POLÍTICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES EN POSESIÓN DE LA SECRETARÍA DE TRABAJO DEL GOBIERNO DEL ESTADO DE PUEBLA

ÍNDICE

POLÍTICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES EN POSESIÓN DE LA SECRETARÍA DE TRABAJO DEL GOBIERNO DEL ESTADO DE PUEBLA

CAPÍTULO I
DEL OBJETIVO

PRIMERO. Establecer e Implementar los principios y deberes en materia de protección de datos personales en los procesos internos de gestión y tratamiento de datos personales de la Secretaría, conforme a lo previsto en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla y los Lineamientos Generales en Materia de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla.

CAPÍTULO II
ÁMBITO DE APLICACIÓN

SEGUNDO. El presente documento es de aplicación y observancia general y obligatoria para todas las personas servidoras públicas adscritas a la Secretaría, que conforme a sus facultades, atribuciones y funciones realicen tratamiento de datos personales.

TERCERO. Para los efectos de las presentes Políticas Internas, se entenderá por:

I. **Aviso de Privacidad.** Documento físico, electrónico o en cualquier otro formato generado por el Responsable, que es puesto a disposición del Titular con el objeto de informarle las características principales del Tratamiento al que serán sometidos sus Datos Personales.

II. **Bases de datos.** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

III. **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.

IV. **Capacitación.** Medida de seguridad preventiva para establecer las políticas y procedimientos de entrenamiento basado en roles y responsabilidades.

V. **Comité de Transparencia.** Instancia a la que hace referencia el artículo 20 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla.

VI. **Confidencialidad.** Propiedad de la información para no estar a disposición o ser revelada a personas, entidades o procesos no autorizados.

VII. **Consentimiento.** Manifestación de la voluntad libre, específica e informada del Titular, mediante la cual autoriza el Tratamiento de sus Datos Personales.

VIII. **Datos personales.** Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información.

IX. **Datos Personales sensibles.** Aquéllos 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 éste. Se consideran sensibles, de manera enunciativa mas 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 o datos biométricos.

X. **Derechos ARCO.** Los derechos de acceso, rectificación y cancelación de Datos Personales, así como la oposición al Tratamiento de los mismos.

XI. **Días:** Días hábiles.

XII. **Disociación.** El procedimiento mediante el cual los Datos Personales no pueden asociarse al Titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

XIII. **Disponibilidad.** Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.

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

XV. **Encargado.** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

XVI. **Identificar el riesgo.** Proceso para encontrar, enlistar y describir los elementos del riesgo.

XVII. **Integridad.** La propiedad de salvaguardar la exactitud y completitud de los activos.

XVIII. **Instituto Nacional**. El Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI).

XIX. **ITAIPUE o Instituto.** Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado Puebla.

XX. **Ley de Archivos**. Ley de Archivos del Estado de Puebla.

XXI. **Ley de Transparencia.** A la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla.

XXII. **Ley o LPDPPSOEP.** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla.

XXIII. **Lineamientos Generales en Materia de Clasificación o LGMCDIEVP**. Lineamientos de Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

XXIV. **Lineamientos Generales o LGMPDPSPEP.** Lineamientos Generales en Materia de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla.

XXV. **Medidas de Seguridad.** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan garantizar la confidencialidad, disponibilidad e integridad de los Datos Personales.

XXVI. **Plataforma Nacional.** Plataforma Nacional de Transparencia a que se refiere el artículo 49 de la Ley General de Transparencia.

XXVII. **Responsable.** De acuerdo con lo establecido en los artículos 3 y 5 fracción XXX de la LPDPPSOEP, el responsable es cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, fideicomisos y fondos públicos, ayuntamientos y partidos políticos del Estado de Puebla que decide y determina los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales. Por lo que respecta a la Secretaría de Trabajo del Gobierno del Estado, el responsable de los

tratamientos de datos personales son las personas Titulares de las Unidades Administrativas adscritas a la misma. Lo anterior, con fundamento en los artículos 36 de la Ley Orgánica de la Administración Pública del Estado de Puebla, 5 y 6 del Reglamento Interior de la Secretaría de Trabajo.

XXVIII. **Riesgo.** Combinación de la probabilidad de un evento y su consecuencia desfavorable.

XXIX. **Secretaría.** Secretaría de Trabajo del Gobierno del Estado de Puebla.

XXX. **Seguridad de la información.** Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

XXXI. **Sistema de Gestión de Seguridad de Datos Personales o SGSDP**. Sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley General, los Lineamientos Generales, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

XXXII. **Sujeto Obligado.** Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, fideicomisos y fondos públicos, del ámbito federal y partidos políticos que en el ejercicio de sus atribuciones y funciones lleven a cabo tratamientos de datos personales de personas físicas, en términos de lo dispuesto en la normatividad aplicable.

XXXIII. **Supresión.** La baja archivística de los Datos Personales conforme a la normatividad aplicable en la materia, que resulte en la eliminación, borrado o destrucción de los Datos Personales bajo las medidas de seguridad previamente establecidas por el Responsable.

XXXIV. **Titular.** A la persona física a quien hacen referencia o pertenecen los Datos Personales objeto del Tratamiento establecido en la presente Ley.

XXXV. **Tratamiento.** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los Datos Personales, relacionadas, de manera enunciativa mas 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.

