del Comité.
E12	Analiza la respuesta de las AR´s. ¿Es correcta la respuesta? **Sí.** Continúa con las actividades descritas en los numerales **A7** a **A13.** **No.** Continúa en la actividad **E7.**	**JDSI**.	Oficio de respuesta y anexos.
E13	Asesora al personal de las AR's para la respuesta a la solicitud ARCO.	**JDSI**.	Oficio de respuesta y anexos.
E14	Continúa con las actividades **A7** a **A13.**	**JDSI, STyDP, Titular de la OTAIPDPyA.**	Solicitud de Acceso a datos personales, Registro **SISAI 2.0**, oficio de respuesta y anexos.
Fin de las actividades para la atención de solicitudes ARCO, cuando se propone declaración de inexistencia de datos.			

F. Atención a solicitudes ARCO, cuyo trámite implica su traducción a una lengua indígena o al castellano.			
#	**Actividad**	**Área responsable**	**Documento empleado**
F1	Recibe la Solicitud ARCO a través de alguno de los instrumentos de gestión, pero requiere de la intervención de un intérprete en lenguas indígenas para su traducción al castellano, a fin de proceder a su registro en el **SISAI 2.0**, lo comunica a la ST.	**JDSI**.	Solicitud ARCO
F2	Informa a la persona Titular de la **OTAIPDPyA**.	**STyDP.**	Solicitud ARCO
F3	Instruye a la **STyDP** realizar las gestiones ante las instancias correspondientes para atender la solicitud ARCO.	**Titular de la OTAIPDPyA.**	Instrucción de trabajo.
F4	Instruye a la **JDSI elaborar proyecto de oficio** dirigido a la Secretaría de Pueblos y Barrios Originarios y Comunidades Indígenas Residentes (**SEPI**) del Gobierno de la Ciudad de México.	**STyDP**	Proyecto de oficio
F5	Elabora proyecto de oficio dirigido a la Secretaría de Pueblos y Barrios Originarios y Comunidades Indígenas Residentes (**SEPI**) del Gobierno de la	**JDSI**.	Convenio de colaboración IECM-SEPI, Solicitud ARCO

	Ciudad de México, para solicitar su colaboración a fin de que en el plazo máximo de 4 días hábiles, se traduzca el documento, para registrar la solicitud ARCO en el **SISAI 2.0**.		
F6	Firma el oficio y lo devuelve a la **JDSI**, para que sea presentado a la SEPI.	**Titular de la OTAIPDPyA.**	Solicitud ARCO, Oficio de colaboración.
F7	Devuelve al Instituto Electoral el documento traducido al castellano, en un plazo máximo de 4 días hábiles.	**SEPI.**	Oficio, Documento traducido.
F8	Registra la solicitud ARCO de conformidad con la traducción realizada por la SEPI y la turna a las AR´s.	**JDSI**.	Solicitud ARCO y su traducción al castellano.
F9	Analiza la procedencia del ejercicio de los derechos ARCO y elabora el proyecto de oficio para dar respuesta a la solicitud ARCO y lo turna para firma de la/el Titular de las AR´s.	**Enlace de las AR´s.**	Proyecto de oficio de Respuesta.
F10	Firma el oficio de procedencia y lo remite a la **OTAIPDPyA**, en su caso, con la información anexa para dar respuesta a la solicitud ARCO.	**Titular de AR´s.**	Oficio de Respuesta, en su caso, anexos.
F11	Elabora proyecto de oficio de respuesta a la solicitud ARCO, así como el proyecto de oficio para solicitar a la SEPI la traducción de la respuesta a la lengua indígena correspondiente.	**JDSI**.	Proyecto de oficio de Respuesta.
F12	Revisa y, en su caso, otorga el Visto bueno al proyecto de oficio y los presenta a la persona Titular de la **OTAIPDPyA**.	**STyDP.**	Oficio de Respuesta.
F13	Firma el oficio e instruye al **JDSI** para que sea presentado a la SEPI, a fin de que en un plazo máximo de 4 días hábiles se realice la traducción a la lengua indígena correspondiente.	**Titular de la OTAIPDPyA.**	Oficio de Respuesta, Oficio de Colaboración, Oficio de Respuesta de las AR´s.
F14	Devuelve al IECM el documento traducido en la lengua indígena.	**SEPI.**	Oficio, Documento traducido.
F15	Notifica oficio de respuesta a la solicitud ARCO, a través del **SISAI 2.0** y del medio señalado para tal fin.	**JDSI**.	Oficio de Respuesta.
Fin de la Actividad para la Atención a solicitudes ARCO, cuyo trámite implica su traducción a una lengua indígena o al castellano.			

9. Formatos

9.1. Formato de Solicitud de Acceso a Datos Personales

9.2. Formato de Solicitud de Rectificación a Datos Personales

9.3. Formato de Solicitud de Cancelación a Datos Personales

9.4. Formato de Solicitud de Oposición a Datos Personales

9.1.1.-Instructivo de llenado solicitud de acceso

1. Se anotará el número de folio que corresponda de acuerdo al registro en el **SISAI 2.0**.

2. Se anotará el día de la fecha en que se recibe la solicitud de Acceso a Datos Personales en la Unidad de Transparencia.

3. Se anotará el mes de la fecha en que se recibe la solicitud de Acceso a Datos Personales en la Unidad de Transparencia.

4. Se anotará el año de la fecha en que se recibe la solicitud de Acceso a Datos Personales en la Unidad de Transparencia.

5. Se anotará la hora en que se recibe la solicitud de Acceso a Datos Personales en la Unidad de Transparencia.

6. Se anotará el nombre del Instituto Electoral de la Ciudad de México, por ser el sujeto obligado ante el cual se ejercerá el derecho de acceso a datos personales.

7. Se anotará el nombre de la o el solicitante que acude a la Unidad de Transparencia para presentar su solicitud de derecho de acceso a sus datos personales.

8. Se anotará el apellido paterno de la o el solicitante que acude a la Unidad de Transparencia para presentar su solicitud de derecho de acceso a sus datos personales.

9. Se anotará el apellido materno de la o el solicitante que acude a la Unidad de Transparencia para presentar su solicitud de derecho de acceso a sus datos personales.

10. En caso de que la o el titular de los datos personales no pueda acudir a las oficinas de la Unidad de Transparencia, podrá hacer la solicitud a través de su representante legal, quien tendrá que proporcionar su nombre y anexar documentación que acredite su personalidad, por lo que en este rubro se anotará el nombre del representante legal de la o el solicitante.

11. Se anotará el tipo de documento oficial (credencial para votar, cédula profesional, pasaporte vigente, credencial de afiliación al IMSS, ISSSTE o INAPAM o cartilla del servicio militar) con el que se identifique la o el solicitante, o en su caso el representante legal de éste.

12. Se anotará el lugar o medio por el cual la o el solicitante desea recibir notificaciones, puede seleccionar: correo electrónico, tendrá que anotar una dirección de correo electrónico; acudir a la Unidad de Transparencia; o domicilio (deberá ser dentro de la Ciudad de México), tendrá que anotar la Calle, Número exterior, Número interior, Colonia, Alcaldía, Código Postal. De manera opcional podrá anotar su número telefónico.

13. Se anotará la modalidad en que desea la entrega de los datos solicitados, puede seleccionar: consulta directa, acudiendo a las oficinas de la Unidad de Transparencia, copia simple de los documentos o copia certificada.

14. Se anotará de forma clara y precisa los datos personales a los que solicita acceso.

15. Se anotará de forma opcional otros datos para facilitar su localización.

16. En caso de que la o el solicitante requiera más espacio para hacer su solicitud, podrá anexar un documento especificando el número de hojas.

17. La o el solicitante y la persona servidora pública de la Unidad de Transparencia que recibe la solicitud de derecho de acceso a datos personales deberán firmar dicha solicitud.

18. Sólo de manera opcional y para fines estadísticos la o el solicitante anotará: Sexo, Femenino o Masculino, Edad y Nacionalidad.

19. Se anotará de forma opcional la ocupación actual de la o el solicitante: Empresario/a, Persona Servidora Pública, Empleado/a u Obrero/a, Medios de Comunicación, Asociación Política, Organización no Gubernamental, Comerciante, Académico o Estudiante u Otro.

20. Se anotará de forma opcional el último grado de estudios de la o el solicitante: Sin estudios, Primaria, Secundaria, Bachillerato, Licenciatura, Maestría o Doctorado.

9.2.1.-Instructivo de llenado solicitud de rectificación

1. Se anotará el número de folio que corresponda de acuerdo al registro en el **SISAI 2.0**.

2. Se anotará el día de la fecha en que se recibe la solicitud de rectificación de datos personales en la Unidad de Transparencia.

3. Se anotará el mes de la fecha en que se recibe la solicitud de rectificación de datos personales en la Unidad de Transparencia.

4. Se anotará el año de la fecha en que se recibe la solicitud de rectificación de datos personales en la Unidad de Transparencia.

5. Se anotará la hora en que se recibe la solicitud de rectificación de datos personales en la Unidad de Transparencia.

6. Se anotará el nombre del Instituto Electoral de la Ciudad de México, por ser el sujeto obligado ante el cual se ejercerá el derecho de rectificación de datos personales.

7. Se anotará el nombre de la o el solicitante que acude a la Unidad de Transparencia para presentar su solicitud de derecho de rectificación de sus datos personales.

8. Se anotará el apellido paterno de la o el solicitante que acude a la Unidad de Transparencia para presentar su solicitud de derecho de rectificación de sus datos personales.

9. Se anotará el apellido materno de la o el solicitante que acude a la Unidad de Transparencia para presentar su solicitud de derecho de rectificación de sus datos personales.

10. En caso de que el titular de los datos personales no pueda acudir a las oficinas de la Unidad de Transparencia, podrá hacer la solicitud a través de su representante legal, quien tendrá que proporcionar su nombre y anexar documentación que acredite su personalidad, por lo que en este rubro se anotará el nombre del representante legal de la o el solicitante.

11. Se anotará el tipo de documento oficial (credencial para votar, cédula profesional, pasaporte vigente, credencial de afiliación al IMSS, ISSSTE o INAPAM o cartilla del servicio militar) con el que se identifique de la o el solicitante, o en su caso el representante legal de éste.

12. Se anotará el lugar o medio por el cual la o el solicitante desea recibir notificaciones, puede seleccionar: Correo electrónico, tendrá que anotar una dirección de correo electrónico; Acudir a la Unidad de Transparencia; o Domicilio (tendrá que ser en la Ciudad de México), tendrá que anotar la Calle, Número exterior, Número interior, Colonia, Alcaldía, Código Postal. De manera opcional podrá anotar su número telefónico.

13. Se anotarán detalladamente los datos personales de los cuales se solicita su rectificación.

14. Se anotarán detalladamente los datos personales incorrectos que detente el IECM.

15. Se anotarán los datos personales que son correctos.

16. Se enlistarán los documentos probatorios con los cuales la o el solicitante sustenta su solicitud de rectificación de datos personales.

17. Se anotará de forma opcional otros datos para facilitar su localización.

18. Se anotará el número de hojas que corresponden a su anexo respecto de los documentos probatorios.

19. La o el solicitante y la persona servidora pública de la Unidad de Transparencia que recibe la solicitud de derecho de rectificación de datos personales deberán firmar dicha solicitud.

20. Sólo de manera opcional y para fines estadísticos la o el solicitante anotará: Sexo Femenino o Masculino, Edad y Nacionalidad.

21. Se anotará de forma opcional la ocupación actual de la o el solicitante: Empresario/a, Persona Servidora Pública, Empleado/a u Obrero, Medios de Comunicación, Asociación Política, Organización no Gubernamental, Comerciante, Académico o Estudiante u Otro.

22. Se anotará de forma opcional el último grado de estudios de la o el solicitante: Sin estudios, Primaria, Secundaria, Bachillerato, Licenciatura, Maestría o Doctorado.

9.3.1.-Instructivo de llenado solicitud de cancelación

1. Se anotará el número de folio que corresponda de acuerdo al registro en el **SISAI 2.0**.

2. Se anotará el día de la fecha en que se recibe la solicitud de cancelación de datos personales en la Unidad de Transparencia.

3. Se anotará el mes de la fecha en que se recibe la solicitud de cancelación de datos personales en la Unidad de Transparencia.

4. Se anotará el año de la fecha en que se recibe la solicitud de cancelación de datos personales en la Unidad de Transparencia.

5. Se anotará la hora en que se recibe la solicitud de cancelación de datos personales en la Unidad de Transparencia.

6. Se anotará el nombre del Instituto Electoral de la Ciudad de México, por ser el sujeto obligado ante el cual se ejercerá el derecho de cancelación de datos personales.

7. Se anotará el nombre de la o el solicitante que acude a la Unidad de Transparencia para presentar su solicitud de derecho de cancelación de sus datos personales.

8. Se anotará el apellido paterno de la o el solicitante que acude a la Unidad de Transparencia para presentar su solicitud de derecho de cancelación de sus datos personales.

9. Se anotará el apellido materno de la o el solicitante que acude a la Unidad de Transparencia para presentar su solicitud de derecho de cancelación de sus datos personales.

10. En caso de que el titular de los datos personales no pueda acudir a las oficinas de la Unidad de Transparencia, podrá hacer la solicitud a través de su representante legal, quien tendrá que proporcionar su nombre y anexar documentación que acredite su personalidad, por lo que en este rubro se anotará el nombre del representante legal de la o el solicitante.

11. Se anotará el tipo de documento oficial (credencial para votar, cédula profesional, pasaporte vigente, credencial de afiliación al IMSS, ISSSTE o INAPAM o cartilla del servicio militar) con el que se identifique la o el solicitante, o en su caso el representante legal de éste.

12. Se anotará el lugar o medio por el cual la o el solicitante desea recibir notificaciones, puede seleccionar: Correo electrónico, tendrá que anotar una dirección de correo electrónico; Acudir a la Unidad de Transparencia; o Domicilio (tendrá que ser en la Ciudad de México), tendrá que anotar la Calle, Número exterior, Número interior, Colonia, Alcaldía, Código Postal. De manera opcional podrá anotar su número telefónico.

13. Se anotarán detalladamente los datos personales de los cuales solicita su cancelación.

14. Se anotarán detalladamente las razones por las que considera que los datos personales deben ser cancelados.

15. En caso de requerir más espacio podrá anexar un documento, por lo que en este rubro deberá especificar el número de hojas utilizadas.

16. Se anotará el número de hojas que corresponden a su anexo respecto de los documentos probatorios.

17. El o la solicitante y la persona servidora pública de la Unidad de Transparencia que recibe la solicitud de derecho de cancelación de datos personales deberán firmar dicha solicitud.

18. Sólo de manera opcional y para fines estadísticos la o el solicitante anotará: Sexo, Mujer u Hombre, Edad y Nacionalidad.

19. Se anotará de forma opcional la ocupación actual de la o el solicitante: Empresario/a, Persona Servidora Pública, Empleado/a u Obrero/a, Medios de Comunicación, Asociación Política, Organización no Gubernamental, Comerciante, Académico/a o Estudiante u Otro.

20. Se anotará de forma opcional el último grado de estudios de la o el solicitante: Sin estudios, Primaria, Secundaria, Bachillerato, Licenciatura, Maestría o Doctorado.

9.4.1.-Instructivo de llenado solicitud de oposición

1. Se anotará el número de folio que corresponda de acuerdo al registro en el **SISAI 2.0**.

2. Se anotará el día de la fecha en que se recibe la solicitud de oposición de datos personales en la Unidad de Transparencia.

3. Se anotará el mes de la fecha en que se recibe la solicitud de oposición de datos personales en la Unidad de Transparencia.

4. Se anotará el año de la fecha en que se recibe la solicitud de oposición de datos personales en la Unidad de Transparencia.

5. Se anotará la hora en que se recibe la solicitud de oposición de datos personales en la Unidad de Transparencia.

6. Se anotará el nombre del Instituto Electoral de la Ciudad de México, por ser el sujeto obligado ante el cual se ejercerá el derecho de oposición de datos personales.

7. Se anotará el nombre de la o el solicitante que acude a la Unidad de Transparencia para presentar su solicitud de derecho de oposición de sus datos personales.

8. Se anotará el apellido paterno de la o el solicitante que acude a la Unidad de Transparencia para presentar su solicitud de derecho de oposición de sus datos personales.

9. Se anotará el apellido materno de la o el solicitante que acude a la Unidad de Transparencia para presentar su solicitud de derecho de oposición de sus datos personales.

10. En caso de que el titular de los datos personales no pueda acudir a las oficinas de la Unidad de Transparencia, podrá hacer la solicitud a través de su representante legal, quien tendrá que proporcionar su nombre y anexar documentación que acredite su personalidad, por lo que en este rubro se anotará el nombre del representante legal de la o el solicitante.

11. Se anotará el tipo de documento oficial (credencial para votar, cédula profesional, pasaporte vigente, credencial de afiliación al IMSS, ISSSTE o INAPAM o cartilla del servicio militar) con el que se identifique la o el solicitante, o en su caso el representante legal de éste.

12. Se anotará el lugar o medio por el cual la o el solicitante desea recibir notificaciones, puede seleccionar: Correo electrónico, tendrá que anotar una dirección de correo electrónico; Acudir a la Unidad de Transparencia; o Domicilio (tendrá que ser en la Ciudad de México), tendrá que anotar la Calle, Número exterior, Número interior, Colonia, Alcaldía, Código Postal. De manera opcional podrá anotar su número telefónico.

13. Se anotarán detalladamente los datos personales de los cuales se opone a su tratamiento.

14. Se anotarán detalladamente las razones por las cuales se opone al tratamiento de sus datos personales.

15. En caso de requerir más espacio podrá anexar un documento, por lo que en este rubro deberá especificar el número de hojas utilizadas.

16. Se anotará el número de hojas que corresponden a su anexo respecto de los documentos probatorios.

17. La o el solicitante y la persona servidora pública de la Unidad de Transparencia que recibe la solicitud de derecho de oposición de datos personales deberán firmar dicha solicitud.

18. Sólo de manera opcional y para fines estadísticos la o el solicitante anotará: Sexo, Femenino o Masculino, Edad y Nacionalidad.

19. Se anotará de forma opcional la ocupación actual de la o el solicitante: Empresario/a, Persona Servidora Pública, Empleado/a u Obrero/a, Medios de Comunicación, Asociación Política, Organización no Gubernamental, Comerciante, Académico/a o Estudiante u Otro.

20. Se anotará de forma opcional el último grado de estudios de la o el solicitante: Sin estudios, Primaria, Secundaria, Bachillerato, Licenciatura, Maestría o Doctorado.

Contenido

1. Objetivo 2
2. Alcance 2
3. Marco normativo 2
4. Definiciones y Abreviaturas 2
5. Responsabilidades 5
6. Políticas de operación 7
7. Diagrama de flujo 10
8. Descripción de las actividades 13
9. Formatos 16

Control de Cambios

Revisión	Fecha	Descripción del Cambio
00	09 febrero 2023	Emisión del documento

1. Objetivo

Establecer las directrices para la elaboración y/o actualización de los avisos de privacidad del Instituto Electoral de la Ciudad de México; así como su difusión, a fin de cumplir con las disposiciones normativas en materia de Datos Personales.

2. Alcance

El presente Manual es aplicable a la Oficina Transparencia, Acceso a la Información Pública, Datos Personales y Archivo, así como para las Áreas Responsables del Instituto Electoral de la Ciudad de México, que a continuación se indican.

- Presidencia;
- Oficinas de Consejeras y Consejeros Electorales;
- Secretaría Ejecutiva;
- Secretaría Administrativa;
- Contraloría Interna;
- Direcciones Ejecutivas;
- Unidades Técnicas, y
- Órganos Desconcentrados.

3. Marco normativo

- Constitución Política de los Estados Unidos Mexicanos;
- Constitución Política de la Ciudad de México;
- Código de Instituciones y Procedimientos Electorales de la Ciudad de México;
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Ley General de Archivos;
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;
- Ley de Archivos Local. Ley de Archivos, aplicable en la Ciudad de México;
- Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México,
- Reglamento Interior del Instituto Electoral de la Ciudad de México;
- Reglamento del Instituto Electoral de la Ciudad de México, en materia de Protección de Datos Personales; y
- Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

4. Definiciones y Abreviaturas

Aviso de privacidad: Documento a disposición de la persona titular de los datos personales, generado por las áreas que posean, de forma física, electrónica o en cualquier formato, previo a la obtención de sus datos, con objeto de informarle sobre la finalidad y tratamiento de los datos

recabados, así como su derecho a acceder, rectificar, oponerse, cancelar o solicitar la portabilidad de los mismos.

Aviso de privacidad integral: Documento mediante el cual se da a conocer al titular de los datos personales, la información detallada sobre el tratamiento de los datos que serán recabados; tales como su finalidad o finalidades, transferencias, mecanismos y medios para manifestar negativa al tratamiento, domicilio del Responsable, datos personales sometidos a tratamiento, fundamento legal que lo faculta, mecanismos y procedimientos para ejercer derechos de acceso, rectificación cancelación u oposición de datos personales, datos de la Unidad de Transparencia y medios por los cuales se comunica los cambios al aviso de privacidad.

Aviso de privacidad simplificado: Documento por el cual de primera instancia se da a conocer al titular de los datos personales, de manera breve el tratamiento de los datos que serán recabados. Dicho documento especificará la finalidad o finalidades, información relacionada con las transferencias que requieran consentimiento, mecanismos y medios para manifestar la negativa al tratamiento; así como la información donde podrá consultar el aviso integral.

AR´s: Cada una de las áreas administrativas del Instituto Electoral de la Ciudad de México, que posea o administre bases de datos o Sistemas de Datos Personales, en términos de la legislación aplicable.

Circular: Documento emitido por la Secretaría Ejecutiva, mediante el cual se solicita a las AR's, que, de conformidad con sus atribuciones, informen sobre la actualización, modificación o cancelación de los avisos de privacidad.

Consentimiento: Manifestación de la voluntad libre, específica, informada e inequívoca de la persona titular de los datos a través de la cual autoriza mediante declaración o acción afirmativa, que sus datos personales puedan ser tratados por el responsable.

Consentimiento escrito: Cuando el Titular de los datos, manifieste su voluntad en un documento físico o electrónico, a través de una declaración en sentido afirmativo, firma autógrafa, huella dactilar, firma electrónica o cualquier otro mecanismo o procedimiento equivalente contenido en la normativa aplicable, otorga su anuencia para el tratamiento de sus datos personales.

Consentimiento verbal: Cuando el titular de los datos personales externe oralmente, de manera presencial, ante el responsable o mediante el uso de cualquier otra tecnología que permita la interlocución oral, aprueba el tratamiento de sus datos personales.

Correo electrónico: Medio oficial, a través del cual la Oficina Transparencia, Acceso a la Información Pública, Datos Personales y Archivo, los enlaces de las AR´s mantienen comunicación, respecto del envío, retroalimentación y difusión de los avisos de privacidad.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como: origen racial o étnico, estado de salud presente o futuro,

información genética, información biométrica, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Enlace: Persona designada en cada AR´s para la gestión y trámite en materia de datos personales.

INFO: Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

Instituto Electoral: Instituto Electoral de la Ciudad de México.

JDDPyAJ: Jefatura de Departamento Datos Personales y Apoyo Jurídico, adscrita a la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo.

Ley de Datos: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Lineamientos Generales de Datos: Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Medidas compensatorias: Mecanismos alternos para dar a conocer al titular de los datos personales el aviso de privacidad, a través de su difusión por medios masivos de comunicación, cuando no se haya podido recabar el consentimiento previo al tratamiento de los datos personales de una persona física, sea por emergencias de salud pública, seguridad o desastres naturales.

OTAIPDPyA: Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral de la Ciudad de México, a la cual también se le denominará indistintamente como Unidad de Transparencia.

Oficial de Protección de Datos Personales: Persona servidora pública especialista en materia de datos personales, designada por el responsable del Instituto Electoral, adscrita a la Unidad de Transparencia; quien coordina las actividades para atender los asuntos relacionados con la protección de datos personales.

Oficio de respuesta: Documento a través del cual las AR's comunican a la Unidad de Transparencia la respuesta a la Circular de actualización, modificación o supresión de los avisos de privacidad.

Oficio de difusión: Documento mediante el cual se solicita a la Unidad Técnica de Comunicación Social y Difusión, la publicación de los avisos de privacidad, a través del sitio de Internet: www.iecm.mx.

Responsable del Sistema de Datos Personales: Persona servidora pública del Instituto Electoral, con el cargo de titular del área que administra el sistema de datos personales; que decide y determina la finalidad, fines, medios, medidas de seguridad y todo aquello relacionado con el tratamiento de datos personales;

Revocación del consentimiento: Manifestación expresa, mediante escrito libre o vía electrónica, dirigido a la Unidad de Transparencia, mediante el cual la persona Titular de los datos personales retira su consentimiento para el tratamiento de sus datos, lo que podrá realizar en cualquier momento.

SDP: Sistema de Datos Personales.

SE: Secretaría Ejecutiva.

Sitio de Internet: Página electrónica del Instituto Electoral: www.iecm.mx.

STyDP: Subdirección de Transparencia y Datos Personales, adscrita a la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral.

Titular: Persona física a quien corresponden los datos personales.

Titular de la Oficina: Titular de la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral, también denominada Unidad de Transparencia.

Unidad de Transparencia: Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral.

UTCSyD: Unidad Técnica de Comunicación Social y Difusión.

5. Responsabilidades

OTAIPDPyA	• Generar de manera semestral, el proyecto de Circular que suscribirá la SE, en la que se solicita a las diversas AR´s del Instituto Electoral la revisión y, en su caso, la actualización, modificación o supresión de los avisos de privacidad. Dicha Circular deberá **elaborarse y distribuirse 15 días hábiles antes de la conclusión de cada semestre.** • Asesorar y apoyar permanentemente a las AR's en materia de datos personales y coordinar con los Enlaces, para llevar a cabo la elaboración, actualización, modificación o supresión de los avisos de privacidad. • Implementar acciones para el cumplimiento de las obligaciones en materia de datos personales, para lo cual, tendrá la facultad de validar, o solicitar adecuaciones a los avisos de privacidad, conforme a la normatividad aplicable, previo a su publicación en el Sitio de Internet.

	• Revisar y validar los avisos de privacidad remitidos por las AR's, de conformidad con la Ley de Datos y los Lineamientos Generales. • Solicitar y dar seguimiento a la correcta publicación en el Sitio de Internet, por parte de la Unidad Técnica de Comunicación Social y Difusión de los avisos de privacidad, que para tal efecto remitan las AR´s. • Notificar ante el INFO la elaboración, actualización, modificación o supresión de los avisos de privacidad; así como su difusión en el Sitio de Internet.
AR´s	• Enviar semestralmente a la OTAIPDPyA, en respuesta a la Circular que emita, el reporte de actualización, modificación o supresión de los avisos de privacidad, para su debida publicación en el Sitio de Internet. • Solicitar asesoría u opinión a la OTAIPDPyA, respecto a la elaboración, actualización, modificación o supresión de los avisos de privacidad. • Dar seguimiento a la correcta publicación de los avisos de privacidad en el Sitio de Internet; así como su notificación ante el INFO. • Garantizar que, en todo tratamiento de datos personales cuente con los avisos de privacidad simplificado e integral. • Garantizar que la ubicación de los avisos de privacidad se encuentre en lugares visibles que facilite la consulta de la persona Titular y permita acreditar fehacientemente el cumplimiento de esta obligación.
Oficial de Protección de Datos Personales	• Opinar, previo a su difusión, sobre los avisos de privacidad. • Formular dictámenes, opiniones técnicas y cualquier otro documento que se considere necesario para atender los asuntos en materia de protección de datos personales. • **Coordinar las actividades para atender los asuntos relacionados con la protección de datos personales.**

6. Políticas de operación

- ✓ En todo tratamiento de datos personales se debe contar con el consentimiento libre, específico, informado e inequívoco de la persona Titular, otorgado a través del aviso de privacidad.
- ✓ El consentimiento de la persona Titular se recaba, directamente cuando este los proporciona de manera presencial a través de la persona que lo representa, o por algún medio que permita su entrega directa, como pueden ser medios electrónicos, ópticos, vía telefónica, internet o cualquier otra tecnología.
- ✓ El consentimiento de la persona Titular se recaba indirectamente, cuando de manera tácita o expresa autoriza el tratamiento de sus datos personales.
- ✓ Los avisos de privacidad tienen por objeto informar a la persona Titular sobre los alcances y condiciones generales del tratamiento a que serán sometidos sus datos personales, a fin de que esté en posibilidad de tomar decisiones informadas sobre su uso.
- ✓ Los avisos de privacidad deben ser sencillos, con la información necesaria sobre su tratamiento, en lenguaje claro y con una estructura que facilite su entendimiento.
- ✓ En los avisos de privacidad queda prohibido usar frases inexactas, ambiguas, incluir textos que induzcan a la persona Titular a otorgar su consentimiento para el tratamiento de sus datos personales sin manifestación alguna de su parte o remitirlo a textos o documentos que no estén disponibles.
- ✓ El Responsable de los Sistemas de Datos Personales podrá difundir, poner a disposición o reproducir el aviso de privacidad en formatos físicos y electrónicos, o de cualquier otra tecnología que permita su comunicación; asimismo, en todos los casos deberá ubicarlo en un lugar visible que facilite la consulta de la persona Titular.
- ✓ El aviso de privacidad se pondrá a disposición de la persona Titular, en dos modalidades: simplificado e integral, siendo obligatorio la elaboración de ambos avisos por parte del Responsable de los Sistemas de Datos Personales.
- ✓ El Responsable de los Sistemas de Datos Personales deberá poner a disposición de la persona Titular, el aviso de privacidad simplificado en un primer momento, lo que no impide que pueda conocer el aviso de privacidad integral desde el inicio, si así lo prefiere.
- ✓ El aviso de privacidad simplificado se pondrá a disposición de la persona Titular de manera previa a la obtención de datos personales, cuando los mismos se obtengan directamente de la persona Titular, independientemente de los formatos o medios utilizados, o bien, al primer contacto con la persona Titular, cuando estos se hubieran obtenido de manera indirecta.
- ✓ El aviso de privacidad integral deberá estar publicado de manera permanente en el Sitio de Internet, a efecto de que la persona Titular pueda consultarlo en cualquier momento.

