ACUERDO DEL CONSEJO GENERAL DEL INSTITUTO ELECTORAL DEL ESTADO, POR EL QUE APRUEBA EL REGLAMENTO DEL INSTITUTO ELECTORAL DEL ESTADO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

G L O S A R I O

Código Electoral	Código de Instituciones y Procesos Electorales del Estado de Puebla.
Comité	Comité de Transparencia y Acceso a la Información Pública.
Consejo General	Consejo General del Instituto Electoral del Estado.
Instituto	Instituto Electoral del Estado.
Ley de Protección de Datos	Ley de Protección de Datos Personales en posesión de los Sujetos Obligados del Estado de Puebla.
Unidad	Unidad Administrativa de Acceso a la Información del Instituto Electoral del Estado.

A N T E C E D E N T E S

I. El veinticinco de noviembre del año dos mil trece se publicó en el Periódico Oficial del Estado la Ley de Protección de Datos; disposición que en su artículo SEGUNDO transitorio estableció que los Sujetos Obligados contarían con el plazo de un año para adecuar sus Sistemas de Datos Personales de acuerdo a lo dispuesto en la mencionada Ley.

II. El Comité en fecha veintinueve de abril del año dos mil catorce emitió el acuerdo 01/COTAIP/290414, a través del cual aprobó iniciar el procedimiento de análisis y estudio del proyecto de Reglamento materia del presente documento.

III. La Titular de la Unidad, en su carácter de Secretaria del Comité, en seguimiento del acuerdo aludido en el antecedente previo, en fecha diecisiete de julio del año dos mil catorce remitió al citado Comité el "Proyecto de Reglamento del Instituto Electoral del Estado en materia de protección de datos personales", en dicho documento se consideraron los ajustes propuestos por la Dirección Jurídica del Instituto y los formulados por la Unidad.

IV. El Comité en sesión de fecha veintitrés de julio del año en curso mediante acuerdo 21/COTAIP/230714 aprobó el Proyecto del Reglamento materia del presente instrumento; facultando al Consejero Presidente de dicho Órgano Auxiliar para remitir la propuesta en alusión al Consejero Presidente del Instituto.

V. El Consejero Presidente del Comité en fecha veintinueve de julio del año dos mil catorce remitió al Consejero Presidente del Organismo la propuesta de reglamento multicitada, lo que hizo a través del memorándum IEE/PRE/COTAIP-25/14.

VI. La Dirección Técnica del Secretariado, por instrucciones del Secretario Ejecutivo, en fecha veintinueve de julio del año dos mil catorce remitió vía correo electrónico a los integrantes del Consejo General la propuesta de Reglamento a la que se hace referencia en numerales previos.

VII. Durante el desarrollo de la mesa de trabajo de los integrantes del Consejo General de fecha veintiocho de agosto del año dos mil catorce, los asistentes a la misma discutieron el asunto materia del presente documento.

C O N S I D E R A N D O

FINES DEL INSTITUTO Y ATRIBUCIONES DEL CONSEJO GENERAL

1. Que, en términos de lo establecido en el artículo 3 fracción II de la Constitución Local y los diversos 71 y 72 del Código Electoral, el Instituto es un organismo público de carácter permanente, autónomo en su funcionamiento, independiente en sus decisiones y profesional en su desempeño, con personalidad jurídica y patrimonio propio, encargado de la función estatal de organizar las elecciones, en cuya actuación debe observar los principios rectores de legalidad, imparcialidad, objetividad, certeza e independencia, mismos que se señalan en el artículo 8 del mencionado Código Electoral.

2. Que, el artículo 75 del Código Electoral señala que son fines del Instituto, entre otros, vigilar en el ámbito electoral el cumplimiento de la normatividad aplicable que garantice el derecho de organización y participación política de los ciudadanos; contribuir al desarrollo de la vida democrática y asegurar el ejercicio de los derechos político electorales de los ciudadanos y de los partidos políticos.

De acuerdo con lo establecido en el artículo 79 del Código Electoral el Consejo General es el Órgano Superior de Dirección del Instituto, responsable de vigilar el cumplimiento de las disposiciones constitucionales y legales en materia electoral.

Por su parte, el artículo 89 fracciones I, LIII y LVII del Código Electoral estable que son atribuciones del Consejo General, entre otras, expedir los reglamentos, circulares y lineamientos necesarios para el cumplimiento de sus fines; dictar los acuerdos necesarios a fin de cumplir con sus atribuciones; y las demás que le confiera el Código en cita.

DE LA PROTECCIÓN DE DATOS PERSONALES

3. Que, el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos garantiza el derecho al acceso a la información y la protección de los datos personales de todo individuo. En la base A de la citada disposición constitucional se establecen los principios para el ejercicio del derecho de acceso a la información, entre los que destaca la obligación del Estado Mexicano de diseñar y expedir leyes que protejan la información que se refiera a la vida privada y los datos personales. (fracción II).

Bajo ese orden de ideas, el Estado Mexicano, a través de sus órganos legislativos, considerando el contenido de tratados internacionales[1], ha expedido y publicado la normatividad correspondiente, verbigracia Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental; Ley Federal de Protección de Datos Personales en Posesión de los Particulares; en el caso de Puebla la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla; Ley para la Protección de Datos Personales en Posesión de los Particulares y la Ley de Protección de Datos; así como sus correspondientes reglamentos.

[1] Como es el caso de los artículos 12 de la Declaración Universal de los Derechos del Hombre; 8 del Convenio para la Protección de los Derechos y Libertados Fundamentales, 17 del Pacto Internacional de Derechos Civiles y Políticos; 11 apartado 2 de la Convención Americana sobre derechos humanos; entre otras.

Resulta importante señalar que estas disposiciones obligan a todas las instancias que integran el Estado Mexicano por lo que los órganos constitucionalmente autónomos (Federales y Locales) también son considerados sujetos obligados en materia de información pública y protección de datos personales.

De igual forma se han establecido instancias que abonan al adecuado ejercicio de la garantía consagrada en el artículo 6 del Código Político Federal como es el caso a nivel federal del Instituto Federal de Acceso a la Información y Protección de Datos, y a nivel local la Comisión para el Acceso a la Información Pública y Protección de Datos Personales del Estado, creando además figuras como las Unidades de Acceso a la Información Pública en los diferentes órganos de la administración pública, tanto federal como local.

La Comisión aludida en el párrafo anterior cuenta con atribuciones para emitir los lineamientos o criterios necesarios que impulsen el debido ejercicio del acceso a la información y la protección de datos personales de todo individuo, mismos que vinculan a los denominados Sujetos Obligados para su observancia sin invadir su correspondiente esfera de competencia, ya que se circunscriben a lo establecido en el multicitado artículo 6 Constitucional Federal.

Señalado todo lo anterior, es importante destacar que, el artículo 1 de la Ley de Protección de Datos establece que la misma es de orden público y tiene como objeto garantizar la protección de datos personales en posesión de los Sujetos Obligados[2], así como establecer los principios, derechos, obligaciones y procedimientos que regulan la protección y tratamiento de los mismos.

Por su parte, el artículo 8 de la Ley de Protección de Datos establece que los integrantes de los Sujetos Obligados no podrán difundir, distribuir o transmitir los datos personales a los que tenga acceso para el ejercicio de sus funciones, salvo disposición legal o que medie consentimiento expreso, por escrito, del titular de dichos datos.

Dicha prohibición también es aplicable para los Sistemas de Datos Personales[3] desarrollados en el ejercicio de las funciones de los Sujetos Obligados, según lo establece el diverso 9 de la Ley de Protección de Datos.

Los citados Sistemas de Datos personales, en términos del artículo 12 de la Ley de Protección de Datos, no pueden crearse con la finalidad exclusiva de almacenar los datos personales sensibles[4] y solo se tratarán cuando medien razones de interés público; lo disponga la ley; lo consienta expresamente el titular; tenga fines estadísticos, científicos o históricos; siempre y cuando se hubiera realizado previamente el procedimiento de disociación.

En la ejecución de los multicitados Sistemas el responsable de los mismos deberá crear, establecer, modificar, eliminar y llevar a cabo el procedimiento de disociación,

---

[2] En términos del artículo 2 fracción VI de la Ley de Protección de Datos, los Órganos Constitucionales, entre los que se encuentra el Instituto, son considerados sujetos obligados.

[3] La fracción XXII del artículo 2 de la Ley de Protección de Datos los define como todo el conjunto organizado de archivos, registros, bases o banco de datos personales de los Sujetos Obligados, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

[4] El artículo 2 fracción VII los define como aquellos datos personales que atañen a la esfera más íntima de su titular, o cuyo uso indebido propicie discriminación o conlleve un riesgo grave para su titular.

conforme a su respectivo ámbito de competencia; según lo prevé el diverso 16 de la multialudida Ley Estatal.

