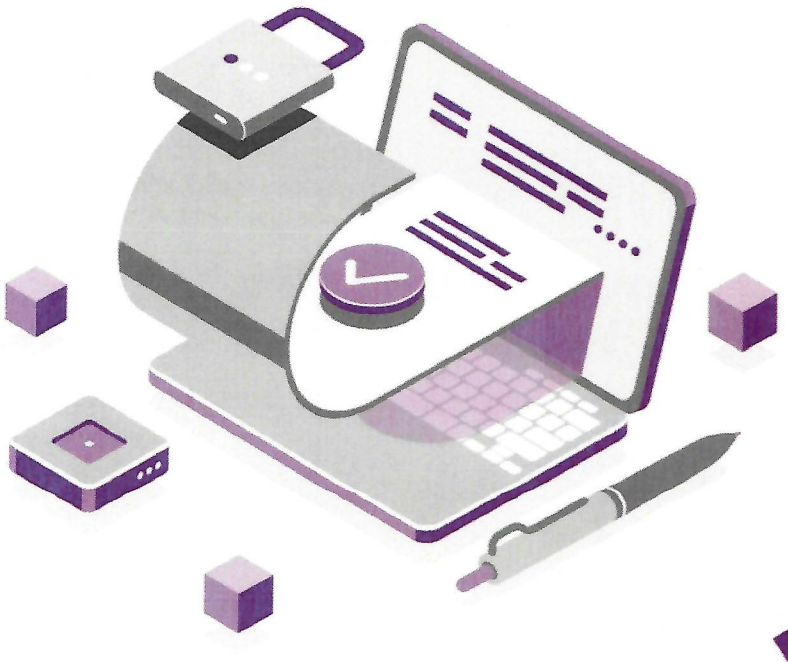
IEC
Instituto Electoral de Coahuila

Documento de Seguridad del Instituto Electoral de Coahuila



Índice

I. Introducción.

En el presente documento se detallan las medidas de seguridad administrativas, físicas y técnicas con las que se contará en el IEC para garantizar la debida protección de los datos personales a los que se les da tratamiento en las Direcciones Ejecutivas, Unidades Técnicas y Coordinaciones que los manejan.

Con este documento de seguridad se da cumplimiento al artículo 29 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Coahuila de Zaragoza, publicada en el Periódico Oficial del Gobierno del Estado de Coahuila de Zaragoza el día 21 de julio de 2017.

II. Glosario de términos.

- **Bases de datos:** Conjunto ordenado de datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, 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;

- **Catálogo de bases de datos personales:** Lista detallada del conjunto ordenado de bases de datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, 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;

- **Datos personales:** Cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

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

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

- **ICAI:** Instituto Coahuilense de Acceso a la Información Pública y Protección de Datos Personales;

- **IEC:** Instituto Electoral de Coahuila;

- **Inventario de datos personales:** Lista ordenada y detallada que posee el responsable o encargado, de cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a una persona física identificada o identificable;

- **Ley:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Coahuila de Zaragoza;

- **Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

- **Medidas de seguridad administrativas:** Políticas, acciones y 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 protección 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 como prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

- **Medidas de seguridad técnicas:** Conjunto de acciones, mecanismos y sistemas de los datos personales y los recursos involucrados en su tratamiento como revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware;

- **Nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;

- **Titular:** La persona física a quien corresponden los datos personales;

- **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, publicación,

almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales;

III. Inventario y catálogo de datos personales y de los sistemas de tratamiento.

1) Se describen las categorías de datos personales con los que cuenta el IEC, esto según el formato que se llenó por cada Dirección Ejecutiva, Unidad Técnica o Coordinación.

- **Datos de identificación y contacto:** nombre, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, firma autógrafa, edad, fotografía y referencias personales.
- **Datos biométricos:** huella dactilar.
- **Datos laborales:** puesto o cargo que desempeña, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información generada durante los procedimientos de reclutamiento, selección y contratación y experiencia/capacitación laboral.
- **Datos académicos:** trayectoria educativa, título, cédula profesional, certificados y reconocimientos.
- **Datos patrimoniales y/o financieros:** ingresos, egresos y cuentas bancarias.
- **Datos sobre pasatiempos, entretenimiento y diversión:** pasatiempos, aficiones, deportes que practica y juegos de interés.
- **Datos legales:** situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros).
- **Datos de salud:** estado de salud físico presente, pasado o futuro y estado de salud mental presente, pasado, o futuro.
- **Datos personales de naturaleza pública:** Datos que por mandato legal son de acceso público.