- ✓ El Responsable de los Sistemas de Datos Personales deberá poner a disposición de la persona Titular, un nuevo aviso de privacidad, cuando cambie su identidad, requiera recabar datos personales sensibles adicionales a aquellos informados en el aviso de privacidad original, cambie las finalidades, o bien, modifique las condiciones para la transferencia de datos personales.

6.1 Políticas de operación específicas para la elaboración de los avisos de privacidad

En el aviso de privacidad simplificado, deben incluirse los datos siguientes:

- ✓ Denominación del responsable y siglas; anotar el nombre del áreas administrativa responsable del SDP; en este apartado deberá incorporarse el nombre completo del Instituto Electoral y las siglas IECM.

- ✓ Finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular; en este rubro el Responsable del Sistema de Datos Personales, deberá describir puntualmente las finalidades del tratamiento de los datos personales con claridad y que no generen confusión, añadiendo en este apartado el ciclo de vida de los datos recabados.

- ✓ Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar: Las autoridades, poderes, entidades, órganos y organismos gubernamentales a las que se transfieren los datos personales, así como, las finalidades de estas transferencias.

- ✓ Mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales. Anotar el nombre del sujeto obligado, el domicilio de la Unidad de Transparencia del IECM, número telefónico y correo de la Unidad de Transparencia.

- ✓ Sitio de Internet.

- ✓ Fecha de última actualización.

En el aviso de privacidad integral, adicionalmente a los datos anteriores, deberán incluirse, los datos siguientes:

- ✓ Domicilio del responsable; en este apartado se señalará el domicilio completo del Instituto Electoral.

- ✓ Datos personales que serán sometidos a tratamiento, de manera enunciativa más no limitativa, el Responsable de los Sistemas de Datos Personales deberá considerar los siguientes tipos de datos: de identificación, electrónicos, laborales, académicos, biométricos, patrimoniales, sobre procedimientos administrativos y/o jurisdiccionales, de tránsito y movimientos migratorios, sobre la salud; identificando aquéllos que son sensibles.

- ✓ Fundamento legal que faculta al Responsable para llevar a cabo el tratamiento; el Responsable de los Sistemas de Datos Personales deberá señalar el o los artículos, apartados, fracciones, incisos y nombre de los ordenamientos vigentes, que faculta o confiere atribuciones para realizar el tratamiento de datos personales, precisando su fecha de publicación, o en su caso, de la última reforma ya sea en la Gaceta Oficial de la Ciudad de México o en el Diario Oficial de la Federación.

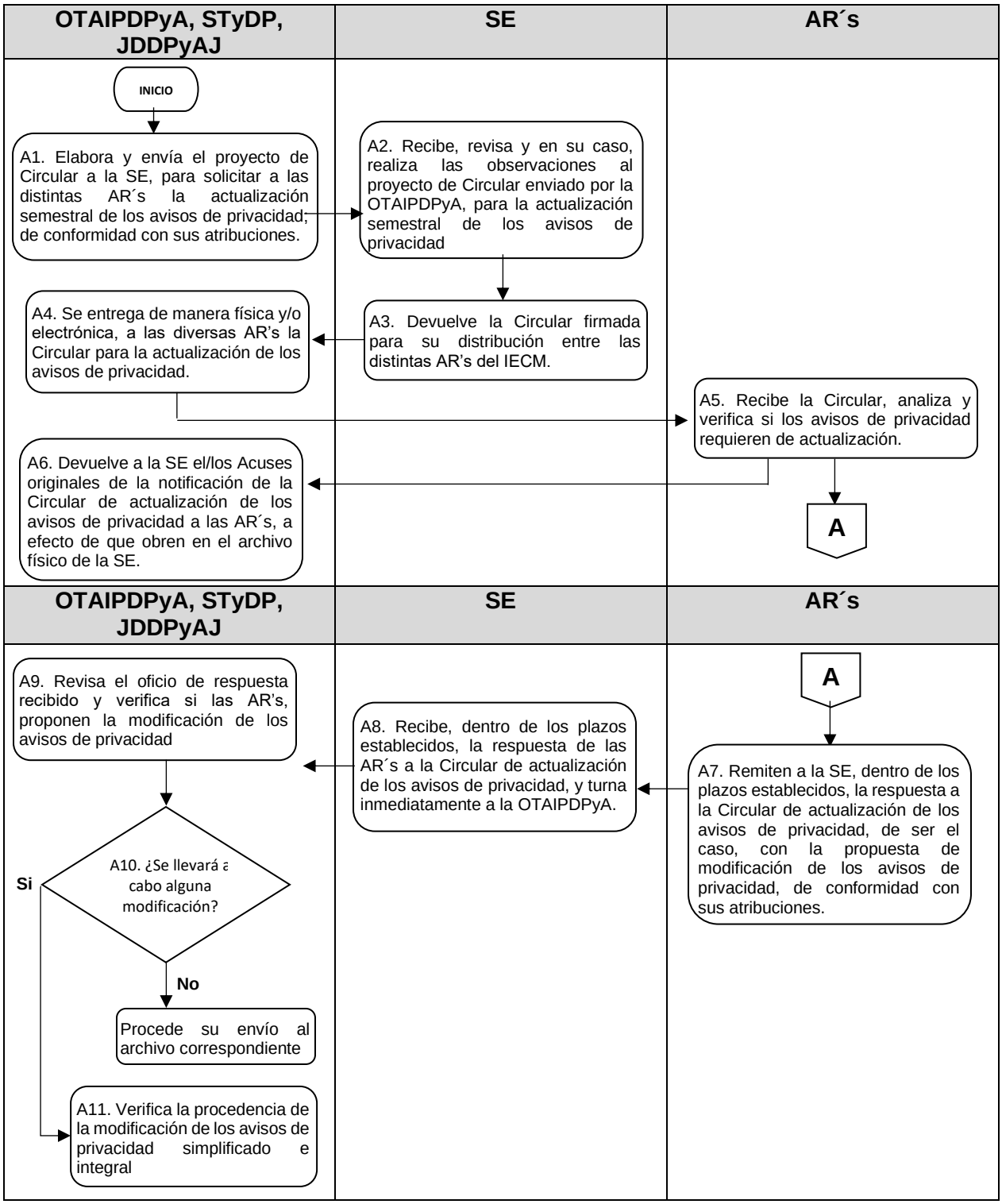
- ✓ Finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular.

- ✓ Mecanismos, medios y procedimientos disponibles para manifestar la negativa al tratamiento de sus datos personales y ejercer los derechos ARCO; el Responsable de los Sistemas de Datos Personales deberá informar sobre los mecanismos, medios y procedimientos habilitados para atender las solicitudes para el ejercicio de los derechos ARCO.

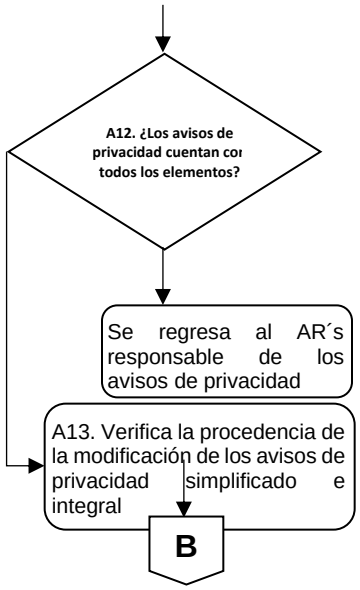
- ✓ Domicilio de la Unidad de Transparencia, En este apartado deberá incluirse la ubicación precisa de la oficina, incluyendo calle, número, piso, colonia, alcaldía, código postal y entidad federativa; podrá incluirse dirección electrónica y página de internet. Indicar la Plataforma Nacional de Transparencia (http://www.plataformadetransparencia.org.mx), o bien mediante el número de TEL INFO 55 5636 4636.

- ✓ Medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad; el Responsable de los Sistemas de Datos Personales deberá señalar el o los medios disponibles a través de los cuales hará del conocimiento del Titular los cambios o actualizaciones efectuadas tanto al aviso de privacidad simplificado como integral.

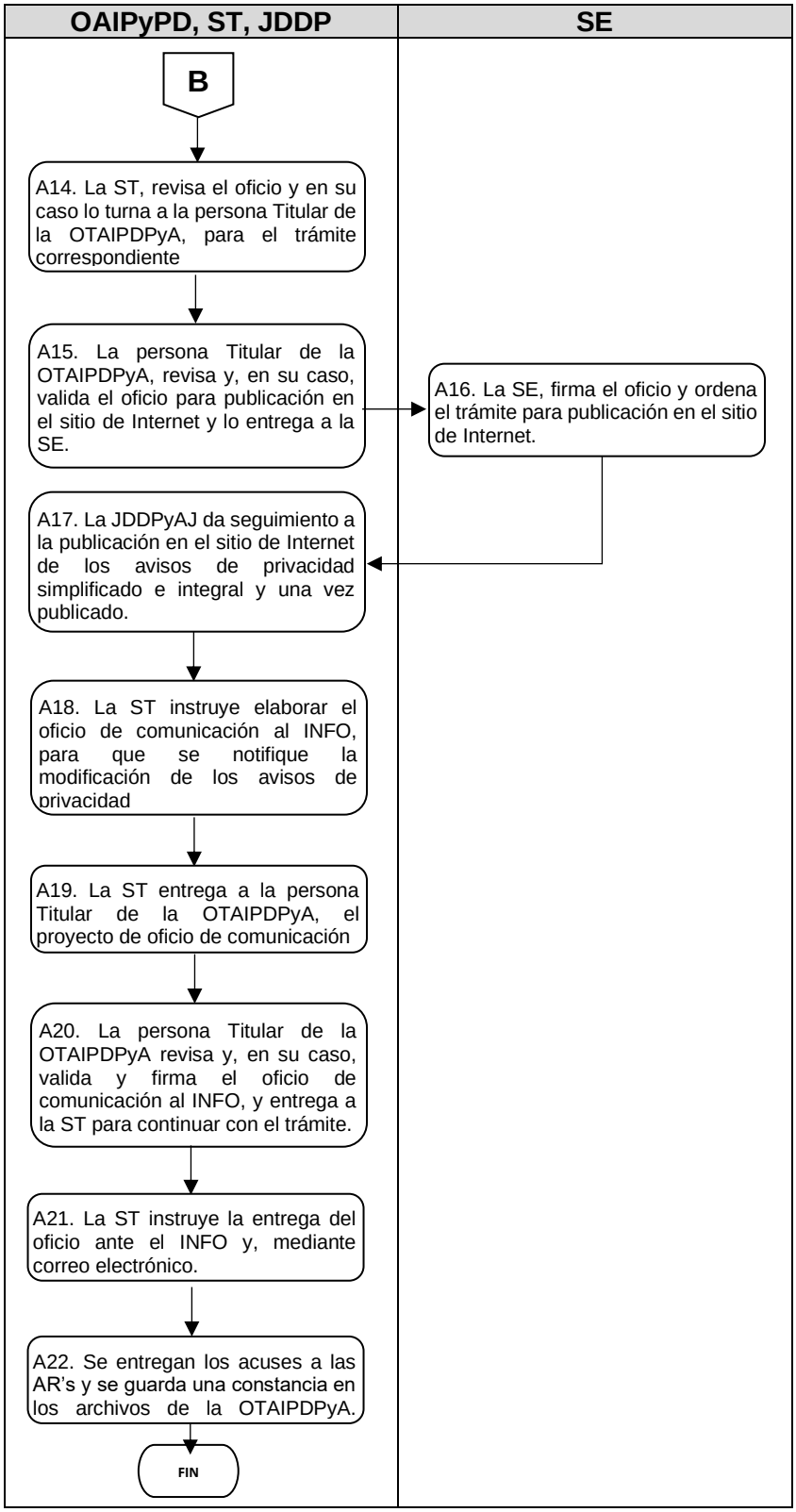
7. Diagrama de flujo



Elaboración y/o actualización de los Avisos de Privacidad

Elaboración y/o actualización de los Avisos de Privacidad



8. Descripción de las actividades

A. Actividades para la elaboración y/o actualización de los avisos de privacidad			
#	**Actividad**	**Área responsable**	**Documento empleado**
A1	Elabora y envía el proyecto de Circular a la SE, para solicitar a las distintas AR´s del Instituto Electoral, la actualización semestral de los avisos de privacidad; de conformidad con sus atribuciones. Dicho documento establece la fecha límite para la respuesta y actualización de los avisos de privacidad.	OTAIPDPyA´, STyDP, JDDPyAJ	Proyecto de Circular.
A2	Recibe, revisa y en su caso, realiza las observaciones al proyecto de Circular enviado por la OTAIPDPyA, para la actualización semestral de los avisos de privacidad.	SE.	Proyecto de Circular.
A3	Devuelve la Circular firmada para su comunicación a las distintas AR's del IECM.	SE.	Circular.
A4	Se entrega de manera física y/o electrónica, a las diversas AR's la Circular para la actualización de los avisos de privacidad.	STyDP, JDDPyAJ.	Circular (copia).
A5	Recibe la Circular, analiza y verifica si los avisos de privacidad de los Sistemas de Datos Personales a su cargo requieren de actualización.	AR´s	Circular (copia).
A6	Devuelve a la SE, el/los Acuses originales de la notificación de la Circular para la actualización de los avisos de privacidad a las AR´s, a efecto de que obren en el archivo físico de la SE.	OTAIPDPyA, JDDPyAJ.	Circular original y Acuses.
A7	Remiten a la SE, dentro de los plazos establecidos, la respuesta a la Circular, de ser el caso, la propuesta de modificación, actualización o cancelación de los avisos de privacidad, de los avisos de privacidad, de conformidad con sus atribuciones.	AR´s.	Oficio de respuesta a la Circular.
A8	Recibe, dentro de los plazos establecidos, la respuesta de las AR´s a la Circular para la actualización de los avisos de privacidad, y turna inmediatamente a la OTAIPDPyA.	SE.	Oficio de respuesta a la Circular.

A9	Revisa el oficio de respuesta recibido y verifica si las AR's, proponen la actualización, modificación o cancelación de los avisos de privacidad de aquellos Sistemas de Datos Personales bajo su resguardo.	STyDP	Oficio de respuesta a la Circular.
A10	Determina si: ¿Se llevará a cabo alguna modificación a los avisos de privacidad? **No.** Procede su envío al archivo correspondiente. **Sí.** Continúa en la Actividad **A 11**	STyDP	Oficio de respuesta a la Circular.
A11	Verifica la procedencia de la modificación de los avisos de privacidad simplificado e integral	OTAIPDPyA, STyDP	Oficio de respuesta a la Circular, proyecto de modificación a los avisos de privacidad simplificado e integral.
A12	Revisa que los proyectos de modificación a los avisos de privacidad simplificado e integral, contengan todos los elementos señalados tanto en la Ley de Datos como en los Lineamientos Generales de Datos y que cumpla con los formatos de los avisos de privacidad ¿Los avisos de privacidad cuentan con todos los elementos? **NO.** Se regresa al AR´s responsable de los avisos de privacidad, con las observaciones, a efecto de que lleve a cabo las modificaciones correspondientes. **SI.** Continúa en la actividad A13.	STyDP, JDDPyAJ	Proyecto de modificación a los avisos de privacidad simplificado e integral y correo electrónico
A 13	Una vez verificado que los proyectos de avisos de privacidad simplificado e integral cumplen con los requisitos señalados en la Ley de Datos, en los Lineamientos Generales de Datos; así como en los formatos correspondientes, elabora el proyecto de oficio para firma de la persona Titular de la SE, para su publicación en el Sitio de Internet.	STyDP, JDDPyAJ, Enlace del AR´s	Avisos de privacidad simplificado e integral, Proyecto de oficio para publicación en sitio de Internet.

A14	La STyDP, revisa el oficio y en su caso lo turna a la persona Titular de la OTAIPDPyA, para el trámite correspondiente.	STyDP Titular de la OTAIPDPyA	Oficio de turnado para publicación
A15	La persona Titular de la OTAIPDPyA, revisa y, en su caso, valida el oficio para publicación en el sitio de Internet y lo entrega a la SE, para el trámite correspondiente.	Titular de la OTAIPDPyA	Oficio de turnado para publicación
A16	La SE, firma el oficio y ordena el trámite para su publicación en el sitio de Internet.	SE	Oficio de turnado para publicación
A17	La JDDPyAJ, da seguimiento a la publicación en el sitio de Internet de los avisos de privacidad simplificado e integral y una vez publicado, inmediatamente comunica a la ST, con la finalidad de continuar el trámite.	JDDPyAJ	Comunicado verbal
A18	La STyDP, instruye elaborar el oficio de comunicación al INFO, para que **dentro de los diez días hábiles siguientes a la publicación en el sitio de Internet,** se notifique la actualización, modificación o cancelación de los avisos de privacidad simplificado e integral de los Sistemas de Datos Personales correspondientes, a efecto de que se realice su registro.	STyDP, JDDPyAJ	Oficio de comunicación al INFO
A19	La STyDP, entrega a la persona Titular de la OTAIPDPyA, el proyecto de oficio de comunicación dirigido al INFO.	STyDP, Titular de la OTAIPDPyA	Oficio de comunicación al INFO.
A20	La persona Titular de la OTAIPDPyA revisa y, en su caso, valida y firma el oficio de comunicación al INFO, y entrega a la ST para continuar con el trámite..	Titular de la OTAIPDPyA, STyDP	Oficio de comunicación al INFO
A21	La STyDP, instruye la entrega del oficio ante el INFO y, mediante correo electrónico, establece comunicación con el Enlace de las AR´s , para comunicarles que dio aviso al INFO, respecto a la actualización, modificación o cancelación de los avisos de privacidad simplificado e integral de los Sistemas de Datos Personales a su resguardo.	STyDP, JDDPyAJ, Enlace del AR´S	Oficio de comunicación al INFO Correo electrónico
A22	Una vez que se recibe el acuse del oficio entregado al INFO, se entregan los acuses a las AR's y se guarda una copia como constancia en los archivos de la OTAIPDPyA, con la finalidad de llevar un control respecto de las actualizaciones a los avisos de privacidad simplificado e integral de los Sistemas de Datos Personales del Instituto Electoral.	OTAIPDPyA, STyDP, JDDPyAJ, AR´s	Documentos en los que consta la modificación a los avisos de privacidad simplificado e integral de los Sistemas de Datos

	La constancia junto con el acuse del oficio de comunicación al INFO, serán resguardados por la JDDPyAJ en los archivos de la OTAIPDPyA.		Personales correspondientes.
Fin de las actividades para la elaboración y/o actualización de los avisos de privacidad.			

9. Formatos

Código: SE/OTAIPDPyA/FR01

9.1. FORMATO DE AVISO DE PRIVACIDAD SIMPLIFICADO.

AVISO DE PRIVACIDAD SIMPLIFICADO

El Instituto Electoral de la Ciudad de México (IECM) a través de la (área administrativa que administra el SDP), es el Responsable del tratamiento de los datos personales que nos proporcione, los cuales serán protegidos en el Sistema de Datos Personales _____**.**

Los datos personales que recabemos, serán utilizados con la **finalidad siguiente** _____**,** **y** serán transferidos a: la Comisión de Derechos Humanos de la Ciudad de México para la investigación de quejas y denuncias por presuntas violaciones a los derechos humanos, Órganos Jurisdiccionales Locales para la sustanciación de los procesos tramitados ante ellos, Órganos de Control para la realización de auditorías o desarrollo de investigaciones por presuntas faltas administrativas, la Auditoría Superior de la Ciudad de México para el ejercicio de sus funciones de fiscalización, y el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México para la sustanciación de recursos de revisión, recurso de inconformidad, denuncias y el procedimiento para determinar el presunto incumplimiento a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, en el ámbito de sus atribuciones, de los cuales no se requiere el consentimiento del titular, al tener la facultad legal para ello, así como a los Órganos de Procuración y Administración de Justicia Federal y/o Local en el cumplimiento de sus atribuciones y competencias.

Este Sistema de Datos Personales cuenta con los Encargados siguientes: _____ (en caso de no contar con Encargados especificarlo); asimismo cuenta con el Despacho de Auditores Externos siguiente:

_____, (en su caso señalar que no se cuenta con Despacho de Auditores externos).

Usted podrá manifestar la negativa al tratamiento de sus datos personales directamente ante la Unidad de Transparencia del Instituto Electoral de la Ciudad de México, ubicada en la Calle de Huizaches No. 25, Colonia Rancho los Colorines, Planta Baja, Tlalpan, C. P. 14386, Ciudad de México, con número telefónico 55 5483 3800 extensión 4727 y correo electrónico unidad.transparencia@iecm.mx.

Para conocer el Aviso de Privacidad Integral puede acudir directamente a la Unidad de Transparencia o ingresar a la página: https://www.iecm.mx/proteccion-de-datos-personales/.

Fecha de última actualización: 00 de _____ de 20__.

Código: SE/OTAIPDPyA/FR02

FORMATO DE AVISO DE PRIVACIDAD INTEGRAL.

Aviso de Privacidad Integral

El Instituto Electoral de la Ciudad de México (IECM), a través de (área administrativa que administra el SDP), con domicilio en la Calle de Huizaches No. 25, Colonia Rancho los Colorines, Tlalpan, C. P. 14386, Ciudad de México, es el Responsable del tratamiento de los datos personales que nos proporcione, los cuales serán protegidos en el **Sistema de Datos Personales** _____, con fundamento en:

a) Constitución Política de los Estados Unidos Mexicanos, artículos 6, Apartado A, fracciones II y III y 16 segundo párrafo; publicada en el DOF el 5/02/1917. Última reforma el _____.

b) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículos 3 fracción II, 21, 22, 23, 24, 25, 26, 27 y 28; publicada en el DOF el 26/01/2017.

c) Ley General de Archivos, artículos 1, 2 fracción VI, 5, 6, 7, 74 fracciones III y IV, 116 y 120; publicada en el DOF el 15/06/2018;

d) Constitución Política de la Ciudad de México, artículos 7, Apartado E, numerales 2 y 4, y 50; publicada en la GOCDMX el 05/02/2017. Última reforma _____

e) Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, artículos 6 fracciones XII y XXII, 7 segundo párrafo, 21, 24 fracciones XVII y XXIII, 28, 186, 191, 193, 194 y 202; publicada en la GOCDMX el 6/05/2016. Última reforma el _____;

f) Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, artículos 12, 13, 14, 16, 17, 18, 19, 20, 21, 21 bis, 21 ter, 22, 23 fracción VI, 24, 25, 26, 36, 37 y 38; publicada en la GOCDMX el 10/04/2018. Última reforma el _____;

g) Ley de Archivos del Distrito Federal, aplicable para la Ciudad de México, artículos 1, 3 fracción V, 10, 11, 30 fracciones VI y VII, 31, 32, 33, 34, 35 fracción VIII, 37, 38 y 40; publicada en la GODF el 08/10/2008. Última reforma _____;

h) Código de Instituciones y Procedimientos Electorales de la Ciudad de México, (señalar los artículos específicos del área)_____; publicado en la GOCDMX el 07/06/2017. Última reforma _____;

i) Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, artículos 2 fracciones X y XII, 5,7, 8, 9, 10, 11, 12, 13, 16, 17, 18, 20, 21, 32, 33, 36, 37, 38, 39 y 41. Publicados en la GOCDMX el 23/09/2019;

j) Lineamientos o Reglamento para (en este apartado se mencionará la norma específica aplicable al área);

k) Reglamento Interior del Instituto Electoral de la Ciudad de México, (artículo específico del área); publicado en la GOCDMX el 16/08/2017. Última reforma _____;

l) Reglamento del Instituto Electoral de la Ciudad de México en materia de Protección de Datos Personales, artículos 1, 3, inciso c), fracciones I, VI, VII, VIII y XIX; 7, 8, 16, 18, 29, 32, 34, 56, 57, 62, 64, 67 y 68; publicado en la GOCDMX el 13/05/2019. Última reforma _____;

m) Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales; publicados en el DOF el 12/02/2018. Última reforma _____;

n) Lineamientos para la realización de verificaciones y auditorías en cumplimiento de los artículos 112, fracción IV y 116 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México; publicados en la GOCDMX el 08/10/2019. Última reforma _____;

o) Manual de Operación de la Unidad de Transparencia del Instituto Electoral de la Ciudad de México, numeral 9; aprobado por el Comité de Transparencia en su Tercera Sesión Ordinaria del 28/08/2017, Última reforma _____, y

p) Manual de Organización y Funcionamiento del Instituto Electoral de la Ciudad de México, páginas 534 a 549; Aprobado Mediante Acuerdo de la Junta Administrativa JA-106-16 el 15/09/2016. Última reforma mediante acuerdo _____, el _____.

q) Criterios para regular el bloqueo de la información, verificación y supresión de los sistemas de datos personales del Instituto Electoral de la Ciudad de México; aprobados por el Comité

de Transparencia mediante Acuerdo CT-IECM-10/2022, en la Quinta Sesión Ordinaria celebrada el 20/05/2022.

Los datos personales que recabemos serán utilizados con la **finalidad de** _____ _____**.**

Para la finalidad antes señalada se solicitarán los siguientes datos personales:

(En este apartado se enlistará las categorías de datos personales que se recaben, conforme a la categoría establecida en el artículo 62 de los Lineamiento Generales), a manera de ejemplo:

Datos identificativos.- _____

Datos laborales.- _____

Los cuales tendrán un **ciclo de vida de** _____ **años**

Usted podrá manifestar la negativa al tratamiento de sus datos personales y ejercer sus derechos de acceso, rectificación, cancelación u oposición, de sus datos personales (ARCO), así como la revocación del consentimiento directamente ante la Unidad de Transparencia del Instituto Electoral de la Ciudad de México, ubicada en la Calle de Huizaches No. 25, Colonia Rancho los Colorines, Planta Baja, Tlalpan, C. P. 14386, Ciudad de México, con número telefónico 55 5483 3800 extensión 4727, en el correo electrónico unidad.transparencia@iecm.mx, a través de la Plataforma Nacional de Transparencia (http://www.plataformadetransparencia.org.mx/), o bien mediante el número de TEL INFO 55 5636 4636.

Si desea conocer el procedimiento para el ejercicio de estos derechos puede acudir a la Unidad de Transparencia, enviar un correo electrónico a la dirección antes señalada o comunicarse al TEL-INFO 55 5636 4636.

El presente aviso de privacidad puede sufrir modificaciones, cambios o actualizaciones derivadas de nuevos requerimientos legales, de nuestras propias necesidades por los trámites y servicios

que ofrecemos, de nuestras prácticas de privacidad o por otras causas. Por lo anterior, nos comprometemos a informarle sobre los cambios que pueda sufrir el presente a través de la Unidad de Transparencia y en el Sitio de Internet https://www.iecm.mx/proteccion-de-datos-personales/.

Última fecha de actualización: 00 de _____ de 20__.