En lo que toca a la integración, tratamiento y tutela de los Sistemas de Datos Personales, el artículo 17 de la Ley de Protección de Datos, establece que deben acreditarse los siguientes extremos:

> I. Se crearán Sistemas de Datos Personales atendiendo a la finalidad o propósito por el que se recaben, contándose al menos con los siguientes:
>
> a) De los integrantes del Sujeto Obligado;
> b) De los proveedores, en su caso; y
> c) De aquéllos que realicen trámites y servicios, en su caso.
>
> II. En la creación o modificación de Sistemas de Datos Personales se indicará por lo menos:
>
> a) La finalidad del Sistema de Datos Personales y los usos previstos para el mismo;
> b) Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos;
> c) El procedimiento de recolección de los datos de carácter personal;
> d) La estructura básica del Sistema de Datos Personales, la categoría de los tipos de datos incluidos en el sistema y el modo de tratamiento;
> e) La transmisión de las que pueden ser objeto los datos;
> f) Las instancias responsables del tratamiento del Sistema de Datos Personales;
> g) La unidad administrativa ante la que podrán ejercitarse los derechos de acceso, rectificación, cancelación u oposición; y
> h) El nivel de protección exigible.

Aunado a lo anterior, el diverso 25 de la Ley de Protección de Datos señala que el Sujeto Obligado establecerá las medidas de seguridad necesarias para garantizar la integridad de cada uno de los Sistemas de Datos Personales que estén bajo su posesión o tratamiento, así como el cumplimiento de los principios de confidencialidad, disponibilidad, responsabilidad y seguridad.

En lo que toca a los tipos y niveles de las medidas de seguridad aludidas, el artículo 27 de la Ley de Protección de Datos Personales prevé las siguientes:

- Tipos de seguridad:
  I. Física: Se refiere a toda medida destinada a la protección de instalaciones, equipos, soportes o sistemas de datos para la prevención de riesgos;
  II. Lógica: Se refiere a las medidas de protección que permitan la identificación y autentificación de cualquier persona o usuario externo autorizado para el tratamiento de los datos personales de acuerdo con su función;
  III. De cifrado: Consiste en la implementación de claves y contraseñas, así como dispositivos de protección, que garanticen la integridad y confidencialidad de la información; y
  IV. De comunicaciones y redes: Conjunto de restricciones preventivas y/o de riesgos que deberán observar los Sujetos Obligados y los usuarios externos

de los Sistemas de Datos Personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones.

- Niveles de seguridad:
  I. Básico: Son las medidas generales de seguridad cuya aplicación es obligatoria para todos los Sistemas de Datos Personales.
  II. Medio: Se refiere a la adopción de medidas de seguridad que deberán implementarse en los Sistemas de Datos Personales relativos a la comisión de infracciones administrativas, hacienda pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.
  III. Alto: Son las medidas de seguridad aplicables a sistemas concernientes a datos personales sensibles; así como los que contengan datos recabados para fines de salud, de seguridad, prevención, investigación y persecución de delitos.

DE LOS DERECHOS EN MATERIA DE DATOS PERSONALES Y LA FORMA PARA EJERCERLOS

4. Que, el artículo 37 de la Ley de Protección de Datos, consigna que todas las personas podrán ejercer por sí o por medio de su representante legal, los derechos de acceso, rectificación, cancelación u oposición de sus datos personales en posesión de los Sujetos Obligados.

La Ley de Protección de Datos Personales señala qué debe entenderse por cada uno de los derechos aludidos en el párrafo previo, acepciones que se enuncian en las viñetas insertas a continuación, seguidas del artículo aplicable, según corresponda, del mencionado ordenamiento jurídico.

- Derecho de acceso: Aquél que tiene toda persona para solicitar y obtener información de sus datos de carácter personal sometidos a tratamiento; se ejerce para solicitar y obtener información de los datos de carácter personal, su origen, así como las transmisiones realizadas o que se prevén hacer. (Artículos 3, fracción VIII y 39)

- Derecho de rectificación de datos del titular: Aquél que posee el titular de solicitar la corrección de datos que resulten inexactos, incompletos o inadecuados o excesivos. (Artículos 3 fracción XI y 40)

- Derecho de cancelación de sus datos personales: Aquél que posee el titular de los datos personales para que se eliminen los que resulten ser inadecuados o excesivos, o cuando el tratamiento no se ajuste a lo dispuesto por las disposiciones legales aplicables; o cuando hubiere ejercido el derecho de oposición y éste haya resultado procedente. (Artículos 3 fracción IX y 41)

- Derecho de Oposición: Aquél que posee el titular de negarse al tratamiento de los datos que le conciernan en caso de que hayan sido recabados sin su consentimiento, o cuando existan motivos fundados para ello y la Ley no disponga lo contrario. (Artículos 3 fracción X y 42)

El Titulo Cuarto, Capítulo II de la Ley de Protección de Datos establece el procedimiento al que se encuentra sujeto el ejercicio de los derechos enlistados previamente, el cual se puede enunciar de forma sintética en lo siguiente:

- Presentación de la solicitud correspondiente.
- Acreditar identidad y personalidad.
- Señalar de forma precisa el dato erróneo; la corrección; o las razones por las cuales el tratamiento de los datos personales no se sujeta a la normatividad.
- La respuesta a la solicitud debe ser por escrito y en un término de quince días hábiles.

DE LA EXPEDICIÓN DEL REGLAMENTO

5. Que, el artículo 3 fracción II de la Constitución Política del Estado Libre y Soberano de Puebla otorga la calidad de Órgano Constitucionalmente Autónomo al Instituto, encomendándole la función estatal de organizar las elecciones locales.

La autonomía otorgada a este Instituto, entendida como la capacidad de auto regularse y que además lo desvincula de los poderes públicos reconocidos en la Constitución Política Estatal, es una figura que asegura el desarrollo adecuado de la función estatal que le fue encomendada, sin que ello excluya a la autoridad electoral de acatar disposiciones legales que buscan asegurar el adecuado ejercicio de los derechos que la constitución reconoce a todo individuo.

Así, en lo relativo a la materia de protección de datos personales, este Instituto debe acatar las disposiciones que el Legislador Local aprobó para asegurar el respeto del artículo 6 de la Constitución Política Federal.

Situación que no implica vulneración alguna a la autonomía del Instituto y obedece al diseño institucional que la Constitución y las Leyes han establecido para reconocer al ciudadano un mayor número de derechos y la posibilidad de oponerlos de manera efectiva a las instancias públicas, cuestión que sin duda es una de las características del Estado constitucional y democrático de derecho que tiene vigencia en nuestro país.

Sirve de sustento a lo anterior la tesis sostenida por la Suprema Corte de Justicia de la Nación, cuyo rubro es: "INSTITUTO DE TRANSPARENCIA E INFORMACIÓN PÚBLICA DE JALISCO. EL QUE TENGA COMO ATRIBUCIÓN PROMOVER LA TRANSPARENCIA ADMINISTRATIVA, ASÍ COMO LA DIFUSIÓN, PROTECCIÓN Y RESPETO AL DERECHO A LA INFORMACIÓN PÚBLICA, NO LO COLOCA POR ENCIMA DE LOS PODERES ESTATALES NI DISMINUYE SU ESFERA DECOMPETENCIA."[5]

Por su parte, el artículo 34 fracciones I, II, VI, VIII y X de la Ley de Protección de Datos señala que los Sujetos Obligados, entre otras, deberán observar las siguientes obligaciones: cumplir con las normas para el manejo, tratamiento, seguridad y protección de datos personales; adoptar las medidas de seguridad necesarias para la protección de datos personales; adoptar los procedimientos adecuados para dar trámite a las solicitudes de acceso, rectificación, cancelación u oposición de datos personales, y en su caso, para la transmisión de los mismos; establecer los criterios específicos sobre el manejo,

[5] Tesis: P. IX/2008, visible en Semanario Judicial de la Federación y su Gaceta, Tomo XXVII, Febrero de 2008, Pag. 1867

mantenimiento, seguridad y protección del Sistema de Datos Personales; coordinar y supervisar la adopción de las medidas de seguridad de los Sistemas de Datos.

Bajo ese orden de ideas, el Comité y la Unidad en el ejercicio de sus atribuciones elaboraron el proyecto del "Reglamento del Instituto Electoral del Estado en materia de protección de datos personales", el cual tiene como objeto que el Instituto cuente con una herramienta jurídica adecuada para el cumplimiento de las obligaciones en lo relativo a la creación, manejo y destrucción de la información personal con la que cuente el Instituto; obligaciones que impone la Ley de Protección de Datos Personales así como las Políticas y Lineamientos emitidos por la Comisión para el Acceso a la Información Pública y Protección de Datos Personales del Estado. [6]

Debe indicarse que en la elaboración y revisión del citado proyecto de Reglamento, participó en el ámbito de su competencia la Dirección Jurídica del Instituto, instancia que en términos del artículo 101 bis, fracción VI del Código Electoral tiene la atribución de revisar los proyectos de los reglamentos y demás ordenamientos internos necesarios para el buen funcionamiento del Instituto.

