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 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 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 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 manera tal que se no 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 la fracción XVII 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 nombre del 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 contados 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.

Artículo 45. Cuando el responsable del Sistema transfiera los datos personales a usuarios externos nacionales o extranjeros, deberá establecer claramente la finalidad para la cual entrega los datos y el tratamiento que se les debe dar de acuerdo con este Reglamento.

Artículo 46. La transferencia de datos personales sólo podrá realizarse cuando el usuario externo garantice por escrito un nivel de protección similar al empleado en el Sistema de Datos Personales y consignado en el documento de seguridad. El usuario externo de los datos personales quedará sujeto a las mismas obligaciones que corresponden al responsable que los transmitió.

No se considerará transferencia de datos el acceso que un tercero tenga a los datos personales con motivo de la prestación de un servicio de mantenimiento o funcionamiento al archivo o banco de datos en que se encuentren.

Artículo 47. Los acuerdos entre el responsable del Sistema y el usuario externo relacionados con el tratamiento de los datos personales, deberán corresponder a lo informado en el aviso de protección de datos personales.

Artículo 48. La relación entre el responsable del Sistema y el usuario externo deberá estar autorizada por disposición legal o administrativa, mediante cláusulas contractuales u otro instrumento jurídico que decida el Instituto a través de sus procedimientos administrativos aplicables, que permita acreditar su existencia, alcance y contenido.

En todo caso, el instrumento jurídico por el que se autorice a un usuario externo el tratamiento de un Sistema, deberá establecer el plazo durante el cual conservará los datos personales, las medidas de seguridad que deberá aplicar, así como la disposición expresa de que al término del plazo los datos personales serán devueltos en su totalidad, sin conservar ninguna copia total o parcial en ningún soporte. Lo anterior con independencia de las responsabilidades que pudieran surgir por el mal uso de los datos personales durante su conservación o con posterioridad.

Artículo 49. En toda transferencia de Sistemas de Datos Personales, el responsable deberá informar al Comité de Transparencia – por conducto de la Unidad de Acceso – la identidad del usuario externo, así como las razones que motivaron el pedimento de la misma, dentro de los treinta días previos a dicho acto.

Artículo 50. El usuario externo tendrá las siguientes obligaciones respecto del tratamiento de datos que realice por cuenta del responsable del Sistema:

I. Tratar únicamente los datos personales conforme a la Ley, el presente Reglamento y el documento jurídico mediante el cual se le haya transmitido el Sistema de Datos Personales.
II. Abstenerse de tratar los datos personales para finalidades distintas.
III. Implementar las medidas de seguridad conforme al documento generado para ello.
IV. Guardar confidencialidad respecto de los datos personales tratados.
V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable del Sistema, siempre y cuando no exista una previsión legal que exija la conservación de los mismos.
VI. Abstenerse de transferir los datos personales, salvo en el caso de que el responsable del Sistema así lo determine; la comunicación derive de una subcontratación previamente autorizada por el responsable o establecida en el documento jurídico mediante el cual se le otorgó el tratamiento del Sistema; o así lo requiera la autoridad competente.

VII. Las demás que se establezcan en el acto jurídico por el cual se le otorgue el tratamiento del Sistema.

CAPÍTULO VI
DE LAS MEDIDAS COMPENSATORIAS

Artículo 51. Las medidas compensatorias tienen como objeto la protección del titular de los datos personales, salvaguardando su derecho a mantener el poder de disposición y control sobre la información que le concierne y, a su vez, de decidir de manera libre e informada sobre el uso, destino y comunicación de sus datos personales a terceros.

Artículo 52. Es facultad del responsable del Sistema determinar el medio que considere más adecuado y eficiente para comunicar a los titulares el aviso de protección de datos personales a través de la medida compensatoria, observando en todo momento el criterio de máximo alcance.

Artículo 53. Las medidas compensatorias implementadas serán aprobadas por acuerdo del Consejo General.

Artículo 54. El acuerdo de aprobación de las medidas compensatorias, además de estar debidamente fundado y motivado, deberá considerar lo siguiente para justificar la implementación de la medida compensatoria:

a) Número de titulares.
b) Antigüedad de los datos.
c) Ámbito territorial.
d) Medida compensatoria a utilizar.
e) Que la medida compensatoria cumpla con el principio de información.

