

**Lineamientos de protección de datos personales
del Instituto Electoral del Estado de Querétaro**

Índice	Págs.
Exposición de motivos	2
Título Primero	
Disposiciones Generales	3
Capítulo Único	
Disposiciones generales	3
Título Segundo	
De la Unidades Administrativas en materia de protección de datos personales	8
Capítulo I	
Atribuciones del Comité	8
Capítulo II	
Atribuciones de la Unidad de Transparencia	8
Capítulo III	
De las personas Enlaces	9
Título Tercero	
Principios y deberes que rigen el tratamiento de los datos personales	10
Capítulo I	
Principios	10
Capítulo II	
Aviso de privacidad	11
Capítulo III	
Deberes	12
Capítulo IV	
De las medidas de seguridad	13
Capítulo V	
De las funciones y obligaciones de la persona responsable del sistema de datos personales	16
Título Cuarto	
Procedimiento para el ejercicio de los derechos	17
Capítulo I	
Del procedimiento para ejercer los derechos ARCO y de portabilidad	17
Capítulo II	
Recurso de revisión	20
Capítulo III	
Procedimiento para la transferencia o remisión de datos	21
Capítulo IV	
Sanciones	21
Artículos Transitorios	21

Exposición de motivos

El artículo 6, apartado A, fracción II y 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos reconoce el derecho a la privacidad de toda persona, la cual constituye la base de la protección de datos personales. De esta manera, la protección a los datos personales no debe ser vista solo como una excepción al derecho de acceso a la información pública, sino como una protección más amplia a los derechos humanos de las personas, el cual debe ser velado a fin de que terceras personas no incurran en conductas que le afecten arbitrariamente.

En este sentido, los presentes Lineamientos tienen como objetivo regular el debido tratamiento de los datos personales recabados derivado del ejercicio de las funciones del Instituto Electoral del Estado de Querétaro; lo anterior, a fin de cumplimentar las obligaciones que le establece la normatividad aplicable como sujeto obligado.

Estos Lineamientos se integran con un Título Primero, Capítulo Único, relativo a las disposiciones generales, en el cual se establece su objeto, un glosario de ordenamientos legales, de órganos, autoridades y conceptos, aportando con ello claridad en su aplicación e interpretación, entre otras.

El Título Segundo hace referencia a los órganos del Instituto que estarán a cargo de la protección de datos personales, a saber, el Comité de Transparencia, la Unidad de Transparencia y el funcionariado enlace.

Por su parte, el Título Tercero prevé los principios y deberes que deben regir el tratamiento de los datos personales; además, establece las medidas de seguridad que deben implementarse para garantizar la integridad del Sistema de Datos Personales, así como las funciones y obligaciones del funcionariado responsable de dicho sistema.

El Título Cuarto contiene los procedimientos para el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales, además de un apartado relativo al recurso de revisión y al procedimiento para la transferencia o remisión de datos.

Los Lineamientos contienen dos artículos transitorios referentes a su entrada en vigor, así como su publicación en el Periódico Oficial del Gobierno del Estado de Querétaro “La Sombra de Arteaga”, en los estrados y en el sitio de Internet del Instituto.

Título Primero

Disposiciones generales

Capítulo Único

Disposiciones generales

Artículo 1. Los presentes Lineamientos son de orden público y tienen por objeto regular el debido tratamiento de los datos personales en posesión del Instituto Electoral del Estado de Querétaro, así como establecer las bases, principios y procedimientos que permitan el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad de los datos personales, a fin de garantizar el derecho que tiene toda persona a la protección de sus datos personales.

Artículo 2. Los presentes Lineamientos son de observancia obligatoria para las Unidades Administrativas y funcionariado del Instituto Electoral del Estado de Querétaro, así como para toda persona o institución vinculada con el tratamiento de datos personales que realice este Instituto.

Los Lineamientos serán aplicables a cualquier tratamiento de datos personales que obre en soportes físicos, electrónicos y mixtos.

Artículo 3. Para los efectos de estos Lineamientos, además de los previstos en las leyes generales y local en la materia, se entenderá por:

I. En cuanto a ordenamientos legales:

- a) **Ley General:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- b) **Ley Local:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Querétaro.
- c) **Ley Electoral:** Ley Electoral del Estado de Querétaro, y
- d) **Lineamientos:** Lineamientos en materia de Protección de Datos Personales del Instituto Electoral del Estado de Querétaro.

II. En cuanto a los órganos y autoridades:

- a) **Consejo General:** Consejo General del Instituto.
- b) **Comité:** Comité de Transparencia del Instituto.
- c) **Infoqro:** Comisión de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Querétaro.
- d) **Instituto:** Instituto Electoral del Estado de Querétaro.
- e) **Unidades Administrativas:** Órganos o áreas del Instituto que cuentan o pueden contar con la información, o en su caso dar tratamiento a los datos personales.
- f) **Unidad de Transparencia:** Unidad de Transparencia del Instituto.