El proyecto de Reglamento puesto a conocimiento del Consejo General se encuentra conformado de la siguiente manera:

Titulo Primero. Disposiciones preliminares

Capítulo I. Disposiciones Generales.
Capítulo II. De los órganos competentes y de la Unidad de Acceso.

Titulo Segundo. De los datos personales.

Capítulo I. Principios que rigen el tratamiento de datos personales.
Capítulo II. De los sistemas de datos personales.
Capítulo III. De las medidas de seguridad.
Capítulo IV. De las funciones y obligaciones del responsable del sistema.
Capítulo V. De la transmisión externa de datos personales.
Capítulo VI. De las medidas compensatorias.

Título Tercero. De los derechos y del procedimiento.

Capítulo I. De los derechos ARCO.
Capítulo II. Del procedimiento.

Título Cuarto. Responsabilidades.

Capítulo Único. Disposiciones Generales.

Artículos Transitorios.

[6] Denominadas "Las Políticas y lineamientos de observancia general para el manejo, tratamiento, seguridad y protección de los datos personales en posesión de los sujetos obligados del Estado de Puebla", emitidas el día veintiséis de marzo del año dos mil catorce.

Una vez que el Consejo General se avocó al estudio del citado documento considera oportuno indicar que el mismo observa de forma puntual lo establecido en la Ley de Protección de Datos, ya que señala, entre otras cosas, lo siguiente:

- Las atribuciones del Consejo General, el Comité y la Unidad, en lo que toca a la protección de datos personales.
- La creación, manejo y destrucción de los Sistemas de Datos Personales.
- La integración, tratamiento y tutela de los citados Sistemas.
- La figura de responsable de los Sistemas de Datos Personales, que recae en el titular de la Unidad Técnica o Administrativa a la que se encuentre adscrito el citado sistema; quien podrá designar a los encargados del tratamiento de los datos, dentro del personal adscrito a su Unidad.
- Se prevé además que el responsable de Seguridad Informática sea la Coordinación de Informática del Instituto.
- Las funciones y obligaciones del responsable del sistema.
- Los tipos y niveles de las medidas de seguridad en el tratamiento de datos personales.
- Las medidas necesarias para asegurar el debido ejercicio de los derechos de acceso, rectificación, cancelación u oposición de datos personales en posesión del Instituto.
- El procedimiento al que se encuentra sujeto el ejercicio de los derechos citados.
- La eventual aprobación por parte del Consejo General de las medidas compensatorias.
- Así como las causales para ser sujeto de responsabilidad en materia de datos personales.
- El momento en que entrará en vigor las disposiciones del multicitado Reglamento.

De igual forma, se considera oportuno indicar que el Reglamento en alusión, se constituye en una herramienta jurídica adecuada para la protección de datos personales, ya que permitirá que aquellos ciudadanos, de los que se recabe la citada información, ejerzan los derechos de acceso, rectificación, cancelación u oposición de sus datos personales en posesión del Instituto, misma que será manejada a través de los sistemas y medidas de seguridad correspondientes.

Asimismo, permitirá al Instituto contar con los elementos normativos necesarios para que sus Unidades Técnicas y Administrativas cuenten con reglas claras en la creación, modificación y, en su caso, destrucción de los Sistemas de Datos Personales que se utilicen con motivo del desarrollo de sus actividades, situación que se ajustará a lo dispuesto por la Ley de Protección de Datos Personales.

El citado Reglamento abonará al ejercicio adecuado del derecho reconocido a todo individuo, en el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos, ya que su implementación permitirá que los datos personales que maneje el Instituto y sus áreas cuenten con mecanismos necesarios para la protección adecuada de los mismos.

Aunado a lo anterior, al aprobar dicho Reglamento este Consejo General estará en posibilidad de cumplir con la obligación que el Legislador Local le impuso al Instituto en su calidad de Sujeto Obligado, misma que se desprende del artículo SEGUNDO Transitorio de

la Ley Estatal de Protección de Datos.[7], ya que contará con la normatividad que fijará las bases para adecuar el actuar institucional en materia de datos personales a lo establecido en la multicitada Ley.

Este Consejo General considera oportuno establecer que respecto a la consideración de los días hábiles e inhábiles el diverso 165 del Código Electoral contempla una disposición que es aplicable a la ejecución de las actividades electorales, razón por la cual no tiene aplicación en lo que es materia de este instrumento.

Expuesto todo lo anterior, en ejercicio de la atribución reglamentaria dispuesta por el artículo 89 fracción I del Código Electoral, este Consejo General determina aprobar en todos sus términos el documento denominado: "Reglamento del Instituto Electoral del Estado en materia de protección de datos personales", mismo que corre agregado al presente acuerdo como **ANEXO ÚNICO**, formando parte integral del mismo.

DE LAS COMUNICACIONES

6. Que, con fundamento en lo dispuesto por el artículo 91 fracción XXIX del Código Electoral del Estado, el Consejo General faculta al Consejero Presidente para remitir el presente acuerdo al Consejero Presidente del Comité para su conocimiento y debida observancia.

Asimismo, se faculta al Consejero Presidente para notificar el presente acuerdo a la Titular de la Unidad para los trámites administrativos y/o efectos legales a los que haya lugar.

De igual forma, el Consejo General con fundamento en lo dispuesto por el artículo 89 fracciones LIII y LVII del Código Electoral, faculta al Comité para que en el ámbito de su competencia y con el auxilio de la Unidad realice un análisis al Reglamento del Instituto Electoral del Estado en materia de transparencia y acceso a la Información Pública, ya que con la aprobación del reglamento materia de este acuerdo varías de sus disposiciones podrían resultar contrarias.

Una vez realizado dicho análisis, de resultar procedente deberá presentarse a este Consejo General las propuestas de reforma al reglamento en cita, para su eventual aprobación.

Por lo anteriormente expuesto y fundado en ejercicio de las facultades que confiere el artículo 89 fracción LIII del Código Electoral, el Consejo General emite el siguiente:

A C U E R D O

PRIMERO. El Consejo General es competente para conocer y pronunciarse sobre el presente asunto en términos de lo plasmado en los considerandos 1 y 2 de este acuerdo.

SEGUNDO. El Consejo General aprueba el Reglamento del Instituto Electoral del Estado en materia de protección de datos personales, en los términos narrados en los considerandos números 3, 4 y 5 de este instrumento.

---

[7] El citado Artículo SEGUNDO TRANSITORIO establece de forma literal lo siguiente: "Los Sujetos Obligados contarán con un plazo de un año para adecuar sus Sistemas de Datos Personales de acuerdo a lo dispuesto por la presente Ley".

TERCERO. El Consejo General faculta al Consejero Presidente para realizar las notificaciones narradas en el número 6 de los considerandos de este acuerdo.

CUARTO. El Consejo General faculta al Comité y a la Unidad para realizar las acciones que les fueron encomendadas en el considerando 6 de este instrumento.

QUINTO. El presente acuerdo entrará en vigor a partir de su aprobación.

SEXTO. Publíquese el presente acuerdo en el Periódico Oficial del Estado, a través del formato aprobado mediante el instrumento CG/AC-004/14, en lo que toca al Reglamento del Instituto Electoral del Estado en materia de protección de datos personales, publíquese de forma íntegra en el citado medio oficial de difusión de esta Entidad Federativa.

Este acuerdo se aprobó por unanimidad de votos de los integrantes del Consejo General del Instituto Electoral del Estado, en sesión ordinaria de fecha veintinueve de agosto de dos mil catorce.

CONSEJERO PRESIDENTE	SECRETARIO EJECUTIVO
LIC. ARMANDO GUERRERO RAMIREZ	LIC. MIGUEL DAVID JIMÉNEZ LÓPEZ

REGLAMENTO DEL INSTITUTO ELECTORAL DEL ESTADO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

TÍTULO PRIMERO
DISPOSICIONES PRELIMINARES

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. El presente ordenamiento tiene por objeto establecer las instancias, los procedimientos y criterios generales para la debida aplicación de la Ley de Protección de Datos Personales en posesión de los Sujetos Obligados del Estado de Puebla; así como para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos personales obtenidos y tratados por el Instituto Electoral del Estado.

Artículo 2. Las disposiciones de este Reglamento son de observancia general para los funcionarios y el personal del Servicio Electoral Profesional y administrativo del Instituto Electoral del Estado.

Artículo 3. Para los efectos del presente Reglamento, se entenderá por:

1. Acuerdo de creación o eliminación de Sistemas de Datos Personales: Documento resolutivo, fundado y motivado, aprobado por el Consejo General del Instituto Electoral del Estado, mediante el cual se crean o eliminan Sistemas de Datos Personales.