XXXVI. **Transferencia.** Toda comunicación de Datos Personales dentro o fuera del territorio mexicano, realizada a persona distinta del Titular, del Responsable o del Encargado.

XXXVII. **Tratar el riesgo.** Procesos que se realizan para modificar el nivel de riesgo.

XXXVIII. **Unidad Administrativa.** Instancias a las que hace referencia el artículo 5 del Reglamento Interior de la Secretaría de Trabajo.

XXXIX. **Unidad de Transparencia.** Instancia a la que hace referencia el artículo 15 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla.

XL. **Valorar el riesgo.** Proceso para asignar valores a la probabilidad y consecuencias del riesgo (impacto).

CAPÍTULO III
DISPOSICIONES GENERALES

CUARTO. Las Unidades Administrativas adscritas a la Secretaría, deberán realizar el tratamiento de datos personales que resulten estrictamente necesarios, en el ejercicio de sus facultades, atribuciones y funciones, dentro del marco legal en la materia y del consentimiento de la persona titular.

QUINTO. Previo a recabar datos personales, se debe mostrar el aviso de privacidad integral y/o simplificado, según sea el caso; el aviso de privacidad debe encontrarse en un lugar visible.

SEXTO. Al momento de recabar datos personales, se deberá hacer del conocimiento de la persona titular la finalidad con la cual se reciben.

SÉPTIMO. Se deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que se reciban en ejercicio de las atribuciones otorgadas a las Unidades Administrativas adscritas a esta Dependencia.

OCTAVO. Es obligación de todas las personas servidoras públicas de la Secretaría, que administren, actualicen o tengan acceso a bases de datos personales, conservar, manejar y mantener de manera estrictamente confidencial dicha información y no revelarla a terceros.

NOVENO. Cuando se recaben datos personales de menores de edad se deberá obtener el consentimiento expreso de quien o quienes ejerzan la patria potestad o tutela sobre éstos.

DÉCIMO. Las Unidades Administrativas deberán identificar todos los Sistemas de Tratamiento de Datos Personales, así como los avisos de privacidad correspondientes.

DÉCIMO PRIMERO. Las Unidades Administrativas deberán elaborar los Inventarios de Bases de Datos Personales y Sistemas de Tratamientos, en los cuales se establezcan los listados de soportes, equipos, sistemas y bienes en general que son propiedad de la Secretaría, pero que están a cargo de las Personas Servidoras Públicas Adscritas al mismo.

DÉCIMO SEGUNDO. Los avisos de privacidad deberán ser elaborados en sus dos modalidades: simplificado e integral y contener todos los elementos informativos que exige la norma, además de estar redactados de manera clara y sencilla.

DÉCIMO TERCERO. Las Unidades Administrativas deberán verificar que sus avisos de privacidad simplificados e integrales se difundan en el portal de la Secretaría y estar disponibles de manera impresa en las instalaciones de la misma, en un lugar visible en las áreas correspondientes, para fácil consulta por parte de las personas titulares.

DÉCIMO CUARTO. Las Unidades Administrativas en el ámbito de sus facultades y atribuciones deberán participar activamente en la elaboración e integración del Documento de Seguridad.

DÉCIMO QUINTO. Las Unidades Administrativas en el ámbito de sus facultades y atribuciones, deberán realizar la ejecución del análisis de riesgo y brecha para la protección de datos personales, para que identifiquen y cuantifiquen los riesgos o amenazas inherentes, esto con el propósito de desarrollar e implementar las correctas medidas de seguridad que deben ser enfocadas especialmente en la protección de los datos personales para prevenir cualquier daño, perdida, alteración, destrucción, uso, acceso o tratamiento no autorizado y pudieran afectar la confidencialidad, mismas que, no podrán ser menores a aquéllas que mantengan para el manejo de su información.

DÉCIMO SEXTO. Las Unidades Administrativas, deberán tomar en cuenta los riesgos inherentes por tipo de dato personal; las posibles consecuencias para las personas titulares por una vulneración; la sensibilidad de los datos personales tratados y el desarrollo tecnológico con el disponen.

DECIMO SÉPTIMO. La confidencialidad de las personas servidoras públicas, no culmina con la terminación del puesto, cargo o comisión; esta obligación subsistirá aún después de finalizar su relación laboral con la Secretaría.

DECIMO OCTAVO. Las Unidades Administrativas, tienen la obligación de notificar a Unidad de Transparencia las vulneraciones de seguridad que se presenten, para dar inicio al protocolo de atención.

DECIMO NOVENO. La Unidades de Transparencia y el Oficial de Datos Personales, pondrán a consideración del Comité de Transparencia, Políticas, Métodos y Técnicas Orientadas para la Supresión, Bloqueo y Eliminación de los Datos Personales en Posesión de la Secretaría.

CAPÍTULO IV
PRINCIPIOS

VIGÉSIMO. En términos del artículo 46 de la LPDPPSOEP, instituye que, con independencia del tipo de sistema en el que se encuentren los Datos Personales o el tipo de Tratamiento que se efectúe, el Responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los Datos Personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o Tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Lo anterior, sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes, cuando éstas contemplen una protección mayor para el Titular o complementen lo dispuesto en la presente Ley y demás normativa aplicable.