III. En cuanto a los conceptos:

- a) **Aviso de privacidad:** Documento a disposición del titular de datos personales de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.
- b) **Base de datos:** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados que permitan su tratamiento, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
- c) **Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.
- d) **Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular, mediante la cual autoriza el tratamiento de sus datos personales al Instituto.
- e) **Datos personales:** Información concerniente a una persona física, identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
- f) **Datos personales sensibles:** Aquellos que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para la persona titular del derecho. Se consideran sensibles, de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, creencias religiosas, filosóficas y morales, opiniones políticas, datos genéticos, datos biométricos y preferencia sexual.
- g) **Derechos ARCO:** Derechos de acceso, rectificación, cancelación y oposición de los datos personales.
- h) **Documentos:** Reportes, estudios, actas, resoluciones, oficios, acuerdos, circulares, contratos, convenios, estadísticas; o cualquier otro registro que genere el ejercicio de las facultades o la actividad del Instituto como sujeto obligado y su estructura orgánica; sin importar su fuente o fecha de elaboración.
- i) **Enlace:** Funcionariado designado por cada Unidad Administrativa, para que colabore con la Unidad de Transparencia en el ejercicio de los derechos ARCO, su portabilidad y su trámite, así como en las labores propias de las necesidades en materia de protección de datos personales.
- j) **Fuentes de acceso público:** Bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución, así como páginas de Internet o medios de comunicación propios del Instituto en los que se difunda información oficial, directorios telefónicos y registros públicos, en términos de la normativa.

- k) Información:** La contenida en los documentos y expedientes que el Instituto, por medio de sus Unidades Administrativas generen, obtengan, adquieran, transformen o conserven por cualquier título, que será de los siguientes tipos:
- 1) Confidencial:** Aquella que contiene datos personales concernientes a una persona identificada o identificable, de tal manera que su identidad pueda determinarse directa o indirectamente a través de cualquier información.
 - 2) De interés público:** Aquella que resulta relevante o beneficiosa para la sociedad, cuya divulgación resulta útil para que el público comprenda las actividades que lleva a cabo el Instituto y no simplemente sea de interés individual.
 - 3) Pública:** Todo registro o dato contenido en documentos creados, obtenidos, adquiridos, transformados o en posesión del Instituto en el ejercicio de sus funciones y previstos en las disposiciones normativas aplicables.
 - 4) Reservada:** Aquella que comprometa la seguridad pública, al poner en peligro las funciones a cargo de la federación, las entidades federativas, los municipios, tendientes a preservar y resguardar la vida, la salud, la integridad y el ejercicio de los derechos de las personas, así como para el mantenimiento del orden público. Asimismo, podrá considerarse como reservada aquella que revele datos que pudieran ser aprovechados para conocer la capacidad de reacción de las instituciones encargadas de la seguridad pública sus planes, estrategias, tecnología, información, sistemas de comunicaciones.
- l) Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales, en términos de la Ley General.
- m) Partidos políticos:** Partidos políticos nacionales y locales.
- n) Plataforma Nacional:** Plataforma Nacional de Transparencia.
- o) Portabilidad:** Derecho de la persona titular de datos personales a obtener una copia de los datos objeto del tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos, de conformidad con los artículos artículo 57 de la Ley General de Protección de Datos y 51 de la Ley Local de Protección de Datos.
- p) Responsable:** Persona titular de la Unidad de Transparencia o el funcionariado de la citada Unidad que lleve a cabo el tratamiento de datos personales.
- q) 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.
- r) Supresión:** La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.
- s) Titular:** Persona física a quien corresponde los datos personales.

- t) Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, transferencia y, en general, cualquier uso o disposición de datos personales.

Artículo 4. La aplicación de los Lineamientos se hará conforme a lo dispuesto por la Constitución Política de los Estados Unidos Mexicanos, Tratados Internacionales de los que el Estado mexicano sea parte, Leyes General y Local en la materia, resoluciones y sentencias vinculantes.

Su interpretación se realizará conforme a los criterios gramatical, sistemático, funcional, así como los criterios, determinaciones y opiniones de los organismos competentes en materia de protección de datos personales en posesión de sujetos obligados.

Artículo 5. El Instituto deberá contar con un sistema de datos personales en términos de la normatividad de la materia, cuya responsabilidad será de la Unidad de Transparencia.

Artículo 6. Las Unidades Administrativas que posean bases de datos personales deberán hacerlo del conocimiento de la Unidad de Transparencia, a efecto de que se mantenga actualizado el registro del sistema de datos personales en posesión del Instituto.

Artículo 7. Las Unidades Administrativas y responsables que intervengan en el tratamiento de datos personales deberán garantizar la protección en el tratamiento, por lo que no podrán comunicarlos a terceros, salvo en los casos previstos en las disposiciones normativas aplicables.

En tal sentido, no podrán difundir, distribuir o comercializar los datos personales contenidos en el sistema de datos personales del Instituto, aquellos recabados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar; o bien que ello atienda a una obligación legal o a un mandato judicial.