2. Acuerdo de modificación de Sistemas de Datos Personales: Documento debidamente fundado y motivado, signado por el responsable del Sistema de Datos Personales, en el que se detallan los cambios realizados a cualquiera de los elementos de la ficha técnica y/o a las medidas de seguridad del Sistema.

3. Archivo: Conjunto orgánico de documentos, sea cual fuere su forma y soporte material, producidos o recibidos por personal del Instituto Electoral del Estado, en ejercicio de sus funciones, atribuciones y actividades.

4. Autentificación: Comprobación de la identidad de aquella persona autorizada para el tratamiento de los datos personales.

5. Automatización: Operaciones efectuadas total o parcialmente con ayuda de procedimientos mecanizados dentro de un Sistema de Datos Personales, tales como el registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión.

6. Aviso de protección de datos personales: Notificación por la que se hace del conocimiento del titular de los datos personales el principio de información contenido en el artículo 7 de la Ley.

7. Bloqueo de datos personales: Impedimento para difundir y tratar datos personales de manera total o parcial.

8. Cancelación de datos personales: Eliminación de datos de un Sistema de Datos Personales, por parte del responsable del mismo, derivada de la procedencia de una solicitud de cancelación de datos.

9. Categoría: Cada uno de los grupos en que pueden incluirse o clasificarse los datos personales.

10. Código: Código de Instituciones y Procesos Electorales del Estado de Puebla.

11. Comisión: Comisión para el Acceso a la Información Pública y Protección de Datos Personales del Estado.

12. Comité: Comité de Transparencia y Acceso a la Información Pública del Instituto Electoral del Estado.

13. Consejo: Consejo General del Instituto Electoral del Estado.

14. Consulta directa: Revisión de la información relativa a los datos personales en el lugar en que se encuentre, previa solicitud en los términos señalados por este ordenamiento.

15. Criterio de máximo alcance: Determinación del medio y periodo de difusión que resulte más eficiente para dar a conocer el Aviso de Protección de Datos Personales y abarcar al mayor número posible de titulares, cuando se implementa una medida compensatoria.

16. Datos personales: La información numérica, alfabética, gráfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o identificable, tal como puede ser, de manera enunciativa más no limitativa: el domicilio y el teléfono particular, el correo electrónico personal y que no haya sido determinado como oficial por alguna regulación; los bienes que conforman el patrimonio; el número de afiliación a cualquier organismo de seguridad social y cualquier otro dato o información que pudiera resultar de características análogas a las previamente enunciadas.

17. Datos personales sensibles: Aquellos datos personales que atañen a la esfera más íntima de su titular, o cuyo uso indebido propicie discriminación o conlleve un riesgo grave para el titular. De manera enunciativa y no limitativa se incluyen en estos: el origen étnico, las características físicas, morales o emocionales; la vida afectiva y familiar; el estado de salud físico o mental; la huella digital, la información genética; la ideología, las creencias, las convicciones filosóficas, morales y religiosas; las opiniones políticas y la preferencia u orientación sexual.

18. Derechos ARCO: Derechos de acceso, rectificación, cancelación y oposición de datos personales.

19. Días hábiles: Todos los días del año, con excepción de los sábados y domingos, los días inhábiles que señala la Ley Federal del Trabajo y aquellos establecidos en el artículo 190 del Reglamento Interior de Trabajo del Instituto Electoral del Estado. En materia de solicitudes de ejercicio de derechos ARCO no resultará aplicable lo dispuesto por los artículos 165 y 166 del Código.

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

21. Documento: Se refiere a los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro de información en posesión del Instituto Electoral del Estado, sin importar su fuente o fecha de elaboración. Los documentos podrán estar soportados en un medio escrito, impreso, sonoro, visual, electrónico, informático o cualquier otro que registre un hecho, un acto administrativo, jurídico, fiscal o contable, creado, generado, recibido, manejado y usado en el ejercicio de sus facultades y actividades.

22. Documento de seguridad: Instrumento que establece las medidas de seguridad administrativas, físicas y técnicas aplicables a los Sistemas de Datos Personales, a fin de asegurar la integridad, protección, confidencialidad y disponibilidad de los datos personales que contienen.

23. Encargado: Persona autorizada por el responsable del Sistema de Datos Personales para tratar la información recabada en el mismo.

24. Expediente: Unidad organizada por uno o varios documentos adecuadamente reunidos para su uso corriente durante el proceso de organización archivística, porque se refieren al mismo tema, actividad o asunto, constituyendo por lo general la unidad básica de la serie documental.

25. Ficha técnica: Cédula de identificación de un Sistema de Datos Personales, que debe contener por lo menos la información a que se refiere el artículo 22 de este Reglamento.

26. Finalidad: Es el propósito legal para la obtención de los datos personales y el empleo, uso o destino que se dará a los mismos, en el marco de las atribuciones de cada Unidad.

27. Incidencia: Cualquier anomalía que afecte o pudiera afectar la seguridad de los datos personales contenidos en un Sistema.

28. Información reservada: La información que se encuentra temporalmente bajo alguno de los supuestos previstos en el artículo 17 del Reglamento del Instituto Electoral del Estado en Materia de Transparencia y Acceso a la Información Pública, y la que en la Ley y otros ordenamientos jurídicos tenga ese carácter.

29. Instituto: Instituto Electoral del Estado.

30. Ley: Ley de Protección de Datos Personales en posesión de los Sujetos Obligados del Estado de Puebla.

31. Medida compensatoria: Prevención temporal por la que se establece el mecanismo de comunicación con el que se dará a conocer de manera generalizada y masiva el Aviso de

Protección de Datos Personales a los titulares de los datos obtenidos antes de la entrada en vigor de la Ley, o de aquellos obtenidos de forma indirecta a través de la transferencia de datos personales.

32. Nivel de seguridad: Medidas exigibles por la Ley para el tratamiento de los datos personales que se encuentran en los Sistemas, atendiendo a la naturaleza de la información en relación con la menor o mayor necesidad de garantizar su confidencialidad e integridad.

33. Órganos centrales: Consejo General y Junta Ejecutiva del Instituto Electoral del Estado.

34. Procedimiento de recolección: Mecanismo de obtención de los datos personales, que puede ser por medios físicos o electrónicos, en formatos, cuestionarios, escritos y similares, o a través de la transmisión de datos en su modalidad de transmisión interna o transferencia.

35. Recurrente: La persona que interpone un recurso de revisión por sí o través de su representante legal, en los términos que señala la Ley.

36. Recurso de revisión: Medio de impugnación interpuesto ante la Comisión por inconformidad con la respuesta del Instituto o la ausencia de ésta, derivada de una solicitud de acceso, rectificación, cancelación u oposición de datos personales.

37. Registro Electrónico de Sistemas de Datos Personales: Aplicación informática desarrollada por la Comisión para que los sujetos obligados notifiquen y actualicen la información referente a los Sistemas de Datos Personales en su poder.

38. Reglamento: Reglamento del Instituto Electoral del Estado en Materia de Protección de Datos Personales.

39. Responsable del Sistema: Titular de la Unidad Técnica o Administrativa a la que se encuentre adscrito el Sistema de Datos Personales, que decide sobre el contenido y finalidad del mismo, así como sobre la protección y tratamiento de la información que lo integra; cualquiera que sea la denominación que ostente, ya sea como Director, Subdirector, Coordinador, Titular, Encargado de Despacho o cualquier otra de acuerdo con la Normatividad Interna aplicable.

40. Responsable de seguridad informática: Unidad Técnica o Administrativa del Instituto designada por el Consejo General, encargada de coordinar y controlar las medidas generales de seguridad informática implementadas en los Sistemas de Datos Personales.

41. Sistema de Datos Personales: Conjunto organizado de archivos, registros, bases o bancos de datos personales del Instituto, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

42. Solicitante: Titular de los datos personales o su representante legal, que ejerce los derechos de acceso, rectificación, cancelación u oposición ante el Instituto.

43. Solicitud: Escrito con los requisitos señalados en el artículo 66 de este Reglamento, a través del cual el solicitante puede ejercer los derechos de acceso, rectificación, cancelación u oposición de datos personales ante el Instituto; o bien, mediante el formato disponible en la oficina de la Unidad de Acceso y en la página web del Instituto.

44. Soporte electrónico: Medios de almacenamiento de datos inteligibles sólo mediante el uso de aparatos con circuitos electrónicos que procesen su contenido para examinarlos, modificarlos, bloquearlos o suprimirlos; entre los cuales se encuentran de manera enunciativa más no limitativa, archivos escaneados o fotografiados, cintas magnéticas de audio, video y datos, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil; así como la información contenida en archivos automatizados o bases de datos.

45. Soporte físico: Medios de almacenamiento de datos inteligibles a simple vista, que no requieren que su contenido sea procesado por ningún medio digital o automatizado para ser examinados, modificados y/o almacenados; entre los que se encuentran de manera enunciativa y no limitativa, documentos, oficios, formularios impresos o llenados a mano, fotografías, carpetas, expedientes.