En este tenor, las personas servidoras públicas adscritas a la Secretaría, deberán dar tratamiento a los datos personales en concordancia con lo establecido en la Ley, observando en todo momento las presentes políticas, las cuales tiene acciones transversales determinadas por este Sujeto Obligado, las cuales son afines a los ***principios*** establecidos en la normatividad, siendo los siguientes:

A. **Principio de licitud.** Los datos personales tienen que ser tratados de manera lícita, esto es, debe sujetarse a las facultades o atribuciones que la normatividad aplicable le otorga.

Para cumplir con este principio, las áreas deberán ajustarse a las siguientes recomendaciones:

I. Las personas servidoras públicas adscritas a la Secretaría, obligatoriamente deberán conocer la normatividad para el tratamiento de datos personales, específicamente la que regule las actividades, funciones y procesos que apliquen en el marco de sus facultades y atribuciones previstas en la Ley Orgánica de la Administración Pública de Estado de Puebla, Reglamento Interior y demás normativa que rige su actuar.

II. Los procesos y actividades que consideren el tratamiento de datos personales, deberán contar con un aviso de privacidad y los datos personales involucrados, deberán ser tratados conforme con las finalidades descritas en el mismo.

III. En el tratamiento de datos personales de menores de edad, así como grupos vulnerables, interseccionales y LGBTTTIQ+, se deberá observar lo previsto en la normatividad aplicable, para salvaguardar sus derechos.

B. **Principio de Finalidad.** Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas a la persona titular en el aviso de privacidad y, en su caso, consentidas por ésta. Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales.

Para cumplir con este principio, las áreas deberán:

I. Los datos personales sólo pueden ser tratados para cumplir con la finalidad específica, que previamente hayan sido informadas al titular en el aviso de privacidad correspondiente, y, en su caso, consentidas por la persona el titular.

II. Los responsables de las Unidades Administrativas adscritas a la Secretaría, deberán señalar la finalidad que justifica el tratamiento de datos personales de manera concreta, explicita, lícita y legítima; debiendo evitar que sean inexacta, ambigua, o vaga.

III. Las Unidades Administrativas deberán conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron su tratamiento, en cumplimiento de los aspectos legales, administrativos, contables, fiscales, jurídicos e históricos; plazos de conservación indicados en las fichas técnicas de valoración documental y el Catálogo de Disposición Documental (CADIDO) y en estricto apego a lo señalado en la Ley General de Archivos.

IV. Las Unidades Administrativas, deberán ofrecer a la persona titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias.

V. La Secretaría, como responsable, podrá modificar las finalidades del tratamiento que se establecieron en un primer momento en el respectivo aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley para tales efectos y medie nuevamente el consentimiento del titular, en los casos procedentes.

VI. Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas a la persona titular en el aviso de privacidad y, en su caso, consentidas por ésta.

VII. Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, y redactarlas de forma tal que sean determinadas.

VIII. Identificar y distinguir en el aviso de privacidad entre las finalidad principal y secundaria, en su caso.

IX. Ofrecer a la persona titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales de la finalidad secundaria.

X. No condicionar el tratamiento para finalidades primarias, a que se puedan llevar a cabo las finalidades secundarias

C. Principio de lealtad. La obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos.

Para cumplir con este principio, las Unidades Administrativas deberán:

I. Únicamente serán reconocidas aquellas bases de datos personales que hayan sido declaradas por la Unidad Administrativa correspondiente, misma que, formarán parte del inventario de datos personales de la Secretaría.

II. Solo se recabarán datos personales a través de los mecanismos y procesos que proporcione este Sujeto Obligado.

III. Las personas servidoras publicas adscritas a este Sujeto Obligado, deberán actuar con diligencia y responsabilidad, respecto a los datos personales otorgados por el titular, debiendo ser tratados conforme la finalidad y procesos correspondientes.

IV. Las personas servidoras públicas adscritas a la Secretaría, deberán abstenerse de obtener y tratar datos personales, a través de medios engañosos o fraudulentos.

V. Revisar los procedimientos y formatos utilizados para recabar datos personales, para verificar que en éstos no se utilicen prácticas que lleven a la obtención de los datos de manera dolosa, de mala fe o con negligencia.

VI. Dar vista al Órgano Interno de Control en caso del uso de prácticas dolosas, de mala fe o negligentes para la obtención de los datos personales.

VII. Respetar en todo momento la expectativa razonable de privacidad de la persona titular de los datos personales.

VIII. Tratar los datos conforme lo acordado e informado a la persona titular de los datos personales.

IX. Verificar los tratamientos, a fin de confirmar que los mismos no den lugar a discriminación o trato injusto o arbitrario en contra del titular.

X. Elaborar avisos de privacidad con todos los elementos informativos que establece la normatividad aplicable en la materia, y con información que corresponda a la realidad del tratamiento que se efectúa.

XI. Incluir en los avisos de privacidad todas las finalidades de los tratamientos, las cuales deberán estar redactadas de forma clara y concreta, para que no haya lugar a confusión al respecto.

D. Principio del consentimiento. Como regla general, las áreas que realicen tratamiento de datos personales deberán contar con el consentimiento del titular para el tratamiento de sus datos personales, el cual deberá ir siempre ligado a las finalidades concretas del tratamiento que se informen en el aviso de privacidad.

Para cumplir con este principio, las Unidades Administrativas deberán:

I. En el momento previo a recabar los datos personales, las personas servidoras públicas deberán poner a disposición del titular el aviso de privacidad en sus dos modalidades: simplificado e integral; con el propósito de recabar el consentimiento tácito o expreso. Este principio permite a los titulares decidir de manera informada, libre, inequívoca y específica, todo lo relacionado con la finalidad y el tratamiento de sus datos personales.