Artículo 8. Es responsabilidad de las Unidades Administrativas recabar el consentimiento de las personas titulares de acuerdo con sus atribuciones, por regla general será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente, para tal efecto se deberá considerar que:

- I.** El consentimiento será tácito cuando el aviso de privacidad se ponga a disposición de la persona titular y no manifieste su voluntad en sentido contrario.
- II.** El consentimiento será expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.
- III.** Para el tratamiento de datos personales sensibles obligatoriamente se requerirá contar con el consentimiento expreso y por escrito del titular, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación, salvo las excepciones previstas en la Ley General y estos Lineamientos.

Artículo 9. Las Unidades Administrativas o responsables no estarán obligadas a recabar el consentimiento del titular para el tratamiento de sus datos personales en los casos siguientes:

- I. Cuando una ley así lo disponga, por razones de seguridad pública, disposiciones de orden público o protección de derechos de terceros, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en la Ley Local, en ningún caso, podrán contravenirla.
- II. Cuando las transferencias que se realicen entre responsables sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.
- III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente.
- IV. Para el reconocimiento o defensa de derechos de la persona titular ante autoridad competente.
- V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre la persona titular y el Instituto.
- VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a una persona o en sus bienes.
- VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria.
- VIII. Cuando los datos personales figuren en fuentes de acceso público.
- IX. Cuando los datos personales se sometan a un procedimiento previo de disociación.
- X. Cuando la persona titular de los datos personales sea reportada como desaparecida en los términos de la ley en la materia.

Cuando no se actualicen algunas de las causales de excepción previstas en las disposiciones normativas aplicables, los responsables deberán contar con el consentimiento previo del titular, el cual deberá otorgarse de forma:

- a) **Libre:** Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular.
- b) **Específica:** Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento.
- c) **Informada:** Que la persona titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

En la obtención del consentimiento de persona menores de edad o de quienes se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable, así como por los criterios que en materia de uso de la imagen de personas menores de edad emitan las autoridades jurisdiccionales y administrativas electorales.

Artículo 10. Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos

administrativos, contables, fiscales, jurídicos e históricos, lo cual se asentará en el sistema de datos personales del Instituto, conforme a los instrumentos de gestión documental.

Artículo 11. Para el bloqueo y supresión de los datos personales, el Comité, a propuesta de la Unidad de Transparencia, establecerá los procedimientos y plazos de conservación, de conformidad con las disposiciones normativas aplicables, los cuales deberán ser publicados y difundidos en el portal de Internet del Instituto, además deberá realizarse una revisión periódica sobre la necesidad de conservar los datos personales.

TÍTULO SEGUNDO

De las Unidades Administrativas en materia de protección de datos personales

CAPÍTULO I

Atribuciones del Comité

Artículo 12. El Instituto por medio del Comité, será la autoridad en materia de protección de datos personales y se integrará en términos del Reglamento Interior del Instituto.

Artículo 13. Adicional a las atribuciones establecidas en las disposiciones normativas, el Comité tendrá las atribuciones siguientes:

- I.** Vigilar el cumplimiento de la normatividad en materia de datos personales.
- II.** Requerir cualquier información a las Unidades Administrativas para el adecuado cumplimiento de sus funciones.
- III.** Revisar los documentos de seguridad que implementarán las personas responsables en el sistema de datos personales a su cargo.
- IV.** Dar acompañamiento y asesoría a las Unidades Administrativas en materia de datos personales.
- V.** Emitir recomendaciones a las Unidades Administrativas para el debido cumplimiento de la normatividad.
- VI.** Dar vista a la autoridad competente, de las presuntas irregularidades en materia de datos personales en que incurra el funcionariado del Instituto.
- VII.** Conocer el registro actualizado de las bases de datos personales del Instituto.
- VIII.** Las demás que le confiera el Consejo General y la normatividad aplicable.

Capítulo II

Atribuciones de la Unidad de Transparencia

Artículo 14. La Unidad de Transparencia en atención a las atribuciones establecidas en las disposiciones normativas deberá cumplir con las funciones siguientes:

- I.** Ser el vínculo entre la persona solicitante y el Instituto.
- II.** Recibir las solicitudes de ejercicio de los derechos ARCO y su portabilidad, así como efectuar los trámites internos necesarios para su debida atención.

- III. Llevar un registro y control de las solicitudes de ejercicio de derechos ARCO y su portabilidad, que se presenten ante el Instituto.
- IV. Auxiliar a las personas solicitantes en el llenado de la solicitud con los requisitos establecidos en los presentes Lineamientos, y los demás elementos que sean necesarios para el efectivo ejercicio de los derechos ARCO y su portabilidad.
- V. Validar a las Unidades Administrativas los formatos que serán utilizados para recabar el consentimiento de las personas titulares de datos personales que sean necesarios para el tratamiento, transmisión, difusión o distribución de dicha información.
- VI. Proponer al Comité los procedimientos internos que fortalezcan y aseguren mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO y su portabilidad ante el Instituto.
- VII. Promover la capacitación y actualización del personal del Instituto en materia de protección de datos personales.
- VIII. Asesorar a las Unidades Administrativas en materia de protección de datos personales.
- IX. Proponer reformas o modificaciones a los Lineamientos en la materia.
- X. Asesorar en la elaboración del documento de seguridad.
- XI. 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 del Instituto al que haya sido turnada.
- XII. Efectuar las notificaciones que deriven del ejercicio de sus funciones y atribuciones.
- XIII. Supervisar el cumplimiento de criterios, políticas y lineamientos en materia de protección de datos personales.
- XIV. Representar al Instituto en el trámite del recurso de revisión que se substancie ante el Infoqro y rendir el informe con justificación referido en la Ley.
- XV. Las demás que deriven de la normatividad en materia de protección de datos personales.