46. Sujetos obligados: Los enunciados en el artículo 2 de la Ley.

47. Titular: Persona física a quien hacen referencia o pertenecen los datos personales contenidos en los Sistemas.

48. Transferencia de datos personales: Transmisión total o parcial, fundada y motivada, de datos personales en posesión del Instituto a un usuario externo.

49. Transmisión de datos personales: La obtención de datos resultante de la consulta de un archivo, registro, base o banco de datos, su interconexión con otros archivos, registros, base o banco de datos; de la publicación de los datos contenidos en los mismos, así como de la comunicación realizada por una persona autorizada distinta al titular, o de la transferencia entre sujetos obligados.

50. Transmisión interna de datos personales: La obtención de datos resultante de la consulta de un archivo, registro, base o banco de datos, su interconexión con otros archivos, registros, base o banco de datos; y la comunicación de datos realizada por los responsables o encargados de los Sistemas de Datos Personales, en ejercicio de sus funciones y atribuciones.

51. Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados o físicos aplicados a los Sistemas de Datos Personales, relacionadas con la obtención, registro, organización, conservación, elaboración, utilización, transmisión, difusión, interconexión, transferencia o cualquier otra forma que permita obtener información de los mismos, y facilite al titular el acceso, rectificación, cancelación u oposición de sus datos.

52. Unidad de Acceso: Unidad Administrativa de Acceso a la Información del Instituto Electoral del Estado.

53. Unidades: Unidades Técnicas y Administrativas del Instituto, conforme a su estructura orgánica.

54. Usuario externo: Persona física o moral ajena al Instituto, autorizada a través de un instrumento jurídico para el tratamiento de datos personales.

Artículo 4. La interpretación del presente Reglamento se hará conforme a los criterios gramatical, sistemático y funcional, observando lo dispuesto por el último párrafo del artículo 14 de la Constitución Política de los Estados Unidos Mexicanos, así como a los criterios y acuerdos emitidos por el Comité de Transparencia y Acceso a la Información Pública del Instituto.

CAPÍTULO II
DE LOS ÓRGANOS COMPETENTES Y DE LA UNIDAD DE ACCESO

Artículo 5. El Consejo General, como órgano superior de dirección del Instituto, tendrá las siguientes atribuciones:

I. Vigilar en el ámbito de su competencia el cumplimiento del presente Reglamento.
II. Aprobar reformas o modificaciones al Reglamento.
III. Crear o eliminar, mediante acuerdo, los Sistemas de Datos Personales de las Unidades del Instituto.
IV. Aprobar las medidas compensatorias que se deban implementar en términos de este Reglamento.
V. Designar al responsable de seguridad informática.
VI. Las demás que le confiera el Código y las disposiciones legales aplicables.

Artículo 6. La Unidad Administrativa de Acceso a la Información en la aplicación de este Reglamento tendrá las atribuciones siguientes:

I. Ser el vínculo entre el solicitante y el Instituto.
II. Ser el vínculo entre el Instituto y la Comisión.
III. Recibir las solicitudes de ejercicio de los derechos ARCO y efectuar los trámites internos necesarios para su debida atención, requiriendo a las Unidades toda la información pertinente para dar respuesta a las mismas en los términos previstos por este Reglamento.
IV. Llevar un registro y control de las solicitudes de ejercicio de derechos ARCO que se presenten ante el Instituto.
V. Auxiliar a los solicitantes en el llenado de la solicitud con los requisitos establecidos en el presente Reglamento, y los demás elementos que sean necesarios para el efectivo ejercicio de los derechos ARCO; informarles sobre el recurso de revisión, así como la forma y los plazos para interponerlo ante la Comisión.
VI. Elaborar los modelos de formatos de solicitud para el ejercicio de los derechos ARCO ante el Instituto.
VII. Auxiliar a las Unidades en la elaboración de los formatos que serán utilizados para recabar el consentimiento de los titulares de datos personales, necesario para el tratamiento, transmisión, difusión o distribución de dicha información en los casos señalados por la Ley y la normatividad aplicable.

VIII. Proponer los procedimientos internos necesarios para mejorar y eficientar el ejercicio de los derechos ARCO ante el Instituto.
IX. Promover la capacitación y actualización del personal del Instituto en materia de protección de datos personales.
X. Proponer reformas o modificaciones al Reglamento a través del Comité.
XI. Asesorar a los responsables de Sistemas en la elaboración del documento de seguridad.
XII. Auxiliar a los responsables de Sistemas en la elaboración de la ficha técnica a que se refiere el artículo 22 del presente Reglamento.
XIII. Recabar de las Unidades la información de las fichas técnicas, de los acuerdos de modificación y, en su caso, de los acuerdos de eliminación de los Sistemas de Datos Personales a su cargo, para las notificaciones correspondientes a la Comisión.
XIV. Coadyuvar con las Unidades en la elaboración e implementación del aviso de protección de datos personales en los medios físicos o electrónicos por los que recaben esta información.
XV. Tomar las medidas necesarias para la búsqueda exhaustiva de la información objeto de la solicitud, en caso de que no se encuentre en los Sistemas de la Unidad a la que haya sido turnada.
XVI. Informar al Comité en caso de no encontrarse la información objeto de la solicitud.
XVII. Efectuar las notificaciones que deriven del ejercicio de sus funciones y atribuciones, con el apoyo de la Dirección Técnica del Secretariado en los casos que corresponda.
XVIII. Supervisar el cumplimiento de criterios, políticas y lineamientos en materia de protección de datos personales.
XIX. Representar al Instituto en el trámite del recurso de revisión que se substancie ante la Comisión.
XX. Rendir el informe con justificación referido en la Ley.
XXI. Desempeñar las funciones y comisiones que el Consejo le asigne en la materia.
XXII. Las demás que le confiera el Consejo, el Comité, el Consejero Presidente y/o el Secretario Ejecutivo del Instituto, conforme al Código y las disposiciones legales aplicables.

Artículo 7. El Comité de Transparencia y Acceso a la Información Pública tendrá las siguientes atribuciones:

I. Aprobar la normatividad que regulará su funcionamiento.
II. Proponer al Consejo General reformas o modificaciones al Reglamento, a través del Consejero Presidente.
III. Vigilar en el ámbito de su competencia el cumplimiento del presente Reglamento.
IV. Revisar las fichas técnicas de los Sistemas de Datos Personales elaboradas por los responsables, para la posterior aprobación del acuerdo de creación por parte del Consejo General.
V. Revisar los documentos de seguridad que implementarán los responsables en los Sistemas de Datos Personales a su cargo.
VI. Conocer de los acuerdos de modificación emitidos por los responsables de Sistemas cuando haya un cambio en las fichas técnicas de los mismos, así como de los usuarios externos a los que se transfieran datos personales.
VII. Ser el conducto por el cual el responsable solicite al Consejo General la eliminación de los Sistemas a su cargo, en los casos que proceda.

VIII. Resolver las consultas que se presenten sobre la interpretación de las disposiciones de este Reglamento y los casos no previstos en él.

IX. Notificar a los Titulares de los Órganos Centrales y de las Unidades del Instituto, a través de la Secretaría del Comité, todos los criterios y acuerdos tomados por el mismo.

X. Emitir recomendaciones a los Órganos Centrales y Unidades del Instituto para el debido cumplimiento de la Ley y de las disposiciones de este Reglamento.

XI. Coadyuvar en la aplicación de las disposiciones de la Ley y de este Reglamento.

XII. Coadyuvar con la Unidad de Acceso en la capacitación y actualización de los funcionarios y demás personal del Instituto en materia de protección de datos personales.

XIII. Hacer del conocimiento de la Contraloría Interna las conductas en las que incurran los funcionarios y demás personal del Instituto, que pudieran constituir infracciones administrativas con motivo del incumplimiento de la Ley, el presente Reglamento y la normatividad aplicable.

XIV. Supervisar el cumplimiento de las actividades de la Unidad de Acceso.

XV. Las demás que le confiera el Consejo General y las disposiciones reglamentarias aplicables.

TÍTULO SEGUNDO
DE LOS DATOS PERSONALES

CAPÍTULO I
PRINCIPIOS QUE RIGEN EL TRATAMIENTO DE LOS DATOS PERSONALES

Artículo 8. En el tratamiento de los datos personales y el manejo de los Sistemas de Datos Personales, se deberán observar los siguientes principios:

I. **PRINCIPIO DE CALIDAD.** Consiste en que los datos personales recabados serán exactos, de forma que respondan con veracidad a la situación actual del titular.

II. **PRINCIPIO DE CONFIDENCIALIDAD.** Consiste en garantizar que sólo el titular, por sí mismo o a través de su representante legal, puede acceder a sus datos personales, o en su caso, el responsable, encargado o usuario externo del Sistema para su tratamiento.