Modalidades del Consentimiento: Puede otorgarse por parte del titular de datos personales al Responsable en dos diferentes modalidades:

a) Expreso. Se presenta cuando la voluntad del titular se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología aceptada.

b) Tácito. Este tipo de consentimiento se da cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifiesta su voluntad en sentido contrario. 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.

Así mismo la Unidades Administrativas deberán observar las siguientes consideraciones:

I. Definir el tipo de consentimiento que se requiere, según las categorías de datos personales que se vayan a tratar o las disposiciones normativas que regulen el tratamiento.

II. Documentar la puesta a disposición del aviso de privacidad para la obtención del consentimiento tácito.

III. En el caso de recabar datos personales sensibles, el consentimiento para su tratamiento será expreso y por escrito, esto es, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo que se actualice alguno de los supuestos señalados en los artículos 20, 94 y 95 LPDPEPSO.

IV. En el caso del consentimiento expreso, es necesario que el mismo se solicite, ya sea en el cuerpo del aviso de privacidad o en un instrumento aparte. Las Unidades Administrativas no podrán tratar los datos personales si no cuenta con el consentimiento del titular.

V. Redactar las solicitudes de consentimiento expreso, de forma tal que éste sea libre, específico e informado, y que las solicitudes sean concisas e inteligibles, estén en un lenguaje claro y sencillo acorde con el perfil del titular, y se distingan de asuntos ajenos a la protección de datos personales, cuando ello sea necesario.

VI. Cuando existan finalidades que requieran el consentimiento del titular, se deberán implementar mecanismos para que el titular, del ser el caso, también pueda manifestar su negativa.

VII. En el caso del consentimiento de menores de edad, se atenderá la normatividad aplicable, salvaguardando los derechos de los mismos.

VIII. El mecanismo para que el titular manifieste su negativa, deberá establecerse en el aviso integral y simplificado correspondiente, para que éste lo consulte, previo al tratamiento de los datos personales.

IX. La Unidad de Transparencia y el Oficial de Datos Personales supervisarán el establecimiento, actualización y seguimiento de los avisos de privacidad, para cada proceso en el que se realice el tratamiento de datos personales.

X. En el caso de nuevas atribuciones, en las cuales implique el tratamiento de datos personales, la Unidad Administrativa correspondiente, deberá comunicar dicha situación a la Unidad de Transparencia y al Oficial de Datos Personales, a efecto de determinar de manera conjunta, el tipo de consentimiento que se requiere: tácito o expreso, así como la elaboración del aviso de privacidad simplificado e integral correspondiente.

XI. La Unidad de Transparencia y el Oficial de Datos Personales establecerán, revisarán y de ser el caso actualizarán la guía para la atención de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), así como el de Portabilidad al tratamiento de datos personales.

E. Principio de calidad. El principio de calidad significa que, conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos deben ser:

- ✓ **Exactos:** Los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles.
- ✓ **Correctos:** Los datos personales son correctos cuando cumplen y están completos, ya que no falta ningún de los que se requiera para la finalidad para los cuales se obtuvieron y son tratados, de tal forma que no cause daño o perjuicio a su titular.
- ✓ **Actualizados:** Los datos personales son actualizados, cuando están al día y corresponden a la realidad de la situación de su titular.

Para cumplir con este principio, las Unidades Administrativas deberán:

I. Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, correctos y actualizados.

II. Mediante los avisos de privacidad y el análisis del ciclo de vida de los datos personales establecidos en las fichas técnicas de valoración documental, la unidad administrativa responsable del proceso por el cual se traten los datos personales, revisará e implementará, con el apoyo de la Unidad de Transparencia y el Oficial de Datos Personales, las medidas necesarias para mantener los datos personales en posesión de este Ente Obligado, exactos, correctos y actualizados, con la finalidad de que no se altere su veracidad, ni que ello tenga como consecuencia que la persona titular se vea afectada por dicha situación.

III. No se dará tratamiento de datos personales parciales o incompletos que puedan inducir al error, en su caso, se deberán recabar los datos completos para reiniciar el tratamiento.

IV. Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo.

V. Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales.

VI. Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación. Una vez que los datos personales dejaron de ser necesarios para el cumplir de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de estos.

VII. Con independencia de que el titular de los datos personales ejerza su derecho de cancelación, el área responsable del tratamiento está obligada a eliminar, de oficio, los datos personales cuando hayan dejado de ser necesarios para la finalidad para la cual se obtuvieron.

VIII. La supresión de los datos personales deberá de ser de forma definitiva, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima y, de ser posible, nula.

F. Principio de Proporcionalidad. Las áreas que realicen tratamiento de datos personales deberán tratar solo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

Para cumplir con este principio, las áreas Unidades Administrativas deberán:

I. Analizar y revisar que se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate

II. La Unidad de Transparencia y el Oficial de Datos Personales, a través de los procesos declarados por cada unidad administrativa, mediante los cuales se recaben datos personales, incluyendo los sensibles, analizarán la pertinencia de la proporcionalidad de los mismos y realizará las sugerencias correspondientes.

III. Cuando una normativa establezca con precisión los datos personales que deberán obtenerse para cumplir con la finalidad de que se trate, sólo deberán solicitarse dichos datos.