Artículo 55. Las medidas compensatorias implementadas estarán vigentes mientras no se modifiquen las características del tratamiento o las circunstancias que dieron lugar a que el responsable del Sistema aplicara dicho instrumento normativo.

Artículo 56. Las medidas compensatorias se darán a conocer a través de avisos de protección de datos personales que se publicarán o difundirán en cualquiera de los siguientes medios:

I. Diarios de circulación nacional;
II. Diarios locales o revistas especializadas;
III. Páginas o sitios de Internet;
IV. Carteles informativos;
V. Cápsulas informativas radiofónicas; y
VI. Otros medios alternos de comunicación masiva determinados por el Consejo General.

Artículo 57. El responsable del Sistema deberá informar a la Unidad de Acceso – en un plazo mínimo de tres días hábiles previos a la implementación de la medida compensatoria – el acuerdo de aprobación de la misma, a fin de que lo anterior se comunique a la Comisión para los efectos conducentes.

TÍTULO TERCERO
DE LOS DERECHOS Y DEL PROCEDIMIENTO

CAPÍTULO I
DE LOS DERECHOS ARCO

Artículo 58. Todas las personas, previa identificación mediante documento oficial con fotografía, 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 del Instituto Electoral del Estado.

En caso de que el titular haya fallecido, los declarados herederos o el albacea de su sucesión, previa acreditación de su personalidad, podrán acceder a los datos personales del fallecido.

Artículo 59. Los derechos de acceso, rectificación, cancelación u oposición son derechos independientes; no debe entenderse que el ejercicio de alguno de ellos sea requisito previo o impida el ejercicio de otro.

Artículo 60. El derecho de acceso se ejercerá para solicitar y obtener información de los datos de carácter personal sometidos a tratamiento, su origen, así como las transmisiones realizadas o que se prevén hacer, en términos de lo dispuesto por la Ley y este Reglamento.

Artículo 61. El derecho de rectificación de datos en los Sistemas de Datos Personales, procederá cuando los mismos resulten inexactos o incompletos, inadecuados o excesivos.

No obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo o en un proceso judicial, aquellos se considerarán exactos siempre que coincidan con estos.

Artículo 62. El derecho de cancelación es aquel que tiene el titular para que se eliminen del Sistema los datos personales que resulten ser inadecuados o excesivos, o cuyo tratamiento no se ajuste a lo establecido en las disposiciones legales aplicables. El titular podrá también solicitar la cancelación de sus datos personales cuando hubiere ejercido el derecho de oposición y éste haya resultado procedente.

La cancelación originará el bloqueo de los datos personales, cuyo propósito es resguardar y conservar únicamente aquellos necesarios para la atención de posibles responsabilidades relacionadas con el tratamiento, durante el plazo de prescripción de estas. Cumplido el plazo deberá procederse a la eliminación de los datos, en términos de la normatividad aplicable.

De la cancelación de los datos personales podrán ser excluidos aquellos que con fines estadísticos, científicos o históricos, sean previamente sometidos al procedimiento de disociación.

La eliminación de datos no procede cuando pudiese causar perjuicios a derechos o afectar intereses legítimos de terceros, o cuando exista una obligación legal de conservar dichos datos.

Artículo 63. El titular tendrá derecho a oponerse al tratamiento parcial o total de los datos personales que le conciernen, en el supuesto que los mismos se hubiesen recabado sin su consentimiento o cuando existan motivos fundados para ello, y la Ley no disponga lo contrario. Se procederá entonces al bloqueo de datos y, de resultar procedente y previa solicitud del titular, el responsable deberá cancelarlos del Sistema.

Artículo 64. En el supuesto de que los datos personales sean rectificados o cancelados, y éstos hubieran sido transmitidos previamente, el responsable del Sistema deberá notificar la rectificación o cancelación a quien hayan sido transmitidos.

CAPÍTULO II
DEL PROCEDIMIENTO

Artículo 65. Las solicitudes de acceso, rectificación, cancelación u oposición de datos personales deberán presentarse ante la Unidad Administrativa de Acceso a la Información del Instituto Electoral del Estado, por escrito o de manera verbal, conforme al procedimiento establecido en este Capítulo. En caso de una solicitud verbal, la Unidad de Acceso deberá de orientar al solicitante para que registre la misma por escrito, a través de los formatos disponibles para tales efectos, a fin de estar en posibilidad de iniciar los trámites correspondientes.