III. **PRINCIPIO DE CONSENTIMIENTO.** El tratamiento de los datos personales requiere de la anuencia informada, libre, inequívoca, específica y expresa del titular, salvo las excepciones previstas en la Ley.

IV. **PRINCIPIO DE DISPONIBILIDAD.** Los datos deben ser almacenados de modo que permitan en todo momento el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

V. **PRINCIPIO DE FINALIDAD.** Los Sistemas de Datos Personales no pueden tener propósitos contrarios a las leyes o a la moral pública, y en ningún caso pueden ser utilizados para fines distintos o incompatibles a aquellos que motivaron su obtención.

VI. **PRINCIPIO DE INFORMACIÓN.** Previo a la obtención de los datos personales, se debe hacer del conocimiento del titular, de manera completa y precisa, la existencia del Sistema de Datos Personales, su finalidad, el carácter obligatorio u optativo de la información que se está requiriendo, las consecuencias del suministro de los datos, de la negativa a hacerlo o de su inexactitud; la posibilidad de ejercer los derechos ARCO, así como la identidad y dirección del responsable del Sistema.

VII. **PRINCIPIO DE LICITUD.** Consiste en que la posesión y tratamiento de los Sistemas de Datos Personales obedecerá exclusivamente a las atribuciones legales o reglamentarias que tengan los responsables, encargados y, en su caso, los usuarios externos.

VIII. **PRINCIPIO DE PERTINENCIA.** Sólo pueden recabarse y utilizarse los datos personales para fines oficiales y lícitos, por lo que los mismos deberán ser adecuados y no excesivos en relación con el ámbito y finalidades para los que se hayan obtenido.

IX. **PRINCIPIO DE RESPONSABILIDAD.** Los datos personales no deben ser divulgados o puestos a disposición de terceros para usos diferentes a los especificados por quien los obtuvo, excepto en los casos previstos expresamente en las leyes y disposiciones reglamentarias aplicables.

X. **PRINCIPIO DE SEGURIDAD.** Únicamente el responsable, el encargado o el usuario externo autorizado, en su caso, pueden llevar a cabo el tratamiento de los datos personales.

XI. **PRINCIPIO DE TEMPORALIDAD.** El tiempo de conservación de los datos personales será el necesario para el cumplimiento de los fines que justifican su tratamiento.

Artículo 9. Para los efectos del presente Reglamento, se entenderá que:

I. En relación al PRINCIPIO DE CALIDAD, los datos personales son exactos cuando se mantienen actualizados de tal manera que no se altere la veracidad de la información, que traiga como consecuencia que el titular se vea afectado por dicha situación.

II. En relación al PRINCIPIO DE CONSENTIMIENTO este es:
   a) Libre, cuando es obtenido sin la intervención de vicio alguno de la voluntad;
   b) Inequívoco, cuando existen elementos que de manera indubitable demuestran su otorgamiento;
   c) Específico, cuando se otorga para una determinada finalidad;
   d) Expreso, cuando consta por escrito en el documento elaborado para tal efecto.

III. En relación al PRINCIPIO DE PERTINENCIA los datos personales recabados son:
   a) Adecuados, cuando se observa una relación proporcional entre los datos recabados y la finalidad o finalidades de su tratamiento.
   b) No excesivos, cuando la información requerida al titular es la estrictamente necesaria para cumplir con los fines para los cuales fue recabada.

Artículo 10. En caso de que los responsables o encargados detecten que hay datos personales inexactos, deberán de oficio actualizarlos en el momento en que tengan conocimiento de la inexactitud de los mismos, siempre que posean los documentos que justifiquen la actualización.

Artículo 11. El tratamiento posterior de los datos personales no se considerará incompatible con la finalidad de su obtención ni violatorio del principio de temporalidad, cuando sea con fines históricos, estadísticos o científicos.

Artículo 12. Para su clasificación, los datos personales se integrarán de acuerdo con las categorías que se señalan de manera enunciativa más no limitativa:

I. Datos de identificación: el nombre, domicilio, teléfono particular, teléfono celular, firma, Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), clave de elector, cartilla militar, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía y demás análogos.

II. Datos electrónicos: las direcciones electrónicas tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección *Media Access Control* o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica o cualquier otra información empleada por la persona para su identificación en Internet u otra red de comunicaciones electrónicas.

III. Datos laborales: documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio y demás análogos.

IV. Datos patrimoniales: los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales o crediticias y demás análogos.

V. Datos sobre procedimientos administrativos y/o jurisdiccionales: información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho.

VI. Datos académicos: Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos, y demás análogos.

VII. Datos de tránsito y movimientos migratorios: información relativa al tránsito de las personas dentro y fuera del país, así como sobre su situación migratoria.

VIII. Datos sensibles: además de los mencionados en el punto 17 del artículo 3 del presente Reglamento, se consideran los siguientes:

a) Datos sobre la salud.- El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona.

b) Datos de características físicas.- Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión y análogos.

c) Datos de características personales o biométricas.- Huella digital, tipo de sangre, ADN, geometría de la mano, características de iris y retina, y demás análogos.

Artículo 13. Ninguna persona está obligada a proporcionar datos personales sensibles.

Artículo 14. Los datos personales son información irrenunciable, intransferible e indelegable, entendiéndose por:

a) Irrenunciable, que el titular está imposibilitado de privarse voluntariamente de las garantías que le otorga la legislación en materia de protección de datos personales.

b) Intransferible, que el titular es el único a quien pertenecen los datos personales y éstos no pueden ser cedidos a otra persona.

c) Indelegable, que sólo el titular tiene la facultad de decidir a quién transmite sus datos.

Artículo 15. Los funcionarios y demás personal del Instituto no podrán transmitir, difundir, transferir o distribuir los datos personales a que tengan acceso por el ejercicio de sus atribuciones, salvo disposición legal o que haya mediado el consentimiento expreso del titular de dichos datos. Esta prohibición subsistirá aún después de finalizada la relación entre el Instituto y el titular de los datos personales, la relación laboral que el responsable o el encargado del Sistema tenga con el Instituto, o la relación contractual con los usuarios externos.

El responsable, encargado o usuario externo quedará exceptuado de esta prohibición por resolución judicial y en los casos de emergencia, seguridad pública, seguridad nacional o salud pública, cuando medien razones fundadas.

Artículo 16. No será necesario el consentimiento del titular para el tratamiento de los datos personales:

I. Cuando se encuentre previsto en una Ley.
II. Cuando impliquen datos obtenidos para la realización de las funciones propias de la administración pública en el ámbito de su competencia, y se cumpla con el principio de pertinencia.
III. Cuando exista una orden judicial.
IV. Cuando la transmisión se produzca entre organismos gubernamentales y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
V. Cuando se trate de la prevención o gestión de servicios de salud, así como la asistencia médica en la que por la situación específica del caso no sea posible recabar la autorización del titular.
VI. Cuando se den a conocer al usuario externo para la prestación de un servicio cuya finalidad sea el tratamiento de los datos personales.
VII. Cuando los datos figuren en registros públicos y su tratamiento sea necesario siempre que no se vulneren los derechos y libertades fundamentales del titular.

Artículo 17. El consentimiento para el tratamiento de los datos personales podrá ser revocado por escrito en cualquier momento, sin que pueda dejarse de difundir o distribuir aquella información publicitada derivada del consentimiento inicialmente otorgado, cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

Artículo 18. Los datos personales deben ser eliminados de los Sistemas cuando hayan dejado de ser necesarios o pertinentes para los fines para los que hubiesen sido obtenidos, excepto cuando deban ser tratados con posterioridad para fines estadísticos o científicos, siempre que cuenten con el procedimiento de disociación.

Únicamente podrán ser conservados de manera íntegra, permanente y bajo tratamiento los datos personales con fines históricos, previa valoración documental.

Artículo 19. Los responsables de los Sistemas, los encargados, usuarios externos y toda persona que intervenga en cualquier etapa del tratamiento de los datos personales, están obligados a guardar absoluta confidencialidad respecto de los mismos.

CAPÍTULO II
DE LOS SISTEMAS DE DATOS PERSONALES

Artículo 20. La integración de los Sistemas de Datos Personales se regirá por las siguientes disposiciones generales:

I. Se deberá crear un Sistema por cada finalidad o propósito por el que se recaben datos personales.

II. Los Sistemas se conformarán con los archivos, registros, bases o bancos de datos que sean producto del ejercicio de las actividades, atribuciones y funciones de las Unidades, de acuerdo con el Código y la normatividad aplicable.

III. La creación o eliminación de los Sistemas de Datos Personales sólo podrá efectuarse por acuerdo del Consejo General.

IV. Deberán integrarse por lo menos los siguientes Sistemas:
   a) Sistema de Datos Personales de los integrantes del Instituto.
   b) Sistema de Datos Personales de los proveedores del Instituto.
   c) Sistema de Datos Personales de aquellos que realicen trámites y servicios, en su caso.