2) Personas de quienes se obtienen los datos personales:

a) Personas que laboran en el IEC.

b) Personas externas que prestan algún servicio para el IEC.

c) Personas externas que participan en actividades que llevan a cabo las Direcciones Ejecutivas y Unidades Técnicas del IEC (capacitaciones, concursos y programas).

Los datos personales se recaban por medio de documentos presentados y/o por el llenado de formularios físicos y/o electrónicos por los titulares de los datos personales.

3) Nivel de seguridad de los datos personales a los que se les da tratamiento en el IEC:

Para mayor garantía de seguridad en los datos personales y en las bases de datos personales, físicas o electrónicas, donde se concentran los mismos, las medidas de seguridad que se implementarán corresponden a un nivel de seguridad medio, siempre garantizando la confidencialidad, integridad y disponibilidad de los datos personales, tal y como lo expresa la Ley.

4) Transferencias de los datos personales:

Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 16, 68 y 72 de la Ley.

5) Catálogo de bases de datos personales de las Direcciones Ejecutivas, Unidades Técnicas y Coordinaciones del IEC:

El catálogo de bases de datos personales con las que cuentan las Direcciones Ejecutivas, Unidades Técnicas y Coordinaciones del IEC, esto con la finalidad de que el titular de los datos personales conozca en donde se almacenan sus datos y más información relevante. Esto coadyuva al ejercicio de los derechos ARCO.

IV. Las funciones y obligaciones de las personas que traten datos personales.

Las Direcciones Ejecutivas, Unidades Técnicas y Coordinaciones encargadas de tratar datos personales son las siguientes:

- Secretaría Ejecutiva
- Contraloría Interna
- Dirección Ejecutiva de Asuntos Jurídicos
- Dirección Ejecutiva de Administración
- Dirección Ejecutiva de Prerrogativas y Partidos Políticos
- Dirección Ejecutiva de Vinculación con el INE y OPLES
- Dirección Ejecutiva de Educación Cívica

- Dirección Ejecutiva de Participación Ciudadana
- Dirección Ejecutiva de Organización Electoral
- Dirección Ejecutiva de Innovación e Informática
- Unidad Técnica de Fiscalización
- Unidad Técnica de Transparencia y Acceso a la Información Pública
- Unidad Técnica de Archivo y Gestión Documental
- Unidad Técnica de Paridad e Inclusión
- Coordinación de Administración y Cuenta Pública
- Coordinación de Servicios y Apoyo Logístico
- Coordinación de Adquisiciones
- Coordinación de Auditoría
- Coordinación de Recursos Humanos

Las personas que desempeñan los puestos anteriormente mencionados, tienen como funciones y obligaciones las siguientes:

a) Garantizar la seguridad en el tratamiento de datos personales, esto con la finalidad de evitar algún riesgo, como la pérdida, robo, alteración o acceso no autorizado.

b) Garantizar la debida protección de los datos personales, conforme a la Ley y las demás disposiciones aplicables en la materia.

c) Implementar medidas de seguridad físicas, técnicas y administrativas convenientes para el tratamiento diario de los datos personales.

d) Garantizar la confidencialidad de los datos personales derivada de los procedimientos que tienen a su cargo.

e) Conocer y aplicar las acciones derivadas de este Documento de Seguridad.

f) Garantizar el cumplimiento de los derechos ARCO a los titulares de los datos personales.

V. Registro de incidencias.

Las incidencias con datos personales que se produzcan vulnerarán la debida protección de los mismos, por lo tanto, es necesario que, en las Direcciones Ejecutivas, Unidades Técnicas y Coordinaciones del IEC, en donde se dé tratamiento a datos personales lleven a cabo un registro de las incidencias que comprometen la seguridad de los datos.

El registro de incidencias deberá contener, por lo menos, la fecha de la incidencia, el tipo, descripción, la persona quien la registra, persona a quien se la comunica y la o las consecuencias que tendrá esa incidencia.

El personal del IEC que trate datos personales deberá de contar con el registro de incidencias, ya que quien identifique la incidencia será el encargado de registrarla y notificar a su superior inmediato, quien a su vez se encargará de notificar a la o las personas afectadas para que éste tome las precauciones debidas en caso de uso inadecuado de la información.

VI. Identificación y autentificación.

La Dirección Ejecutiva de Innovación e Informática es quien administra las bajas y altas de correos electrónicos del personal del IEC, así como las sesiones en los equipos de cómputo y la nube utilizada.

La persona encargada del departamento de informática asigna usuarios y contraseñas, siendo estas últimas aleatorias y se exige que se modifiquen.

La reserva y confidencialidad de estas contraseñas queda bajo la responsabilidad de la persona a la que se le asignó la cuenta de usuario.