IV. Crear bases de datos con datos personales sensibles sólo cuando:

i. Obedezca a un mandato legal;
ii. Se justifique para la seguridad nacional, el orden, la seguridad y la salud públicos, así como derechos de terceros, o
iii. Se requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

G. Principio de Información. Las Unidades Administrativas que realizan tratamientos de datos personales se encuentran obligadas a informar a las personas titulares de los datos personales, a través de los avisos de privacidad integral y simplificado, las características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

Para cumplir con este principio, las Unidades Administrativas deberán:

I. Informar a los titulares de los datos personales, el propósito del tratamiento al que será sometida su información personal, lo que se materializará a través del aviso de privacidad correspondiente.

II. Los responsables del proceso o actividad en la cual se traten datos personales, deberán asegurarse de que el aviso de privacidad sea difundido por los medios físicos y electrónicos con los que cuenta la Secretaría y que faciliten la consulta de los titulares.

III. En el caso de que los datos personales se recaben por medio de formulario electrónico o vía correo electrónico, el responsable del proceso deberá asegurarse de que el aviso se encuentre publicado en el sitio correspondiente.

IV. Poner a disposición del titular el aviso de privacidad previo a iniciar el uso de los datos personales para las nuevas finalidades (aprovechamiento), cuando requiera tratar los datos

personales para finalidades distintas y no compatibles con aquéllas para las cuales los recabó inicialmente.

V. Demostrar el cumplimiento del principio de información, en caso de que así se requiera.

H. Principio de Responsabilidad. A este principio se le conoce también como el principio de "rendición de cuentas", ya que establece la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales

Para cumplir con este principio, las Unidades Administrativas deberán:

I. Cumplir con el programa integral de capacitación y actualización de la Secretaría, aprobado por el Comité de Transparencia.

II. Analizar los riesgos que implica todo tratamiento de datos personales en el ámbito de sus facultades, atribuciones y funciones.

III. La persona servidora pública que trate datos personales o que tenga acceso a los mismos, derivado de las funciones encomendadas, deberá guardar la confidencialidad, para lo cual, queda establecida la Carta de Confidencialidad, así como las cláusulas de confidencialidad de los contratos, convenios y demás instrumentos jurídicos.

IV. El responsable de la Unidad Administrativa que tenga bajo su resguardo los expedientes que contengan datos personales y que sean solicitados mediante requerimiento de información de una autoridad competente, que estén debidamente fundados y motivados, deberán proporcionar la misma en términos del artículo 20 fracción II de la LPDPEPSO.

V. Para el cumplimiento de obligaciones de transparencia, la Unidad Administrativa Responsable, deberá constatar que la información que forme parte de la mismas, no vulnera la confidencialidad de los titulares de los Datos Personales, a través de las versiones publicas correspondientes, las cuales invariablemente deberán cumplir con lo establecido en los Lineamientos de Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

VI. En el caso que se requiera llevar a cabo el tratamiento de datos personales en los cuales no estén involucrados Responsables, se deberá formalizar la transferencia de datos mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normativa que le resulte aplicable a este Sujeto Obligado, que permita demostrar el alcance del Tratamiento de los Datos Personales, así como las obligaciones y responsabilidades asumidas por las partes, referentes a las medidas de seguridad y de tratamiento de datos personales, para verificar su correspondencia con los requerimientos de la Secretaria, atendiendo lo señalado en el artículo 95 de la LPDPEPSO.

VII. La Unidad Administrativa que corresponda, deberá comunicar a la Unidad de Transparencia la información relativa al instrumento jurídico que se formalice para el tratamiento de datos personales, a efecto de llevar el registro correspondiente.

VIII. En caso de vulneraciones, la persona servidora pública responsable del proceso en cuestión, deberá notificar a la Unidad de Transparencia para se informe al titular de los datos y al ITAIPUE, en un plazo máximo de 72 horas, a partir de que confirme la ocurrencia de éstas y la persona servidora pública haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación, informando al menos la naturaleza del incidente; los datos personales comprometidos; las recomendaciones al Titular acerca de las medidas que éste pueda adoptar para proteger sus intereses; las acciones correctivas realizadas de forma inmediata; los medios donde puede obtener información al respecto; la descripción de las circunstancias generales en torno a la vulneración recurrida, que ayuden al titular a entender el impacto del incidente.

IX. La Secretaría, a través de la Unidad de Transparencia deberá llevar una bitácora de las vulneraciones a la seguridad ocurridas en la que se describa:

i. La fecha en la que ocurrió;
ii. El motivo de la vulneración de seguridad, y
iii. Las acciones correctivas implementadas de forma inmediata y definitiva, conforme lo establecido en el artículo 54 de la LPDPEPSO.

CAPÍTULO V
DEBERES

VIGÉSIMO PRIMERO. De conformidad con lo establecido en el artículo 17 de los LGMPDPSPEP, indica que, en todo tratamiento de datos personales el responsable deberá cumplir con los siguientes deberes rectores de la protección de datos personales:

I. **Deber de seguridad:** Establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o acceso no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

II. **Deber de confidencialidad:** 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 aun después de finalizar sus relaciones con el mismo.