Capítulo III

De las personas Enlaces

Artículo 15. Las personas titulares de las Unidades Administrativas designarán a quien funja como enlace, debiendo notificarle mediante oficio a la Unidad de Transparencia.

Artículo 16. El funcionariado responsable del tratamiento de derechos ARCO y su portabilidad proporcionarán a quien funja como enlace la información necesaria, a fin de que ésta, a su vez, dé respuesta a la Unidad de Transparencia para los trámites respectivos y para que se dé cumplimiento a las resoluciones emitidas por las autoridades en la materia. Dicha información deberá ser proporcionada en tiempo y forma, acorde con los plazos y términos establecidos por la referida Unidad.

Artículo 17. Son funciones de quien funja como enlace:

- I. Asistir a las capacitaciones, cursos, talleres y conferencias que se convoque en materia de protección de datos personales.
- II. Verificar que la información publicada por la Unidad Administrativa al que tenga adscripción no contenga datos personales y en su caso, realizar la versión pública de acuerdo con la normatividad.
- III. Recibir y dar trámite a las solicitudes de ejercicio de los derechos ARCO y su portabilidad que le hayan sido turnadas por la Unidad de Transparencia del-Instituto.
- IV. Enviar las respuestas de ejercicio de los derechos ARCO y su portabilidad a la Unidad de Transparencia, dentro de los plazos establecidos.

TÍTULO TERCERO

Principios y deberes que rigen el tratamiento de los datos personales

CAPÍTULO I

Principios

Artículo 18. En el tratamiento de datos personales, las Unidades Administrativas y su funcionariado deberá regirse por los principios siguientes:

- I. **Licitud:** Sujetarse a las facultades o atribuciones del Instituto.
- II. **Finalidad:** El tratamiento de los datos personales deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

La persona responsable podrá tratar datos personales para finalidades distintas a aquellas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento de su titular, o al actualizarse una causa de excepción, en los términos previstos en las disposiciones que resulten aplicables en la materia.
- III. **Lealtad:** Evitar obtener y tratar datos personales, a través de medios engañosos o fraudulentos.
- IV. **Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.
- V. **Calidad:** Adoptar medidas para que los datos personales que traten sean exactos, completos, correctos y actualizados, sin que se altere su veracidad.
- VI. **Proporcionalidad:** Solo se tratarán datos que resulten adecuados, relevantes y estrictamente necesarios para las finalidades del Instituto.
- VII. **Información:** Hacer del conocimiento del titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.
- VIII. **Responsabilidad:** Actuar con apego a los principios, deberes y obligaciones establecidos la normatividad aplicable en materia de datos personales.

Artículo 19. Las Unidades Administrativas sólo podrán acceder a los datos de niñas, niños y adolescentes cuando sea estrictamente necesario para el ejercicio de sus funciones, privilegiando el interés superior de las personas menores de edad de conformidad con la normatividad aplicable.

Las Unidades Administrativas que recaben dichos datos deberán poner a disposición el aviso de privacidad correspondiente en formato comprensible, así como la versión integral que corresponda conforme a los parámetros que establezca Infoqro.

Los datos que se recaben no podrán ser objeto de transferencias, salvo las excepciones previstas por la ley, y se resguardarán preservando su identificación y su derecho a la intimidad.

Capítulo II

Aviso de privacidad

Artículo 20. El aviso de privacidad se presentará en modalidad simplificada e integral.

El aviso simplificado deberá contener al menos la información siguiente:

- I. La denominación del responsable del Instituto del tratamiento de datos personales.
- II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieran el consentimiento de la persona titular.
- III. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:
 - a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales estatales o municipales y las personas físicas o morales a las que se podrán transferir los datos personales.
 - b) La finalidad de las transferencias.
- IV. Los mecanismos y medios disponibles para que la persona titular, en su caso, manifieste su derecho de oposición, para el tratamiento de sus datos personales cuando se trate de transferencias de datos personales que requieren el consentimiento del titular, y
- V. El sitio de internet y/o tecnologías que desarrolle el Instituto para prestar servicios por medios electrónicos o remotos donde se podrá consultar el aviso de privacidad integral, sin embargo, la puesta a disposición del aviso de privacidad simplificado no exime a la Unidad Administrativa de su obligación de proveer los mecanismos para que la persona titular pueda conocer el contenido del aviso de privacidad integral.

Los mecanismos y medios a los que se refiere la fracción IV de este artículo, entre otros, podrán ser por correo electrónico, escrito o comparecencia ante el Instituto a través de la Unidad de Transparencia y deberán estar disponibles para que la persona titular pueda manifestar su negativa al tratamiento de sus datos personales para las finalidades o transferencias que requieran el consentimiento del titular, previo a que ocurra dicho tratamiento.