Por ningún motivo las cuentas y las contraseñas de los usuarios de los correos electrónicos y de los equipos de cómputo serán transferibles.

VII. Control de acceso y gestión de soporte.

En todo momento, las Direcciones Ejecutivas y Unidades Técnicas del IEC que dan tratamiento a datos personales deberán tener un control de acceso a sus bases de datos personales físicas o electrónicas, en el cual establecerán medidas de seguridad que salvaguarden la confidencialidad e integridad de la información resguardada.

A efecto de evitar riesgos que vulneren los datos personales y la información que se resguarda por el personal del Instituto, se establecen contraseñas para ingresar a los equipos de cómputo, así como el acceso controlado a las áreas de trabajo, a través de un sensor que no permite que las puertas sean abiertas, únicamente con tarjeta de acceso habilitada por la Dirección Ejecutiva de Innovación e Informática.

Año tras año las Direcciones Ejecutivas y Unidades Técnicas del IEC deberán enviar la información física que contenga datos personales a la Unidad Técnica de Archivo y Gestión Documental (UTAGD), la cual deberá de contar con las instalaciones y protección adecuada para el resguardo de la misma información.

La UTAGD del IEC, por su parte, evitará en la medida de lo posible extraer información que contenga datos personales, esto con la finalidad de evitar el mal uso o la pérdida de la información.

VIII. Copias de respaldo y recuperación.

Las Direcciones Ejecutivas y Unidades Técnicas deberán digitalizar la información que se tenga de manera física, a fin de realizar la copia de seguridad correspondiente, evitando la pérdida de esta. La información digitalizada y electrónica será respaldada en un dispositivo de disco duro externo, mismo que deberá resguardarse en un lugar con acceso restringido a través de cerradura.

Dichas copias de seguridad de la información física y electrónica deberán realizarse anualmente y estarán bajo el resguardo de la persona que les da el tratamiento.

IX. Análisis de riesgos.

De acuerdo a una matriz de análisis de riesgos aplicada a las Direcciones Ejecutivas y Unidades Técnicas del IEC que dan tratamiento a datos personales, se consideran como riesgos más comunes con baja probabilidad de que suceda, los siguientes:

a) Daños por situaciones fortuitas o de fuerza mayor.
b) Extravío de documentación en las multifuncionales de uso común de las áreas.
c) Vulneración de los sistemas informáticos que resguardan la información del Instituto.
d) Manejo inadecuado de la información, por parte del personal que tiene acceso a ella, derivado de sus facultades y funciones.

X. Análisis de brecha.

Derivado del estudio del cuestionario denominado "Medidas de seguridad existentes VS medidas de seguridad faltantes" el cual se aplicó a las direcciones del IEC se concluyó que, actualmente, se tiene un nivel de medidas de seguridad óptimo en relación con los datos personales que se manejan.

Asimismo, con las medidas de seguridad que se señalan en este documento de seguridad se pretende que queden asentadas y uniformes.

XI. El plan de trabajo.

El plan de trabajo para la protección de los datos personales que el IEC llevará a cabo será cumplir con el proyecto que se tiene implementado en la Dirección de Datos Personales del ICAI, el cual se denomina "Certificación a Sujetos Obligados en materia

de Datos Personales", que cuenta con los siguientes pasos (sujeto a implementación del ICAI, por pandemia no se llevó a cabo desde 2020):

1. Canalizar a cada unidad administrativa que trate datos personales, la encuesta sobre el estado actual del cumplimiento de las obligaciones en materia de datos personales para que sea contestada y así poder conocer las áreas de oportunidad con las cuales se trabajará.
2. Capacitar al personal del IEC en materia de protección de datos personales e informarles del proyecto de Certificación (cuando así lo informe el ICAI).
3. Implementar medidas de seguridad físicas, administrativas y técnicas para la debida protección de los datos personales.
4. Conformar el documento de seguridad como lo requiere la Ley.
5. Llevar a cabo visitas de seguimiento y de verificación, esto con el objetivo de corroborar el cumplimiento de las obligaciones que marca la Ley.
6. Conformar la carpeta de evidencia del cumplimiento de las obligaciones según la para que ésta sea revisada y aprobada por la Comisión de Datos Personales del IEC.
7. De ser aprobada la carpeta de evidencia, el IEC tendrá por cumplidas las obligaciones de la Ley.
8. Vigilar el cumplimiento del correcto manejo y uso de datos personales, reportando cualquier vulneración que se llegare a suscitar, a través del formato de incidencia.

