INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

SECRETARÍA EJECUTIVA

Ciudad de México, 14 de mayo de 2026

CIRCULAR No. 30

PERSONAS TITULARES Y/O ENCARGADAS DE LA SECRETARÍA ADMINISTRATIVA, CONTRALORÍA INTERNA, DIRECCIONES EJECUTIVAS Y UNIDADES TÉCNICAS DEL INSTITUTO ELECTORAL DE LA CIUDAD DE MÉXICO
Presentes.

De conformidad con lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (Ley de Datos), el Instituto Electoral de la Ciudad de México (IECM) tiene la obligación de garantizar la protección de los datos personales a los que da tratamiento en el ejercicio de sus atribuciones, con el deber de establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales.

En este contexto, con independencia del tipo de sistema de datos personales en el que se encuentren los datos o el tipo de tratamiento que se efectúe, como sujeto obligado y responsable, el IECM debe establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

La descripción e implementación de las medidas de seguridad que aseguren un tratamiento adecuado de la información personal en posesión de este Instituto debe incorporarse en un sistema de gestión denominado ***Documento de Seguridad***.

De acuerdo con la Ley de Datos, la actualización de este instrumento se realiza cuando se presenten modificaciones sustanciales en el tratamiento de los datos que impliquen un cambio en el nivel de riesgo, ante una vulneración, con la implementación de medidas preventivas o correctivas; o bien, por recomendación del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFOCDMX).

De esta manera, considerando la revisión periódica de las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran; así como la coordinación y supervisión sobre la adopción de medidas de seguridad a que se encuentren sometidos los sistemas de datos personales institucionales; se ha determinado la actualización anual de este documento como parte de un proceso de mejora continua.

INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

SECRETARÍA EJECUTIVA

Ciudad de México, 14 de mayo de 2026

CIRCULAR No. 30

En consecuencia, a través de la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo (Oficina de Transparencia) y, con el propósito de homologar el formato y los apartados de información conforme a lo establecido en los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y la Guía elaboración del documento de seguridad; con fundamento en los artículos 86, fracciones I y XIX del Código de Instituciones y Procedimientos Electorales de la Ciudad de México, así como 19, fracciones VII y XX del Reglamento Interior del Instituto Electoral de la Ciudad de México, **se solicita a las áreas administrativas, de autonomía de gestión, ejecutivas y técnicas del IECM**, que tienen bajo su resguardo Sistemas de Datos Personales (SDP), **realizar la actualización correspondiente de sus Documentos de Seguridad**, utilizando el formato anexo.

Para tal efecto, se solicita que, a más tardar el **29 de mayo de 2026**, cumplan con la actualización de referidos instrumentos en el formato anexo y comuniquen a esta instancia ejecutiva, con atención a la Oficina de Transparencia, a las cuentas de correo institucional: otaipdpya@iecm.mx e iveth.morales@iecm.mx, que la han llevado a cabo.

Finalmente, y en caso de existir dudas o aclaraciones al respecto, podrán ponerse en contacto con la Licenciada Iveth Morales Leal, Titular de la Oficina de Transparencia, en la extensión 4726, o bien, a través de los correos institucionales indicados.

Sin otro particular, reciban un saludo cordial.

Atte. Bernardo Núñez Yedra
Secretario Ejecutivo

C.c.p. **Mtra. Patricia Avendaño Durán.** Consejera Presidenta del Consejo General del IECM. Para su conocimiento. Presente.
Consejeras y Consejero Electorales Integrantes del Consejo General del IECM. Para su conocimiento. Presentes.
Lic. Iveth Morales Leal. Titular de la Oficina de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo del IECM. Para seguimiento. Presente.
Archivo.

Validó	Iveth Morales Leal
Revisó	Arturo Feria Valencia
Elaboró	Nadia Edurne Martínez Morales

Documento de Seguridad

Sistema de Datos Personales ...

Área

INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

2026

	Documento de Seguridad	
	Sistema de Datos Personales ….	
	Fecha de elaboración **XX de XXXXXX de XXXX**	Fecha de la última Actualización **XX de XXXXX de 2026**
	Elaboró **XXXXXXX**	Aprobó **XXXXXX**

I. DATOS GENERALES DEL SISTEMA DE DATOS PERSONALES

Nombre del sistema: [Indicar el nombre del sistema de datos personales].