Artículo 21. El aviso de privacidad integral, además de lo dispuesto en las fracciones del artículo anterior, deberá contener la siguiente información:

- I. El domicilio del responsable del tratamiento de datos personales del Instituto.
- II. Los datos personales que serán sometidos a tratamiento, identificando aquellos que son sensibles.
- III. El fundamento legal que faculta al Instituto para llevar a cabo el tratamiento.

- IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieren el consentimiento de la persona titular.
- V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO y su portabilidad.
- VI. El domicilio de la Unidad de Transparencia.
- VII. Los medios a través de los cuales se comunicarán los cambios al aviso de privacidad.

Artículo 22. Los órganos del Instituto deberán difundir el aviso de privacidad en su modalidad simplificada e integral a través de las oficinas del Instituto, el sitio de Internet y/o las tecnologías que desarrolle el Instituto para prestar servicios por medios electrónicos o remotos.

Artículo 23. En los casos que determine el Comité, el Instituto podrá instrumentar medidas compensatorias de comunicación masiva para dar a conocer el aviso de privacidad.

CAPITULO III

Deberes

Artículo 24. Las Unidades Administrativas informarán al Comité las medidas de seguridad de carácter administrativo, físico y técnico para la protección de datos personales, contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como para garantizar su confidencialidad, integridad y disponibilidad que estimen pertinentes conforme a sus actividades y facultades.

El Comité conocerá la implementación de dichas medidas de seguridad emitidas por la Dirección de Tecnologías de la información del Instituto a través de las cuales las Unidades Administrativas del Instituto deberán resguardar la información que posean. Lo anterior en términos de los Lineamientos para la utilización de las tecnologías de la información y comunicaciones del Instituto.

Artículo 25. La responsable deberá elaborar un documento de seguridad con relación a los datos personales objeto de tratamiento, mismo que debe contener al menos, el inventario de datos personales y de los sistemas de tratamiento; las funciones y obligaciones de las personas que traten datos personales; el análisis de riesgos; el análisis de brecha; el plan de trabajo; los mecanismos de monitoreo y revisión de las medidas de seguridad, y el programa general de capacitación.

Artículo 26. Las Unidades Administrativas, en sus respectivos ámbitos de competencia, deberán llevar un registro de las vulneraciones a la seguridad de los datos personales, mediante la bitácora digital que establezca la Unidad de Transparencia para tal efecto, en la que se describa:

- I. La vulneración.
- II. La fecha en la que ocurrió.
- III. El motivo de vulneración.
- IV. Las acciones correctivas implementadas de forma inmediata y definitiva, establecidas por el Comité.

- V.** Las acciones preventivas que, en su caso, puedan ser implementadas para evitar vulneraciones posteriores.

Artículo 27. Las Unidades Administrativas responsables del tratamiento de los datos personales en los ámbitos de sus respectivas competencias, deberán informar a la Unidad de Transparencia, para que dicho órgano informe a la persona titular de Infoqro o al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales sobre las posibles vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, sin dilación alguna, en cuanto confirmen que ocurrió la vulneración y que hubiere empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación.

Lo anterior, a fin de que las personas titulares afectadas, puedan tomar las medidas correspondientes, para la defensa de sus derechos.

Artículo 28. Las Unidades Administrativas deberán establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos, obligación que subsistirá, aún después de que haya finalizado la relación entre los mismos.

Dicho deber quedará asentado en los contratos o convenios que suscriban con el Instituto, así como con aquellas entidades, personas físicas o morales con quien se realice alguna actividad.

CAPÍTULO IV

De las medidas de seguridad

Artículo 29. Las medidas de seguridad son los medios por los cuales se busca garantizar la integridad del sistema de datos personales, así como el cumplimiento de los principios de confidencialidad, disponibilidad, responsabilidad y seguridad. En su implementación podrán coadyuvar las diversas Unidades Administrativas, principalmente la Dirección de Tecnologías de la Información, la Unidad de Transparencia y el Comité.

Artículo 30. 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 y se regirán conforme a lo siguiente:

A. TIPOS DE SEGURIDAD.

- I. Física:** destinadas a la protección de instalaciones, equipos, soportes o sistemas de datos para la prevención de riesgos.
- II. Lógica:** permiten la identificación y autenticación 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:** 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:** restricciones preventivas y/o de riesgos que deberán observar las Unidades Administrativas, responsables, enlaces y usuarias de los Sistemas, para

acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicación.

B. NIVELES DE SEGURIDAD.

I. Básico. Medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas, debiendo cubrir, al menos, los aspectos siguientes:

- a) Documento de seguridad.
- b) Unidad Administrativa responsable de seguridad informática.
- c) Registro del personal que intervenga en el tratamiento.
- 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. 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 de la persona. Este nivel de seguridad, además de las medidas del nivel básico, 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. 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, así como:

- a) Identificación y autenticación de la persona responsable, encargada y usuaria externa, en su caso.
- b) Protección contra escritura y modificación de documentos, salvo consentimiento expreso por escrito de la persona responsable.
- c) Auditorías realizadas por la Contraloría Interna del Instituto.
- d) Autorización expresa de la persona 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 por el Instituto, lo cual debe hacerse del conocimiento de la Unidad de Transparencia, para la actualización del sistema de datos personales que corresponda.