Contenido

1. Objetivo 2
2. Alcance 2
3. Marco normativo 2
4. Definiciones y Abreviaturas 3
5. Responsabilidades 6
6. Políticas de operación 8
7. Diagrama de flujo 11
8. Descripción de las actividades 12
9. Formatos 19

Control de Cambios

Revisión	Fecha	Descripción del Cambio
00	09 febrero 2023	Emisión del documento

1. Objetivo

Establecer las directrices para la creación, modificación o supresión de los Sistemas de Datos Personales del Instituto Electoral de la Ciudad de México; así como su registro ante el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, a fin de cumplir con las disposiciones normativas en materia de Datos Personales.

2. Alcance

El presente Manual es aplicable para la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo, así como para las distintas Áreas Responsables del Instituto Electoral de la Ciudad de México, para la creación, modificación o supresión de los Sistemas de Datos Personales institucionales:

- Presidencia;
- Oficinas de Consejeras y Consejeros Electorales;
- Secretaría Ejecutiva;
- Secretaría Administrativa;
- Contraloría Interna;
- Direcciones Ejecutivas;
- Unidades Técnicas; y
- Órganos Desconcentrados.

3. Marco normativo

- Constitución Política de los Estados Unidos Mexicanos;
- Constitución Política de la Ciudad de México;
- Código de Instituciones y Procedimientos Electorales de la Ciudad de México;
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Ley General de Archivos;
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;
- Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México,
- Ley de Archivos Local. Ley de Archivos, aplicable en la Ciudad de México;
- Reglamento Interior del Instituto Electoral de la Ciudad de México;
- Reglamento del Instituto Electoral de la Ciudad de México, en materia de Protección de Datos Personales;
- Reglamento de Funcionamiento del Comité de Transparencia del Instituto Electoral de la Ciudad de México;
- Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;
- Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales;

- Criterios para regular el bloqueo de la información, verificación y supresión de los Sistemas de Datos Personales del Instituto Electoral, y
- Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.

4. Definiciones y Abreviaturas

Acuerdo de creación: Documento mediante el cual se implementa un Sistema de Datos Personales del Instituto Electoral de la Ciudad de México, mediante su publicación en la Gaceta Oficial de la Ciudad de México.

Acuerdo de evaluaciones: Documento aprobado por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, mediante Acuerdo CONAIP/SNT/ACUERDO/ORD01-15/12/2017-06, por el que se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales; publicado en el Diario Oficial de la Federación el 28 de enero de 2018.

Acuerdo de modificación: Documento mediante el cual se reforma un Sistema de Datos Personales del Instituto Electoral de la Ciudad de México, mediante su publicación en la Gaceta Oficial de la Ciudad de México.

Acuerdo de supresión: Documento mediante el cual se elimina un Sistema de Datos Personales del Instituto Electoral de la Ciudad de México, al desaparecer la finalidad para la cual fue creado; lo anterior, mediante su publicación en la Gaceta Oficial de la Ciudad de México y, por lo tanto, la correspondiente cancelación de datos e inscripción de su registro.

AR´s: Cada una de las áreas administrativas del Instituto Electoral de la Ciudad de México que posea o administre bases de datos o Sistemas de Datos Personales, en términos de la legislación aplicable.

Bloqueo: Proceso para la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas o mediante el ejercicio de los Derechos ARCO. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y una vez transcurrido, se procederá a su cancelación o supresión definitiva, en la base de datos o sistema de datos personales que corresponda, debiendo observar los Criterios para bloqueo en los sistemas de datos personales.

Circular: Documento emitido por la Secretaría Ejecutiva, mediante el cual se solicita a las AR's la actualización de los Sistemas de Datos Personales, de conformidad con sus atribuciones.

Correo electrónico: Medio electrónico oficial, a través del cual la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo, los enlaces de las AR´s mantienen comunicación, respecto del envío, retroalimentación y publicación de las actualizaciones de los Sistemas de Datos Personales.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como: origen racial o étnico, estado de salud presente o futuro, información genética, información biométrica, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Disociación: Procedimiento mediante el cual los datos personales no pueden asociarse a la persona titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

Enlace: Persona designada en cada AR´s para la gestión y trámite en materia de datos personales.

Evaluación de impacto: Documento mediante el cual el Instituto Electoral pretenda poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos que comprometan el cumplimiento de los principios, deberes y derechos de las personas titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

Gaceta: Gaceta Oficial de la Ciudad de México.

INFO: Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

Informe de Exención: Documento mediante el cual, el Responsable del Sistema de Datos Personales dentro de los 30 días posteriores a la puesta en operación o modificación de la política pública, programa, sistema, plataforma electrónica o cualquier otra que implique un tratamiento intensivo o relevante de datos personales; de manera fundada y motivada hace constar las razones de emergencia, por las cuales no realizó la evaluación de impacto en la protección de datos personales.

Instituto Electoral: Instituto Electoral de la Ciudad de México.

JDDPyAP: Jefatura de Departamento de Datos Personales y Apoyo Jurídico adscrita a la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo.

Ley de Datos: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Lineamientos Generales de Datos: Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

OTAIPDPyA: Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral de la Ciudad de México, a la cual también se le denominará indistintamente como Unidad de Transparencia.

Oficial de Protección de Datos Personales: Persona servidora pública especialista en materia de datos personales, designada por el responsable del Instituto Electoral, adscrita a la Unidad de Transparencia; quien coordina las actividades para atender los asuntos relacionados con la protección de datos personales.

Oficio de respuesta: Documento a través del cual las AR's comunican a la OTAIPDPyA la respuesta a la Circular de actualización de los Sistemas de Datos Personales.

Oficio de comunicación al INFO: Documento a través del cual la OTAIPDPyA comunica al INFO la inscripción de los Sistemas de Datos Personales institucionales en el Registro Electrónico de Sistemas de Datos Personales y su correspondiente publicación en la Gaceta.

RESDP: Registro Electrónico de Sistemas de Datos Personales es una aplicación informática desarrollada por el Instituto de Transparencia, para la inscripción de los sistemas de datos personales en posesión de los sujetos obligados para su custodia y protección.

Responsable del Sistema de Datos Personales: Persona servidora pública del Instituto Electoral, con el cargo de titular del área que administra el sistema de datos personales; que decide y determina la finalidad, fines, medios, medidas de seguridad y todo aquello relacionado con el tratamiento de datos personales.

SDP: Sistema de Datos Personales.

SE: Secretaría Ejecutiva.

STyDP: Subdirección de Transparencia y Datos Personales, adscrita a la Oficina de Transparencia, Acceso a la Información Pública Datos Personales y Archivo del Instituto Electoral de la Ciudad de México.

Supresión: Eliminación, borrado o destrucción de los SDP o de datos personales de una persona física, bajo las medidas de seguridad previamente establecidas por el responsable, una vez que ha cumplido con la finalidad y el dato personal ha cumplido con su ciclo de vida.

Titular de la Oficina: Titular de la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral, también denominada Unidad de Transparencia.

Tratamiento intensivo o relevante de datos personales: Cuando se está ante la presencia de alguno de los supuestos y condiciones establecidos en los artículos 68 de la Ley de Datos; 8 y 9 del Acuerdo de evaluaciones.

Usuario: Personas autorizadas por el responsable, adscritas al área del Instituto Electoral que dé tratamiento, tenga acceso a los datos personales y a los sistemas de datos personales.

5. Responsabilidades

OTAIPDPyA	• Generar de manera semestral, el proyecto de Circular que suscriba la Secretaría Ejecutiva, en la que se solicite a las diversas AR´s del Instituto Electoral la actualización de los SDP, en cuanto a la creación, modificación o supresión. Dicha Circular deberá **elaborarse y distribuirse 15 días hábiles antes de la conclusión de cada semestre.** • Asesorar permanentemente a las AR's en materia de datos personales y coordinar con los Enlaces, para llevar a cabo la creación, modificación, actualización o supresión de los SDP. • Implementar acciones para el cumplimiento de las obligaciones en materia de datos personales, para lo cual, tendrá la facultad de validar, o solicitar adecuaciones a los Acuerdos de creación, modificación o supresión de SDP, conforme a la normatividad aplicable, previo a su publicación en la Gaceta. • Revisar y validar la información remitida por las AR's correspondiente a los Acuerdos de creación, modificación o supresión de los SDP, de conformidad con la Ley de Datos y los Lineamientos Generales. • Coordinar y supervisar la publicación en la Gaceta de los Acuerdos de creación, modificación o supresión de SDP, que para tal efecto remitan las AR´s. • Registrar ante el INFO la creación de SDP; así como las modificaciones o supresiones de los mismos. • Asesorar a las AR´s en los casos en los que se requiera la Evaluación de Impacto. • Tramitar ante el INFO las Evaluaciones de impacto, en términos de lo dispuesto en los artículos 69 y 71 de la Ley de Datos y conforme al procedimiento establecido en el Acuerdo de evaluaciones.

AR´s	• Enviar semestralmente a la OTAIPDPyA el reporte de actualización de los SDP, para su debida creación, modificación o supresión correspondiente. • Administrar adecuadamente los SDP bajo su custodia. • Dar seguimiento a la correcta publicación de los Acuerdos de creación, modificación o supresión de SDP, en la Gaceta; así como su inscripción en el RESDP. • Garantizar el correcto bloqueo de datos personales previo a la supresión de SDP, de conformidad con el procedimiento que para tal efecto se establece en los Criterios para regular el bloqueo de la información, verificación y supresión de los sistemas de datos personales del Instituto Electoral de la Ciudad de México. • Elaborar, las Evaluaciones de impacto, conforme a los requisitos establecidos en el Acuerdo de evaluaciones. • Solicitar opinión técnica al Oficial de protección de datos personales, respecto del tratamiento intensivo o relevante de datos, conforme a sus atribuciones.
Oficial de Protección de Datos Personales	• Asesorar a las AR's en materia de protección de datos personales. • Opinar, previo a su publicación en la Gaceta, sobre los Acuerdos de creación, modificación o supresión de SDP. • Emitir opinión y consideraciones técnicas respecto al tratamiento intensivo o relevante de datos personales. • Plantear, en su caso, recomendaciones que permitan mitigar y reducir la generación de los impactos y riesgos que se detecten en materia de protección de datos personales. • Formular dictámenes, opiniones técnicas y cualquier otro documento que se considere necesario para atender los asuntos en materia de protección de datos personales. • Proponer a la OTAIPDPyA los procedimientos internos para la gestión de las solicitudes para el ejercicio de derechos ARCO.

6. Políticas de operación

- Toda creación, modificación o supresión de SDP sólo podrá efectuarse mediante Acuerdo emitido por la persona titular de la Secretaría Ejecutiva y publicado en la Gaceta.
- Previo a la creación o modificación del SDP, deberá publicarse el Acuerdo respectivo en la Gaceta, y notificar al INFO dentro **de los 10 días hábiles siguientes a su publicación.**
- Queda prohibida la creación de SDP que tengan como finalidad tratar datos personales sensibles.
- Los datos personales sensibles solo podrán ser tratados cuando medien razones de interés general, así lo disponga una ley, exista el consentimiento expreso, inequívoco, libre e informado de la persona Titular, con fines estadísticos o históricos siempre y cuando se elabore previamente el proceso de disociación. El único caso en que no será necesario el consentimiento de su titular, será cuando se trate de estudios científicos o de salud pública.
- En los Acuerdos de creación y/o modificación que implique un tratamiento intensivo o relevante de datos personales, se elaborará la Evaluación de impacto correspondiente y presentará ante el INFO, al menos, **treinta días hábiles anteriores** a la fecha en que se pretenda poner en operación o modificar la política pública, programa o sistema informático, en cumplimiento a lo establecido en el Acuerdo de evaluaciones.
- Las Evaluaciones de impacto en materia de datos personales, deberán realizarse conforme a lo establecido en el capítulo III del Acuerdo de evaluaciones y contendrán al menos, la información siguiente: descripción de la política pública, programa o sistema informático, justificación de la necesidad de implementar o modificar la política o el sistema, el ciclo de vida de los datos personales; identificación, análisis y descripción de la gestión de riesgos para la protección de datos personales, análisis de cumplimiento normativo, resultados de consultas externas, opinión técnica del oficial de protección de datos personales y cualquier otro documento que se considere conveniente hacer del conocimiento del INFO.
- El responsable solo quedará exento de presentar la evaluación de impacto en la protección de datos personales, cuando se trate de una situación de emergencia o urgencia en los términos establecidos en la Ley de Datos y Acuerdo de evaluaciones.
- Tratándose de lo anterior, el responsable deberá presentar un informe de exención ante el INFO, **durante los treinta días hábiles posteriores** a la fecha de la puesta en operación o modificación de la política pública, programa o sistema informático.

- Los Informes de exención de Evaluación de impacto, deberán elaborarse conforme al procedimiento establecido en el capítulo V del Acuerdo de evaluaciones y contendrán al menos los siguientes elementos: denominación, objetivos generales y específicos, finalidades del tratamiento, razones o motivos que permitieron determinar que la evaluación de impacto en la protección de datos personales compromete los efectos de la política pública, las consecuencias negativas que se derivarían de la elaboración y presentación, fundamento legal para el tratamiento de datos personales, fecha de operación o modificación del SDP, opinión técnica del oficial de Datos y los mecanismos o procedimientos adoptados por el responsable para que la política pública o el programa, cumpla desde su diseño con las obligaciones previstas en la Ley de Datos.
- Toda creación, modificación, actualización, supresión de un SDP, deberá inscribirse en el RESDP, **dentro de los diez días hábiles siguientes a su publicación en la Gaceta.**
- Los Acuerdos de supresión de SDP, siempre considerarán la finalidad, el destino, ciclo vital de los datos personales y, en su caso, las previsiones adoptadas para su destrucción. Asimismo, se publicarán en Gaceta, **al menos 30 días hábiles previos a la supresión del SDP** y se notificará al INFO dentro de **los diez días hábiles siguientes de su publicación**, para que proceda a la cancelación de su inscripción en el registro correspondiente.
- No será procedente la supresión de SDP, cuando exista previsión expresa en una Ley que exija su conservación.
- En la supresión de SDP, el Responsable deberá establecer las políticas, y técnicas atinentes, de tal manera que sea imposible la probabilidad de recuperarlos y reutilizarlos.
- El Responsable de los SDP al momento de establecer las políticas para la supresión de datos personales, tomará en cuenta al menos los elementos siguientes: que el procedimiento utilizado no permita recuperar datos; que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad; que el método utilizado produzca el mínimo de desperdicios que afecten el medio ambiente.

6.1 Políticas de operación específicas para la elaboración de Acuerdos de creación, modificación o supresión de SDP:

- En los Acuerdos de creación o modificación de SDP deberá incluirse al menos los siguientes datos:
    - ✓ Identificación del Sistema, se deberá indicar denominación, finalidad, normativa aplicable y transferencias;
    - ✓ Personas físicas o grupos de personas de las que se recabarán o tratarán los datos personales;

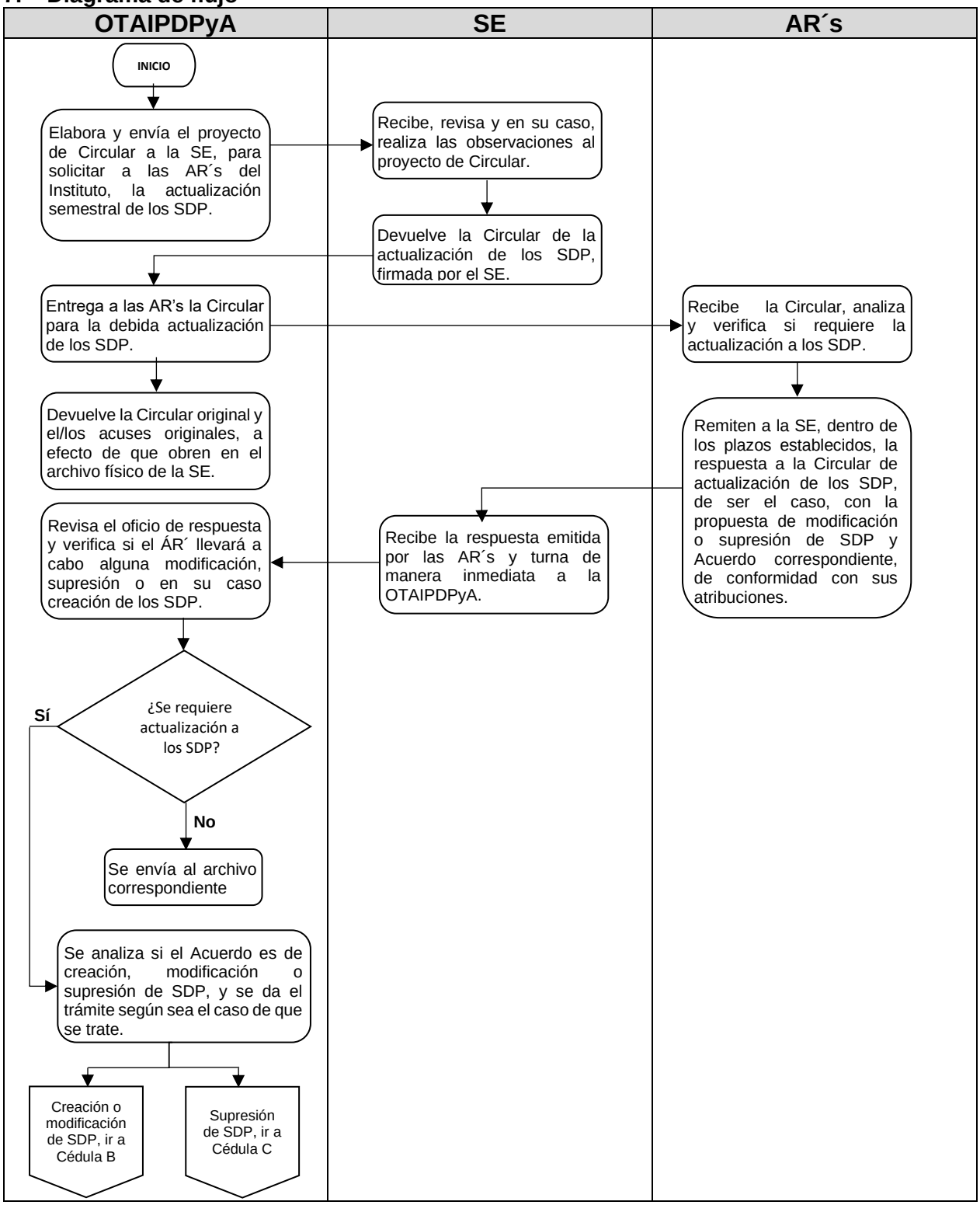
- ✓ Estructura básica del SDP, la descripción de los tipos y categorías de datos;
- ✓ AR´s del tratamiento del SDP; Titular del Instituto Electoral, usuarios y encargados, si los hubiera.
- ✓ Áreas ante las que se podrán ejercer los Derechos de Acceso, Rectificación, Cancelación y Oposición de Datos Personales, domicilio oficial y dirección electrónica de la OTAIPDPyA;
- ✓ Procedimiento a través del cual podrán ejercerse los derechos de Acceso, Rectificación, Cancelación y Oposición de Datos Personales;
- ✓ Nivel de seguridad y mecanismos de protección;

- Para los Acuerdos de supresión de SDP además de los datos precedentes, debe tomarse en consideración el ciclo vital del dato personal, la finalidad y destino, en su caso las previsiones adoptadas para su destrucción; así como el procedimiento establecido en los Criterios para regular el bloqueo de la información, verificación y supresión de los Sistemas de Datos Personales del Instituto Electoral.

  En la destrucción de datos personales podrán ser excluidos aquellos que no se opongan a las finalidades originales, como son procesos de disociación, finalidades históricas, estadísticas o científicas.

- Todos los Acuerdos de creación, modificación o supresión de SDP deben ser publicados en la Gaceta, conforme a los requisitos y características establecidos para ello por la Consejería Jurídica y de Servicios Legales del Gobierno de la Ciudad de México. Por lo anterior, las AR´s deberán prever los recursos para el pago respectivo a la inserción y publicación.

7. Diagrama de flujo



8. Descripción de las actividades

A. Actividades generales para la creación, modificación o supresión de SDP			
#	**Actividad**	**Área responsable**	**Documento empleado**
A1	Elabora y envía el proyecto de Circular a la Secretaría Ejecutiva, para solicitar a las distintas AR´s del Instituto Electoral, la actualización semestral de los SDP; de conformidad con sus atribuciones. Dicho documento establece la fecha límite para la respuesta y actualización de los SDP.	OTAIPDPyA´, STyDP, JDT	Proyecto de Circular.
A2	Recibe, revisa y en su caso, realiza las observaciones al proyecto de Circular enviado por la OTAIPDPyA, para la actualización semestral de los SDP.	SE.	Proyecto de Circular.
A3	Devuelve la Circular firmada por el SE, para su distribución entre las distintas AR's del Instituto Electoral.	SE.	Circular.
A4	Se entrega a las diversas AR's la Circular para la actualización de los SDP.	STyDP, JDT.	Circular (copia).
A5	Recibe la Circular, analiza y verifica si los SDP requieren de actualización.	AR´s	Circular (copia).
A6	Devuelve a la SE y el/los Acuses originales de la notificación de la Circular de actualización de los SDP a las AR´s, a efecto de que obren en el archivo físico de la SE.	OTAIPDPyA JDT	Circular original y Acuses.
A7	Remiten a la SE, dentro de los plazos establecidos, la respuesta a la Circular de actualización de los SDP, de ser el caso, con la propuesta de modificación o supresión de SDP y Acuerdo correspondiente, de conformidad con sus atribuciones.	AR´s.	Oficio de respuesta a la Circular y de ser el caso el Acuerdo correspondiente.
A8	Recibe, dentro de los plazos establecidos, la respuesta de las AR´s a la Circular de actualización de los SDP, y turna inmediatamente a la OTAIPDPyA.	SE.	Oficio de respuesta a la Circular y de ser el caso el Acuerdo correspondiente.

A9	Revisa el oficio de respuesta recibido y verifica si las AR's, proponen la creación, modificación o supresión de SDP.	STyDP	Oficio de respuesta a la Circular y de ser el caso el Acuerdo correspondiente.
A10	Determina si: ¿Se llevará a cabo alguna actualización a los SDP? **No.** Procede su envío al archivo correspondiente. **Sí.** Analiza si el proyecto de Acuerdo es de creación, modificación o supresión de SDP, y ordena el trámite según el supuesto.	STyDP	Oficio de respuesta a la Circular y de ser el caso el Acuerdo correspondiente.
Fin de las actividades generales para la creación, modificación o supresión de SDP.			

B. Actividades para la creación o modificación de SDP que no requieren Evaluación de impacto.			
#	**Actividad**	**Área responsable**	**Documento empleado**
B1	Procede de la Actividad **A10**. Determina la procedencia de la creación, modificación o actualización de los SDP. **SI.** Continúa en la actividad B2	Titular de la OTAIPDPyA, STyDP, JDT, Enlace de AR.	Documentación empleada en numerales 1 al 10 del apartado A
B2	La OTAIPDPyA verifica con las AR´S que el proyecto de Acuerdo propuesto sea previo a la creación o modificación del SDP, al menos treinta días antes de la creación o modificación del SDP.	STyDP, JDT	Oficio de respuesta a la Circular y la propuesta de Acuerdo de creación o modificación del SDP correspondiente.
B3	Verifica que el Acuerdo contenga todos los elementos establecidos tanto en la Ley de Datos como en los Lineamientos Generales de Datos y que cumpla con el formato para la creación o modificación del SDP. ¿El Acuerdo cuenta con todos los elementos? **NO.** Se regresa el proyecto de Acuerdo a las AR´s de la creación o modificación del SDP, con las observaciones, a efecto de que realicen las modificaciones correspondientes. **SI.** Continúa en la actividad B4	STyDP, JDT	Acuerdo de creación o modificación y correo electrónico

B4	Una vez que se ha verificado que el proyecto de Acuerdo cumple con los requisitos establecidos en la Ley de Datos y los Lineamientos Generales de Datos, analiza si la creación o modificación del SDP, requiere la evaluación de impacto. **NO.** Continúa con la actividad B5 **SI.** Continúa en la actividad B16.	STyDP, JDT, Enlace del AR´s	Acuerdo de creación o modificación
B5	La JDDPyAJ, elabora proyecto de oficio para firma de la SE, para solicitar la publicación del Acuerdo en Gaceta.	JDDPyAJ	Oficio de turnado para publicación
B6	La STyDP, revisa y, en su caso, valida el oficio y turna al Titular de la OTAIPDPyA, para el trámite correspondiente.	STyDP Titular de la OTAIPDPyA	Oficio de turnado para publicación
B7	La SE, firma el oficio y ordena trámite para la publicación en Gaceta.	SE	Oficio de turnado para publicación
B8	La JDDPyAJ da seguimiento a la publicación en Gaceta del Acuerdo de creación o modificación del SDP y una vez que ha sido publicado, **a más tardar al día hábil siguiente de su publicación,** mediante correo electrónico notifica a las AR´s competentes para que realicen el registro correspondiente en el RESDP.	JDDPyAJ	Correo electrónico
B9	El Enlace de las AR´s dispondrá de **cinco días hábiles contados a partir del día siguiente de la recepción del correo electrónico,** para llevar a cabo el registro en el RESDP y comunicar mediante correo electrónico a la OTAIPDPyA, que ha efectuado el registro correspondiente.	Enlace del AR´s	Correo electrónico
B10	La JDDPyAJ, **al momento de recibir la notificación**, **contará con un día hábil a partir de la recepción del correo electrónico para** revisar el RESDP, y verificar la correcta inscripción del SDP y lo comunica de inmediato a la STyDP	JDDPyAJ	Registro del RESDP
B11	La STyDP de manera inmediata valida la inscripción del SDP en el RESDP e instruye se elabore oficio de comunicación al INFO.	STyDP, JDDPyAJ	Registro del RESDP
B12	La JDDPyAJ dentro del término de los **diez días hábiles siguientes a la publicación en Gaceta,** elabora el proyecto de oficio comunicando al INFO, la creación o modificación del SDP y su inscripción en el RESDP, y lo turna para su revisión.	JDDPyAJ	Proyecto de Oficio de comunicación al INFO

B13	La STyDAP revisa el oficio, valida los Anexos y presenta al Titular de la OTAIPDPyA para firma,	STyDP	Proyecto fr. Oficio de comunicación al INFO y anexos, Publicación en Gaceta Acuse de inscripción en el RESDP
B14	La persona Titular de la OTAIPDPyA revisa el oficio y anexos, en su caso, firma el oficio para su trámite ante el INFO.	Titular de la OTAIPDPyA	Oficio de comunicación al INFO y anexos, Publicación en Gaceta Acuse de inscripción en el RESDP
B15	La STyDP gestiona la entrega del oficio ante el INFO y en su oportunidad ordena archivar el acuse respectivo.	STyDP	Oficio de comunicación al INFO, Publicación en Gaceta Acuse de inscripción en el RESDP
Fin de las actividades para la creación o modificación de un SDP que no requiere evaluación de impacto.			
Actividades para la creación o modificación de SDP que requieren Evaluación de impacto			
B16	Una vez analizado el Acuerdo de creación o modificación del SDP, determina que es necesario que el Responsable del SDP, elabore la Evaluación de impacto, con apoyo de la OTAIPDPyA.	OTAIPDPyA., STyDP, JDDPyAJ, AR´S	Correo electrónico
B17	El Enlace de la AR´s, con asesoría del Oficial de Protección de Datos Personales elabora el proyecto de Evaluación de impacto, de conformidad con el presente Manual y el Acuerdo de Evaluaciones, lo presenta ante el Responsable del SDP para su visto bueno.	Enlace del AR´S, Responsable del SDP Oficial de Protección de Datos Personales	Proyecto de evaluación de impacto Acuerdo de Evaluaciones
B18	El Responsable del SDP, en su caso, otorga su visto bueno, firma y turna mediante oficio a la OTAIPDPyA	Enlace del AR´S	Proyecto de Evaluación de impacto
B19	La OTAIPDPyA recibe oficio y proyecto de Evaluación de impacto y turna al Oficial de Protección de Datos Personales para que emita opinión técnica respecto del tratamiento intensivo o relevante de datos personales, y a la ST, para su revisión y seguimiento.	OTAIPDPyA	Proyecto de Evaluación de Impacto

B20	Emite opinión y consideraciones técnicas sobre tratamiento intensivo o relevante de datos personales y remite a la ST.	Oficial de Protección de Datos Personales	Opinión técnica Acuerdo de Evaluaciones
B21	La STyDP revisa que la opinión técnica y el proyecto de Evaluación de Impacto cumplan con los requisitos establecidos en el Acuerdo de evaluaciones y en su caso, emite observaciones y presenta al Titular de la OTAIPDPyA.	ST	Proyecto de Evaluación de Impacto
B22	La persona Titular de la OTAIPDPyA, revisa y, en su caso, valida el documento, firma y ordena el trámite correspondiente.	Titular de la OTAIPDPyA	Evaluación de impacto.
B23	La STyDP, gestiona ante el INFO la entrega de la evaluación de impacto, al menos **treinta días anteriores a la fecha en que pretenda poner en operación o modificar la política pública, programa o sistema informático** y da seguimiento al dictamen que al efecto emita el INFO.	STyDP, JDDPyAJ	Evaluación de impacto
B24	Una vez que la OTAIPDPyA, reciba el dictamen del INFO, podrá dar continuidad al trámite de la creación y/o modificación del SDP conforme a la actividad **B5 a B15.**	OTAIPDPyA	Dictamen del INFO
Fin de actividades relacionadas con la creación o modificación de SDP, que requieren Evaluación de impacto.			