Fecha de publicación en la GOCDMX del acuerdo de creación: [Indicar la fecha de publicación en la GOCDMX del acuerdo de creación del sistema de datos personales y adjuntarlo como anexo al final (en caso de que aplique)].

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 y adjuntarlo como anexo al final].

Fecha de publicación en GOCDMX del Acuerdo de Modificación: [Indicar la fecha de publicación en la GOCDMX del acuerdo de modificación del sistema de datos personales y adjuntarlo como anexo (en caso de que aplique)].

Fecha de última modificación en el RESDP: [Indicar la fecha de modificación del sistema de datos personales en el RESDP y adjuntarlos como anexos].

Normatividad aplicable para el tratamiento

[Indicar la normativa aplicable al sistema de datos personales, de acuerdo con la publicación en la GOCDMX y el RESDP, enlistándola con artículos y fracciones].

Avisos de Privacidad (integral y simplificado): [verificar que las áreas cuenten con la última actualización]

II. INVENTARIO DE DATOS PERSONALES

Obtención

Las personas sobre las que se pretenden obtener datos de carácter personal son… **(indicar el grupo de personas objetivo).**
La recolección de los datos personales que contiene es de carácter **(enlistar los medios y agregar como anexo, así mismo, indicar los medios por los cuales se recaba la información, ya sean físicos, electrónicos o mixtos).**
Modo de tratamiento: El procesamiento de los datos personales se llevará a cabo a través de procedimientos **(indicar físicos, electrónicos o mixtos).**
Medio de actualización: la actualización de los datos personales se llevará a cabo **(indicar si es a petición del interesado, revisión periódica o mediante oficio).**

Finalidades del tratamiento

Finalidad y uso previsto: las finalidades de cada tratamiento de datos Personales **(indicar la finalidad o finalidades y usos previstos del sistema de datos personales, como en la GOCDMX y/o el RESDP).**

Remisiones (responsable – encargados)

[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, y, en su caso, las obligaciones encaminadas a cada uno, anexar copia del contrato, según sea el caso].

Transferencias

[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 estadísticos o científicos].

[En su caso indicar aquellas transferencias que se formalizaron mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad aplicable al responsable, se sugiere actualizar cada semestre, si es posible].

Interrelación

(Señalar si el sistema de datos personales se interrelaciona con otro sistema de datos personales del mismo sujeto obligado, indicando nombre y finalidad de la interrelación).

El catálogo de los tipos de datos personales

[Enlistar y agrupar los tipos de datos personales que recaban en el sistema de datos personales, en cada una de las categorías, indicando si tratan datos sensibles].
Los datos personales del sistema **(en físico, automatizado o mixto)** se encuentran contenidos **(señalar donde se encuentran contenidos, las series documentales en donde se consten todas las vinculadas a los SDP. Anexar Catálogo de Disposición Documental del sujeto obligado).**

Ciclo de vida de los datos

[Describir el tiempo de conservación de los datos personales con lo que señala el Catálogo de Disposición Documental del sujeto obligado).

- En medio automatizado:
- En archivo de trámite:
- En archivo de concentración:
- [En caso de que aplique se debe señalar si se contempla la transferencia de información al archivo histórico].

Nivel de seguridad: [Indicar el nivel de seguridad aplicable de acuerdo con el tipo de datos recabados, este puede ser básico, medio o alto].

Medidas de seguridad: [Indicar las medidas de seguridad adoptadas, aplicables conforme a lo establecido en la Ley de Datos local, estas pueden ser administrativas, físicas y/o técnicas].

Catálogo de las formas de almacenamiento:

Los expedientes del sistema de datos personales denominado **[Indicar el nombre del sistema],** se encuentran resguardados en el inmueble localizado en **[Indicar el domicilio de ubicación].**

[De igual forma se sugiere indicar la 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 sistema de datos personales en sus diferentes destinos, es decir, archivo de trámite, archivo de concentración, histórico y resguardo automatizado].

Lista de las personas servidoras públicas que tienen acceso al sistema de datos personales. [Indicar el nombre y cargo del responsable del sistema de datos personales y de los usuarios involucrados en el tratamiento].

Solo los siguientes servidores públicos, podrán acceder a los datos personales del sistema, en cumplimiento al desarrollo de las funciones y atribuciones que les han sido conferidas.

1. **Nombre**
   Cargo
2. **Nombre**
   Cargo

[Se sugiere agregar el organigrama correspondiente].

III. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE INTERVENGAN EN EL TRATAMIENTO DEL SISTEMA DE DATOS PERSONALES

Funciones y obligaciones del responsable del sistema de datos personales:
[Enlistar el nombre, cargo, domicilio oficial, correo oficial, teléfono oficial, así mismo se deberán indicar las funciones y obligaciones que tiene el responsable del sistema en materia de protección de datos personales].

Funciones y obligaciones del (los) usuario (s) del sistema de datos personales:
[Enlistar en un anexo el nombre y cargo de todos los usuarios, junto con los acuses de notificación a estos como parte del sistema, de igual forma se deberá indicar de acuerdo con las atribuciones del sujeto obligado las funciones y obligaciones que le competen a los usuarios del sistema, en materia de protección de datos personales, considerando las facultades que cada uno tiene].

Funciones y obligaciones del encargado del sistema de datos personales:
[Enlistar los datos de identificación del encargado como: denominación nombre, domicilio oficial, correo oficial, teléfono oficial; así mismo, indicar las funciones y obligaciones que, de acuerdo a las atribuciones del sujeto obligado, le competen, estas deben coincidir con lo establecido en los artículos 55 y 56 de la Ley de Datos local, así como, en el documento jurídico por el que se haya formalizado la relación con el responsable].

Establecer las obligaciones generales no incluidas en las categorías señaladas al principio de este apartado.
[Establecer las políticas generales de seguridad que aplican a todo el personal o a persona ajena a la unidad administrativa responsable del sistema de datos personales].

Funciones y obligaciones del responsable de seguridad del sistema de datos personales:
[Indicar el nombre, cargo, domicilio oficial, correo oficial, teléfono oficial del responsable de seguridad, así como las funciones y obligaciones que este tiene en materia de protección de datos personales].

IV. REGISTRO DE INCIDENCIAS

[Indicar el procedimiento o aspectos a considerar en caso de que ocurra una vulneración/incidencia; se sugiere incluir como anexos los formatos, reporte de incidencia y acta de hechos, los cuales podrá encontrar como anexos en la presente guía].

V. IDENTIFICACIÓN Y AUTENTIFICACIÓN

[Indicar el procedimiento o aspectos a considerar respecto de:

- Mecanismos de identificación y autentificación
- Medidas de seguridad implementadas para controlar el acceso de personas (en este caso puede ser para el acceso a las instalaciones o al interior del sujeto obligado)].

VI. CONTROL DE ACCESO, GESTIÓN DE SOPORTES Y COPIAS DE RESPALDO Y RECUPERACIÓN.

[Indicar el procedimiento o aspectos a considerar respecto a:

- Control de acceso
- Gestión de soportes
- Respaldo y recuperación

Para este apartado se pueden apoyar de su área tecnológica]

VII. ANÁLISIS DE RIESGOS

[Identificar Amenazas: El valor y exposición; identificar vulnerabilidades; e identificar escenarios de vulneración y consecuencias.

Se sugiere realizar una tabla en donde se describan los elementos antes mencionados].

VIII. ANÁLISIS DE BRECHA

[Se sugiere realizar una tabla en donde se describan los elementos faltantes para cubrir sus medidas de seguridad].

IX. REGISTRO DE ACCESO Y TELECOMUNICACIONES

[Agregar como anexo el registro de quién tiene acceso al sistema, así mismo, se deberá elaborar una bitácora.

Indicar si se consideran transferencias telemáticas de datos, es decir, que datos o de qué forma pueden transferirse de manera que no puede ser manipulada.

Solamente el responsable del sistema de datos personales podrá conceder, alterar o anular la autorización para el acceso al sistema de datos personales].

X. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

[Indicar las acciones o los procedimientos a considerar para mantener actualizadas las medidas de seguridad y revisión de estas, lo anterior en cumplimiento al artículo 25 de la Ley de Datos local].

XI. PLAN DE TRABAJO

[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; considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes].

XII. PLAN GENERAL DE CAPACITACIÓN

[Indicar, de acuerdo con la naturaleza del sistema de datos personales, las temáticas de interés sobre las que se quiere o pretende sensibilizar al personal involucrado en el tratamiento de datos personales, así como, incluir, temporalidad y especificar quienes son los que deben dar cumplimiento.

Para este apartado se puede considerar lo acordado en su programa anual de capacitación institucional, para ello, se sugiere incluir como anexo el mismo de manera íntegra].