Artículo 31. 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, las personas responsables, encargadas y usuarias, así como las medidas de seguridad concretas implementadas.

La persona responsable del sistema de datos personales, con la asesoría de la Unidad de Transparencia, elaborará el documento de seguridad que será de observancia obligatoria para todo el personal permanente y eventual que labore en el Instituto a cargo, así como para las personas usuarias externas que tenga acceso al Sistema de Datos Personales y/o al sitio donde se ubica el mismo.

Artículo 32. El documento de seguridad deberá contener al menos los datos siguientes:

- I.** Nombre, cargo y adscripción de la persona responsable.
- II.** Nombre, cargo y adscripción de la o las personas encargadas del tratamiento del sistema de datos personales, y en su caso, de las personas usuarias.
- III.** Tratándose de personas usuarias diversas a enlaces o responsables, deberá indicarse el acto jurídico por el cual se otorgará el tratamiento de los datos.
- 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 funcionariado 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 33. Las medidas enfocadas en garantizar el nivel de seguridad deberán considerar lo siguiente:

- I.** Procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y en su caso, claves de acceso para la operación del sistema.
- II.** Actualización de información contenida en el sistema.
- III.** Procedimientos de creación de copias de respaldo y de recuperación de los datos automatizados, así como para el archivo físico conforme a los instrumentos de gestión documental.
- IV.** Bitácoras anuales de acceso y acciones llevadas a cabo en el sistema.
- V.** Procedimiento de notificación, gestión y respuesta ante incidentes.
- VI.** Procedimiento para la cancelación de un sistema.
- VII.** Procedimientos para la realización de revisiones internas de las medidas de seguridad.
- VIII.** Mecanismos de protección contra escritura y modificación de documentos.

Artículo 34. El documento de seguridad será revisado por lo menos una vez al año por el funcionariado responsable, remitiendo a la Unidad de Transparencia constancia de la revisión.

La persona responsable del sistema de datos personales deberá remitir a la Unidad de Transparencia durante los primeros diez días hábiles del enero de cada año, el documento de seguridad aplicable al sistema que se encuentre a su cargo.

Una vez que la Unidad de Transparencia cuente con los datos de actualización de los documentos de seguridad, deberá informarlo al Comité en la siguiente sesión ordinaria.

Cuando se produzcan cambios relevantes en el tratamiento de los datos personales que puedan repercutir en el cumplimiento de las medidas de seguridad implementadas, la persona responsable del sistema deberá remitir el documento de seguridad a la Unidad de Transparencia, a efecto de que lo someta a consideración del Comité.

Artículo 35. Las funciones y obligaciones de quienes intervengan en el tratamiento de los datos personales de un sistema deberán estar claramente definidas en el documento de seguridad. La persona 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 36. 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 General y la demás normatividad aplicable, siempre y cuando medie previa solicitud por parte de la Unidad Administrativa al Comité.

CAPÍTULO V

De las funciones y obligaciones de la persona responsable del sistema de datos personales

Artículo 37. Son funciones de la persona responsable del sistema de datos personales:

- I.** Decidir sobre el contenido y finalidad del sistema de datos personales a su cargo.
- II.** Elaborar e implementar el documento de seguridad aplicable a los sistemas a su cargo.
- III.** Designar a las personas encargadas del tratamiento del sistema de datos personales y de vigilar el cumplimiento de las medidas de seguridad establecidas en el documento de seguridad.
- IV.** Determinar la eliminación del sistema de datos personales a su cargo.
- V.** Crear, establecer, modificar, eliminar y llevar a cabo el procedimiento de disociación de datos personales, conforme a su competencia.
- VI.** Conceder o anular la autorización para el acceso a los sistemas, previo aviso a la Unidad de Transparencia.

Artículo 38. En ningún caso la designación de la persona enlace o encargada supone una delegación de las facultades y atribuciones que le corresponden a la persona responsable del mismo y/o a la persona responsable de seguridad.

TITULO CUARTO
Procedimiento para el ejercicio de los derechos.

CAPÍTULO I
Del procedimiento para ejercer los derechos ARCO y de portabilidad

Artículo 39. Las solicitudes para el ejercicio de los derechos ARCO y su portabilidad deberán presentarse ante la Unidad de Transparencia, a través de los mecanismos señalados en los Lineamientos de Transparencia y Acceso a la Información Pública del Instituto.

El ejercicio de los derechos ARCO y su portabilidad, será gratuito y sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío, aprobado por el Consejo General.

Artículo 40. La identidad de la persona titular de los datos personales y, en su caso, de su representante legal deberán ser acreditadas previo al ejercicio del derecho ARCO y su portabilidad que corresponda, a través de la presentación de un documento de identificación oficial vigente en original para su cotejo y copia simple.