V. No podrán crearse Sistemas de Datos Personales que tengan como finalidad exclusiva el almacenamiento de datos personales sensibles; estos sólo podrán ser tratados cuando medien razones de interés público, así lo disponga una Ley o lo consienta expresamente el titular, o bien, se persigan fines estadísticos, científicos o históricos, siempre y cuando se haya realizado previamente el procedimiento de disociación.

VI. Los Sistemas que contengan datos personales sensibles no podrán ser sometidos a automatización, con excepción de lo establecido en la fracción inmediata anterior.

VII. Los Sistemas de Datos Personales deberán ser eliminados cuando dejen de ser necesarios para los fines para los cuales fueron creados, y una vez que concluyan los plazos y términos de conservación establecidos por las disposiciones legales aplicables.

VIII. No procederá la eliminación de un Sistema cuando exista una previsión legal expresa que exija su conservación.

Artículo 21. Los Sistemas de Datos Personales pueden ser:

I. Físicos. Conjunto ordenado de datos personales que para su tratamiento están contenidos en registros, manuales, impresos, sonoros, magnéticos, visuales u holográficos, estructurados conforme a criterios específicos.

II. Automatizados. Conjunto ordenado de datos personales que están contenidos o que para su tratamiento se utiliza una herramienta tecnológica.

III. Mixtos. Cuando los datos personales se encuentran contenidos en soportes físicos y automatizados.

Artículo 22. El responsable, al integrar o determinar la existencia de un Sistema de Datos Personales, deberá elaborar una ficha técnica con la siguiente información:

a) Denominación del Sistema.
b) La finalidad del Sistema y los usos previstos para el mismo.
c) Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a proporcionarlos al Instituto durante el desarrollo de algún procedimiento, trámite, registro, convocatoria, base, licitación, etc.
d) El procedimiento de recolección de los datos personales.
e) La estructura básica del Sistema, conforme a la categoría de los datos incluidos en el mismo, y el modo de tratamiento.
f) La transmisión de la que son o pueden ser objeto los datos, indicando en su caso los usuarios externos.

g) El encargado del tratamiento del Sistema y, en su caso, las Unidades que intervengan en el mismo.
h) Los datos de la Unidad de Acceso ante la que se podrán ejercerse los derechos ARCO.
i) El nivel de seguridad a que está sujeto el Sistema: básico, medio o alto.

Artículo 23. Por lo que hace a la información señalada en el inciso e) del artículo inmediato anterior, deberá considerarse lo siguiente:

I. La estructura básica se refiere a la descripción de los datos contenidos en los archivos, registros, bases o bancos de datos que componen cada Sistema.
II. Los datos tratados en cada Sistema se deberán clasificar conforme a las categorías establecidas en el artículo 12 de este Reglamento.
III. El modo de tratamiento utilizado en la organización de los datos personales contenidos en el Sistema será físico, automatizado o mixto.

Artículo 24. Las fichas técnicas de los Sistemas de Datos Personales serán revisadas por el Comité de Transparencia antes de la aprobación del acuerdo de creación correspondiente por parte del Consejo General. Para tales efectos, los responsables de los Sistemas deberán remitir el documento donde conste la ficha técnica a la Unidad de Acceso dentro de los tres días hábiles siguientes a la determinación de los mismos, para que ésta en un plazo no mayor a cinco días hábiles contado a partir de la fecha de recepción, lo haga del conocimiento de los miembros del Comité para la revisión correspondiente.

Una vez que los miembros del Comité hayan revisado las fichas técnicas, éstas serán remitidas dentro de los cinco días hábiles siguientes al Consejo General, a través del Consejero Presidente, para la emisión del acuerdo de creación correspondiente.

Artículo 25. El acuerdo de creación del Sistema de Datos Personales deberá contener todos los datos de la ficha técnica. Podrá elaborarse un acuerdo de creación por todos los Sistemas de Datos Personales que sean identificados al momento de la emisión del mismo.

Artículo 26. Los Titulares de las Unidades Técnicas y Administrativas deberán tomar las medidas necesarias a fin de que los acuerdos de creación de los nuevos Sistemas de Datos Personales que integren, sean emitidos antes de la fecha programada para recabar los datos personales que los conformarán, a fin de contar oportunamente con los elementos para elaborar y difundir el "Aviso de protección de datos personales".

Artículo 27. Si alguno de los elementos de la ficha técnica es modificado, el responsable del Sistema deberá emitir un "Acuerdo de modificación de Sistema" indicando los cambios que se hayan realizado al mismo. Los rubros que no sufran cambios, deberán transcribirse en el acuerdo tal como quedaron establecidos en el acuerdo de creación del Sistema.

El responsable del Sistema deberá hacer los ajustes que sean necesarios al "Aviso de protección de datos personales", conforme a las modificaciones realizadas.

Artículo 28. El Acuerdo de modificación de Sistemas deberá ser remitido por el responsable a la Unidad de Acceso dentro de los diez días hábiles siguientes a la fecha del mismo, a fin de que se

haga del conocimiento de los miembros del Comité, para la revisión a que haya lugar de acuerdo con la Normatividad Interna aplicable.

Una vez hecha la revisión correspondiente por el Comité, la Unidad de Acceso notificará a la Comisión los acuerdos de modificación de Sistemas que generen los responsables, para su registro en términos del artículo 19 de la Ley.

Artículo 29. En caso de que el Consejo General determine la eliminación de un Sistema de Datos Personales, en el acuerdo respectivo se establecerá el destino que vaya a darse a los datos, o en su caso, las previsiones que se adopten para su destrucción, de conformidad con la Ley del Archivo del Estado y demás disposiciones legales y reglamentarias aplicables.

Artículo 30. La eliminación de un Sistema deberá ser notificada a la Comisión, por conducto de la Unidad de Acceso, dentro de los diez días hábiles siguientes a la emisión del acuerdo respectivo, para las cancelaciones que procedan en el Registro Electrónico de Sistemas de Datos Personales.

Artículo 31. A efecto de cumplir con el principio de información, previo a la recopilación de datos personales por cualquier medio, la Unidad a través del responsable, encargado o la persona que lleve a cabo dicha actividad, deberá hacer del conocimiento del titular las advertencias previstas en la fracción VI del artículo 8 de este Reglamento, mediante el "Aviso de protección de datos personales".

CAPÍTULO III
DE LAS MEDIDAS DE SEGURIDAD

Artículo 32. Las medidas de seguridad son los medios por los cuales se busca garantizar la integridad de cada uno de los Sistemas de Datos Personales, así como el cumplimiento de los principios de confidencialidad, disponibilidad, responsabilidad y seguridad.

Artículo 33. Las medidas de seguridad serán adoptadas en relación con el menor o mayor grado de protección que ameriten los datos personales, y deberán constar por escrito en el documento de seguridad. Se regirán conforme a lo siguiente:

A. TIPOS DE SEGURIDAD.

I. Física: se refiere a toda medida destinada a la protección de las instalaciones, equipos, soportes o sistemas de datos para la prevención de riesgos.
II. Lógica: se refiere a las medidas de protección que permitan la identificación y autentificación de cualquier persona o usuario externo autorizado para el tratamiento de los datos personales, de acuerdo con sus funciones, atribuciones y actividades.
III. De cifrado: consiste en la implementación de claves y contraseñas, así como de dispositivos de protección, que garanticen la integridad y confidencialidad de la información.
IV. De comunicaciones y redes: conjunto de restricciones preventivas y/o de riesgos que deberán observar los responsables, encargados y usuarios externos de los Sistemas, para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicación.

B. NIVELES DE SEGURIDAD.

I. Básico. Son las medidas generales de seguridad cuya aplicación es obligatoria para todos los Sistemas, debiendo cubrir los aspectos siguientes:
   a) Documento de seguridad.
   b) Responsable de seguridad informática.
   c) Registro del personal que intervenga en el tratamiento de los Sistemas de Datos Personales.
   d) Mecanismos que impidan acceder a información diferente a la autorizada.
   e) Restricción de acceso a los archivos físicos.
   f) Establecimiento de contraseñas.

II. Medio. Se refiere a la adopción de medidas de seguridad que deberán implementarse en los Sistemas relativos a la comisión de infracciones administrativas, hacienda pública, servicios financieros, datos patrimoniales, así como a los que contengan datos personales que permitan obtener una evaluación de la personalidad del individuo.

   Este nivel de seguridad, además de las medidas calificadas como básicas, deberá considerar los siguientes aspectos:

   a) Cambio semestral de contraseñas.
   b) Registro de funciones y obligaciones del personal que intervenga en el tratamiento del Sistema.
   c) Revisiones internas.
   d) Limitación de la posibilidad de intentar reiteradamente el acceso no autorizado.