Cumplir con el proyecto de certificación será la acción prioritaria en materia de datos personales.

XII. Los mecanismos de monitoreo y revisión de las medidas de seguridad.

Las medidas de seguridad administrativas, físicas y técnicas serán de aplicación a todas las bases de datos personales que manejan las personas a cargo de las Direcciones Ejecutivas, Unidades Técnicas y Coordinaciones mencionadas en la fracción V del presente documento, esto de acuerdo a sus funciones y obligaciones.

Las medidas de seguridad que deberán observar las personas servidoras públicas del Instituto son las siguientes:

- Identificar los documentos que contienen datos personales, y darles un tratamiento confidencial, al no compartir la información con personas no autorizadas.
- Resguardar los documentos y expedientes que contengan información confidencial y reservada, en archiveros que cuenten cerradura.

- Mantener escritorio libre de documentos que pudieran estar a la vista de personas no autorizadas.
- Restringir el acceso al área de trabajo, a través del bloqueo de puertas, utilizando el sensor instalado para tal efecto.
- Bloqueo de acceso a los equipos de cómputo, a través de usuario y contraseña que únicamente podrá conocer la persona que utiliza el equipo.
- Modificación de contraseñas proporcionadas por las áreas para el uso de sistemas informáticos, con la finalidad de que únicamente la persona tenga acceso a los sistemas.
- Realizar respaldo electrónico de la información en un disco duro extraíble, el cual deberá resguardarse en un sitio seguro bajo llave.
- Utilizar las fotocopiadoras de uso común de manera cautelosa, asegurándose de no dejar documentos en ellas, así como cancelar los trabajos que no hayan sido impresos o fotocopiados por cualquier motivo.
- Llevar a cabo un registro de entradas y salidas de expedientes y documentos que contengan datos personales, en caso de que tengan que ser compartidos con otras áreas, y únicamente para dar cumplimiento al objeto por el que fueron solicitados.
- Portar en todo momento la tarjeta de acceso a las áreas de trabajo, a fin de no permitir el ingreso de personas no autorizadas, evitando abrir a personal que no cuente con la tarjeta habilitada.

XIII. Los programas de capacitación y actualización.

El personal de la Unidad Técnica de Transparencia y Acceso a la Información Pública capacitará al personal del IEC en materia de protección de datos personales una vez al año. La fecha se designará en el transcurso del mismo, esto con la intención de que todas las personas servidoras públicas estén presentes.

En caso de que en el transcurso del año se presente alguna modificación a la Ley de la materia, surja alguna actualización en el tema o alguna de las Direcciones Ejecutivas y/o Unidades Técnicas tenga la necesidad de capacitación, se solicitará la programación de la misma.

Asimismo, el personal de la Unidad Técnica de Transparencia y Acceso a la Información Pública del IEC estará en capacitación constante por medio de cursos y/o talleres presenciales o en línea por parte del ICAI y/o el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

XIV. Actualización del documento de seguridad.

I. El presente documento de seguridad se actualizará cuando ocurran los siguientes eventos:
II. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
III. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
IV. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad, e
V. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.
VI. Cuando surjan documentos, formatos, recomendaciones, etc. por parte del INAI para la mejora del documento de seguridad.

XV. Anexos.

Se anexan los análisis de riesgos y de brecha realizados por las Direcciones Ejecutivas y Unidades Técnicas, así como el catálogo de bases de datos personales de cada una de las áreas del Instituto Electoral de Coahuila y el formato de registro de incidencias.

Documento de seguridad aprobado por unanimidad de los presentes en la reunión ordinaria de la Comisión de Transparencia y Acceso a la Información, de fecha ocho (08) de septiembre de dos mil veintitrés (2023).

Mtra. Leticia Bravo Ostos
Consejera Electoral, Presidenta de la Comisión de Transparencia y Acceso a la Información

Mtro. Juan Antonio Silva Espinoza
Consejero Electoral, Integrante de la Comisión de Transparencia y Acceso a la Información

Mtro. Óscar Daniel Rodríguez Fuentes
Consejero Electoral, Integrante de la Comisión de Transparencia y Acceso a la Información

Licda. Erika Georgina Oyervides González
Secretaria Técnica de la Comisión de Transparencia y Acceso a la Información

Anexo

Registro de incidencias

Fecha de incidencia:	Número de incidencia:
Tipo de incidencia:	
Descripción detallada de la incidencia:	
Nombre y cargo de la persona que registra la incidencia:	
Nombre y cargo de la persona a quien se le comunica la incidencia:	
Consecuencias de la incidencia:	

Firma de quien registra la incidencia

Firma de a quien se le comunicó la incidencia