Además, en el caso de la persona representante, deberá presentar el documento en el que consten sus facultades de representación: instrumento público o carta poder simple firmada ante dos testigos, anexando copia simple de las identificaciones oficiales de quienes intervengan en la suscripción de este.

Artículo 41. Cuando las Unidades Administrativas reciban una solicitud para el ejercicio de los derechos ARCO y su portabilidad, deberán remitirla a la Unidad de Transparencia dentro del día hábil siguiente, para su registro y trámite correspondiente.

Artículo 42. En caso de que la Unidad de Transparencia advierta que la solicitud no tenga relación con el ejercicio de los derechos ARCO y su portabilidad remitirá la solicitud al órgano del Instituto competente para su atención.

Artículo 43. En caso de que la solicitud de derechos ARCO y su portabilidad no satisfaga alguno de los requisitos previstos en estos Lineamientos, y el Instituto no cuente con elementos para subsanarla, se prevendrá a el titular dentro de los cinco días hábiles siguientes a la presentación de la solicitud, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días hábiles contados a partir del día hábil siguiente al de la notificación.

Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud para el ejercicio de los derechos ARCO y su portabilidad.

La prevención tendrá el efecto de interrumpir el plazo para dar respuesta a la solicitud de ejercicio de los derechos ARCO y su portabilidad.

En caso de que la persona titular atienda satisfactoriamente el requerimiento de información, el plazo para dar respuesta a la solicitud empezará a correr al día hábil siguiente al del desahogo.

Artículo 44. Cuando sea notoria la incompetencia del Instituto para atender la solicitud de ejercicio de los derechos ARCO y su portabilidad, la Unidad de Transparencia deberá hacerlo del

conocimiento de la persona titular dentro de los tres días hábiles siguientes a la presentación de la solicitud, en caso de poderlo determinar, dicha unidad orientará a el titular hacia la persona responsable competente.

Artículo 45. La respuesta a las solicitudes de derechos ARCO y su portabilidad deberá notificarse a la persona titular, o en su caso, quien la represente, a través de la Unidad de Transparencia, en un plazo que no deberá exceder de veinte días hábiles contados a partir del día siguiente a la recepción de la solicitud.

El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por diez días hábiles cuando así lo justifiquen las circunstancias, siempre y cuando se le notifique a la persona titular dentro del plazo de respuesta.

Artículo 46. En caso de resultar procedente el ejercicio del derecho ARCO y su portabilidad, el mismo se hará efectivo en un plazo que no podrá exceder de quince días hábiles contados a partir del día hábil siguiente en que se haya notificado la respuesta al titular o a su representante, según sea el caso, y se haya acreditado su identidad o personalidad, respectivamente.

Artículo 47. Para cada uno de los supuestos de ejercicio de derechos ARCO y su portabilidad, la Unidad de Transparencia deberá considerar lo siguiente:

I. Acceso:

- a) La persona titular deberá señalar la modalidad en que requiere se le otorgue el acceso a sus datos, la cual podrá ser mediante consulta directa, expedición de copias simples o certificadas, o la reproducción en cualquier otro medio, incluidos los digitales.
- b) La Unidad de Transparencia preferentemente deberá atender la solicitud en la modalidad requerida por la persona titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en dicha modalidad en cuyo caso se deberán ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.

II. Rectificación:

- a) La persona titular, en la medida de lo posible, señalará la base de datos en la que obran los datos personales y/o la finalidad para la que fueron recabados, y especificará la corrección o actualización solicitada, para lo cual deberá aportar la documentación que sustente su petición.
- b) En caso de que omita señalar la base de datos, ello no será impedimento para continuar con el desahogo de la solicitud.

III. Cancelación:

- a) La persona titular deberá señalar las causas que motiven la supresión de sus datos personales en los archivos, registros o bases de datos del Instituto.
- b) El Instituto podrá hacer del conocimiento de la persona solicitante las excepciones por cuestiones laborales, administrativas, fiscales o judiciales que implican la conservación de determinados datos.

IV. Oposición:

- a) La persona titular deberá manifestar las causas o la situación específica que llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer este derecho.
- b) En ese sentido, la persona titular deberá expresar si la oposición solicitada **es** total o parcial.

V. Portabilidad:

- a) La persona titular podrá solicitar al Instituto sus datos personales, en los formatos estructurados que permitan su reutilización.

Artículo 48. En el procedimiento de gestión interna para dar trámite a las solicitudes para el ejercicio de derechos ARCO y su portabilidad, se deberá atender lo siguiente:

- I. El Instituto implementará mecanismos electrónicos para la gestión interna de las solicitudes para el ejercicio de los derechos ARCO y su portabilidad, así como la Plataforma Nacional de Transparencia.
- II. Las personas enlaces de transparencia fungirán como enlaces de protección de datos personales, salvo que la persona titular de la Unidad Administrativa del Instituto determine nombrar a una persona diferente con dicho carácter.
- III. Cuando la solicitud del ejercicio de los derechos ARCO y su portabilidad resulte improcedente, la Unidad Administrativa del Instituto que haya recibido el turno deberá remitir al Comité, por conducto de la Unidad de Transparencia, en un plazo no mayor de cinco días hábiles contados a partir de que recibió la referida solicitud, un oficio en el que funde y motive su determinación, acompañando, en su caso, las pruebas que resulten pertinentes y el expediente correspondiente, para que el Comité resuelva si confirma, modifica o revoca la improcedencia manifestada.