C. Actividades para la supresión de SDP.			
#	**Actividad**	**Área responsable**	**Documento empleado**
C1	Procede de la Actividad **A10**.	JDDPyAJ	Documentación empleada en numerales 1 al 10 del apartado A
C2	La actualización de los SDP, consiste en la supresión de un SDP. **SI.** Continúa en la actividad C3.	Titular de la OTAIPDPyA, STyDP, JDDPy AJ, Enlace de AR.	Documentación empleada en numerales 1 al 10 del apartado A
C3	La OTAIPDPyA verifica con el AR´S que no se suprima ni cancele ningún dato personal, ya que primero deberá emitirse el Acuerdo de supresión y publicar en la Gaceta, al menos treinta días hábiles previos a la supresión del Sistema de que se trate. Para tal efecto, deberá además llevarse a cabo el procedimiento que se establece en los Criterios para regular el bloqueo de la información, verificación y	STyDP, JDDPyAJ, Enlace del AR´S	Oficio de respuesta a la Circular y la propuesta de Acuerdo de supresión del SDP correspondiente.

	supresión de los Sistemas de Datos Personales del Instituto Electoral, y		
C4	Verifica que el proyecto de Acuerdo contenga todos los elementos señalados tanto en la Ley de Datos como en los Lineamientos Generales de Datos y que cumpla con el formato para la supresión del SDP. ¿El Acuerdo cuenta con todos los elementos? **NO.** Se regresa al AR´s responsable de la supresión del SDP, con las observaciones, a efecto de que lleve a cabo las modificaciones correspondientes. **SI.** Continúa en la actividad C5.	STyDP, JDDPyAJ	Proyecto de Acuerdo de supresión y correo electrónico
C5	Una vez verificado que el Acuerdo cumple con los requisitos señalados en la Ley de Datos y en los Lineamientos Generales de Datos; así como el destino de los datos contenidos en el SDP y las previsiones adoptadas para su destrucción, la JDDPyAJ elabora el proyecto de oficio para firma de la persona Titular de la SE, para su publicación en Gaceta.	STyDP, JDDPyAJ, Enlace del AR´s	Acuerdo de supresión, Proyecto de oficio para publicación en Gaceta.
C6	La ST, revisa el oficio y en su caso lo turna a la persona Titular de la OTAIPDPyA, para el trámite correspondiente.	ST Titular de la OTAIPDPyA,	Oficio de turnado para publicación
C7	La persona Titular de la OTAIPDPyA,, revisa y, en su caso, valida el oficio para publicación en Gaceta y lo entrega a la SE, para el trámite correspondiente.	Titular de la OTAIPDPyA,	Oficio de turnado para publicación
C8	La SE, firma el oficio y ordena el trámite para publicación en Gaceta.	SE	Oficio de turnado para publicación
C9	La JDDPyAJ da seguimiento a la publicación en Gaceta del Acuerdo de supresión del SDP y una vez publicado, inmediatamente comunica a la STyDP, con la finalidad de continuar el trámite de supresión.	JDDPyAJ	Comunicado verbal
C10	La STyDP instruye elaborar el oficio de comunicación al INFO, para que **dentro de los diez días hábiles siguientes a la publicación en Gaceta,** se notifique la supresión del SDP, a efecto de que se realice la cancelación en el RESDP.	JDDPyAJ, STyDP	Oficio de comunicación al INFO

C11	La STyDP entrega a la persona Titular de la OTAIPDPyA, el proyecto de oficio de comunicación dirigido al INFO.	STyDP, Titular de la OTAIPDPyA	Oficio de comunicación al INFO.
C12	La persona Titular de la OTAIPDPyA revisa y, en su caso, valida y firma el oficio de comunicación al INFO, y entrega a la STyDP para continuar con el trámite de supresión de SDP.	Titular de la OTAIPDPyA, STyDP	Oficio de comunicación al INFO
C13	La STyDP instruye la entrega del oficio ante el INFO y, mediante correo electrónico, establece comunicación con el Enlace del AR´s, para continuar con el trámite de supresión del SDP.	STyDP, JDDPyAJ, Enlace del AR´S	Oficio de comunicación al INFO Correo electrónico
C14	El Enlace del AR´s coordina la supresión del SDP y elabora constancia donde de manera fundada y motivada expone los motivos por los cuales se suprime el SDP, precisa los datos personales que se recabaron, finalidad y periodo de vigencia del sistema. Dicha constancia será firmada por el Responsable del SDP, la persona Titular de la OTAIPDPyA, y el representante de la Contraloría Interna	Enlace AR´s, Titular de la OTAIPDPyA, Representante de la Contraloría Interna y	Constancia de supresión de SDP
C15	Una vez que realizada la supresión del SDP y firmada la Constancia correspondiente, el original formará parte de los archivos del AR´S que suprimió el SDP, y entregará una copia a la OTAIPDPyA.	Enlace AR´S	Constancia de supresión de SDP
C16	La constancia junto con el acuse del oficio de comunicación al INFO, serán resguardados por la JDDPyAJ en los archivos de la OTAIPDPyA	JDDPyAJ	Documentos en los que consta la supresión del SDP
Fin de la Actividad para la supresión de SDP			

9. Formatos

Código: SE/OTAIPDPyA/FR03

9.1 Formato para elaborar Acuerdo de creación de SDP (ANEXO A)

MODELO DE ACUERDO DE CREACIÓN DE SDP.

ACUERDO POR EL QUE SE CREA, EL "SISTEMA DE DATOS PERSONALES _____ (COLOCAR LA DENOMINACIÓN)

Nombre de la persona titular de la Secretaría Ejecutiva, fundamento legal que faculta para realizar publicaciones en Gaceta y/o actos jurídicos]..

En este apartado, se debe desarrollar el fundamento legal que confiere la facultad para realizar la publicación en Gaceta Oficial de la CDMX, se recomienda referir atendiendo a la jerarquía normativa (Constitución, Ley, Reglamento, etc.).

CONSIDERANDOS

Los Considerandos son la justificación o razones jurídicas, en la cual se describe el motivo de la creación, la facultad que tiene el Responsable del Sistema de Datos Personales para recabar y tratar los datos personales, de acuerdo con sus atribuciones.

Se sugiere que los Considerandos se estructuren de forma individual, es decir, por cada normativa y artículo en orden de relevancia, exponiendo con precisión el contenido de los artículos.

En caso de requerir la Creación de varios SDP, es recomendable exponer las consideraciones por las cuales es necesaria la creación de cada Sistema, y referir la facultad de las AR´s para tratar datos personales.

- Los siguientes **Considerandos** se sugieren como sustento en materia de datos personales; adicionalmente deberán describir la(s) facultad (es) legal(es) del Responsable del SDP para tratar datos personales:

1. Que el 20 de julio de 2007 se publicó en Diario Oficial de la Federación la reforma al artículo 6 apartado A fracción II de la Constitución Política de los Estados Unidos Mexicanos, el cual establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

2. Que el 1º de junio de 2009 se publicó en Diario Oficial de la Federación la reforma al artículo 16 párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, la cual señala que toda persona tiene el derecho humano a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición.

3. Que el 5 de febrero de 2017 se publicó en la Gaceta Oficial de la Ciudad de México el Decreto por el que se expidió la Constitución Política de la Ciudad de México (Constitución Local), que en su artículo 7, apartado E, numerales 2, 3 y 4, estableció el deber de proteger la información que se

refiera a la privacidad y los datos personales, en los términos y con las excepciones previstas en la Constitución Federal y las leyes; asimismo prohibió cualquier injerencia arbitraria, oculta o injustificada en la vida de las personas y dispuso que toda persona tiene derecho al acceso, rectificación y cancelación de sus datos personales y a manifestar su oposición respecto del tratamiento de los mismos. Su manejo se regirá por los principios de veracidad, licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

4. Que la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (Ley de Datos local), en su artículo 3 fracción XXIX define a los Sistema de Datos Personales como el conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de los Sujetos Obligados, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

5. Que el artículo 9 de la Ley de Datos local, establece que el Responsable del tratamiento de Datos Personales observará los principios de: calidad, confidencialidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad, transparencia y temporalidad.

6. Que en términos del artículo 36 de Ley de Datos local, la o el Titular de los Sujetos Obligados en su función de Responsable del tratamiento de datos personales, conforme a su respectivo ámbito de competencia, determinará la creación, modificación o supresión de los Sistemas de Datos Personales.

7. Que de acuerdo a lo establecido en el artículo 37 fracción I de la Ley de Datos local y 63 primer párrafo de los Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (Lineamientos Generales de Datos local), la creación, modificación o supresión de los Sistemas de Datos Personales se efectuará mediante Acuerdo emitido por la persona Titular del Sujeto Obligado, o en su caso el órgano competente, y publicado en la Gaceta Oficial de la Ciudad de México.

8. Que el mismo artículo 37 en su fracción II de la Ley de Datos en concordancia con el 64 de los Lineamientos Generales de Datos local, establecen el contenido mínimo de los Acuerdos de Creación y Modificación de los Sistemas de Datos Personales.

9. Que en cumplimiento al artículo 63 segundo párrafo de los Lineamientos Generales de Datos local, se establece que en los casos de creación y modificación, el Acuerdo deberá dictarse y publicarse previamente a la Creación o modificación del Sistema de Datos Personales correspondientes y ser notificado al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO) dentro de los diez días siguientes a su publicación.

10. Que el artículo 23 fracción XIII de la Ley de Datos Local, señala que el Responsable para cumplir con el tratamiento lícito, transparente y responsable de los datos personales, tendrá el deber de registrar ante el INFO los Sistemas de Datos Personales, así como la modificación o supresión de los mismos.

Por los anteriores Considerandos, se emite el presente (redacción opcional):

ACUERDO POR EL QUE SE CREA, EL "SISTEMA DE DATOS PERSONALES (COLOCAR LA DENOMINACIÓN)

Ejemplo:

ACUERDO POR EL QUE SE **CREA** EL "SISTEMA DE DATOS PERSONALES DE **[nombre del Sistema]** DEL INSTITUTO ELECTORAL DE LA CIUDAD DE MÉXICO"

[PUNTOS DE ACUERDO]-

ÚNICO/PRIMERO. Se crea el sistema de datos personales [Anotar nombre del sistema], para quedar como se establece a continuación:

- En caso de contemplar distintos Sistemas, se sugiere estructurar de la siguiente forma:

PRIMERO. Se crea el Sistema de Datos Personales denominado (nombre del sistema 1):

SEGUNDO. Se crea el Sistema de Datos Personales denominado (nombre del sistema 2):
…

Así sucesivamente con los Sistemas de Datos se quieran incluir en el Acuerdo.

A) Finalidad o finalidades y usos previstos:

Describir la finalidad o finalidades que sustentan el tratamiento de datos personales y los usos previstos.

Para la identificación de la finalidad y usos de un Sistema de Datos Personales se deberá responder los siguientes cuestionamientos:

- ✓ ¿De quién se obtienen los Datos Personales?
- ✓ ¿Por qué realizó la acción que involucra el tratamiento de Datos Personales?
- ✓ ¿Para qué voy a utilizar los datos y que voy a generar con ellos?

B) Normativa aplicable:

Se describe toda aquella legislación a manera de lista y sin artículos, que faculte al Responsable del Sistema para recabar y tratar datos personales, contemplando lo siguiente:

- ✓ La **normativa específica** del Sujeto Obligado en la que se señalan las facultades o atribuciones del Responsable del Sistema para el tratamiento de los Datos Personales.
- ✓ La **normativa que sustenta** el derecho a la protección de datos personales (Constitución Federal, Constitución Local, Ley de Datos, Lineamientos de Datos, Ley de Transparencia, Ley de Archivos); se recomienda utilizar la jerarquía normativa (Constitución, Ley, Reglamento, etc.)
- ✓ Verificar las fechas de las últimas reformas y nomenclatura Distrito Federal/CDMX.

C) Transferencias:

De conformidad con el artículo 64 de la Ley de Datos local, el responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento de la persona titular, en los siguientes supuestos:

I. Cuando la transferencia esté prevista en esta Ley u otras leyes, convenios o Tratados Internacionales suscritos y ratificados por México;

II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;

IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;

V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;

VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y la persona titular;

VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés de la persona titular, por el responsable y un tercero; y

VIII. Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento de la persona titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 16 de la presente Ley.

En ese sentido, a continuación, de manera enunciativa, se enlistan las instituciones a las cuales se podrán realizar transferencias:

- ✓ Comisión de Derechos Humanos de la Ciudad de México
- ✓ Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México
- ✓ Órganos Jurisdiccionales Locales y Federales
- ✓ Órganos de Control
- ✓ Auditoría Superior de la Ciudad de México
- ✓ Órganos de procuración o administración de Justicia

D) Personas físicas o grupos de personas sobre las que se recaben o traten datos personales:

En este rubro se describirá a personas de los cuales se obtienen los datos personales que se dará tratamiento, es decir, ¿De quién se recaban los datos? de conformidad con el artículo 2 fracción II de la Ley de Datos Local, el cual señala que el objetivo de ésta, es garantizar el tratamiento de los datos personales de toda persona física por parte de los Sujetos Obligados de la Ciudad de México sea lícito.

E) Estructura Básica del Sistema de Datos Personales y la descripción de los tipos de datos incluidos:

- ✓ **Datos identificativos:**
- ✓ **Datos electrónicos:**
- ✓ **Datos académicos:**

De conformidad con en el artículo 62 de los Lineamientos Generales de Datos, se sugiere revisar que los datos que se recaben se cataloguen conforme a lo establecido en el citado artículo, de igual manera, los datos que se recaben, deben coincidir con la finalidad y atribución, es decir, apegados al artículo 9 de la Ley de Datos Local.

Se recomienda realizar una lista de los documentos o formatos que se recaben y de ellos desglosar todos los datos que contienen, ejemplo:

La credencial para votar contiene: Nombre, domicilio, edad, sexo, CURP, Clave de elector, Huella digital, firma, clave OCR, fotografía, etc.

F) Instancias Responsables del tratamiento del Sistema de Datos Personales:

Se sugiere estructurar de la siguiente forma:

El Responsable del tratamiento del Sistema de Datos Personales es la **[Nombre del Sujeto Obligado]** a través de **[Nombre de la Unidad Administrativa Responsable].**

Usuarios:

Son las Unidades o Áreas que tratan Datos Personales al interior del Sujeto Obligado, de conformidad con el artículo 3 fracción XXXVI de la Ley de Datos Local, el cual establece lo siguiente:

> **XXXVI.** Usuario: Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales.

Se recomienda realizar un diagrama de flujo del tratamiento de los datos personales, apoyándose del organigrama del Sujeto Obligado, con la finalidad de identificar a cada persona relacionada en las etapas del tratamiento de los datos personales, es decir, antes de recolectar, durante la recolección, durante el tratamiento y al término del ciclo de vida de éstos.

Ejemplo.

- ✓ Director/a de la Dirección,
- ✓ Subdirección,
- ✓ JUD,
- ✓ Líder Coordinador A,
- ✓ Líder Coordinador B,
- ✓ Honorarios,
- ✓ Servicio social.

<u>EN SU CASO</u>

Encargados:

De conformidad con el artículo 3 fracción XV de la Ley de Datos local, el concepto de Encargado es el siguiente:

XV. Encargado: Persona física o jurídica, pública o privada, ajena a la organización del Responsable, que sola o conjuntamente con otras trate datos personales a nombre o por cuenta del Responsable.

Ejemplo:

- ✓ Instituciones Bancarias,
- ✓ Instituciones de Seguridad Social,
- ✓ Aseguradoras,
- ✓ Persona física o moral que sea adjudicado mediante los procesos de contratación correspondiente.

- Es importante recordar que, la relación Responsable-Encargado deberá esta formalizada mediante instrumento jurídico, de conformidad con los artículos 55 y 56 de la Ley de Datos Local.

No se debe confundir la acción de comunicación entre el Encargado y el Responsable, la cual se denomina REMISIÓN con la acción de comunicación entre el Responsable y un tercero, siendo ésta una Transferencia.

REMISIÓN: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

TRANSFERENCIA: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

G) Áreas ante las que podrán ejercerse los derechos de acceso, rectificación, cancelación y oposición (ARCO):
Se deberá estructurar de la siguiente forma:

El titular de los datos personales, podrá ejercer su derecho de acceso, rectificación, cancelación y oposición así como la revocación del consentimiento en términos de lo establecido en el Titulo Tercero de la LPDPPSOCDMX, en la Unidad de Transparencia del Instituto Electoral de la Ciudad de México sita [**Domicilio del Instituto Electoral de la Ciudad de México**]; o a través del Sistema INFOMEX (www.infomex.org.mx), la Plataforma Nacional de Transparencia (www.plataformadetransparencia.org.mx) o a través de Tel-INFO al 56364636.

H) Nivel de seguridad:

Derivado de los datos personales que se recaben, se determinará el nivel de seguridad utilizado para su resguardo, es decir, de conformidad con lo previsto en los artículos 3 fracciones XXIII, XXIV y XXV, y 25 segundo párrafo de la Ley de Datos Local, 38 y 41 de los Lineamientos Generales de Datos Local.

TRANSITORIOS

PRIMERO. En cumplimiento a lo establecido en el artículo 37 fracción I de la Ley Datos local, publíquese el presente Acuerdo en la Gaceta Oficial de la Ciudad de México.

SEGUNDO. Se instruye al Responsable del Sistema de Datos Personales en términos del artículo 2 fracción XII del Lineamientos Generales de Datos local, para que realice la inscripción del **[SISTEMA DE DATOS PERSONALES "NOMBRE DEL SISTEMA DE DATOS PERSONALES"],** en el Registro de Sistemas de Datos Personales a cargo del Instituto de Transparencia, Acceso a la Información Pública,

Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, en términos del artículo 38 de la Ley de Datos local y 67 de los Lineamientos Generales de Datos local.

TERCERO.- Se instruye al Enlace en materia de Datos Personales para que notifique al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, la publicación del presente Acuerdo de Creación del **[SISTEMA DE DATOS PERSONALES "NOMBRE DEL SISTEMA DE DATOS PERSONALES"]** de conformidad con el artículo 63 de los Lineamientos Generales de Datos local; así como el nivel de seguridad aplicable de conformidad con lo establecido en el artículo 25 último párrafo de la Ley Datos local, dentro de los diez días hábiles siguientes a su publicación en la Gaceta Oficial de la Ciudad de México, para los efectos legales y administrativos a que haya lugar.

CUARTO. - El presente Acuerdo entrará en vigor al día siguiente de su publicación en la Gaceta Oficial de la Ciudad de México.

Ciudad de México, a los XXXX días del mes de XXX de dos mil XXX.

_____

NOMBRE DE LA PERSONA TITULAR QUE REALIZA LA PUBLICACIÓN
(SECRETARIO EJECUTIVO)

9.2. Formato para elaborar Acuerdo de modificación de SDP (ANEXO B)

Código: SE/OTAIPDPyA/FR04

MODELO DE ACUERDO DE MODIFICACIÓN DE SDP

ACUERDO POR EL QUE SE MODIFICA, EL "SISTEMA DE DATOS PERSONALES _____ (COLOCAR LA DENOMINACIÓN)

Nombre de la persona titular de la Secretaría Ejecutiva (fundamento legal para realizar la publicación).

En este apartado, se debe desarrollar el fundamento legal que confiere la facultad para realizar la publicación en Gaceta Oficial de la CDMX, se recomienda utilizar la jerarquía normativa correspondiente.

CONSIDERANDOS

En los considerandos habrá de redactarse la fundamentación jurídica, en la cual se describe el motivo de la Modificación, la facultad que tiene el Responsable del SDP para recabar y tratar los datos personales.

Se sugiere que los Considerandos se estructuren de forma individual, es decir, por cada normativa y artículo en orden de relevancia, citando textualmente el contenido de los artículos.

En el caso de realizar en una sola publicación la modificación de varios SDP, es recomendable redactar un Considerando por Sistema con la siguiente información: fecha de publicación de la Creación y/o Modificación de la Gaceta Oficial, fecha de inscripción y folio en el Registro de Sistemas de Datos Personales (RESDP) de cada SDP, justificación fundada y motivada, ejemplo:

- Que con fecha XXXX se publicó en Gaceta Oficial de la D.F/CDMX el Acuerdo de Creación del **[Nombre del Sistema de Datos Personales],** [justificación fundada y motivada].

- Que con fecha XXXX fue inscrito en el Registro de Sistemas de Datos Personales (RESDP) administrado por el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México el **[Nombre del Sistema de Datos Personales],** asignándole el folio de identificación [XXXXXXXXXXXXXXXXXXX].

EN SU CASO

- Que con fecha XXXX, se publicó en Gaceta Oficial de la D.F/CDMX el Acuerdo por el que se Modifica el **[Nombre del Sistema de Datos Personales],** a efectos de [ejemplo: actualizar y modificar la estructura básica del sistema y el nivel de seguridad]

Este Considerando se deberá repetir por cada Modificación realizada al SDP

- Los siguientes **Considerandos** se sugieren como base en materia de datos personales; adicionalmente deberán describir la(s) facultad (es) legal(es) del Responsable del SDP para tratar datos personales:

1. Que el 20 de julio de 2007 se publicó en Diario Oficial de la Federación la reforma al artículo 6 apartado A fracción II de la Constitución Política de los Estados Unidos Mexicanos, el cual establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

2. Que el 1º de junio de 2009 se publicó en Diario Oficial de la Federación la reforma al artículo 16 párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, la cual señala que toda persona tiene el derecho humano a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición.

3. Que el 5 de febrero de 2017 se publicó en la Gaceta Oficial de la Ciudad de México el Decreto por el que se expidió la Constitución Política de la Ciudad de México (Constitución Local), que en su artículo 7, apartado E, numerales 2, 3 y 4, estableció el deber de proteger la información que se refiera a la privacidad y los datos personales, en los términos y con las excepciones previstas en la Constitución Federal y las leyes; asimismo prohibió cualquier injerencia arbitraria, oculta o injustificada en la vida de las personas y dispuso que toda persona tiene derecho al acceso, rectificación y cancelación de sus datos personales y a manifestar su oposición respecto del tratamiento de los mismos. Su manejo se regirá por los principios de veracidad, licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

4. Que la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (Ley de Datos local), en su artículo 3 fracción XXIX define a los Sistema de Datos Personales como el conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de los Sujetos Obligados, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

5. Que el artículo 9 de la Ley de Datos local, establece que el Responsable del tratamiento de Datos Personales observará los principios de: calidad, confidencialidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad, transparencia y temporalidad.

6. Que en términos del artículo 36 de Ley de Datos local, la persona Titular de los Sujetos Obligados en su función de Responsable del tratamiento de datos personales, conforme a su respectivo ámbito de competencia, determinará la creación, Modificación o supresión de los Sistemas de Datos Personales.

7. Que de acuerdo a lo dispuesto en el artículo 37 fracción I de la Ley de Datos local y 63 primer párrafo de los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (Lineamientos Generales de Datos local), establece que la creación, modificación o supresión de sus Sistemas de Datos Personales se efectuará mediante Acuerdo emitido por la persona Titular del Sujeto Obligado, o en su caso el órgano competente, publicado en la Gaceta Oficial de la Ciudad de México.

8. Que el mismo artículo 37 en su fracción II de la Ley de Datos local en complemento con el 64 de los Lineamientos Generales de Datos local, establecen el contenido mínimo de los Acuerdos de Creación y modificación de los Sistemas de Datos Personales.

9. Que en cumplimiento al artículo 63 segundo párrafo de los Lineamientos Generales de Datos local, se establece que en los casos de creación y modificación, el Acuerdo deberá dictarse y publicarse previamente a la creación o Modificación del Sistema de Datos Personales correspondientes y ser notificado al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFOCDMX) dentro de los diez días siguientes a su publicación.

10. Que el artículo 23 fracción XIII de la Ley de Datos Local, señala que el Responsable para cumplir con el tratamiento lícito, transparente y responsable de los datos personales, tendrá el deber de registrar ante el INFOCDMX los Sistemas de Datos Personales, así como la Modificación o supresión de los mismos.

Por los anteriores Considerandos, se emite el presente (redacción opcional):

ACUERDO POR EL QUE SE MODIFICA EL SISTEMA DE DATOS PERSONALES [NOMBRE DEL SISTEMA DE DATOS PERSONALES]

Ejemplo:

ACUERDO POR EL QUE SE **MODIFICA** EL SISTEMA DE DATOS PERSONALES “SISTEMA DE DATOS PERSONALES DE NÓMINA DEL INSTITUTO ELECTORAL DE LA CIUDAD DE MÉXICO”

[PUNTOS DE ACUERDO]-

ÚNICO. Se Modifica el Sistema de Datos Personales **[nombre del Sistema],** en los siguientes rubros**,** para quedar como se establece a continuación:

PRIMERO. Se Modifica el Sistema de Datos Personales denominado (nombre del sistema 1) en los siguientes rubros**,** para quedar como se establece a continuación:

SEGUNDO. Se Modifica el Sistema de Datos Personales denominado (nombre del sistema 2) en los siguientes rubros**,** para quedar como se establece a continuación:
…
Así sucesivamente con los Sistemas de Datos que se quieran incluir en el Acuerdo.

- Se sugiere que el Acuerdo se estructure solamente con los rubros que se modificarán del Sistema en virtud de lo siguiente:

DATOS DEL SISTEMA

- ✓ **Nombre del Sistema**: debe establecer una idea clara y general de la razón de ser del Sistema, evitando el uso de acrónimos, nombres de personas o Unidades Administrativas. ***Cualquier Modificación sí implica una previa publicación en la Gaceta Oficial de la Ciudad de México (GOCDMX).***

- ✓ **Finalidad y usos previstos**: para la identificación de la finalidad y usos de un sistema de datos personales se deberá responder…
    i. ¿De quién se obtienen los Datos Personales?
    ii. ¿Por qué realizo la acción que involucra el tratamiento de Datos Personales?

iii. ¿Para qué voy a utilizar los datos y que voy a generar con ellos?

Toda Modificación sí implica una previa publicación en la GOCDMX.

- ✓ **Normativa aplicable:**
  - La ***normativa específica*** del Sujeto Obligado en la que se señalan las facultades o atribuciones del Responsable del Sistema para tratar Datos Personales.
  - La ***normativa que da soporte*** al derecho a la protección de datos personales (Ley de Datos, Lineamientos de Datos, Ley de Transparencia, Ley de Archivos, Constitución Federal, Constitución Local).

    Como citar la normativa:
  - En la ***GOCDMX***, únicamente deberá citarse el nombre completo de la normativa específica y soporte que faculta para dar tratamiento a los datos personales.
  - En el ***RESDP***, se cita el nombre completo de la normativa, la fecha de publicación, fecha de última reforma, los artículos y fracciones específicas que da la facultad para detentar el sistema.

    La eliminación o adición de una norma, sí implica publicación previa en la GOCDMX; en el caso de actualizar la denominación, fechas, artículos y fracciones no requiere de publicación, solamente se actualiza en el RESDP y el Aviso de Privacidad.

- ✓ **Transferencias**

Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de la o el titular, del responsable o del encargado. Se deben de indicar al menos las ***transferencias básicas***, cuando apliquen.

Ejemplo:

- ✓ Comisión de Derechos Humanos de la Ciudad de México
- ✓ Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México
- ✓ Órganos Jurisdiccionales Locales y Federales
- ✓ Órganos de Control
- ✓ Auditoría Superior de la Ciudad de México
- ✓ Órganos de administración o procuración de justicia

La eliminación o adición en los campos que integran este apartado sí implica una previa publicación en la GOCDMX.

- ✓ **Instancias Responsables del Tratamiento del Sistema de Datos Personales**

Este apartado refiere al Servidor Público, Responsable del Sistema, que decide sobre el tratamiento de los datos personales, su finalidad, la protección y las medidas de seguridad de los mismos.