Artículo 66. La solicitud de acceso, rectificación, cancelación u oposición de datos personales deberá contener, cuando menos, los siguientes requisitos:

I. Nombre completo del titular y, en su caso, del representante legal;
II. Descripción clara y precisa de los datos personales respecto de los que se quiere ejercer alguno de los derechos antes mencionados, así como cualquier otro elemento que facilite su localización, como pudiera ser la Unidad o Dirección ante la cual se otorgaron dichos datos;
III. Domicilio en el municipio de Puebla o correo electrónico para recibir cualesquier tipo de notificaciones; y
IV. La modalidad en la que se prefiera tener acceso a los datos personales en cuestión, ya sea a través de consulta directa, vía electrónica, copias simples o certificadas.

La solicitud deberá ser acompañada con los documentos con los que se acredite la identidad del titular y, en su caso, del representante legal, así como la personalidad de éste, de acuerdo con lo señalado en el artículo siguiente.

Artículo 67. El titular de los datos personales que presente una solicitud de acceso, rectificación, cancelación u oposición de datos, deberá identificarse mediante documento oficial con fotografía en original y copia simple. Para tales efectos, podrá presentar: credencial para votar, pasaporte, licencia o permiso de conducir, cartilla del Servicio Militar Nacional, cédula profesional, credencial de afiliación al Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, al Instituto Mexicano del Seguro Social o al Instituto Nacional de Personas Adultas Mayores (INAPAM).

Si la solicitud es formulada a través de representante legal, este deberá identificarse con alguno de los documentos mencionados, y acreditar la representación con la que se ostenta de acuerdo a la Ley aplicable, donde de manera expresa se le autorice para llevar a cabo el ejercicio de los derechos ARCO del titular. Además, deberá anexar a la solicitud copia simple de la identificación oficial con fotografía del titular de los datos.

La identificación y acreditación del titular de los datos personales y/o de su representante legal, podrán ser requeridas tantas veces sea necesario durante el desarrollo del procedimiento, desde su inicio y hasta la entrega de la información correspondiente.

Artículo 68. En el caso de solicitudes de rectificación de datos personales, deberá indicarse el dato que es erróneo y la corrección a realizarse, acompañando la documentación probatoria que

sustente la petición, salvo que la misma dependa exclusivamente del consentimiento del titular y ésta sea procedente.

Artículo 69. En el caso de solicitudes de cancelación de datos personales, deberán señalarse las razones por las cuales se considera que el tratamiento de los datos no se ajusta a lo dispuesto en la Ley, o en su caso, acreditar la procedencia del ejercicio del derecho de oposición.

Artículo 70. La respuesta a cualquiera de los derechos mencionados deberá ser proporcionada en forma legible y entendible, por escrito o mediante el correo electrónico proporcionado para tal fin en la solicitud, en un plazo máximo de quince días hábiles contados desde la presentación de la misma.

En caso de que la respuesta sea favorable, es decir, que se determine como procedente el ejercicio del derecho solicitado, la misma se hará efectiva dentro de los quince días hábiles siguientes a la fecha en que sea notificada.

El plazo de quince días podrá ser prorrogado por una sola ocasión, por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

Artículo 71. Si la solicitud se presenta directamente ante la Unidad de Acceso y no es precisa o no contiene todos los datos requeridos, en ese momento el personal de la Unidad de Acceso deberá orientar al solicitante para que subsane las deficiencias.

En el caso de las solicitudes no presentadas directamente ante la Unidad de Acceso, o si de la revisión posterior que lleve a cabo el Representante del Sistema se detecta que los detalles proporcionados por el solicitante no bastan para localizar sus datos personales en el Sistema o son erróneos, se le deberá prevenir por una sola vez y dentro de los cinco días hábiles siguientes a la presentación de la solicitud, para que la aclare o complete en el mismo plazo, apercibido que de no desahogar la prevención, la solicitud se tendrá por no presentada. Este requerimiento interrumpe los plazos establecidos en el artículo anterior.

Artículo 72. Una vez recibida la solicitud, la Unidad de Acceso deberá remitirla al responsable del Sistema de Datos Personales dentro de los tres días hábiles siguientes a la fecha de recepción de la misma.