Las causas de improcedencia a que se refiere el párrafo anterior son:

- a) Cuando la persona titular o su representación no estén debidamente acreditadas para ello.
- b) Cuando los datos personales no se encuentren en posesión del Instituto.
- c) Cuando exista un impedimento legal.
- d) Cuando se lesionen los derechos de una tercera persona.
- e) Cuando se obstaculicen actuaciones judiciales o administrativas.
- f) Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de estos.
- g) Cuando la cancelación u oposición haya sido previamente realizada.

- h) Cuando la Unidad Administrativa no sea competente.
- i) Cuando sean necesarios para proteger intereses jurídicamente tutelados de la persona titular.
- j) Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por la persona titular.
- k) Cuando en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano.

IV. Cuando los datos personales no obren en los archivos, registros, sistemas o expedientes del Instituto, la Unidad de Transparencia deberá rendir un informe fundado y motivado en el que se expongan las gestiones que realizó para la ubicación de los datos personales.

Artículo 49. Los dictámenes del Comité deberán ser emitidas a la brevedad posible, sin más limitante que el plazo de respuesta o a la ampliación de este.

La resolución completa deberá notificarse a el titular dentro del plazo señalado por la ley para atender las solicitudes de ejercicio de derechos ARCO y su portabilidad.

Artículo 50. Las Unidades Administrativas deberán emitir y/o reproducir los documentos de acceso, rectificación, cancelación, oposición o portabilidad hasta que sean notificados por la Unidad de Transparencia respecto a la procedencia de la solicitud de ejercicio de dichos derechos.

Artículo 51. Las notificaciones correspondientes deberán realizarse a través de la Plataforma Nacional de Transparencia, correo electrónico, y/o cualquier mecanismo señalado por la persona titular, siempre y cuando se garantice el tratamiento adecuado de los datos personales.

Para llevar a cabo las notificaciones se observará lo previsto en la normatividad en materia de protección de datos personales, así como los ordenamientos supletorios de las mismas, y en su caso, la Ley Electoral.

CAPÍTULO II

Recurso de revisión

Artículo 52. Contra la negativa a la solicitud de ejercicio de derechos ARCO y su portabilidad o la falta de respuesta del Instituto, la persona titular por sí misma o a través de su representante, podrá interponer el recurso de revisión ante el Infoqro o la Unidad de Transparencia.

En caso de que el recurso de revisión sea presentado ante la Unidad Administrativa, deberá enviarlo a la Unidad dentro del día hábil siguiente a su recepción, a efecto de que se remita a Infoqro.

Artículo 53. La Unidad de Transparencia realizará las funciones de enlace con el Infoqro, quien dará el trámite conducente a los recursos que se presenten, para lo cual podrá requerir la información que resulte necesaria a las Unidades Administrativas.

CAPÍTULO III

Procedimiento para la transferencia o remisión de datos

Artículo 54. Los acuerdos que suscriba el Instituto para la transferencia o remisión de datos personales deberán garantizar su protección. En su caso, toda transferencia o remisión deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la Ley General, la Ley Local y demás normatividad que le resulte aplicable en donde se conozcan los alcances de las obligaciones y responsabilidades asumidas por las partes.

Artículo 55. El Instituto está obligado a prever cláusulas y obligaciones para asegurar que a quienes se realicen las transferencias o remisión de datos lleve a cabo las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido de este, así como limitar sus actuaciones a los términos fijados por el Instituto, en términos de la Ley General y Ley Local en materia de protección de datos personales.

Artículo 56. La persona encargada no podrá subcontratar servicios que impliquen el tratamiento de datos personales por cuenta del Instituto, siempre y cuando medie la autorización expresa de este último.

Artículo 57. La Unidad de Transparencia será la responsable de la programación e implementación de esquemas de mejores prácticas en la protección de datos personales en el Instituto.

Artículo 58. La Unidad de Transparencia será la responsable de realizar la evaluación de impacto en la protección de datos personales, en los casos previstos en la Ley General, la Ley Local, y las demás disposiciones normativas aplicables.

Artículo 59. El Instituto podrá realizar transferencia de datos personales sin necesidad del consentimiento de la persona titular en los supuestos previstos en el artículo 70 de la Ley General.

CAPÍTULO IV

Sanciones

Artículo 60. Las sanciones al incumplimiento de este ordenamiento se atenderán conforme a lo previsto en las leyes de responsabilidad administrativa y de protección de datos personales, en atención al caso concreto.

Transitorios

PRIMERO. Los presentes Lineamientos entrarán en vigor una vez que aprobados por el Consejo General.

SEGUNDO. Se ordena la publicación de Lineamientos del Instituto Electoral del Estado de Querétaro en materia de protección de datos personales en el Periódico Oficial del Gobierno del Estado de Querétaro “La Sombra de Arteaga” y en el sitio de Internet del Instituto.