- ✓ **Nombre**: El cambio del nombre del Servidor Público Titular de la Unidad Administrativa Responsable del Sistema de Datos Personales, ***no implica publicación en GOCDMX.***

- ✓ **Cargo Administrativo**: El Cargo Administrativo debe corresponder con la Unidad Administrativa que detenta el Sistema de Datos Personales, la Modificación de este*, **sí implica una publicación previa en la GOCDMX.***

- ✓ **Domicilio Oficial**: Cualquier cambio en los campos de este rubro (datos de contacto) ***no implica publicación en la GOCDMX.***

- ✓ **Unidad Administrativa**: Es el área responsable del Sistema de Datos Personales, en este caso ***sí implica una previa publicación en la GOCDMX.***

- ✓ **Usuarios:**

Personal de las Unidades Administrativas que en el cumplimiento de sus funciones intervienen en el tratamiento de los datos personales, ***cualquier Modificación (actualización, incorporación o baja) de los cargos sí implica una publicación previa en la GOCDMX., cualquier Modificación del nombre del servidor público, no implica publicación en Gaceta.***

- ✓ **Encargados:**

Persona física o jurídica, pública o privada, ajena a la organización del Responsable, que sola o conjuntamente con otras trate datos personales a nombre o por cuenta del Responsable.

Persona física o moral que sea adjudicado mediante los procesos de contratación correspondiente.

Cualquier Modificación (actualización, incorporación o baja) sí implica una publicación previa en la GOCDMX.

- ✓ **Personas Físicas o Grupos de Personas sobre las que se Recaben o Traten Datos Personales:**

En este apartado se describen las personas físicas o grupos de personas sobre las que se recaban y tratan datos personales, así como la estructura básica del sistema de datos personales (categorías y tipos de datos). Se sugiere recurrir al artículo 62 de los Lineamientos Generales de Datos local.
.
Cualquier Modificación en los campos que integran este apartado sí implica una previa publicación en la GOCDMX.

- ✓ **Interrelación:**

Refiere a la Correspondencia o relación entre el Sistema y otros Sistemas del mismo Sujeto Obligado. ***No implica una publicación en GOCDMX.***

- ✓ ***Estructura Básica del Sistema de Datos Personales y la Descripción de los Tipos de Datos:***

- ✓ **Datos identificativos:**
- ✓ **Datos electrónicos:**
- ✓ **Datos académicos:**

Cualquier Modificación de este rubro, sí implica una publicación en GOCDMX.

- ✓ **Conservación:**

En este apartado se deberá desglosar el ciclo de vida de los datos personales desde que se recaban hasta el término de su utilidad. Esto va relacionado al Catálogo de Disposición documental del Sujeto Obligado e

incluye el archivo de trámite, concentración, así como el histórico. ***Cualquier Modificación de este rubro, no implica una publicación en GOCDMX.***

- ✓ **Seguridad:**

En dicho rubro se describe, de acuerdo a las Categorías y los tipos de datos personales que se recaban, el Nivel de Seguridad, así como las Medidas de Seguridad aplicables a dicho Sistema.

- **Nivel de Seguridad**: Básico, Medio, Alto.
- **Medidas de Seguridad**: Administrativas, físicas y técnicas.

Cualquier Modificación, sí implica una previa publicación en la GOCDMX.

TRANSITORIOS

PRIMERO. En cumplimiento al artículo 37 fracción I de la Ley de Datos local, publíquese el presente Acuerdo en la Gaceta Oficial de la Ciudad de México.

SEGUNDO. Se instruye al Responsable del Sistema de Datos Personales en términos del artículo 2 fracción XII del Lineamientos Generales de Datos local, para que realice la Modificación del **[SISTEMA DE DATOS PERSONALES "NOMBRE DEL SISTEMA DE DATOS PERSONALES"],** en el Registro de Sistemas de Datos Personales a cargo del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, en términos del artículo 38 de la Ley de Datos local y 65 y 67 de los Lineamientos Generales de Datos local.

TERCERO. Se instruye al Enlace de Datos Personales para que notifique al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México la publicación del presente Acuerdo de Modificación del **[SISTEMA DE DATOS PERSONALES "NOMBRE DEL SISTEMA DE DATOS PERSONALES"]** de conformidad con los artículos 63 y 65 de los Lineamientos Generales de Datos local. En su caso, el nivel de seguridad aplicable en términos del artículo 25 último párrafo de la Ley de Datos de la entidad , dentro de los diez días hábiles siguientes a su publicación en la Gaceta Oficial de la Ciudad de México, para los efectos legales y administrativos a que haya lugar.

CUARTO. El presente Acuerdo entrará en vigor al día siguiente de su publicación en la Gaceta Oficial de la Ciudad de México.

Ciudad de México, a los XXX del mes de XXXXX de dos mil XXXXX

_____

NOMBRE DE LA O EL TITULAR QUE REALIZA LA PUBLICACIÓN
(SECRETARÍO EJECUTIVO)

9.3. Formato para elaborar Acuerdo de supresión de SDP (ANEXO C)

Código: SE/OTAIPDPyA/FR05

MODELO PARA ACUERDO DE SUPRESIÓN DE SDP

ACUERDO POR EL QUE SE SUPRIME, EL "SISTEMA DE DATOS PERSONALES (COLOCAR LA DENOMINACIÓN)"

[Nombre de la persona titular de la Secretaría Ejecutiva)

En este apartado, se debe desarrollar el fundamento legal que confiere la facultad para realizar la publicación en Gaceta Oficial de la CDMX, se recomienda utilizar la jerarquía normativa correspondiente.

CONSIDERANDOS

En los Considerandos se habrá de incorporar la fundamentación jurídica, en la cual se describe el motivo de la Supresión, la facultad que tiene el Responsable del SDP para recabar y tratar los datos personales.

Se sugiere que los Considerandos se estructuren de forma individual, es decir, por cada normativa y artículo en orden de relevancia, citando textualmente el contenido de los artículos.

En el caso de realizar en una sola publicación la Supresión de varios SDP, es recomendable redactar un Considerando por Sistema con la siguiente información: describa la fecha de publicación de la Creación y/o Modificación en Gaceta Oficial, fecha de inscripción y folio en el Registro de Sistemas de Datos Personales (RESDP) de cada SDP, justificación fundada y motivada, ejemplo:

- Que con fecha XXXX se publicó en Gaceta Oficial de la D.F/CDMX el Acuerdo de Creación del **[Nombre del Sistema de Datos Personales],** [justificación fundada y motivada].

- Que con fecha XXXX fue inscrito en el Registro de Sistemas de Datos Personales (RESDP) administrado por el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México el **[Nombre del Sistema de Datos Personales],** asignándole el folio de identificación [XXXXXXXXXXXXXXXXXXX].

- Que con fecha XXXX, se publicó en Gaceta Oficial de la D.F/CDMX el Acuerdo por el que se Modifica el **[Nombre del Sistema de Datos Personales],** a efectos de [ejemplo: actualizar y modificar la estructura básica del sistema y el nivel de seguridad]

El anterior Considerando se deberá repetir por cada Modificación realizada al SDP

- Que con fecha XXXX, se celebró Sesión de COTECIAD del cual se derivó el Acuerdo No. XXXX, a través del cual se autoriza la baja documental del **[Nombre del Sistema de Datos Personales],** derivado de [concluyó la finalidad, ciclo vital, extinción del Sujeto Obligado]

- Los siguientes **Considerandos** se sugieren como base en materia de datos personales; adicionalmente deberán describir la(s) facultad (es) legal(es) del Responsable del SDP para tratar datos personales:

  - Que el 20 de julio de 2007 se publicó en Diario Oficial de la Federación la reforma al artículo 6 apartado A fracción II de la Constitución Política de los Estados Unidos Mexicanos, el cual establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

  - Que el 1º de junio de 2009 se publicó en Diario Oficial de la Federación la reforma al artículo 16 párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, la cual señala que toda persona tiene el derecho humano a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición.

  - Que el 5 de febrero de 2017 se publicó en la Gaceta Oficial de la Ciudad de México el Decreto por el que se expidió la Constitución Política de la Ciudad de México (Constitución Local), que en su artículo 7, apartado E, numerales 2, 3 y 4, estableció el deber de proteger la información que se refiera a la privacidad y los datos personales, en los términos y con las excepciones previstas en la Constitución Federal y las leyes; asimismo prohibió cualquier injerencia arbitraria, oculta o injustificada en la vida de las personas y dispuso que toda persona tiene derecho al acceso, rectificación y cancelación de sus datos personales y a manifestar su oposición respecto del tratamiento de los mismos. Su manejo se regirá por los principios de veracidad, licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

  - Que la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (Ley de Datos local), en su artículo 3 fracción XXIX define a los Sistema de Datos Personales como el conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de los Sujetos Obligados, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

  - Que el artículo 9 de la Ley de Datos local, establece que el Responsable del tratamiento de Datos Personales observará los principios de: calidad, confidencialidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad, transparencia y temporalidad.

  - Que en términos del artículo 36 de Ley de Datos local, el Titular de los Sujetos Obligados en su función de Responsable del tratamiento de datos personales, conforme a su respectivo ámbito de competencia, determinará la creación, modificación o supresión de los Sistemas de Datos Personales.

  - Que de acuerdo a lo dispuesto en el artículo 37 fracción I de la Ley de Datos local y 63 primer párrafo de los Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (Lineamientos Generales de Datos local), establece que la creación, modificación o supresión de los Sistemas de Datos Personales se efectuará mediante Acuerdo emitido por el Titular del Sujeto Obligado, o en su caso el órgano competente, publicado en la Gaceta Oficial de la Ciudad de México.

  - Que el mismo artículo 37 fracción III de la Ley de Datos local, contempla que las disposiciones que se dicten para la supresión de los Sistemas de Datos Personales, considerarán el ciclo vital del dato personal, la finalidad, y los destinos de los datos contenidos en el mismo o, en su caso, las previsiones adoptadas para su destrucción.

  - Que el artículo 66 primer párrafo de los Lineamientos Generales de Datos Personales local, establece que el Titular del Sujeto Obligado o, en su caso, el Responsable del Sistema de Datos

Personales determine la supresión de un sistema de datos personales, deberá publicarse el Acuerdo respectivo en la Gaceta Oficial de la Ciudad de México, en la cual se incluirán las disposiciones que se dicten para la supresión de los Sistemas de Datos Personales, para lo que se debe tomar en consideración el ciclo vital del dato personal, la finalidad, y los destinos de los datos contenidos en el sistema o, en su caso, las previsiones adoptadas para su destrucción.

- Que el artículo 66 en el párrafo Segundo de los Lineamientos Generales de Datos local, establece que la publicación de la supresión en la Gaceta Oficial de la Ciudad de México deberá ser, al menos, treinta días hábiles previos a la supresión del sistema de que se trate.

- Que el artículo 37 en su fracción IV de la Ley de Datos local, refiere que en la destrucción de los datos personales, podrán ser excluidos aquellos que no se opongan a las finalidades originales, como son los procesos de disociación, las finalidades ulteriores estadísticas, históricas o científicas, entre otras.

- Que el artículo 66 en su último párrafo de los Lineamientos Generales de Datos local, seña la que no procederá la Supresión de los Sistemas de Datos Personales cuando exista una previsión expresa en una Ley que exija su conservación.

En los Considerandos se deberá justificar jurídica e históricamente el motivo por el cual se realiza la supresión, por ejemplo:

- ✓ Fecha de publicación en GOCDMX o si el Sistema es preexistente.
- ✓ Fecha de inscripción en el Registro de Sistemas de Datos Personales (REDSP).
- ✓ Fecha y Sesión del COTECIAD.
- ✓ Precisar que, de conformidad con los artículos 9 numerales 4 y 11; 37 fracción III y, 66 de los Lineamientos Generales de Datos Local, el Sistema **ha cumplido con su finalidad y/o ciclo de vida**.

Por los anteriores Considerandos, se emite el presente (redacción opcional):

ACUERDO POR EL QUE SE SUPRIME EL SISTEMA DE DATOS PERSONALES [NOMBRE DEL SISTEMA DE DATOS PERSONALES]

Ejemplo:

ACUERDO POR EL QUE SE **SUPRIME** EL SISTEMA DE DATOS PERSONALES “SISTEMA DE DATOS PERSONALES DE NÓMINA DEL INSTITUTO ELECTORAL DE LA CIUDAD DE MÉXICO”

[PUNTOS DE ACUERDO]-

ÚNICO. Se Suprime el Sistema de Datos Personales **(nombre del Sistema)** que actualmente se encuentra activo en el Registro de Sistemas de Datos Personales administrado por el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, en virtud de que (citar el motivo de la supresión, considerando):

- Las atribuciones del responsable
- Que ya no se lleve a cabo la finalidad del sistema
- Que el ciclo de vida haya concluido]

- En caso de contemplar distintos Sistemas, se sugiere estructurar de la siguiente forma:

  PRIMERO. Se **SUPRIME** el Sistema de Datos Personales denominado (nombre del sistema):

  SEGUNDO. Se **SUPRIME** el Sistema de Datos Personales denominado (nombre del sistema):

Así sucesivamente con los sistemas de datos que se quieran incluir en el acuerdo.

En ambos casos especificar el destino de los datos contenidos en los mismos o, en su caso, las previsiones que se adopten para su destrucción, de conformidad con la Ley de General de Archivos, Ley de Archivos del Distrito Federal y demás normativa que resulte aplicable.

TRANSITORIOS

PRIMERO. Publíquese el presente acuerdo a través de un Aviso en la Gaceta Oficial de la Ciudad de México.

SEGUNDO. Se instruye al Responsable del Sistema de Datos Personales en términos del artículo 2 fracción XII y 66 tercer párrafo del Lineamientos Generales de Datos local, para que una vez notificado al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México el presente Acuerdo de Supresión del sistema de datos personales [NOMBRE DEL SISTEMA DE DATOS PERSONALES], proceda a la cancelación de inscripción en el Registro de Sistemas de Datos Personales

TERCERO. Se instruye al Enlace de Datos Personales para que notifique al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México la publicación del presente Acuerdo de Supresión del [NOMBRE DEL SISTEMA DE DATOS PERSONALES] de conformidad con el artículo 37 fracción I de la Ley de Datos local, y 66 tercer párrafo de los Lineamientos Generales de Datos local, dentro de los diez días hábiles siguientes a su publicación en la Gaceta Oficial de la Ciudad de México.

CUARTO. El presente Acuerdo entrará en vigor al día siguiente de su publicación en la Gaceta Oficial de la Ciudad de México.

Ciudad de México, a los XXX del mes de XXXXX de dos mil XXXXX

_____

NOMBRE DE LA O EL TITULAR QUE SUSCRIBE EL ACUERDO
(SECRETARIO EJECUTIVO)

Contenido

1. Objetivo 2
2. Alcance 2
3. Marco normativo 2
4. Definiciones y Abreviaturas 3
5. Responsabilidades 7
6. Políticas de operación 9
7. Diagrama de flujo 12
8. Descripción de las actividades 14
9. Formatos 17

Control de Cambios

Revisión	Fecha	Descripción del Cambio
00	09 febrero 2023	Emisión del documento

1. Objetivo

Establecer las directrices para la elaboración y/o actualización de los documentos de seguridad de los Sistemas de Datos Personales del Instituto Electoral de la Ciudad de México, a fin de cumplir con las disposiciones normativas en materia de Datos Personales.

2. Alcance

El presente Manual es aplicable para la Oficina Transparencia, Acceso a la Información Pública, Datos Personales y Archivo, así como para las distintas Áreas Responsables del Instituto Electoral de la Ciudad de México, que a continuación se indican.

- Presidencia;
- Oficinas de Consejeras y Consejeros Electorales;
- Secretaría Ejecutiva;
- Secretaría Administrativa;
- Contraloría Interna;
- Direcciones Ejecutivas;
- Unidades Técnicas; y
- Órganos Desconcentrados.

3. Marco normativo

- Constitución Política de los Estados Unidos Mexicanos;
- Constitución Política de la Ciudad de México;
- Código de Instituciones y Procedimientos Electorales de la Ciudad de México;
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Ley General de Archivos;
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;
- Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México,
- Ley de Archivos Local. Ley de Archivos, aplicable en la Ciudad de México;
- Reglamento Interior del Instituto Electoral de la Ciudad de México;
- Reglamento del Instituto Electoral de la Ciudad de México, en materia de Protección de Datos Personales;
- Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales;
- Lineamientos para la realización de verificaciones y auditorías en cumplimiento de los artículos 112, fracción IV y 116 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;
- Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México; y
- Guía para la elaboración del documento de seguridad.

4. Definiciones y Abreviaturas

Análisis de brecha: Es el estudio comparativo que se realiza, respecto de las medidas de seguridad existentes contra las medidas de seguridad faltantes; es decir (estado actual y el objetivo a alcanzar).

Análisis de riesgo: Proyectos o iniciativas de mejora en cuanto a la seguridad de información, en la que deben considerarse las amenazas, vulneraciones y los recursos involucrados en el tratamiento.

Autenticación: Comprobación de la identidad de aquella persona autorizada para el tratamiento de datos personales.

AR´s: Cada una de las áreas administrativas del Instituto Electoral de la Ciudad de México que administre bases de datos o Sistemas de Datos Personales, en términos de la legislación aplicable.

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

Baja documental: Eliminación de aquellos documentos que hayan prescrito en su vigencia archivística (administrativa, legal o fiscal), de conformidad con los plazos de conservación y técnica de selección, establecidos en el Catálogo de Disposición Documental y que no posean los valores secundarios o históricos considerados para ser conservados de manera permanente, de acuerdo con la Ley de Archivo, los Criterios para bloqueo en los sistemas de datos personales, y las disposiciones jurídicas aplicables.

Bitácora de vulneraciones: Documento en donde se anotará nombre y cargo de quien reporta el incidente, el número de vulneraciones y descripción de la misma, fecha en que ocurrió, el motivo de ésta y las acciones implementadas de forma inmediata y definitiva.

Bloqueo: Proceso para la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas o mediante el ejercicio de los Derechos ARCO

Ciclo vital: Etapas por las que atraviesan los documentos de archivo desde su producción o recepción hasta su baja documental o transferencia a un archivo histórico; creados por el tratamiento de los datos personales, para después ser suprimidos, cancelados o destruidos por parte del Responsable de los SDP.

Circular: Documento emitido por la Secretaría Ejecutiva, mediante el cual se solicita a las AR's la actualización de los documentos de seguridad de los Sistemas de Datos Personales, de conformidad con sus atribuciones.

Control de acceso.- Documento mediante el cual se lleva el registro detallado de accesos a un sistema automatizado que permite de forma eficaz, aprobar o negar el paso de personas o grupo de personas a zonas restringidas en función de seguridad.

Copia de respaldo: Se refiere al duplicado de archivos físicos o bases de datos a un sitio secundario para su preservación en caso de incidencias que fueran causadas por falla del equipo, catástrofe, desastre y que es fundamental para la recuperación de la información.

Copia de recuperación: Se refiere a las técnicas y procedimientos utilizados para acceder y extraer la información acumulada en medios de almacenamiento digital que por daño o avería no pueden ser accesibles de manera usual ya sea por falla en el equipo, catástrofe o desastre natural.

Correo electrónico: Medio oficial, a través del cual la Oficina Transparencia, Acceso a la Información Pública, Datos Personales y Archivo y los Enlaces de las AR´s mantienen comunicación, respecto de la retroalimentación y actualización de los documentos de seguridad de los Sistemas de Datos Personales del Instituto Electoral de la Ciudad de México.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve a un riesgo grave para éste. De manera enunciativa más no limitativa se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, información biométrica, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Destrucción: Aplicación de técnicas que hacen imposible la recuperación de datos utilizando mecanismos para su eliminación ya sea de manera física o electrónica y con lo cual se imposibilita el uso posterior de los medios para el almacenamiento de datos;

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

Disociación: Procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;
Enlace: Persona designada en cada AR´s para la gestión y trámite en materia de datos personales.

Gestión de Soportes.- Documento que permite llevar el registro de localización, consulta y conservación de los documentos, en el cual se pueden almacenar datos o documentos, u objetos susceptibles de ser tratado en un sistema de información y se puedan grabar y recuperar datos en discos duros externos, CD'S, DVD'S, memorias USB, scanner; además de inventariar, registrar las salidas y entradas de información aún de los correos electrónicos, el traslado de información, cifrado de datos, generar contraseñas y usuarios.

Guía: Documento emitido por el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, que establece las bases para la elaboración e integración de los Documentos de Seguridad.

Autentificación: Comprobación de la identidad de aquella persona autorizada para el tratamiento de datos personales;

Identificación: Persona autorizada (Encargado y/o Usuario) por el responsable para que acceda al SDP.

Incidencia: Cualquier anomalía que afecte o pudiera afectar la seguridad de los datos personales.

INFO: Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

Instituto Electoral: Instituto Electoral de la Ciudad de México.

Inventario de datos: Consiste en enlistar el tipo y categorías de los datos personales y en su caso los datos personales sensibles recabados.

JDDPyAJ: Jefatura de Departamento Datos Personales y Apoyo Jurídico, adscrita a la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo.

Ley de Datos: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Lineamientos Generales de Datos: Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Mecanismo de monitoreo: Documento de control en el que se establece, cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo y como resultado de un proceso de mejora continua.

Medidas de mitigación: Análisis que permite implementar medidas de seguridad que minimicen la posibilidad de que un incidente se repita, mediante la recolección de evidencias con herramientas especiales de hardware y software propio o contratado, a fin de obtener mayor información y revertir sus efectos.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales y los Sistemas de Datos Personales.

Medidas de seguridad administrativas: Procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado

seguro de la información, así como la sensibilización y capacitación del personal, en materia de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento; algunas de las que se consideran: prevenir el acceso no autorizado o interferencia a las instalaciones, proteger los recursos móviles o portátiles, soportes físicos y electrónicos y proveer con mantenimiento eficaz los equipos que almacenan datos personales.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología para proteger el entorno digital de los datos personales y su tratamiento; algunos como: prevenir el acceso a bases de datos, revisar configuraciones de seguridad en la adquisición, operación, gestión y desarrollo de las comunicaciones y medios de almacenamiento.

OTAIPDPyA: Oficina Transparencia, Acceso a la Información Pública, Datos Personales y Archivo, también denominada Unidad de Transparencia.

Oficial de Protección de Datos Personales: Persona servidora pública especialista en materia de datos personales, designada por el responsable del Instituto Electoral, adscrita a la Unidad de Transparencia; quien coordina las actividades para atender los asuntos relacionados con la protección de datos personales.

Oficio de respuesta: Documento a través del cual las AR's comunican a la Unidad de Transparencia la respuesta a la Circular de actualización o supresión de los documentos de seguridad de los Sistemas de Datos Personales.

Registro de acceso y telecomunicaciones: Documento mediante el cual se deja constancia de ingresos al SDP mediante la identificación, autenticación y autorización; así como de la recepción o almacenamiento de mensajería y aplicaciones que contienen datos personales.

Registro de incidencias: Es el registro de vulneraciones a la seguridad del SDP y consiste en la pérdida o destrucción no autorizada, robo, extravío o copia no autorizada, uso, acceso, o tratamiento no autorizado, daño, alteración o modificación de la información.

Responsable del Sistema de Datos Personales: Persona servidora pública del Instituto Electoral, con el cargo de titular del área que administra el sistema de datos personales; que decide y determina la finalidad, fines, medios, medidas de seguridad y todo aquello relacionado con el tratamiento de datos personales;

Responsable de seguridad: Persona servidora pública designada por la o el titular del área que administra sistemas de datos personales, quien coordinará y controlará las medidas de seguridad definidas en el documento de seguridad;

SDP: Sistema de Datos Personales.

SE: Secretaría Ejecutiva.

Soporte físico: Medios de almacenamiento que no requieren de ningún aparato o equipo para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados a mano o máquina, fotografías, carpetas, expedientes y demás análogos.

Soporte electrónico: Medios de almacenamiento mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), Discos magnéticos (flexibles y duros), tarjetas de memoria (USB y SD) y demás medios de almacenamiento móvil.

STyDP: Subdirección de Transparencia y Datos Personales, adscrita a la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral.

Supresión: Eliminación, borrado o destrucción de los SDP o de datos personales de una persona física bajo las medidas de seguridad previamente establecidas por el responsable, una vez que se ha cumplido la finalidad y el dato personal ha cumplido su ciclo vital; con estricto apego a lo establecido en la Ley de Protección de Datos y los Criterios para bloqueo en los sistemas de datos personales.

Titular de la Oficina: Titular de la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas sobre datos personales o conjunto de datos personales, mediante procedimientos manuales o automatizados.

Vulneraciones a la seguridad: Posibilidad de que ocurra un incidente respecto a la seguridad de los datos personales contenidos en los SDP, en cualquier fase del tratamiento; que puede ser: pérdida o destrucción, robo, extravío o copia no autorizada, uso, acceso o tratamiento no autorizado o bien daño, alteración o modificación.

5. Responsabilidades

OTAIPDPyA	• Generar de manera anual, el proyecto de Circular que suscriba la SE, en la que solicita a las diversas AR´s, lleven a cabo la actualización de los Documentos de seguridad de los SDP. Dicha Circular deberá **elaborarse y distribuirse durante los primeros 15 días hábiles del mes de enero de cada año.** • Asesorar permanentemente a las AR's en materia de datos personales y coordinar con los Enlaces, la actualización de los Documentos de seguridad.

	• Implementar un registro de las actualizaciones de los Documentos de seguridad de los SDP del Instituto Electoral. • Establecer de manera permanente, acciones de capacitación para que los Enlaces cuenten con las herramientas necesarias para la elaboración de los Documentos de seguridad de los SDP. • Avisar oportunamente al INFO cualquier vulneración de seguridad en los SDP.
AR´s	• Llevar a cabo anualmente, la actualización del o los documentos de seguridad de los SDP bajo su resguardo, en respuesta a la Circular que la OTAIPDPyA emita para tales efectos. • Enviar anualmente a la OTAIPDPyA el reporte de actualización de los Documentos de seguridad. • Adoptar las medidas de seguridad de carácter administrativo, físico y técnico, para la protección de datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar la confidencialidad, integridad y disponibilidad. Lo cual deberá quedar debidamente asentado en el Documento de seguridad de cada SDP bajo su resguardo. • Revisar periódicamente las políticas de seguridad de datos personales, para determinar las modificaciones que se requieran y, en su caso, las adecuaciones a los Documentos de seguridad. • Garantizar que en los SDP en los que se utilicen aplicaciones electrónicas o cualquier otra tecnología que implique tratamiento de datos personales, cumpla con las medidas de protección y las obligaciones previstas en la Ley de Datos, especificándose en el Documento de seguridad.

	• Solicitar opiniones técnicas al Oficial de protección de datos personales, respecto a la adopción de medidas de seguridad de los SDP, conforme a sus atribuciones. • Comunicar en el término de 48 horas, a la OTAIPDPyA, cualquier vulneración de seguridad en el o los SDP, con la finalidad de que se comunique oportunamente al INFO. • Informar a la persona Titular de los Datos Personales dentro del plazo máximo de 72 horas, cualquier vulneración de seguridad relacionada con sus datos personales. • Guardar estricta confidencialidad de las medidas que se establezcan en el Documento de seguridad.
Oficial de Protección de Datos Personales	• Asesorar a las AR's en materia de protección de datos personales. • Formular dictámenes, opiniones técnicas y cualquier otro documento que se considere necesario para atender los asuntos en materia de protección de datos personales. • Monitorear y revisar de manera periódica las medidas de seguridad implementadas. • Proponer a la OTAIPDPyA los procedimientos internos para la adopción de medidas de seguridad que formen parte de los Documentos de seguridad. • **Coordinar las actividades para atender los asuntos relacionados con la protección de datos personales.**

6. Políticas de operación

- Toda medida de seguridad deberá considerar al menos lo siguiente: riesgo inherente a los datos tratados, sensibilidad de los datos personales recabados, desarrollo tecnológico, posibles consecuencias de una vulneración, transferencias de datos personales que se realicen, número de titulares, vulneraciones previas ocurridas en los SDP.