III. Alto. Son las medidas de seguridad aplicables a los Sistemas que contienen datos personales sensibles, así como datos recabados para fines de salud, de seguridad, prevención, investigación y persecución de delitos. En estos Sistemas se deberán implementar medidas de nivel básico y de nivel medio, complementadas con las que se detallan a continuación:

   a) Identificación y autentificación del responsable, encargado y usuario externo, en su caso.
   b) Protección contra escritura y modificación de documentos, salvo consentimiento expreso por escrito del responsable.
   c) Auditorías realizadas por la Contraloría Interna del Instituto.
   d) Autorización expresa del responsable para el tratamiento de datos fuera de las instalaciones de la Unidad a su cargo.

Los diferentes niveles de seguridad serán establecidos atendiendo a las características propias de la información.

Artículo 34. El documento de seguridad tiene como propósito identificar el universo de Sistemas de Datos Personales que posee el Instituto, el tipo de datos que contiene cada uno, los responsables, encargados y usuarios externos, así como las medidas de seguridad concretas implementadas.

El responsable del Sistema, con la asesoría de la Unidad Administrativa de Acceso a la Información y del responsable de seguridad informática, elaborará el documento de seguridad que será de observancia obligatoria para todo el personal permanente y eventual que labore en la Unidad a su cargo, así como para los usuarios externos con los que trate y en general, para toda persona que debido a la prestación de un servicio tenga acceso al Sistema y/o al sitio donde se ubica el mismo.

Artículo 35. El documento de seguridad deberá contener como mínimo los siguientes datos:

I. Nombre, cargo y adscripción del responsable del Sistema de Datos Personales.
II. Nombre, cargo y adscripción del o los encargados del tratamiento del Sistema, y en su caso, de los usuarios externos.
III. Tratándose de usuarios externos, deberá indicarse el acto jurídico por el cual se otorgó a los mismos el tratamiento de los datos personales.
IV. Estructura y descripción del Sistema.
V. Especificación detallada del tipo de datos personales contenidos en el Sistema, de acuerdo con las categorías de clasificación.
VI. Funciones y obligaciones del personal autorizado para acceder al Sistema y para el tratamiento de los datos personales.
VII. Las medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad adoptado.
VIII. Consecuencias del incumplimiento de las medidas de seguridad.

Artículo 36. Las medidas, normas, procedimientos y criterios enfocados a garantizar un determinado nivel de seguridad, deberán considerar lo siguiente:

a) Procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y en su caso, claves de acceso para la operación del Sistema.
b) Actualización de información contenida en el Sistema.
c) Procedimientos de creación de copias de respaldo y de recuperación de los datos automatizados, así como para el archivo físico.
d) Bitácoras de acceso y acciones llevadas a cabo en el Sistema.
e) Procedimiento de notificación, gestión y respuesta ante incidentes.
f) Procedimiento para la cancelación de un Sistema.
g) Procedimientos para la realización de revisiones internas de las medidas de seguridad.
h) Los mecanismos de protección contra escritura y modificación de documentos, en su caso.

Artículo 37. El documento de seguridad será revisado por lo menos una vez al año, dejando por escrito constancia de la revisión, o bien, cuando se produzcan cambios relevantes en el tratamiento de los datos personales que puedan repercutir en el cumplimiento de las medidas de seguridad implementadas.

En el primer caso, los responsables de los Sistemas de Datos Personales deberán remitir al Comité de Transparencia durante los primeros cinco días hábiles del mes de junio de cada año, el documento de seguridad aplicable al Sistema que se encuentre a su cargo. Lo anterior se hará por conducto de la Unidad de Acceso, quien deberá hacerlo del conocimiento de los miembros del Comité en un plazo no mayor a cinco días hábiles contados a partir de la fecha de recepción.

Para el caso del segundo supuesto, el responsable deberá remitir el documento de seguridad al Comité para su revisión, dentro de los diez días hábiles siguientes a los cambios realizados; lo hará

de igual manera por conducto de la Unidad de Acceso, quien tendrá el plazo ya señalado para hacerlo del conocimiento de los miembros del Comité.

Artículo 38. Las funciones y obligaciones de todos los que intervengan en el tratamiento de los datos personales de un Sistema, deberán estar claramente definidas en el documento de seguridad. El responsable adoptará las medidas necesarias para que el personal a su cargo conozca las normas de seguridad que afecten el desarrollo de sus funciones, así como las responsabilidades y consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 39. Por la naturaleza de la información, las medidas y tipos de seguridad que se adopten serán considerados información reservada en términos de la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla, y del Reglamento del Instituto Electoral del Estado en Materia de Transparencia y Acceso a la Información Pública.

CAPÍTULO IV
DE LAS FUNCIONES Y OBLIGACIONES DEL RESPONSABLE DEL SISTEMA

Artículo 40. Son funciones del responsable del Sistema:

I. Decidir sobre el contenido y finalidad de los Sistemas de Datos Personales a su cargo.
II. Elaborar e implementar el documento de seguridad aplicable a los Sistemas a su cargo.
III. Designar a los encargados del tratamiento del Sistema de Datos Personales y de vigilar el cumplimiento de las medidas de seguridad establecidas en el documento de seguridad. Esta designación podrá ser única para todos los Sistemas de Datos a cargo del responsable, o diferenciada dependiendo de los métodos de organización y tratamiento de los datos. En cualquier caso, esta circunstancia deberá especificarse en el documento de seguridad.
IV. Adoptar medidas para que los encargados y usuarios externos, en su caso, tengan acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
V. Determinar la eliminación de los Sistemas de Datos Personales a su cargo, en los términos previstos por la Ley y el presente Reglamento.
VI. Crear, establecer, modificar, eliminar y llevar a cabo el procedimiento de disociación de datos personales, conforme a su respectivo ámbito de competencia.
VII. Establecer los procedimientos de creación y modificación de contraseñas (longitud, formato y contenido), en los casos que corresponda.
VIII. Conceder, alterar o anular la autorización para el acceso a los Sistemas de Datos Personales.
IX. Verificar, al menos cada seis meses, la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Artículo 41. Son obligaciones del responsable del Sistema:

I. Cumplir con las políticas y lineamientos, así como las normas aplicables para el manejo, tratamiento, seguridad y protección de datos personales.
II. Adoptar las medidas de seguridad necesarias para la protección de datos personales.

III. Coordinar y supervisar a los encargados de los Sistemas de Datos Personales.

IV. Remitir a la Unidad de Acceso las fichas técnicas de los Sistemas a su cargo y los acuerdos de modificación que genere, para las revisiones y notificaciones correspondientes.

V. Informar al titular al momento de recabar sus datos personales, sobre la existencia y finalidad de los Sistemas, así como el carácter obligatorio u optativo de proporcionar sus datos y las consecuencias de ello, así como sobre la posibilidad de ejercer los derechos de acceso, rectificación, cancelación u oposición de datos personales. Lo anterior, a través del aviso de protección de datos personales.

VI. Instrumentar e implementar las medidas compensatorias que sean necesarias, respecto de los Sistemas de Datos Personales a su cargo.

VII. Adoptar los procedimientos internos adecuados para dar contestación a las solicitudes de acceso, rectificación, cancelación u oposición de datos personales que ingresen a través de la Unidad de Acceso.

VIII. Utilizar los datos personales únicamente cuando éstos guarden relación con la finalidad para la cual se hayan obtenido.

IX. Resolver sobre el ejercicio de los derechos de acceso, rectificación, cancelación u oposición de los datos personales.

X. Las demás que deriven de la Ley, el presente Reglamento y demás ordenamientos jurídicos aplicables.

Artículo 42. En ningún caso la designación del encargado del Sistema de Datos Personales supone una delegación de las facultades y atribuciones que le corresponden al responsable del mismo y/o al responsable de seguridad de acuerdo con la Ley, este Reglamento y las disposiciones que sean aplicables.

CAPÍTULO V
DE LA TRANSMISIÓN EXTERNA DE DATOS PERSONALES

Artículo 43. La transmisión externa de datos personales podrá ser entre organismos nacionales e internacionales, en términos de la legislación aplicable.

Artículo 44. La transmisión de los datos de carácter personal o su comunicación a usuarios externos se regirá por lo siguiente:

I. Toda transmisión o comunicación a usuarios externos deberá contar con el consentimiento expreso del titular, excepto en aquellos casos previstos por la Ley;

II. El usuario externo de los datos de carácter personal estará obligado a acatar las disposiciones de la Ley y del presente Reglamento, así como los lineamientos, políticas y criterios específicos que sean aplicables;

III. Cuando la comunicación a usuarios externos resulte de la prestación de servicios al responsable del Sistema, el usuario externo se considerará obligado en los términos del presente Reglamento, en las mismas condiciones que el responsable; y

IV. Quien obtenga los datos en virtud de liquidación, fusión, escisión u otra figura jurídica, ya sea que los datos provengan de personas jurídicas o físicas, queda obligado a acatar las disposiciones de la Ley y del presente Reglamento.