La confidencialidad es un deber a cargo del responsable del tratamiento que consiste en implementar medidas de seguridad para que cualquier persona que intervenga en el tratamiento de los datos personales en cualquiera de sus fases, los mantenga resguardados y se abstenga de divulgarlos, así mismo se busca combatir el escenario de vulneración en el que se realice un tratamiento indebido, particularmente, el uso y divulgación no autorizados de los datos personales, que puedan realizar las personas servidoras públicas o terceros involucrados en el tratamiento de los datos personales de este Sujeto Obligado.

Lo anterior, se consolida con las medidas de seguridad, controles o mecanismos que, en su caso, implemente el responsable del tratamiento y que sean acordes a los alcances establecidos, tanto temporales como subjetivos; es decir, dirigidos a todas las personas involucradas, incluidas sus relaciones con terceros y encargados, a fin de evitar la falta de discreción o deber de secrecía que deben tener estos en los tratamientos de datos durante y después de finalizar las relaciones jurídicas que se tengan con la Secretaría.

En este tenor se establecen las medidas que se consideran a acordes para que, de manera enunciativa más no limitativa, las Unidades Administrativas lleven a cabo controles adecuados para el tratamiento de los Datos Personales que obran en poder de la Secretaría, derivado de sus facultades y atribuciones.

A. **Deber de seguridad.** Este deber se refiere a la obligación de establecer y mantener medidas de seguridad tanto técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Para cumplir con este deber, las Unidades Administrativas deberán:

Las personas servidoras públicas adscritas a la Secretaría, deberán observar las siguientes medidas de seguridad, de manera enunciativa, más no limitativas para la protección de los datos personales que se encuentren a su cargo:

I. Medidas de Seguridad Físicas.

a) Resguardar los expedientes en archiveros y gavetas bajo llave, en los cuales solo tengan acceso el personal autorizado.

b) Evitar reciclar documentos que contengan datos personales, así como verificar que no se utilicen hojas que puedan contener información confidencial de la Dependencia, que pudieran ser divulgados o expuestos y utilizados para finalidades distintas a las legítimas establecidas en el aviso de privacidad correspondiente.

c) Evitar tirar o desechar documentos con datos personales en fotocopiadoras, escáner o impresoras.

d) Mantener los escritorios limpios, cualquier documento o expediente debe estar resguardado, fuera de la vista, cuando no se esté utilizando.

e) Proteger el acceso físico al lugar en el que se encuentra el medio de almacenamientos, mediante el acceso restringido a cualquier persona ajena a la Unidad Administrativa.

f) Bloquear los datos personales una vez agotado el periodo de conservación.

II. Medias de Seguridad Administrativas.

a) Cada Unidad Administrativa deberá identificar los procesos en los cuales se realice el tratamiento de datos personales, los riesgos y su valoración documental en relación con su impacto y probabilidad de ocurrencia.

b) Cada Unidad Administrativa deberá integrar un inventario de datos personales que considere la totalidad de los procesos que, en el ejercicio de sus atribuciones competencias y funciones implique el tratamiento de datos personales.

c) La Unidad de Transparencia, establecerá los procedimientos, guías o protocolos mediante los cuales se facilite a las unidades administrativas la elaboración de los inventarios de datos personales;

d) La Unidad de Transparencia integrará los resguardos de los Inventarios Institucionales de datos personales, los cuales deben ser notificados de manera oficial por escrito;

e) Cada Unidad Administrativa, actualizará periódicamente su inventario de datos personales, atendiendo a los cambios, mejoras y deberá informarlo a la Unidad de Transparencia para que realice la actualización correspondiente en el Inventario Institucional de Datos Personales.

f) La Unidad de Transparencia y el Oficial de Datos Personales, promoverán conjuntamente con las unidades administrativas y la Dirección de Administración, a través del Departamento de Informática y Soporte Técnico, la implementación de medidas de seguridad para la protección de datos personales.

g) Las Unidades Administrativas que recaben datos personales, así como la Unidad de Transparencia, el Oficial de Datos Personales, la Dirección General Jurídica y la Dirección de Administración y el Departamento de Informática y Soporte Técnico, en el ámbito de sus competencias, determinarán, los términos de los protocolos específicos para la transferencia de datos personales, así como las medidas de seguridad pertinentes.

h) Los plazos de conservación de los documentos que contengan datos personales, no deberán exceder aquellos señalados en las fichas de valoración documental y el catálogo de disposición documental.

III. Medidas de Seguridad Técnicas.

a) Cada Unidad Administrativa deberá integrar un inventario de sistemas, en el cual se registren aquellos que, en el ejercicio de atribuciones, competencias y funciones, se dé tratamiento a datos personales.

b) La Unidad de Transparencia, el Oficial de Datos Personales y la Dirección de Administración, a través del Departamento de Informática y Soporte Técnico, en el ámbito de su competencia, establecerán la implementación de mecanismos de monitoreo y de revisión de las medidas de seguridad para la protección de datos personales.

c) La Dirección de Administración, a través del Departamento de Informática y Soporte Técnico, identificará y mantendrá actualizado el inventario de infraestructuras esenciales y/o críticas, así como los mecanismos para garantizar su protección.

d) La Unidad de Transparencia y el Oficial de Datos Personales, realizarán monitoreo y establecerá conjuntamente con la Dirección de Administración, a través del Departamento de

Informática y Soporte Técnico, una cadena de avisos en caso de vulnerabilidad a la seguridad de la información; así mismo, se harán periódicamente pruebas de intrusión.