- El Responsable del Sistema de Datos Personales podrá adoptar las medidas adicionales que estime necesarias para brindar mayor seguridad en la protección de los datos personales.
- En todo tratamiento de datos personales se establecerán y documentarán los roles y responsabilidades del personal involucrado, asegurándose que conocen sus funciones y las consecuencias del incumplimiento.
- En todo tratamiento de datos personales se elaborará un inventario de datos personales, con la información básica del tratamiento y deberá contar al menos con la información siguiente: catálogos de medios físicos y electrónicos, finalidades de cada tratamiento, catálogo de tipos de datos que se traten, indicando si son sensibles o no, formatos de almacenamiento, descripción de la ubicación física, lista de personas servidoras públicas que tienen acceso, nombre o razón social del Encargado y en su caso los destinatarios.
- En los inventarios de datos personales, invariablemente se deberá incluir su ciclo vital, tomando en cuenta el almacenamiento y uso de los datos, conforme a su acceso, manejo, aprovechamiento, divulgación y en su caso cancelación, actualización, y/o rectificación, supresión o destrucción de datos personales.
- En el tratamiento de los datos personales se deberá contar con un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgo y de brecha en el cual se dará prioridad para establecer las medidas de seguridad relevantes e inmediatas.
- En las medidas de seguridad que se implementen, invariablemente se llevará a cabo el monitoreo y supervisión, a fin de verificar el estricto cumplimiento de la seguridad de los datos personales.
- Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales, mencionadas con antelación, deberán estar documentadas y contenidas en el sistema de gestión denominado Documento de seguridad.
- Invariablemente los Documentos de seguridad serán actualizados anualmente, o bien, cuando ocurran los eventos siguientes:
    - ✓ Se presenten modificaciones sustanciales al tratamiento de los datos personales que deriven en un cambio en el nivel de riesgo;
    - ✓ Como resultado de un proceso de mejora, derivado del monitoreo y revisión del SDP;
    - ✓ Para mitigar el impacto ante una vulneración a la seguridad del SDP;
    - ✓ Cuando se lleven a cabo acciones correctivas y preventivas ante la vulneración de seguridad; y
    - ✓ Por recomendación del INFO.

- En los casos en que ocurra una vulneración a la seguridad, el Responsable de los Sistemas de Datos Personales deberá analizar las causas por las cuales se presentó e implementar de forma inmediata un plan de trabajo que contemple acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales, con la finalidad de evitar que se repitan las vulneraciones.
- El Responsable deberá llevar una bitácora de las vulneraciones a la seguridad, en la que describirá: la fecha en que ocurrió, el motivo o motivos, y las acciones correctivas implementadas.
- En caso de presentarse una vulneración de seguridad, se informará necesariamente a la persona titular de los datos personales, al menos lo siguiente: la naturaleza del incidente, los datos personales comprometidos, los derechos que puede adoptar para proteger sus datos, las acciones correctivas realizadas de forma inmediata y los medios donde puede obtener información al respecto.
- Asimismo, de dicha vulneración la OTAIPDPyA informará por escrito al INFO, dentro de las 48 horas siguientes al evento, señalando la hora y fecha en que ocurrió, así como del momento en que se inició la investigación de la vulneración; naturaleza del incidente; detalle de la vulneración ocurrida; categorías y número de titulares afectados; los sistemas de tratamientos y datos personales comprometidos; acciones correctivas realizadas de forma inmediata, y cualquier otra información o documento que se considere conveniente hacer del conocimiento del INFO.
- Todas aquellas personas que tengan bajo su resguardo el tratamiento de datos personales, deberán establecer controles y mecanismos para garantizar la debida confidencialidad.
- Los Documentos de seguridad no podrán ser públicos, ni mucho menos, podrá divulgarse su información, por lo que queda bajo estricto resguardo del Responsable del Sistema de Datos Personales y del Responsable de Seguridad. En el caso que se presente una solicitud, se elaborará versión pública para su entrega.

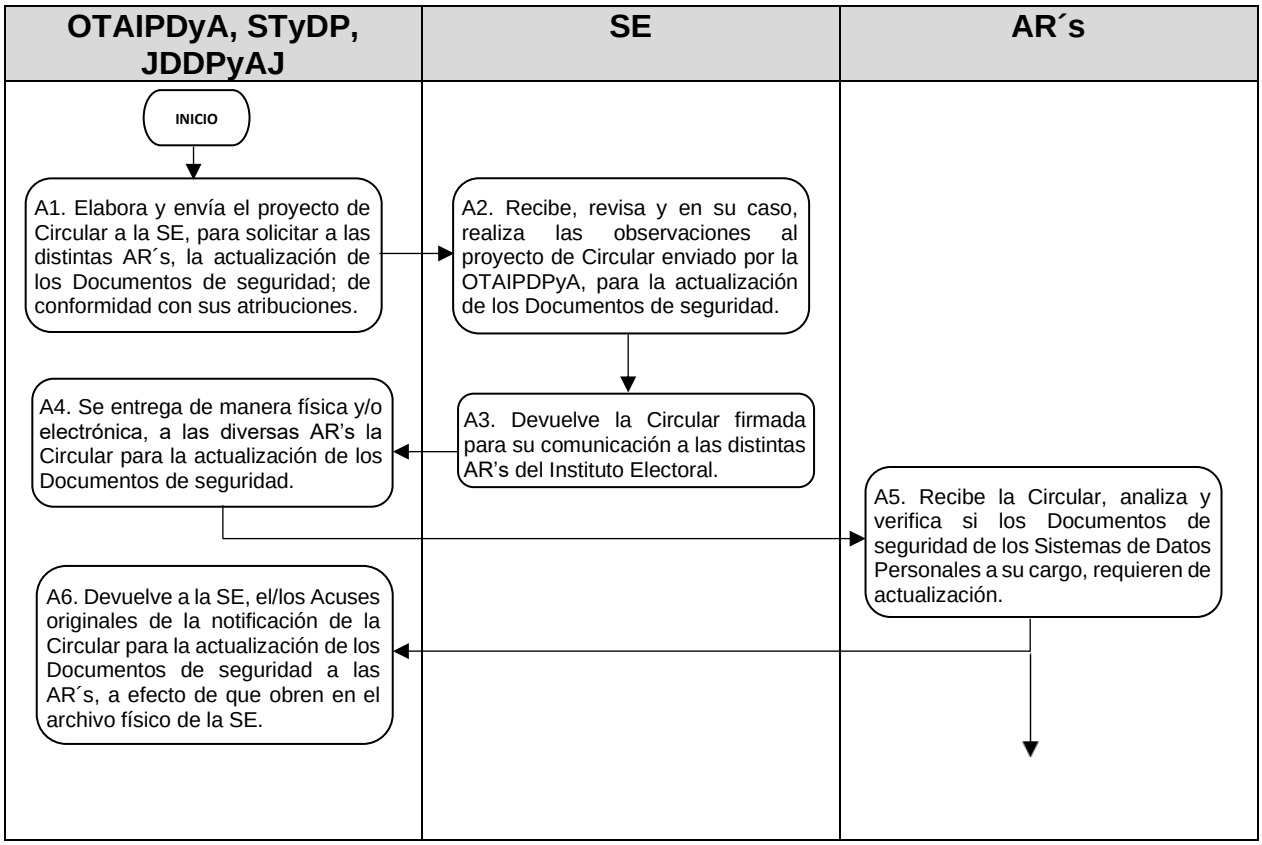
6.1 Políticas de operación específicas para la elaboración de los Documentos de seguridad.

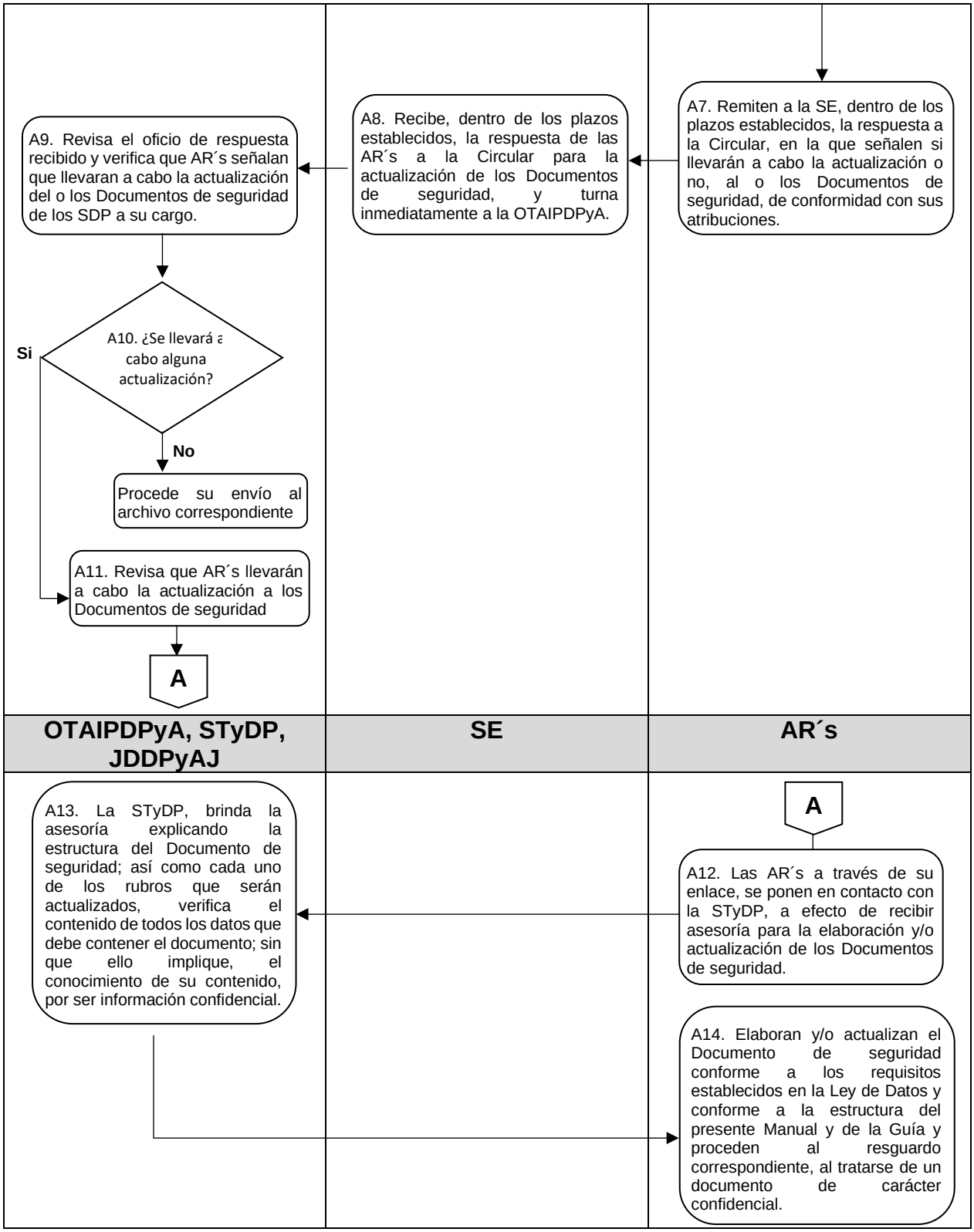
La estructura y contenido de los Documentos de seguridad de los SDP, deberán realizarse conforme a los requisitos señalados en la Ley de Datos, en el presente Manual; y específicamente conforme al formato que se establece en la Guía y deberá incluirse al menos los siguientes:

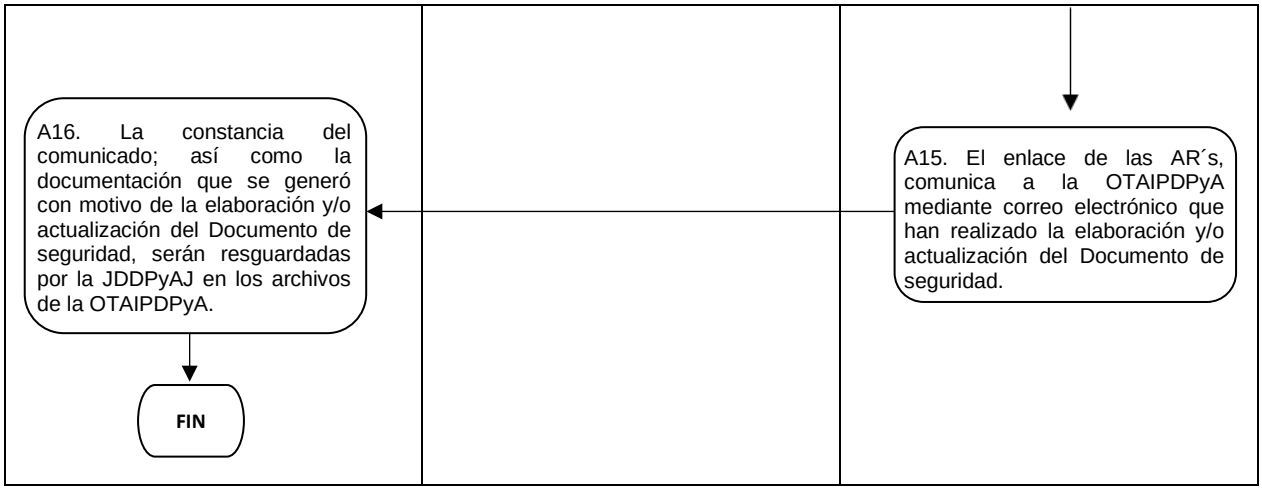
- ✓ El inventario de datos personales contenidos en los SDP;
- ✓ Las funciones y obligaciones de las personas que intervengan en el tratamiento de los datos personales, usuarios y encargados, en su caso;

- ✓ Registro de incidencias;
- ✓ Identificación y autentificación;
- ✓ Control de acceso; gestión de soportes y copias de respaldo y recuperación;
- ✓ El análisis de riesgos;
- ✓ El análisis de brecha;
- ✓ Responsable de seguridad;
- ✓ Registro de acceso y telecomunicaciones;
- ✓ Los mecanismos de monitoreo y revisión de las medidas de seguridad;
- ✓ El plan de trabajo; y
- ✓ El programa general de capacitación.

7. Diagrama de flujo




A7. Remiten a la SE, dentro de los plazos establecidos, la respuesta a la Circular, en la que señalen si llevarán a cabo la actualización o no, al o los Documentos de seguridad, de conformidad con sus atribuciones.
A8. Recibe, dentro de los plazos establecidos, la respuesta de las AR´s a la Circular para la actualización de los Documentos de seguridad, y turna inmediatamente a la OTAIPDPyA.
A9. Revisa el oficio de respuesta recibido y verifica que AR´s señalan que llevaran a cabo la actualización del o los Documentos de seguridad de los SDP a su cargo.
A10. ¿Se llevará a cabo alguna actualización?
Si
No
Procede su envío al archivo correspondiente
A11. Revisa que AR´s llevarán a cabo la actualización a los Documentos de seguridad
A
OTAIPDPyA, STyDP, JDDPyAJ
SE
AR´s
A
A12. Las AR´s a través de su enlace, se ponen en contacto con la STyDP, a efecto de recibir asesoría para la elaboración y/o actualización de los Documentos de seguridad.
A13. La STyDP, brinda la asesoría explicando la estructura del Documento de seguridad; así como cada uno de los rubros que serán actualizados, verifica el contenido de todos los datos que debe contener el documento; sin que ello implique, el conocimiento de su contenido, por ser información confidencial.
A14. Elaboran y/o actualizan el Documento de seguridad conforme a los requisitos establecidos en la Ley de Datos y conforme a la estructura del presente Manual y de la Guía y proceden al resguardo correspondiente, al tratarse de un documento de carácter confidencial.



8. Descripción de las actividades

A. Actividades para la elaboración y/o actualización de los Documentos de seguridad.			
#	**Actividad**	**Área responsable**	**Documento empleado**
A1	Elabora y envía el proyecto de Circular a la SE, para solicitar a las distintas AR´s del Instituto Electoral, la actualización de los Documentos de seguridad; de conformidad con sus atribuciones. Dicho documento establece la fecha límite para la respuesta y actualización de los Documentos de seguridad.	OTAIPDPyA, STyDP, JDDPyAJ	Proyecto de Circular.
A2	Recibe, revisa y en su caso, realiza observaciones al proyecto de Circular enviado por la OTAIPDPyA, para la actualización de los Documentos de seguridad.	SE.	Proyecto de Circular.
A3	Devuelve la Circular firmada para su comunicación a las distintas AR's del Instituto Electoral.	SE.	Circular.
A4	Se entrega de manera física y/o electrónica, a las diversas AR's la Circular para la actualización de los Documentos de seguridad.	STyDP, JDDPyAJ.	Circular (copia).

A5	Recibe la Circular, analiza y verifica si los Documentos de seguridad de los Sistemas de Datos Personales a su cargo, requieren de actualización.	AR´s	Circular (copia).
A6	Devuelve a la SE, el/los Acuses originales de la notificación de la Circular para la actualización de los Documentos de seguridad a las AR´s, a efecto de que obren en el archivo físico de la SE.	OTAIPDPyA, JDDPyAJ.	Circular original y Acuses.
A7	Remiten a la SE, dentro de los plazos establecidos, la respuesta a la Circular, en la que señalen si llevarán a cabo la actualización o no al o los Documentos de seguridad, de conformidad con sus atribuciones.	AR´s.	Oficio de respuesta a la Circular.
A8	Recibe, dentro de los plazos establecidos, la respuesta de las AR´s a la Circular para la actualización de los Documentos de seguridad, y turna inmediatamente a la OTAIPDPyA.	SE.	Oficio de respuesta a la Circular.
A9	Revisa el oficio de respuesta recibido y verifica qué AR´s llevarán a cabo la actualización del o los Documentos de seguridad de los SDP a su cargo.	STyDP	Oficio de respuesta a la Circular.
A10	Determina si: ¿Se llevará a cabo alguna actualización a los Documentos de seguridad? **No.** Procede a su registro y envío al archivo correspondiente. **Sí.** Continúa en la Actividad **A 11**	STyDP	Oficio de respuesta a la Circular. Registro de actualización de los Documentos de seguridad de los SDP
A11	Revisa qué AR´s llevarán a cabo actualización a los Documentos de seguridad y se pone en contacto con el Enlace correspondiente, a efecto de brindarle orientación para la elaboración y/o actualización de los Documentos de seguridad.	STyDP	Oficio de respuesta a la Circular. Correo electrónico
A12	Las AR´s a través de su enlace, se ponen en contacto con la STyDP a efecto de recibir asesoría para la elaboración y/o actualización de los Documentos de seguridad.	AR´s	Comunicación verbal

A13	La STyDP, brinda asesoría explicando la estructura del Documento de seguridad; así como cada uno de los rubros que serán actualizados, revisando todos los datos que debe llevar el documento; sin que ello implique conocimiento del contenido, al ser información confidencial.	OTAIPDPyA STyDP	Comunicación verbal o correo electrónico según sea el caso.
A14	Las AR´s, elaboran y/o actualizan el Documento de seguridad conforme a los requisitos establecidos en la Ley de Datos y conforme a la estructura del presente Manual y de la Guía y proceden al resguardo correspondiente, al tratarse de un documento de carácter confidencial.	AR´s	Documento de seguridad.
A15	El enlace de las AR´s, comunica a la OTAIPDPyA, mediante correo electrónico, que han realizado la elaboración y/o actualización del Documento de seguridad.	AR´s	Correo electrónico
A16	La constancia del comunicado; así como la documentación que se generó con motivo de la elaboración y/o actualización del Documento de seguridad, serán resguardadas por la JDDPyAJ en los archivos de la OTAIPDPyA.	OTAIPDPyA STyDP, JDDPyAJ	Correo electrónico y Documentos en los que consta que el AR´s ha llevado a cabo la actualización del Documento de seguridad.
Fin de las actividades para la elaboración y/o actualización de los Documentos de seguridad.			

9. Formatos

Código: SE/OTAIPDPyA/FR06

9.1. FORMATO DE DOCUMENTO DE SEGURIDAD INTEGRADO

	DOCUMENTO DE SEGURIDAD	
	Nombre del Sistema de Datos Personales	
	Fecha de elaboración	Fecha de la última Actualización
	Elaboró el documento	Aprobó
	(Nombre y firma)	(Nombre y firma)

DATOS GENERALES DEL SISTEMA

Nombre del sistema: [El nombre del sistema de datos personales, debe coincidir con el Acuerdo de Creación (en caso de que aplique) publicado en Gaceta Oficial de la Ciudad de México **GOCDMX** y/o con la inscripción en el Registro Electrónico de Sistemas de Datos Personales **RESDP**]

Fecha de publicación en la GOCDMX del Acuerdo de Creación: [Indicar la fecha de publicación en la Gaceta Oficial de la Ciudad de México del Acuerdo de creación del sistema de datos personales (en caso de que aplique)]
[Adjuntar como anexo copia de la publicación en la Gaceta Oficial de la Ciudad de México]

Fecha de inscripción en el RESDP: [Indicar la fecha de inscripción del sistema de datos personales en el RESDP]

Folio de inscripción en el RESDP: [Indicar el número de folio señalado en el Acuse de Registro del Sistema de Datos Personales]

[Adjuntar como anexo el Acuse de Registro del sistema de datos personales]

Fecha de publicación en GOCDMX del Acuerdo de Modificación: [Indicar la fecha de publicación del Acuerdo de modificación del sistema de datos personales, en la Gaceta Oficial de la Ciudad de México]

Fecha de última modificación en el RESDP: [Indicar la fecha de modificación del sistema de datos personales en el RESDP]

[Adjuntar como anexo los Acuses de edición del sistema de datos personales.
Normatividad aplicable para el tratamiento

(Señalar el nombre de la norma, los artículos; así como la fecha de publicación en GOCDMX o DOF).

I. INVENTARIO DE DATOS PERSONALES

Se debe crear y mantener actualizado un inventario de los datos personales o sus categorías. El inventario deberá identificar o estar vinculado con la información básica que permita conocer el tratamiento a que serán sometidos.

A.- Señalar el tipo de datos personales que contiene el Sistema (Datos Personales, Datos Personales Sensibles, o ambos).

B.- Además de listar cada uno de los datos personales recabados por ejemplo (nombres, apellido paterno, apellido materno, domicilio, estado civil), Datos laborales (correo electrónico institucional y teléfono institucional).

Aplicación

Las medidas de seguridad contenidas en el presente documento son de aplicación obligatoria para garantizar que los datos personales contenidos en el SDP denominado **(nombre del sistema),** se ajuste a las disposiciones establecidas en la Ley.

Obtención

Las personas sobre las que se pretenden obtener datos de carácter personal son **(_____)**

La recolección de los datos personales que contiene es de carácter **(enlistar y agregar como anexo, los medios por los cuales se recaba la información, ya sean físicos, electrónicos o mixtos),** con un nivel de seguridad **(señalar: básico, medio o alto),** dado el tipo de datos personales que se contienen en el SDP referido.

Modo de tratamiento: El procesamiento de los datos personales se llevará a cabo a través de procedimientos **(físicos, electrónicos o mixtos)**

Medio de actualización: la actualización de los datos personales se llevará a cabo **(a petición del interesado, revisión periódica o mediante oficio)**

Finalidades del tratamiento

Finalidad y uso previsto: las finalidades de cada tratamiento de datos Personales **(Debe coincidir con la publicada en la GOCDMX, en caso de que aplique)**

- Uso:

- Acceso
- Manejo
- Aprovechamiento
- Monitoreo

Remisiones (Responsable – Encargados)

Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano

[Enlistar a la(s) persona(s) física(s) o jurídica(s), pública(s) o privada(s) ajena(s) al responsable y que tratan datos personales, a nombre y por cuenta del responsable. (Anexar copia del contrato, según sea el caso)]

Transferencias

Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

[En su caso, enlistar los terceros receptores, a los que una normativa faculta la transferencia de datos personales, así como las finalidades que la justifican. Cuando las transferencias se realicen entre sujetos obligados se encuentre de manera expresa en una ley o tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos]

Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad aplicable al responsable.

Interrelación **(Señalar si el SDP se interrelaciona con otro SDP del mismo Sujeto Obligado e indicar nombre del SDP y finalidad de la interrelación)**

El catálogo de los tipos de datos personales

Indicar el tipo de datos personales recabados en cada una de las categorías, indicando si son sensibles o no.

Ejemplo:

Datos identificativos: (Nombre, teléfono particular, edad, etc.)

Los datos personales del sistema **(en físico, automatizado o mixto)** se encuentran contenidos **(señalar donde se encuentran contenidos, series documentales. Anexar Catálogo de Disposición Documental)**

Ciclo de vida de los datos (Esta información deberá coincidir con lo que señala el Catálogo de Disposición Documental**):**

- En medio automatizado
- En archivo de trámite
- En archivo de concentración

Así como señalar si se contempla la transferencia de información al archivo histórico.

Nivel de seguridad: Indicar el nivel de seguridad aplicable de acuerdo al tipo de datos recabados:

- BÁSICO
- MEDIO
- ALTO

Medidas de seguridad: Describir las medidas de seguridad adoptada, aplicable a cada caso conforme a lo establecido en la Ley:

- Medidas de seguridad Administrativas
- Medidas de seguridad Físicas
- Medidas de seguridad Técnicas

Catálogo de las formas de almacenamiento:

Los expedientes del sistema de datos personales denominado **(nombre del sistema),** se encuentran resguardados en el inmueble localizado en (**domicilio de ubicación)**

Descripción general de la ubicación física y/o electrónica de los Datos personales. Se puede hacer uso de mapas, planos etc., para señalar la ubicación específica donde se resguarda el SDP.

(Insertar plano o mapa de ubicación del SDP y en su caso anexar el mapa de ubicación como un Anexo).

Lista de los servidores públicos que tienen acceso a los sistemas de tratamiento. (Responsable y usuarios involucrados en el tratamiento)

Solo los siguientes servidores públicos, podrán acceder a los contenidos del SDP, a objeto de dar paso al desarrollo de las funciones y atribuciones que les han sido conferidas.

NOMBRE:_____
CARGO: _____

II. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE INTERVENGAN EN EL TRATAMIENTO DE LOS SISTEMAS DE DATOS PERSONALES

Funciones y obligaciones del Encargado del Sistema:

La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Funciones: Además de lo que establece los artículos 55 y 56 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, indicar las funciones específicas que, de acuerdo a las atribuciones, le competen al Responsable de Seguridad del SDP.

Obligaciones: Además de lo que establece los artículos 55 y 56 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, indicar las obligaciones que de acuerdo a las atribuciones le competen al Responsable de Seguridad del SDP.

Funciones y obligaciones del (los) Usuarios (s) del Sistema

Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales.

Funciones: Indicar, todas aquellas actividades que deberá llevar a cabo para el debido tratamiento y protección de los datos personales, con la finalidad de evitar que existan posibles vulneraciones.

Obligaciones: Indicar, las acciones que de conformidad con sus facultades deberá establecer para el debido resguardo y protección del o los SDP a su cargo: Lo anterior, de conformidad con lo establecido en la Ley de Datos.

Ejemplo:

FUNCIONES

1.- Nombre de la Unidad Administrativa
2.- Nombre del sistema

Responsable:

• Nombre:
• Cargo:
• Funciones, *con relación al tratamiento de los datos personales en el manejo del sistema.*
• Obligaciones: *en cuanto al tratamiento de los datos personales en el sistema.*

Encargado:

• Nombre:

• Cargo:
• Funciones:
• Obligaciones:

Usuario:

• Nombre:
• Cargo:
• Funciones:
• Obligaciones:

OBLIGACIONES

3.- Nombre de la Unidad Administrativa
4.- Nombre del sistema

Responsable:

• Nombre:
• Cargo:
• Funciones *con relación al tratamiento de los datos personales en el manejo del sistema.*
• Obligaciones: *en cuanto al tratamiento de los datos personales en el sistema.*

Encargado:

• Nombre:
• Cargo:
• Funciones:
• Obligaciones:

Usuario:

• Nombre:
• Cargo:
• Funciones:
• Obligaciones:

NOTA: Las funciones deben relacionarse con las de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de las facultades y atribuciones que le corresponden al Responsable del SDP de acuerdo con la Ley y los Lineamientos.

Si hay dos o más encargados del sistema y si existen dos o más usuarios del sistema, se recomienda agregar la información como Anexo al Documento de Seguridad, para hacer más fácil la integración del documento.
Establecer las obligaciones generales no incluidas en las categorías señaladas al principio de este apartado.

Ejemplo:

a) Guardar la debida secrecía sobre los datos personales que conozcan en el desarrollo de sus funciones, evitando su difusión y/o transmisión.

b) Informar al Responsable del Sistema o Responsable de Seguridad sobre cualquier incidencia que tenga conocimiento.

c) No dejar información visible cuando abandone su puesto, ya sea que se ausente de manera temporal o si hay alguna persona ajena a la Unidad Administrativa a la que esté adscrito.

d) Conservar el buen estado físico de los soportes documentales a que tengan acceso, con motivo del ejercicio de sus funciones.

e) Reportar alguna vulneración de los datos personales.

Establecer las políticas generales de seguridad que aplican a todo el personal o a persona ajena a la Unidad Administrativa que detenta el SDP.

III. REGISTRO DE INCIDENCIAS

1.- Los datos de la incidencia:

a) Nombre de la persona que resolvió el incidente;
b) Método aplicado (elaboración y entrega de informe donde precise los soportes físicos y técnicos afectados y los recuperados).
c) Soportes físicos: (oficios, expedientes, archiveros, ficheros, computadoras, discos duros robados o dañados)
d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados.