Si de la revisión que se menciona en el artículo anterior el responsable del Sistema detecta que los datos proporcionados no son suficientes para dar trámite a la solicitud o son erróneos, deberá informarlo por escrito a la Unidad de Acceso en un plazo máximo de dos días hábiles contados a partir de la fecha en que reciba la solicitud, especificando en su caso la información que necesite para continuar con el trámite, a fin de que se pueda realizar la prevención de aclaración en tiempo y forma de acuerdo con lo señalado en el artículo anterior.

Artículo 73. En el supuesto de que los datos personales a que se refiere la solicitud obren en los Sistemas a cargo del responsable, y éste considere improcedente la solicitud de acceso, rectificación, cancelación u oposición, deberá emitir una respuesta debidamente fundada y motivada al respecto.

Artículo 74. Cuando los datos personales respecto de los cuales se ejerzan los derechos de acceso, rectificación, cancelación u oposición no sean localizados en los Sistemas de Datos Personales a cargo del responsable, se hará del conocimiento del solicitante a través de acta circunstanciada en la que se indiquen el o los Sistemas en los que se realizó la búsqueda. Dicha acta deberá estar firmada por el encargado y el responsable del Sistema.

Artículo 75. Los medios por los cuales el solicitante podrá recibir notificaciones serán por correo electrónico, de manera personal o en los estrados del Instituto.

En caso de que en la solicitud se señale un domicilio para recibir notificaciones fuera del municipio de Puebla, no se indique domicilio o correo electrónico para tal fin, las notificaciones se harán a través de los estrados del Instituto.

Artículo 76. Una vez recibida la solicitud de acceso, rectificación, cancelación u oposición de datos personales, la Unidad de Acceso iniciará el siguiente procedimiento:

I. Procederá al registro de la solicitud, debiendo entregar al solicitante un acuse de recibo que deberá contener el sello institucional, la hora y la fecha de recepción;

II. Verificará que la solicitud cumple con los requisitos establecidos en el artículo 66 de este Reglamento; de no ser así, en el momento orientará al solicitante para que subsane las deficiencias. De cumplir con los requisitos, turnará la solicitud al responsable del Sistema de Datos Personales correspondiente, dentro de los tres días hábiles siguientes, para que éste proceda a la localización de la información y emita una respuesta;

III. El responsable del Sistema informará por escrito a la Unidad de Acceso la respuesta que corresponda, antes del vencimiento del plazo que señala el artículo 70 del presente Reglamento, tomando en cuenta el plazo establecido para la prevención de aclaración por insuficiencia o error en la información proporcionada por el solicitante.

IV. En caso de que la información no se encuentre en los Sistemas a cargo del responsable al que se haya remitido la solicitud, la Unidad de Acceso tomará las medidas necesarias para que se proceda a la búsqueda exhaustiva en otra área o Unidad Administrativa diferente, en los casos que sea aplicable;

V. La Unidad de Acceso será la encargada de notificar, según corresponda, cualquier respuesta que se emita al solicitante en un plazo máximo de quince días hábiles contados a partir de que se reciba la solicitud; y

VI. Previa exhibición del original del documento con el que se acreditó la identidad del titular y/o su representante legal, así como la personalidad de éste, se hará entrega personalmente de la información requerida, o mediante el correo electrónico proporcionado y autorizado para tal fin por el titular al momento de hacer su solicitud.

Artículo 77. El trámite de solicitud de acceso, rectificación, cancelación u oposición de datos personales es gratuito. Sin embargo, en caso de solicitar su reproducción en copia simple o certificada o en cualquier otro medio previsto en la normatividad aplicable, se deberán cubrir previamente a su entrega los costos respectivos.

En el caso de las solicitudes de acceso, si la fuente lo permite, se podrá realizar la consulta directa, misma que no tendrá ningún costo.

Artículo 78. La Unidad de Acceso deberá notificar el costo de reproducción de la información requerida al solicitante, de acuerdo con el tabulador vigente, quien tendrá veinte días hábiles para realizar el pago en los medios y lugares destinados para tal fin, y presentar el respectivo comprobante, expidiéndose el comprobante correspondiente; de no realizar el pago, la Unidad de Acceso no tendrá la obligación de entregar la información.

A partir de que el solicitante compruebe haber realizado el pago, se deberá entregar la información dentro de los cinco días hábiles siguientes, en horario de oficina. Dicha información estará a disposición del solicitante durante un plazo de sesenta días hábiles. Agotado dicho plazo, la Unidad de Acceso no tendrá la obligación de entregar la información.