e) La Dirección de Administración, a través del Departamento de Informática y Soporte Técnico, supervisará y asesorará a las Unidades Administrativas, a efecto de que se realicen respaldos de la información de manera regular y pruebas de recuperación.

f) La Dirección de Administración, a través del Departamento de Informática y Soporte Técnico, revisará de manera periódica la administración y asignación de contraseñas robustas, con el fin de apoyar a los administradores y usuarios de servicios de tecnología a reducir los impactos de los riesgos generados por el manejo y resguardo de la información.

g) Las Personas Servidoras Públicas adscritas a la Secretaría, como usuarios y responsables de los equipos informáticos, deberá tener un identificador único en el sistema el cual se vincularán sus privilegios y accesos. Así mismo, cada persona usuaria deberá ser responsable de guardar en secreto la (s) contraseña (s) y/o mecanismos correspondientes para su acceso.

h) En un ambiente de multiusuario no se deberán compartir datos personales, excepto que se establezcan por escrito la protección de datos personales con el fin de conceder privilegios en función de los roles y responsabilidades para el cumplimiento de sus deberes, sin que se exponga al acceso, eliminación, copia o alteración no autorizados de la información.

i) Ningún usuario, está autorizado a llevar consigo o sacar, discos ópticos, discos compactos, memorias o cualquier otro medio electrónico con información propiedad de la Secretaría.

j) Ningún usuario, está autorizado a instalar, desinstalar, o borrar parcial o totalmente datos, información, bases de datos, paquetería o aplicaciones en los bienes informáticos que este bajo su resguardo.

B. Deber de confidencialidad. Este deber implica la obligación de guardar secreto respecto de los datos personales que son tratados. Este deber debe cumplirse para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información.

Para cumplir con este deber, las Unidades Administrativas deberán:

a) Atender las capacitaciones para que conozca sus obligaciones con relación al tratamiento de datos personales.

b) Guardar confidencialidad en cualquier fase del tratamiento de los datos personales, incluso después de finalizar la relación con la persona titular.

c) Verificar que los encargados también guarden confidencialidad de los datos personales que tratan a nombre y por cuenta del responsable, aun después de concluida la relación con éste.

d) Establecer procedimientos para evitar fuga de información o el acceso indebido a los datos personales.

e) Incluir en los contratos u otros instrumentos jurídicos que celebre con terceros, cláusulas de confidencialidad y para que quienes tengan acceso a los datos personales en posesión del responsable cumplan con esta obligación de confidencialidad.

f) Las personas servidoras públicas adscritas a la Unidad Administrativa, deberán suscribir la Carta Compromiso de Confidencialidad y Responsabilidad de Gestión de la Información y Datos Personales que se tratan derivado de sus funciones. **(ANEXO 1)**

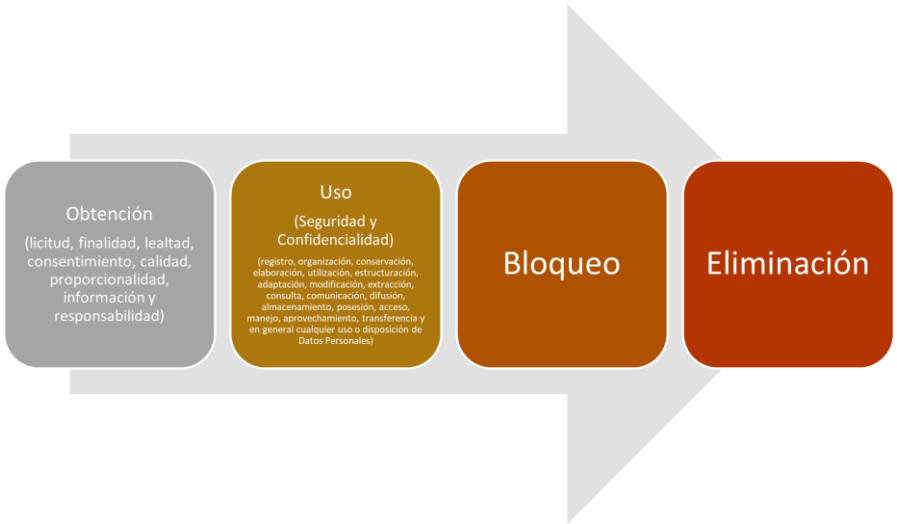
g) Realizar verificaciones o supervisiones periódicas al trabajo realizado por los encargados, a fin de constatar que se cumplan con sus obligaciones en torno a la protección de los datos personales.

CAPÍTULO VI
CICLO DE VIDA DE LOS DATOS PERSONALES

VIGÉSIMO SEGUNDO. De conformidad con lo establecido en la Ley de Archivos, los Sujetos Obligados deberán mantener los documentos contenidos en sus archivos en el orden original en que fueron producidos, conforme a los procesos de gestión documental que incluyen la producción, organización, acceso, consulta, valoración documental, disposición documental y conservación. Tratándose de la gestión documental electrónica, en los procesos se debe de contemplar la incorporación, asignación de acceso, seguridad, almacenamiento, uso y trazabilidad, mismos que, deberán estar sujetos a los principios determinados en el artículo 5, de dicha Ley.

VIGÉSIMO TERCERO. Las Unidades Administrativas adscritas a la Secretaría, deberán llevar a cabo la identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados.

Diagrama 1
CICLO DE VIDA DE LOS DATOS PERSONALES



En este tenor, la Unidades Administrativas que realizan tratamiento de datos personales deberán:

I. Identificar el flujo y ciclo de vida de los datos personales: por qué medio se recaban, en qué procesos se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen.