2.- Registro de la incidencia física o electrónica;

3.- Asegurar la incidencia;

4. Quién autorizó la recuperación de datos.

REPORTE DE INCIDENCIAS
FORMATO (A)

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

Versión del anexo			
Elaborado por:	Fecha elaboración	Aprobado por:	Fecha de aprobación:

En caso de presentarse una incidencia, deberá registrarse, tipo, fecha y hora, quien observó la incidencia, a quién se comunica y acciones a implementar para atender la incidencia.

Tipo de incidencia: _____

El momento en que se produjo: _____

Nombre y cargo de quién notifica la incidencia: _____

Nombre y cargo de quién recibe la notificación: _____

Las acciones que se implementan a consecuencia de la incidencia:

_____

Soportes físicos: (oficios, expedientes, archiveros, ficheros, computadoras, discos duros robados o dañados)
……

Soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados.
_.....
_____

Quién autorizó la recuperación de datos: _____

En caso de que se presente la incidencia, se generará un acta circunstanciada de hechos.

FORMATO DE ACTA CIRCUNSTANCIADA DE HECHOS

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

Tipo de incidencia
FORMATO (B)

Una incidencia de seguridad puede ser cualquier incumplimiento de las disposiciones establecidas en el documento de Seguridad, y cualquier anomalía que afecte o pueda afectar la seguridad de los datos de carácter personal en el sistema.

Estas, pueden ser generadas por el actuar de las personas que tienen acceso al sistema o a causa de desastres naturales y/o tecnológicos, así como a la comisión de delitos.

La Organización de las Naciones Unidas señala que los desastres se clasifican en:

1) Naturales; y
2) Tecnológicos.

IV. IDENTIFICACIÓN Y AUTENTIFICACIÓN

Mecanismos de identificación y autentificación

- El Responsable del sistema deberá elaborar una relación actualizada de los servidores públicos que tengan acceso autorizado al SDP. (Anexar relación) Indicar el Procedimiento de notificación o políticas de bajas de personal.
- El Responsable del sistema establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de toda persona que intente acceder al SDP. (Ejemplo: presentando identificación) [Incluir el procedimiento]

- Para SDP automatizados el Responsable del Sistema implementará procedimientos para el acceso seguro mediante asignación de claves y contraseñas al personal autorizado. Indicar el Procedimiento de creación y modificación de claves y contraseñas, señalando longitud, formato y contenido, así como inactivación de cuentas por baja de personal.

Medidas de seguridad implementadas para controlar el acceso de personas.

A las instalaciones:

a) identificarlo(a);
b) autenticarlo(a);
c) quien autoriza la identificación y la autenticación;
d) quien autoriza el acceso.

Al interior: *medidas de seguridad implementadas para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema.* (Oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos)

a) identificarlo(a);
b) autenticarlo(a);
c) quien autoriza la identificación y la autenticación;
d) quien autoriza el acceso.

V. CONTROL DE ACCESO, GESTIÓN DE SOPORTES Y COPIAS DE RESPALDO Y RECUPERACIÓN.

GESTIÓN DE SOPORTES

- Identificar el tipo de información que contienen los soportes físicos y electrónicos mediante el uso de etiquetas y ser inventariados. Sólo el personal autorizado podrá acceder a los soportes.

- Llevar un registro de la salida de las instalaciones u oficinas, de la información del SDP, la cual sólo podrá ser autorizada por la Responsable del mismo.

- Indicar el procedimiento para el traslado de información que contenga datos del sistema, debiendo adoptar medidas que eviten la sustracción, pérdida o acceso indebido a la misma. (Ejemplo: sobre cerrado con el sello o leyenda de CONFIDENCIAL y solo deberá de ser trasladado por personal autorizado)

- En caso de proceder alguna acción cuyo objeto sea la disposición documental autorizada, en cualquier medio, por destrucción o baja de la misma, cualquier soporte que contenga datos de carácter personal deberá destruirse o borrarse, adoptando medidas eficaces que eviten completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento, con el fin de evitar el acceso a la información contenida en el mismo, aplicando técnicas físicas o electrónicas.(Ejemplo: destruir en trituradora por el personal autorizado, los documentos físicos que contengan datos personales, formatear las computadoras que contengan información con datos personales, etc.)

- Se puede tomar la decisión de considerar medidas adicionales, si a través de la evaluación del riesgo se determina que no hay necesidad inmediata de implementar controles adicionales o que estos controles se pueden implementar posteriormente. Por ejemplo: el equipo 26 de cómputo actual falla, pero se genera un respaldo de esa información al final del día, por lo que se decide retener ese riesgo durante un mes y esperar para cambiar el equipo de cómputo por uno nuevo.

- Señalar si el responsable del tratamiento de datos personales contrata o se adhiere a servicios, aplicaciones e infraestructura de cómputo en la nube, y otros servicios que impliquen el tratamiento de datos personales, el proveedor externo estará obligado a garantizar la protección de datos personales con los principios y deberes establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

- En su caso, el responsable deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos, de conformidad con la Ley de Datos.

- Descripción de perfiles del usuario y contraseñas implementados por el responsable para tener control de acceso mediante una red electrónica:

A.- El Control de acceso podrá ser

- *Obligatorio;*
- *Discrecional;*
- *Rol desempeñado;*
- *Grupo perteneciente;*
- *De acuerdo al reglamento interior.*

B.- Por el Perfil del usuario y contraseña para el manejo del sistema operativo podrá ser porque:

- *Cuenta con un sistema operativo de red instalado en su equipo;*
- *Sistema operativo maneja rigurosos perfiles de usuario y contraseñas;*
- *El sistema operativo solo reconoce los nombres de usuarios y las contraseñas cuando los almacena.*

C.- Por el Perfil del usuario y contraseñas para el manejo del software podrá ser porque:

- El software *maneja rigurosos perfiles de usuario y contraseñas;*
- *El* software *solo reconoce los nombres de usuarios y las contraseñas cuando los almacena.*

D.- La administración de perfiles de usuario y contraseñas podrá ser por:

- *Alta de nuevos perfiles;*
- *La creación de nuevos perfiles;*
- *Registro de la creación de nuevos perfiles.*

E.- Acceso remoto al sistema de datos personales podrá ser porque:

- *Requieren los usuarios acceso remoto al equipo de cómputo para trabajar con el sistema;*
- *Requiere el administrador acceso remoto al equipo para realizar tareas de mantenimiento.*

RESPALDO Y RECUPERACIÓN

Establecer procedimientos conforme a las políticas existentes.

a) Copias de respaldo y recuperación.

- Procedimiento para realizar las copias de respaldo (establecer el procedimiento correspondiente).

-En soporte físico se procede a la digitalización de los documentos;
-En el soporte electrónico se realizará en discos, memorias externas, discos duros externos, etc.

- Periodo de realización; (lo establecerá el sujeto obligado)
- Verificación por parte del responsable. (al menos cada 6 meses)
- Establecer los procedimientos para recuperar datos contenidos en soportes electrónicos.

b) Pruebas con datos reales; (únicamente a sistemas informáticos y con previa copia de respaldo)

Se debe verificar la correcta aplicación y funcionamiento de los procedimientos para obtener copias de respaldo y de recuperación de los datos.

Las pruebas en nuevos sistemas informáticos diseñados para dar tratamiento al sistema, no se realizarán con datos reales, salvo que se asegure y garantice el nivel de seguridad correspondiente al tipo de datos tratados.

Previo a la realización de pruebas con datos reales, se debe elaborar una copia de respaldo.

VI. ANÁLISIS DE RIESGOS

Estudio de valor de los datos personales, el ciclo de vida, así como las causas, consecuencias, incidencias, amenazas y vulneraciones al sistema de tratamiento de datos personales.

- Benéfico; (nivel de riesgo inherente a los datos y numero de titulares que pueden ser afectados)
- Accesibilidad; (riesgo al número de accesos potenciales al sistema)
- Anónimo; (nivel de riesgo por el tipo de personas no identificables que tiene acceso al sistema)

- **Factores para Determinar las Medidas de Seguridad**. Conjunto de consideraciones que las organizaciones deben plantear como directrices para tratar el riesgo en función de sus alcances y objetivos.

- **Valoración Respecto al Riesgo**. Proceso de ponderación para identificar los escenarios de riesgo prioritarios y darles tratamiento proporcional, se compone de los siguientes pasos:

1. Identificar el tipo de nivel de seguridad y el valor de los datos personales, de acuerdo con su clasificación:

   - El incumplimiento con las obligaciones legales y contractuales relacionadas con el titular;
   - Vulneraciones de seguridad;

- Daño a la integridad de los titulares de datos personales;
- Daño a la reputación del Sujeto Obligado.

2. Identificar Amenazas: El valor y exposición;
3. Identificar Vulnerabilidades;
4. Identificar Escenarios de Vulneración y Consecuencias.

- **Criterios de aceptación del riesgo.** El Sujeto Obligado podría aceptar o no ciertos niveles de riesgo, siempre y cuando la naturaleza del riesgo, sus consecuencias o su probabilidad sean consideradas como muy poco significativas.

Se debe expresar el beneficio o el riesgo estimado para la organización, aplicando diferentes criterios de aceptación correspondientes al riesgo. Por ejemplo, riesgos que pueden resultar del incumplimiento a la Ley que no pueden ser aceptados.

Se deben incluir múltiples umbrales, correspondientes a diferentes niveles de aceptación, previendo que los responsables acepten riesgos sobre esos niveles en circunstancias específicas.

El análisis de riesgos y las medidas de seguridad implementadas como resultado de lo arriba descrito, se deberá enfocar en la protección de datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, así como en evitar las vulneraciones de conformidad con el artículo 3 fracción XVI de la Ley de Datos.

Ahora bien, la protección de datos personales deberá estar relacionada con el ciclo de vida de los datos personales previamente identificado y sus distintos tratamientos. Para el tratamiento de los datos personales, se deben identificar y ponderar con suficiente nivel de detalle para proveer información que permita hacer la valoración del riesgo. Se pueden identificar tres tipos de tratamiento de datos: físicos, automatizados o mixtos.

De conformidad con el artículo 4 de la Ley de Datos, será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

[Nota: Para mayor referencia, se anexa a la presente, el formato que servirá de guía de manera enunciativa más no limitativa, mismo que podrá utilizarse para llevar a cabo el análisis de riesgo, y el cual deberá de adaptarse a las condiciones de cada Sujeto Obligado. **(Anexo 1)]**

VII. ANÁLISIS DE BRECHA

Análisis de Brecha. Proceso de evaluación de las medidas de seguridad que ya existen en la organización contra las que sería conveniente tener, que resultan necesarias para la protección de Datos Personales.

Los controles de seguridad, sin que sean limitativos, deben considerar los dominios siguientes:

- Políticas del Sistema de Gestión Sistema de Datos Personales;
- Cumplimiento legal;
- Estructura organizacional de la seguridad;
- Clasificación y acceso de los activos;
- Seguridad del personal;
- Seguridad física y ambiental (Aéreas seguras y protección de equipamiento);
- Gestión de comunicaciones y operaciones;
- Control de acceso;
- Desarrollo y mantenimiento de sistemas;
- Vulneraciones de seguridad;
- Seguridad institucional; (control de las transferencias de datos)
- Activos responsables; (asignación de responsable y clasificación)
- Seguridad de sistemas de información; (procesos de información, protección de archivos del sistema)
- Incidentes de seguridad en la información; (regularidad con la que se dan).

[Nota: Para mayor referencia, se anexa a la presente, el formato que servirá de guía de manera enunciativa más no limitativa, mismo que podrá utilizarse para llevar a cabo el análisis de brecha, y el cual deberá de adaptarse a las condiciones de cada Sujeto Obligado. **(Anexo 2)]**

VIII. RESPONSABLE DE SEGURIDAD

Sera designado por el responsable y será el encargado de vigilar que se lleven a cabo todas las medidas de seguridad:

I. Desde el nivel básico;
II. Técnico;
III. Organizativo;
IV. Vigilar los centros de tratamiento de datos locales;
V. Equipos;
VI. Sistemas;
VII. Programas;
VIII. Personas que intervienen.

IX. REGISTRO DE ACCESO Y TELECOMUNICACIONES

Registro de quien tiene acceso al sistema:

a) Nombre y cargo de quien accede al sistema;
b) Identificación del sistema;
c) Identificación del expediente;
d) Propósito del acceso;

e) Fecha de acceso;
f) Fecha de término de la consulta;
g) Hora de consulta.

Telecomunicaciones (transferencia telemática de datos) Se determina que datos pueden transferirse de manera que no puede ser manipulada.

I. Sistemas;
II. Bases de datos;
III. Imágenes;
IV. Archivos:

Control de acceso

- Listado de personal con acceso autorizado (Señalar por figura únicamente aquellos datos y recursos que precisen para el desarrollo de sus funciones)
- Bitácora de acceso, éstas se utilizan en los soportes físicos o electrónicos, debiendo establecer procedimiento para el uso de bitácoras respecto de las acciones cotidianas llevadas a cabo en el SDP, las cuales pueden contener la información siguiente:
  Nombre y cargo de quien accede
  Identificación del expediente
  Propósito del acceso
  Fecha de acceso
  Hora de acceso
  Fecha de devolución
  Hora de devolución

Solamente el Responsable del Sistema podrá conceder, alterar o anular la autorización para el acceso al SDP.

X. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Para cumplimiento de lo establecido en el Artículo 25 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, el responsable deberá monitorear continuamente lo siguiente:

I. Los nuevos activos que se incluyan en la gestión de riesgos;

II. Las modificaciones necesarias a los datos, como podría ser el cambio o migración tecnológica, entre otras;

III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;

IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;

V. Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en el nivel inaceptable de riesgo; y

VII. Los incidentes y vulneraciones de seguridad ocurridas.

Acciones que se toma para mantener actualizadas las medidas de seguridad y revisión de la mismas

a. Política se seguridad;
b. Cumplimiento de la normatividad;
c. Organización de la seguridad en la información;
d. Clasificación e identificación de inventarios;
e. Administración de incidentes;
f. Continuidad en las operaciones;
g. Gestión de comunicaciones y operaciones;
h. Adquisición, desarrollo, uso y mantenimiento del sistema de información;
i. Soportes físicos;
j. Soportes electrónicos;

XI. PLAN DE TRABAJO

El responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nueva o faltante.

Se elaborará respecto de los faltantes en el análisis de brecha

1. Fuga de información; (prevención)
2. Disociación; (cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor)
3. Bloquear y dar de baja puertos y servicios innecesarios en los equipos de cómputo;
4. Ampliación de medidas de seguridad en caso de detectar faltantes;
5. Equipos de cómputo obsoletos;

XII. PLAN DE CAPACITACIÓN

Para los programas de capacitación, el responsable deberá tomar en cuenta lo siguiente:

I. Los requerimientos y actualizaciones del sistema de gestión;

II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de estos;

III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales; y

IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Calendario programático para llevar a cabo:

A. Capacitaciones integrales del personal que opera los sistemas;
B. Actualizaciones;
C. Fechas y duración de la capacitación;
D. Aéreas a capacitar;
E. Temas;
F. Mejoras implementadas;
G. Desaciertos y aciertos;
H. Oportunidades de mejora;
I. Retroalimentación.

FORMATO (C)

Análisis de Riesgo Amenazas, vulnerabilidades y recursos involucrados				
Código	Pregunta o Control	¿Existe? SI	¿Existe? NO	Observaciones (acciones a realizar en caso de no contar con:
1.- Amenazas				
1.1	*¿Tienes identificado los datos personales?*			
1.2	*¿Tienes clasificados los datos personales?*			
1.3	*¿Tienes establecido el ciclo de vida de los datos personales?*			
1.4	*¿Tienes definido el tratamiento que se le da a cada uno de los datos personales?*			
1.5	*¿Tienes capacitaciones sobre qué hacer en caso de que los datos personales queden expuestos?*			

1.6	*¿Tienes un catálogo sobre las consecuencias negativas para los titulares de los datos personales?*			
1.7	*¿Tienes un plan reactivo en caso de sufrir la pérdida de datos personales?*			
1.8	*¿Tienes una bitácora de las causas que originaron el daño al sistema y por ende a los datos personales?*			
1.9	*¿Tienes registro de las amenazas surgidas durante la implementación, puesta en marcha y desarrollo del sistema, el cual contiene datos personales?*			
1.10	*¿Tienes contemplado el riego inherente al tipo de dato personal vulnerado?*			
1.11	*¿Tienes contemplado el riego por el volumen de titulares afectados?*			
2. vulneraciones				
2.1	*¿Tienes una bitácora sobre vulneraciones sufridas en los datos personales?*			
2.2	*¿Tienes requerimientos regulatorios en caso de vulneración de los datos personales?*			

2.3	*¿Tienes una política a seguir en caso de daño al sistema por una vulneración de los datos personales?*			
2.4	*¿Tienes códigos de conducta del personal que trata datos personales?*			
2.5	*¿Tienes claro el beneficio para el atacante al obtener los datos personales?*			
2.6	*¿Tienes un sistema de todas y cada una de las consecuencias que surgieron a raíz de la vulneración del sistema que contiene datos personales?*			
2.7	*¿Tienes procedimientos para actuar ante la vulneración de los sistemas de datos personales?*			
3. recursos involucrados				
3.1	*¿Tienes un software para descubrir la anonimidad del atacante de los datos personales?*			
3.2	*¿Tienes respaldos en el caso de que la información fue vulnerada?*			
3.3	*¿Tienes hardware y software para respaldar los datos personales?*			

3.4	*¿Tienes personal capacitado para llevar a cabo los respaldos hardware y software que contendrán los datos personales?*			
3.5	*¿Tienes calendario, con fechas para dar servicio y mantenimiento a los sistemas, computadoras, discos duros, hardware y software en los que se almacenan datos personales?*			
3.6	*¿Tienes asesoría externa para dar servicio y mantenimiento a los sistemas, computadoras, discos duros, hardware y software en los que se almacenan datos personales?*			

FORMATO (D)

Análisis de brecha Medidas de seguridad existentes y medidas de seguridad faltantes				
Código	Pregunta o Control	¿Existe? SI	¿Existe? NO	Observaciones
1.- Medidas de seguridad basadas en la cultura del personal				
1.1	*¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?*			
1.1.1	Política de escritorio limpio			

1.1.2	Hábitos de cierre y resguardo			
1.1.3	Impresoras, escáneres, copiadoras y buzones limpios			
1.1.4	Gestión de bitácoras, usuarios y acceso			
2.-	*¿Tienes mecanismos para eliminar de manera segura la información?*			
2.1	Destrucción segura de documentos			
2.2	Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico			
2.3	Fijar periodos de retención y destrucción de información			
2.4	Tomar precauciones con los procedimientos de re-utilización			
2.5	*¿Has establecido y documentado los compromisos respecto a la protección de datos?*			
3.- Medidas de seguridad basadas en la cultura del personal				
3.1	Informar al personal sobre sus deberes mínimos de seguridad y protección de datos			
3.2	Fomentar la cultura de la seguridad de la información			
3.3	Difundir noticias en temas de seguridad			

3.4	Prevenir al personal sobre la *Ingeniería Social*			
3.5	Asegurar la protección de datos personales en subcontrataciones			
4	*¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?*			
4.1	Tener un procedimiento de notificación.			
4.2	Realizar revisiones y auditorías.			
5	*¿Realizas respaldos periódicos de los datos personales?*			
6.- Medidas de seguridad en el entorno de trabajo físico				
6.1	*¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?*			
6.1.1	Alerta del entorno de trabajo.			
6.1.2	Mantener registros del personal con acceso al entorno de trabajo			
6.2.1	*¿Tienes medidas de seguridad para evitar el robo?*			
6.2.2	Cerraduras y candados			
6.2.3	Elementos disuasorios.			
6.2.4	Minimizar el riesgo oportunista.			
6.3	*¿Cuidas el movimiento de*			

	información en entornos de trabajo físicos?			
6.3.1	Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico			
6.3.2	Mantener en movimiento sólo copias de la información, no el elemento original			
6.3.3	Usar mensajería certificada			
7.- Medidas de seguridad en el entorno de trabajo digital				
7.1	*¿Realizas actualizaciones al equipo de cómputo?*			
7.2	*¿Revisas periódicamente el software instalado en el equipo de cómputo?*			
7.3	*¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?*			
7.3.1	Uso de contraseñas y/o cifrado			
7.3.2	Uso de contraseñas solidas			
7.3.3	Bloqueo y cierre de sesiones			
7.3.4	Administrar usuarios y accesos			
7.4	*¿Revisas la configuración de seguridad del equipo de cómputo?*			
7.5	*¿Tienes medidas de seguridad para*			

	navegar en entornos digitales?			
7.5.1	Instalar herramientas antimalware y de filtrado de tráfico			
7.5.2	Reglas de navegación segura			
7.5.3	Reglas para la divulgación de información			
7.5.4	Uso de conexiones seguras			
7.6	*¿Cuidas el movimiento de información en entornos de trabajo digitales?*			
7.6.1	Validación del destinatario de una comunicación			
7.6.2	Seguridad de la información enviada y recibida			

FORMATO E

FORMATO DE REGISTRO DE INCIDENCIAS.

REGISTRO DE INCIDENCIAS DEL SISTEMA (NOMBRE DEL SISTEMA DE DATOS PERSONALES).

Versión del anexo			
Elaborado por:	Fecha elaboración	Aprobado por:	Fecha de aprobación:
I. Tipo de incidencia: (Precisar si se trata de pérdida, destrucción, robo, extravío, copia, uso, acceso o tratamiento, daño, alteración o modificación no autorizada)			
II. Motivo (posible o identificado) de la incidencia: (el motivo se relaciona con identificar las acciones u omisiones de cualquier persona que pudieran haber provocado la vulneración y sea posible distinguirlas en ese momento.)			
III. Tipo de soporte (X): Físico Automatizado Mixto			
IV. Momento en que se produjo: Fecha__/__/__ Hora__:__			
V. Valoración de la serie documental vinculada al sistema de datos personales afectado (X): a) Valor primario: Legal Fiscal Contable Administrativo b) Valor secundario: Informativo Testimonial Evidencial c) Tiempo de conservación de los datos personales contenidos en el sistema: Número de hoja: 1			

VI. Tipos de datos personales afectados: Número aproximado de titulares afectados:
VII. Lugar en que se produjo:
VIII. Nombre y cargo de quien notifica la incidencia: (Indicar el nombre y cargo de la persona que tuvo conocimiento por primera vez)
IX. Nombre y cargo de quien recibe la notificación: (Indicar nombre y cargo de la persona responsable de seguridad del sistema de datos personales)
X. Descripción de los hechos: (La descripción detallada de las circunstancias en torno a la vulneración ocurrida). Número de hoja: 2

XI. Efectos que derivan de la incidencia:
XII.Acciones correctivas implementadas de forma inmediata y definitivas, que derivan de la incidencia:

XIII. Nombre y cargo de quien autorizó la recuperación de datos:	
XIV. Comentarios adicionales:	
XV. Firma de las personas que intervinieron:	
_____ **Nombre y firma** Responsable del sistema de datos personales	_____ **Nombre y firma** Responsable de seguridad
_____(en caso que aplique)_____ **Nombre y firma** Encargado	_____ **Nombre y firma** Persona que notifica la incidencia
Número de hoja: 3	

FORMATO F

FORMATO DE ACTA CIRCUNSTANCIADA DE INCIDENCIAS

ACTA CIRCUNSTANCIADA DE INCIDENCIAS DEL SISTEMA DE DATOS PERSONALES (citar el nombre del sistema de datos personales).

En la Ciudad de México, siendo las _(1)_ horas, del _(2)_ de _(3)_ de _(4)_ se reunieron en las oficinas del **(indicar el nombre del sujeto obligado)** ubicadas **(indicar el domicilio del sujeto obligado)**, estando presentes: **quien notificó la incidencia de seguridad**, el(la) C. (5) que se identifica con (6) con domicilio en (7), el (la) C. (8) asignado (a) como responsable de seguridad que se identifica con (9)con domicilio en (10), el (la) C. (11) designado (a) como responsable del sistema de datos personales que se identifica con (12) con domicilio en (13), y el(la) C. (14) en su carácter de enlace en materia de protección de datos personales ante el INFO CDMX, que se identifica con (15) con domicilio en (16).

_____HECHOS

_____

I. Tipo de incidencia

_____(17)_____

II. Tipo de soporte

_____(18)_____

III. Momento en que se produjo la incidencia

_____(19)_____

IV. Lugar en que se produjo la incidencia

_____(20)_____

V. Nombre de quien notifica la incidencia

_____(21)_____

VI. Nombre y cargo de quien recibe la notificación de la incidencia

_____(22)_____

VII. Descripción de los hechos

_____(23)_____

VI. Efectos que derivan de la incidencia

_____(24)_____

VII. Acciones implementadas que derivan de la incidencia

_____(25)_____

_____(26)_____

La/El C. (27), responsable del sistema de datos personales manifiesta haber proporcionado todos los elementos necesarios para la formulación de esta acta circunstanciada, y que no fue omitido asunto alguno, información, documentación, o cualquier aspecto importante relativo a su gestión.

Los anexos que se mencionan en esta acta, constantes de (28) fojas útiles, forman parte integrante dela misma y se firman en todas sus hojas para su identificación y los efectos legales a que haya lugar.

La presencia del enlace en materia de protección de datos personales sólo tiene como finalidad verificar que la celebración del acta se realice conforme a la normatividad aplicable; por consiguiente, no avala su contenido, ni el de sus anexos, lo que queda bajo responsabilidad del personal involucrado en la incidencia, conforme a la normatividad aplicable en la materia.

La presente acta, no implica liberación alguna de responsabilidades que pudieran determinarse por la autoridad competente con posterioridad.

El/La C. (29) detenta todos los recursos y documentos que se precisan en el contenido de la presente acta y sus anexos

.....Cierre de acta.....Previa lectura de lapresente y no habiendo más que hacer constar, se da por concluida a las (30) horas del (31) , firmandopara constancia en todas sus hojas los que en ella intervinieron.---------

Nombre y Firma Persona que notifica la incidencia	**Nombre y Firma** Responsable de seguridad
Nombre y Firma Responsable del sistema de datos personales	**Nombre y Firma** Enlace en materia de datos personales

Contenido

1. Objetivo 2
2. Alcance 2
3. Marco normativo 2
4. Definiciones 3
5. Responsabilidades 4
6. Políticas de operación 6
7. Diagrama de flujo. 8
8. Descripción de las actividades 11

Control de Cambios

Revisión	Fecha	Descripción del Cambio
00	09 febrero 2023	Emisión del documento

1. Objetivo

Establecer las actividades a desarrollar para la actualización, publicación y verificación de las obligaciones de transparencia del Instituto Electoral de la Ciudad de México, en la sección de transparencia del Sitio Institucional de Internet y en la Plataforma Nacional de Transparencia.

2. Alcance

El presente procedimiento es aplicable para la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo, así como para las distintas Áreas Responsables del Instituto Electoral de la Ciudad de México, para realizar la publicación, actualización y verificación de las obligaciones de transparencia, establecidas en la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México y en los Lineamientos Técnicos para Publicar, Homologar y Estandarizar la información de las Obligaciones establecidas en el Título Quinto de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, emitidos por el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, así como para aquella información que se publique de manera proactiva.

3. Marco normativo

- Constitución Política de los Estados Unidos Mexicanos;
- Constitución Política de la Ciudad de México;
- Código de Instituciones y Procedimientos Electorales de la Ciudad de México;
- Ley General de Transparencia y Acceso a la Información Pública;
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México;
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;
- Ley General de Archivos;
- Ley de Archivos Local. Ley de Archivos, aplicable en la Ciudad de México.
- Reglamento Interior del Instituto Electoral de la Ciudad de México;
- Reglamento del Instituto Electoral de la Ciudad de México, en materia de Transparencia, Acceso a la Información Pública y Rendición de Cuentas;
- Lineamientos Técnicos Generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el Título Quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben difundir los Sujetos Obligados en los portales de Internet y en la Plataforma Nacional de Transparencia.
- Lineamientos Técnicos para Publicar, Homologar y Estandarizar la información de las Obligaciones establecidas en el Título Quinto de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

4. Definiciones

Actualización: Colocación de información (archivo, documento, base de datos, formato, video, imagen, hipervínculo, etcétera), por una versión más reciente, en la sección de transparencia del Sitio Institucional de Internet y/o la Plataforma Nacional de Transparencia.

AR´s: Cada una de las áreas administrativas del Instituto Electoral de la Ciudad de México, que generen, obtengan o posean información en términos de la legislación aplicable.