TÍTULO CUARTO
RESPONSABILIDADES

CAPÍTULO ÚNICO
DISPOSICIONES GENERALES

Artículo 79. Independientemente de lo dispuesto por la Normatividad Interna de Responsabilidades del Instituto Electoral del Estado y demás disposiciones en la materia, los funcionarios y demás personal del Instituto incurrirán en responsabilidad administrativa por incumplimiento de los preceptos de la Ley y de este Reglamento en los casos siguientes:

I. Usar, sustraer, destruir, comercializar, falsear, falsificar, dañar, extraviar, ocultar, inutilizar, divulgar o alterar parcial o totalmente en contravención a las disposiciones de la Ley y de este Reglamento, datos, archivos, registros y demás información que contenga datos personales que en razón de su empleo, cargo o comisión generen, obtengan, adquieran, transformen o conserven.
II. Crear Sistemas de Datos Personales sin cumplir con los requisitos establecidos.
III. Incumplir los principios aplicables al tratamiento de los datos personales.
IV. Impedir u obstaculizar las inspecciones que en su caso ordene la Comisión, o su instrucción de bloqueo de Sistemas.
V. Actuar con negligencia, dolo o mala fe en la sustanciación, trámite y respuesta de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales.
VI. El incumplimiento a las resoluciones y recomendaciones emitidas por la Comisión.
VII. Levantar un acta circunstanciada de inexistencia de datos personales en los Sistemas a su cargo, cuando existan total o parcialmente en los mismos.
VIII. Negar intencionalmente el acceso a la información con datos personales que obren en sus Sistemas.
IX. No comunicar sobre los Sistemas de Datos Personales en los que se puede encontrar la información objeto de la solicitud, cuando no obre en los Sistemas a su cargo y tengan conocimiento de ello.
X. Crear, modificar, destruir o transmitir información con datos personales, en contravención a las disposiciones de la Ley y de este Reglamento.
XI. Recabar datos personales en contravención a las disposiciones legales correspondientes.
XII. Mantener los Sistemas de Datos Personales sin las debidas condiciones de seguridad, tratarlos o usarlos posteriormente con fines distintos a los establecidos, o con incumplimiento de los principios, garantías y preceptos de protección que impongan las disposiciones legales aplicables.
XIII. Negar el acceso, rectificación, cancelación u oposición de los datos personales a quien sea titular de los mismos en los casos que proceda.
XIV. El incumplimiento de cualquiera de las disposiciones de la Ley y de este Reglamento.

Artículo 80. El procedimiento para determinar la responsabilidad administrativa de los funcionarios y demás personal del Instituto, y para la imposición de las sanciones que correspondan, se substanciará conforme a lo previsto en el Título Quinto de la Ley, así como en la Normatividad Interna de Responsabilidades del Instituto y demás disposiciones legales aplicables; se iniciará de oficio, por queja o denuncia presentada por el Comité, cualquier persona o por el funcionario y demás personal que tenga conocimiento de los hechos.

Artículo 81. Las sanciones por responsabilidad administrativa que se generen por el incumplimiento de las obligaciones a que se refiere este Reglamento, son independientes de aquellas de orden civil o penal que procedan, y se aplicarán únicamente a los funcionarios y demás personal del Instituto que las autoridades competentes determinen como directamente responsables de tal incumplimiento, sin perjuicio de sus superiores jerárquicos o de la Unidad, cuando a estos no se les haya determinado responsabilidad alguna, salvo que se demuestre posteriormente que los funcionarios o personal responsable actuaron a instancia o por instrucciones de éstos.

ARTÍCULOS TRANSITORIOS

PRIMERO.- El presente Reglamento entrará en vigor al día siguiente de su aprobación por parte del Consejo General.

SEGUNDO.- Se derogan todas las disposiciones que se opongan al presente Relamento.

TERCERO.- Las Unidades Técnicas y Administrativas del Instituto deberán remitir a la Unidad de Acceso las Fichas Técnicas de los Sistemas de Datos Personales a su cargo, con los requisitos que señala el presente Reglamento, dentro de los tres días hábiles siguientes a la entrada en vigor del mismo, para su consecuente aprobación por parte del Comité de Transparencia y del Consejo General.