Circular: Documento emitido por la Secretaría Ejecutiva, mediante el cual se solicita a las AR's la actualización trimestral de las obligaciones en materia de transparencia, de conformidad con sus atribuciones.

Correo electrónico: Medio electrónico oficial, a través del cual la OTAIPDPyA, los Enlaces de las AR´s mantienen comunicación, respecto del envío, retroalimentación y publicación de las obligaciones de transparencia, tanto en la sección de transparencia del Sitio Institucional de Internet como en la Plataforma Nacional de Transparencia.

Datos abiertos: Datos digitales de carácter público generados por el Instituto Electoral de la Ciudad de México, los cuales son accesibles en línea y pueden ser usados, reutilizados y redistribuidos por cualquier interesado.

JDT: Jefatura de Departamento de Transparencia.

Enlace: Persona designada por cada Área Responsable del Instituto Electoral de la Ciudad de México, quien funge de vínculo con la OTAIPDPyA en las actividades de envío, retroalimentación de la información que derive de las obligaciones de transparencia, así como su colocación en la Plataforma Nacional de Transparencia.

Instituto Electoral de la Ciudad de México: Instituto Electoral.

INFO: Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

OTAIPDPyA: Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del Instituto Electoral de la Ciudad de México, a la cual también se le denominará indistintamente como Unidad de Transparencia.

UTCSyD: Unidad Técnica de Comunicación Social y Difusión.

UTSI: Unidad Técnica de Servicios Informáticos.

Oficio: Documento impreso utilizado por las AR´s para realizar una solicitud de publicación, actualización, sustitución o baja de la información contenida en la sección de transparencia del Sitio Institucional de Internet y para dar respuesta a la Circular en la materia y demás información complementaria, cuando así se requiera.

Lineamientos Técnicos: Lineamientos Técnicos Generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el Título Quinto y en la

fracción IV y artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portarles de Internet y en la Plataforma Nacional de Transparencia.

Lineamientos del INFO: Lineamientos Técnicos para Publicar, Homologar y Estandarizar la información de las Obligaciones establecidas en el Título Quinto de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

Ley de Transparencia: Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

PNT: Plataforma Nacional de Transparencia.

Publicación: Incorporación de información (archivo, documento, base de datos, formato, video, imagen, hipervínculo) de nueva creación en la sección de transparencia del Sitio Institucional de Internet.

Portal de Internet: Sitio web oficial del IECM, al que se puede acceder desde www.iecm.mx

Solicitud: Petición que realiza un Área Responsable a la OTAIPDPyA para publicar, actualizar, sustituir o eliminar información en la sección de transparencia.

SE: Secretaría Ejecutiva del Instituto Electoral.

Sección de Transparencia: Apartado específico del Sitio Institucional de Internet del Instituto Electoral, en donde se lleva a cabo la publicación y actualización de las Obligaciones de Transparencia del Instituto Electoral, y desde donde se vincula el Acceso a la PNT.

STyDP.- Subdirección de Transparencia y Datos Personales, adscrita a la Oficina de Acceso a la Información Pública y Protección de Datos Personales.

SIPOT: Sistema de Portales de Obligaciones de Transparencia de la Plataforma Nacional de Transparencia.

5. Responsabilidades

OTAIPDPyA

- Generar trimestralmente, el proyecto de Circular que suscriba la Secretaría Ejecutiva, en la que se solicite a las diversas AR´s del Instituto Electoral la actualización de las obligaciones de transparencia. Dicha Circular deberá **elaborarse y distribuirse 15 días hábiles antes del cierre de cada trimestre.**

- Coordinar a los Enlaces de las AR's, para la actualización y verificación de las Obligaciones de Transparencia, así como las actividades derivadas de dicho proceso.

	• Revisar y validar la información remitida por las AR's correspondiente a las obligaciones de transparencia, que se publican tanto en la sección de transparencia del Sitio Institucional de Internet como en la PNT, de conformidad con la Ley de Transparencia y los Lineamientos del INFO. • Coordinar y supervisar la publicación en la sección de transparencia, de toda aquella documentación que se genere con motivo de la celebración de sesiones de sus diversos órganos colegiados del Instituto Electoral; así como toda aquella que se considere de interés para la ciudadanía y que sea publicada de manera permanente y proactiva. • Dar seguimiento al cumplimiento de las obligaciones de transparencia y tiene la facultad de validar, o solicitar adecuaciones de la información que sea presentada conforme a la normatividad aplicable, para su publicación tanto en la sección de transparencia del Sitio Institucional de Internet, como en la PNT. • Deberá realizar la revisión final de forma y fondo de las obligaciones comunes y específicas, derivadas de los artículos 121, 128, 143, 146, 147 y 172 de la Ley de Transparencia. • Brindará asesoría permanente a los Enlaces de cada AR, respecto del llenado y en su caso corrección de los formatos para la presentación de la información. • Deberá verificar que la información cumpla con los criterios adjetivos y sustantivos de formato y de contenido establecidos en los Lineamientos del INFO.
AR´s	• Serán las encargadas y responsables del contenido de la información que sea publicada en la Sección de Transparencia, derivada de las obligaciones de transparencia. • Serán responsables del envío de la información a la OTAIPDPyA de conformidad con los plazos establecidos en el calendario de actualización de las obligaciones de transparencia, aprobado por el Comité de Transparencia; así como en la Circular que emita la SE de conformidad con sus atribuciones, en los formatos establecidos en los Lineamientos del INFO.
Enlace de las AR´s	• Establecer contacto con la OTAIPDPyA para coordinarse en la publicación o actualización de contenidos en la Sección de Transparencia y en el SIPOT de la PNT.

	• Revisar que la información quede debidamente colocada y/o actualizada en la Sección de Transparencia, y de ser así, comunicar vía correo electrónico su conformidad a la OTAIPDPyA y en su caso, las adecuaciones que resulten procedentes. • Realizar el proceso de carga en el SIPOT de la PNT, de la información acorde a sus atribuciones, tomando como base la información que ya haya sido validada y publicada en la Sección de Transparencia.
UTCSyD	• Brindar apoyo para realizar la publicación en la Sección de Transparencia del Sitio Institucional de Internet, de la información que sea enviada por la OTAIPDPyA.
UTSI	• Dar soporte técnico para el correcto funcionamiento del Sitio Institucional y el hipervínculo que dirige a la PNT.

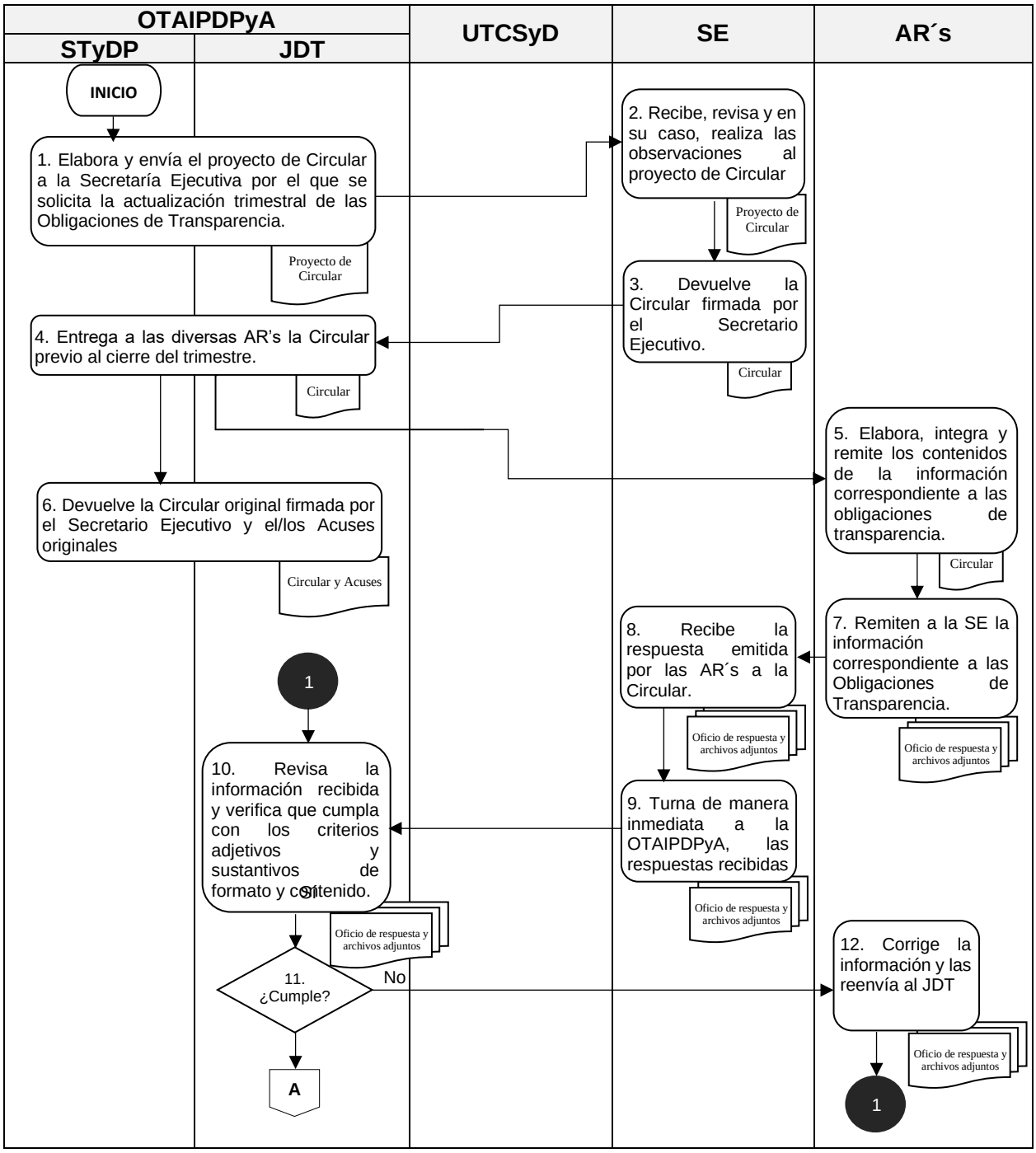
6. Políticas de operación

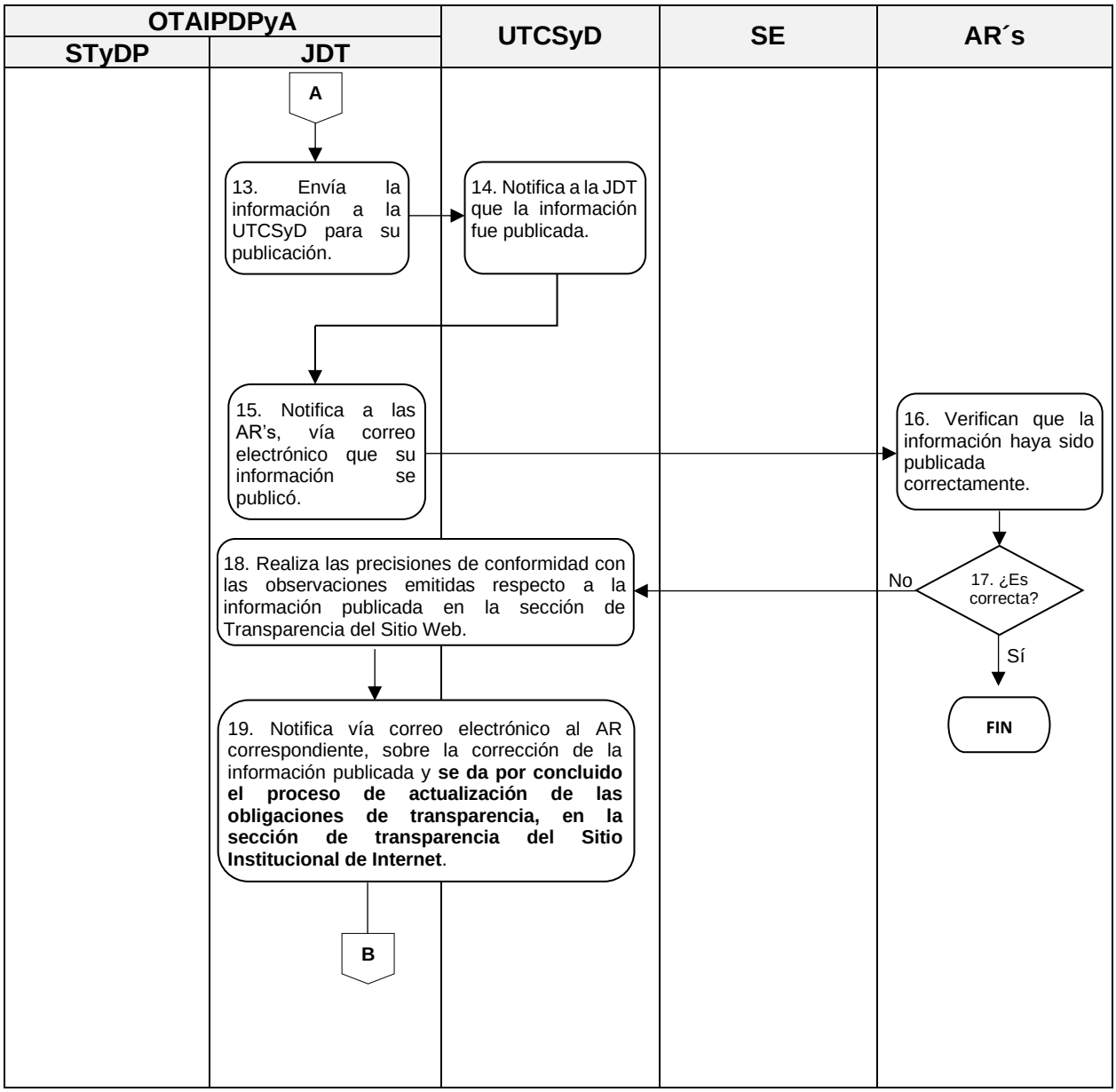
- La persona titular de la OTAIPDPyA a través de la JDT, elaborará durante el mes de diciembre de cada año, el calendario de actualización de la información pública del Instituto Electoral, aplicable para el ejercicio siguiente, con la finalidad de establecer los plazos para la entrega y publicación de las obligaciones de transparencia y en su caso las excepciones temporales para dicha entrega.
- El calendario de actualización de la información pública deberá ser aprobado en la primera Sesión Ordinaria que celebre el Comité de Transparencia y será publicado de manera inmediata en la sección de transparencia del Sitio Institucional de Internet.
- Las AR´s deberán enviar la información mediante oficio, así como sus anexos correspondientes en el término de **10 días hábiles posteriores al cierre de cada trimestre,** en respuesta a la Circular emitida por la Secretaría Ejecutiva; así como mediante correo electrónico a las direcciones que se mencionen en la Circular.
- Los formatos deberán enviarse conforme lo establecido en los Lineamientos del INFO y en estricto apego a los que se descargan directamente del SIPOT de la PNT.
- La información programático-presupuestal, financiera y contable, a que se refiere el artículo 121 fracciones XXI, XXII, XXVI, XXVII y XXXIII de la Ley de Transparencia, generada por la Secretaría Administrativa, podrá ser entregada dentro de los 20 días hábiles posteriores a la conclusión del trimestre, de conformidad con el calendario de actualización de la información, atendiendo a la normatividad correspondiente.

- **Dentro de los 10 días hábiles siguientes a que las AR´s envíen la información,** la OTAIPDPyA deberá notificar por correo electrónico a la persona que funja como Enlace, que su información ya fue publicada en la Sección de Transparencia.
- Las AR´s contarán con **5 días hábiles contados a partir de la notificación de la** OTAIPDPyA para realizar la carga de información correspondiente a las obligaciones de transparencia en el SIPOT de la PNT, haciéndolo del conocimiento de la JDT, para su revisión y validación.
- La JDT, contará con **5 días hábiles** para realizar la revisión de forma y fondo de la totalidad de la información publicada en la sección de transparencia del Sitio Institucional de Internet y que la misma corresponda a la publicada en la PNT.
- Las AR´s y los distintos Órganos Colegiados del Instituto Electoral, que de manera cotidiana generen información que deba hacerse púbica, serán los responsables de enviar la misma a la OTAIPDPyA, para su respectiva publicación en la Sección de Transparencia del Sitio Institucional de Internet, tal es el caso de la información contenida en las fracciones VIII y L, del Artículo 121 de la Ley de Transparencia.

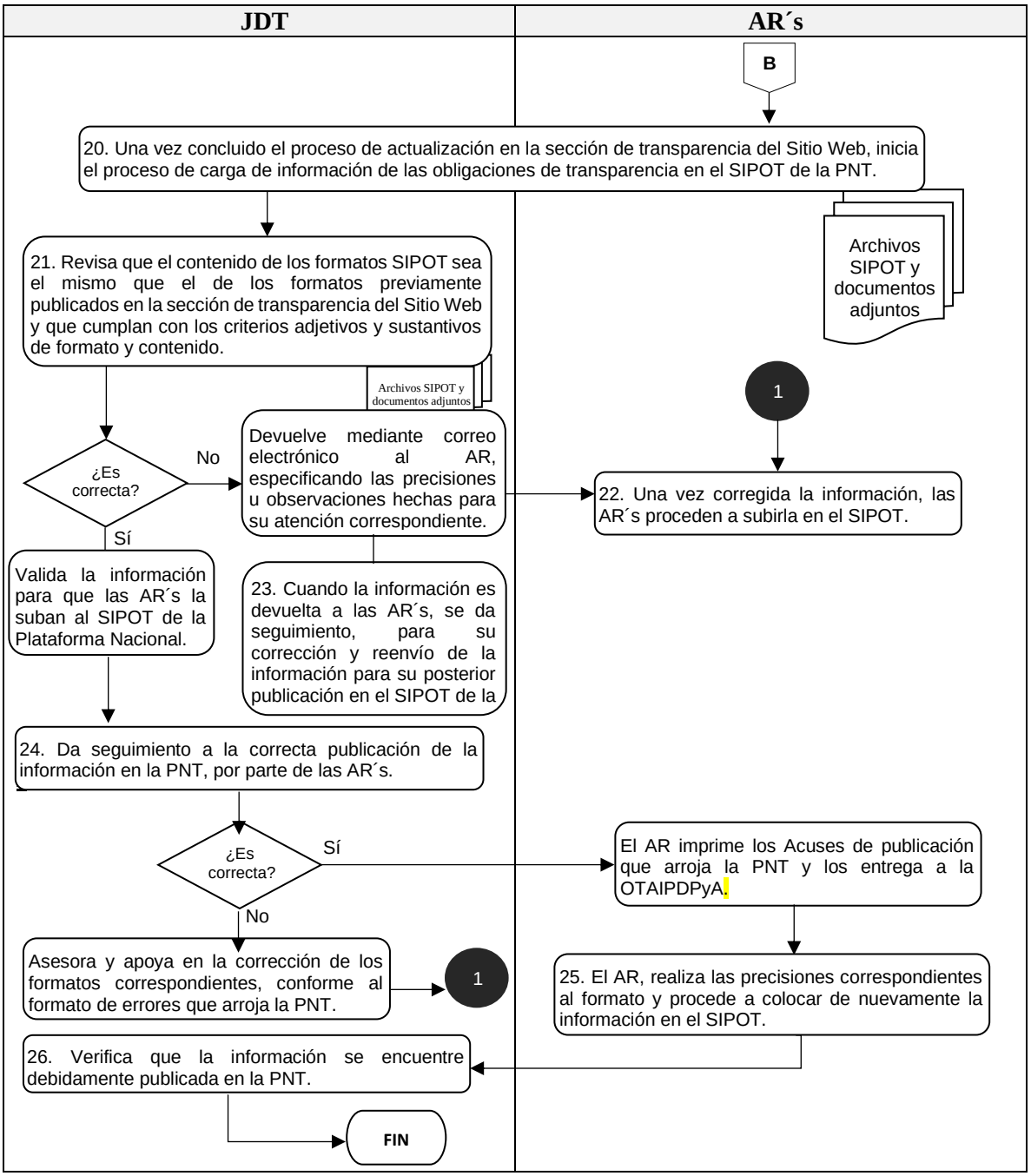
7. Diagrama de flujo.

7.1 Actualización y verificación de las Obligaciones de Transparencia en la sección de transparencia del Sitio Institucional de Internet.




OTAIPDPyA
STyDP
JDT
UTCSyD
SE
AR´s
A
13. Envía la información a la UTCSyD para su publicación.
14. Notifica a la JDT que la información fue publicada.
15. Notifica a las AR's, vía correo electrónico que su información se publicó.
16. Verifican que la información haya sido publicada correctamente.
17. ¿Es correcta?
No
Sí
18. Realiza las precisiones de conformidad con las observaciones emitidas respecto a la información publicada en la sección de Transparencia del Sitio Web.
19. Notifica vía correo electrónico al AR correspondiente, sobre la corrección de la información publicada y **se da por concluido el proceso de actualización de las obligaciones de transparencia, en la sección de transparencia del Sitio Institucional de Internet**.
B
FIN

8.2 Actualización y verificación de las Obligaciones de Transparencia en el Sistema de Portales de Obligaciones de Transparencia (SIPOT), de la Plataforma Nacional de Transparencia (PNT).



8. Descripción de las actividades

8.1 Actualización y verificación de las Obligaciones de Transparencia en la Sección de Transparencia.

Núm	Actividad	Área responsable	Documento empleado
A1	Elabora y envía el proyecto de Circular a la Secretaría Ejecutiva, por el que se solicita a las distintas AR´s del Instituto Electoral, la actualización trimestral de las Obligaciones de Transparencia, para su publicación en la Sección de Transparencia y la PNT; de conformidad con sus atribuciones. Dicho documento establece la fecha límite para la remisión de la información solicitada a las AR´s.	OTAIPDPyA STyDP y JDT	Proyecto de Circular.
A2	Recibe, revisa y en su caso, realiza las observaciones al proyecto de Circular relativa a la actualización trimestral de las obligaciones de transparencia, enviado por la OTAIPDPyA.	SE	Proyecto de Circular.
A3	Devuelve la Circular en materia de transparencia, firmada por el Secretario Ejecutivo, para su distribución entre las distintas áreas del Instituto Electoral.	SE	Circular.
A4	Previo al cierre del trimestre, se entrega a las diversas AR's la Circular en materia de transparencia.	STyDP, JDT	Circular (copia).
A5	Reciben la Circular, a efecto de elaborar, integrar y remitir, los contenidos de la información correspondiente a las Obligaciones de Transparencia, establecidas en la Ley de Transparencia.	AR´s	Circular (copia).
A6	Devuelve la Circular original firmada por el Secretario Ejecutivo y el/los Acuses originales de la Circular de transparencia que fue distribuida a las AR´s, a efecto de que obren en el archivo físico de la Secretaría Ejecutiva	OTAIPDPyA, JDT.	Circular original y Acuses.
A7	Remiten a la SE, dentro de los plazos establecidos, la respuesta a la Circular de Transparencia, con la información correspondiente a las Obligaciones de Transparencia, de conformidad con sus atribuciones.	AR´s	Oficio de respuesta a la Circular, acompañado de los Formatos

Núm	Actividad	Área responsable	Documento empleado
			Excel de los Lineamientos del INFO, así como archivos adjuntos (dependiendo de las necesidades de cada área, pueden ser: Word, PDF, Excel).
A8	Recibe la respuesta emitida por las AR´s a la Circular en materia de Transparencia, dentro de los plazos establecidos en la misma y turna de manera inmediata a la OTAIPDPyA, las respuestas recibidas a la Circular de Transparencia.	SE	Oficio, formatos Excel, en su caso archivos originales, y archivos adjuntos (CD, carpetas, información en medio electrónico) según corresponda.
A9	Revisa la información recibida y verifica que cumpla con los criterios adjetivos y sustantivos de formato y contenido, establecidos en los Lineamientos del INFO y los Lineamientos de clasificación de la información y cuando así proceda.	JDT	Formatos Excel de los Lineamientos del INFO y archivos adjuntos..
A10	Derivado de la revisión se determina si: ¿La información es correcta para su publicación en la sección de transparencia? **No.** Envía por correo electrónico al Enlace de AR´S, la información con las observaciones, lo anterior para su atención inmediata**.** **<u>El proceso continúa en la actividad 11.</u>** **Si.** Valida la información y la envía mediante correo electrónico a la UTCSyD para su publicación. **El proceso continúa en la actividad 14.**	JDT	Correo electrónico.

Núm	Actividad	Área responsable	Documento empleado
A11	Corrige la información de acuerdo a las observaciones realizadas por el JDT y las reenvía a dicho departamento para continuar con el proceso de revisión, validación y publicación.	Enlace de AR´S	Formatos Excel de los Lineamientos del INFO y archivos adjuntos.
A12	Envía la información corregida a la UTCSyD para su publicación, en la Sección de Transparencia.	JDT	Correo electrónico y archivos adjuntos.
A13	La UTCSyD notifica mediante correo electrónico al JDT que la información fue publicada.	UTCSyD	Correo electrónico.
A14	Concluida la publicación de la información en la Sección de Transparencia, las AR´s son notificadas vía correo electrónico, que su información ha sido publicada.	JDT	Correo electrónico
A15	Verifican que la información haya sido publicada correctamente.	AR´s	Revisión en página Web.
A16	Posterior a que las AR´s realizan la verificación de la información publicada se determina si: ¿La información fue correctamente publicada? **No.** Notifica vía correo electrónico al JDT de la OTAIPDPyA, para realizar los ajustes correspondientes. **<u>El proceso continua en la actividad 17.</u>** **Si. Fin del procedimiento de actualización de las Obligaciones de Transparencia en la Sección de Transparencia.**	AR´s	Correo electrónico.
A17	Realiza las precisiones respecto de la información publicada en la Sección de Transparencia, de conformidad con las observaciones emitidas por el Enlace del AR.	JDT en coordinación con personal de la UTCSyD	Documento.
A18	Notifica vía correo electrónico al AR correspondiente, sobre la corrección de la información publicada y se da por concluido el proceso de actualización de las Obligaciones de Transparencia, en la Sección de Transparencia.	JDT en coordinación con personal de la UTCSyD	Correo electrónico.

Núm	Actividad	Área responsable	Documento empleado
	El proceso de actualización continúa a partir de la actividad 19, de la siguiente sección.		

8.2 Actualización y verificación de las Obligaciones de Transparencia en el SIPOT.

Núm.	Actividad	Área responsable	Documento empleado
A19	Una vez concluido el proceso de actualización en la Sección de Transparencia, inicia el proceso de carga de información de las Obligaciones de Transparencia en el SIPOT de la PNT. Se procederá a descargar los formatos del SIPOT, accesando con el nombre de usuario y contraseña con los que cuenta cada Enlace de AR´s.	AR´s con el acompañamiento del JDT	Archivos Excel descargados del SIPOT y documentos adjuntos, en su caso.
A20	Revisa que el contenido de los formatos SIPOT sea el mismo que el de los formatos previamente publicados en la Sección de Transparencia y que cumplan con los criterios adjetivos y sustantivos de formato y contenido, establecidos en los Lineamientos del INFO; así como en los Lineamientos de clasificación de la información, cuando así proceda. ¿La información es correcta para su incorporación en el SIPOT? **No.** Devuelve mediante correo electrónico al enlace del AR, especificando las precisiones u observaciones hechas a la información, para su atención correspondiente. **El proceso continua en la actividad 21.** **Si.** Valida la información para que las AR´s la suban al SIPOT de la PNT. **El proceso continua en la actividad 22.**	JDT	Formato Excel de la PNT, documentos adjuntos y correo electrónico.
A21	Una vez corregida la información, las AR´s proceden a subirla en el SIPOT, con el acompañamiento y asesoría del JDT.	AR´s, JDT	Formato Excel de la PNT, correo electrónico y asesoría personal.

Núm.	Actividad	Área responsable	Documento empleado
A22	Da seguimiento a la publicación de la información en la PNT, por parte de las AR´s. ¿La información fue correctamente publicada en el SIPOT? **No.** Asesora y apoya en la corrección de los formatos correspondientes, conforme al formato de errores que arroja la PNT. **<u>El proceso continua en la actividad 23.</u>** **Si.** El AR imprime los Acuses de publicación que arroja la PNT y los entrega a la OTAIPDPyA.	JDT, AR´s	Acuses de publicación o Informe de errores de la PNT.
A23	Las AR´S corrigen los formatos y proceden a colocar de nuevamente la información en el SIPOT.	AR´s	Informe de errores y formato Excel de la PNT.
A24	Verifica que la información se encuentre debidamente publicada en la PNT, de conformidad con la normatividad aplicable. **Fin del proceso para la actualización de las Obligaciones de Transparencia en la Sección de Transparencia y la PNT.**	JDT	Acuse de publicación de la PNT y Lineamientos del INFO