II. Establecer en los inventarios de datos personales el ciclo de vida de los mismos, así como la serie y subserie archivística, en su caso.

III. Bloquear, cancelar, suprimir o destruir los datos personales, en los casos establecidos en la normatividad aplicable.

CAPÍTULO VII
FUNCIONES Y RESPONSABILIDADES

VIGÉSIMO CUARTO. Con relación a lo dispuesto en el artículo 48, fracción II de la LPDPPSOEP, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado, por lo tanto, se considera lo siguiente:

A. Comité de Transparencia. En términos de los artículos 113 y 114 de la LPDPPSOEP. El Comité de Transparencia de la Secretaría, es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la Secretaría, dicho comité tendrá las siguientes funciones con relación a este programa:

I. Coordinar, realizar y supervisar las acciones necesarias para garantizar el derecho a la protección de los Datos Personales en la organización del Responsable, de conformidad con las disposiciones previstas en la Ley y en aquellas disposiciones que resulten aplicables en la materia, en coordinación con el oficial de protección de Datos

II. Personales, en su caso;

III. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los Derechos ARCO;

IV. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los Datos Personales, o se declare improcedente, por cualquier causa, el ejercicio de alguno de los Derechos ARCO;

V. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de esta Ley y demás ordenamientos que resulten aplicables en la materia;

VI. Coordinar el seguimiento y cumplimiento de las resoluciones emitidas por el Instituto de Transparencia;

VII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de Datos Personales, y

VIII. Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado Tratamiento de Datos Personales.

B. Unidad de Transparencia. En términos de los artículos 115 y 116 de la LPDPPSOEP, cada Sujeto Obligado contará con una Unidad de Transparencia encargada de atender las solicitudes para el ejercicio de los Derechos ARCO, la cual se integrará y funcionará conforme a lo dispuesto en la Ley de Transparencia y demás normativa que resulte aplicable. Además, tendrá las siguientes funciones y atribuciones:

I. Auxiliar y orientar al Titular o, en su caso, a su representante legal que lo requiera con relación al ejercicio del derecho a la protección de Datos Personales;
II. Gestionar las solicitudes para el ejercicio de los Derechos ARCO;
III. Establecer mecanismos para asegurar que los Datos Personales sólo se entreguen a su Titular o su representante debidamente acreditados;
IV. Informar al Titular o su representante el monto de los costos a cubrir por la reproducción y envío de los Datos Personales, con base en lo establecido en las disposiciones normativas aplicables;
V. Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los Derechos ARCO;
VI. Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los Derechos ARCO;
VII. Asesorar a las Áreas adscritas al Responsable en materia de protección de Datos Personales, y
VIII. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto de Transparencia.

C. Oficial de Protección de Datos Personales. En términos de los artículos 119 y 120 de la LPDPPSOEP, el Oficial de Protección de Datos personales de la Secretaría, es la persona especialista en materia de protección de datos personales, quien tiene, entre otras atribuciones, la de auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales; asesorar a las Unidades Administrativas del Sujeto Obligado en materia de protección de datos personales; así como las siguientes funciones:

I. Asesorar al Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de Datos Personales;
II. Diseñar, ejecutar, supervisar y evaluar políticas, programas, acciones y actividades que correspondan para el cumplimiento de la normatividad y disposiciones que resulten aplicables en la materia, en coordinación con el Comité de Transparencia; y
III. Las demás que determine la normativa aplicable.

VIGÉSIMO QUINTO. las Unidades Administrativas por cada uno de los Sistemas de Tratamiento que realicen, deberán identificar el personal que realiza el tratamiento, el área al que está adscrito y las funciones que realizar en dicho tratamiento. Para tal efecto, se determinaron los siguientes niveles:

I. **Responsable**. De acuerdo con lo establecido en los artículos 3 y 5 fracción XXX de la LPDPPSOEP, el responsable es cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, fideicomisos y fondos públicos, ayuntamientos y partidos políticos del Estado de Puebla que decide y determina los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales. Por lo que respecta a la Secretaría, el responsable de los tratamientos de datos personales son las personas Titulares de las Unidades Administrativas adscritas a la misma. Lo anterior, con fundamento en los artículos 36 de la Ley Orgánica de la Administración Pública del Estado de Puebla, 5 y 6 del Reglamento Interior de la Secretaría de Trabajo.

II. **Administrador.** Proponer al responsable la creación del sistema de tratamiento de datos personales, debidamente justificadas, motivadas y fundamentadas; elaborar el Inventario de Datos Personales y Sistemas de Tratamiento y solicitar su registro ante la Unidad de Transparencia; establecer las medidas de seguridad a implementar para el control, uso, manejo y resguardo de los datos personales a su cargo; monitorear, revisar, proponer y establecer acciones de mejora a la seguridad del sistema de tratamiento de datos personales; verificar el debido cumplimiento de los principios, deberes y las políticas internas en el tratamiento de datos personales, así como de las medidas de seguridad acordadas sobre los sistemas de tratamiento; informar al Responsable sobre la vulneración a la seguridad del sistema de tratamiento de datos personales, así mismo registre en la bitácora y se realice el proceso correspondiente ante la Unidad de Transparencia; dar atención a la solicitud de derechos ARCO.

III. **Operativo / Administrativo.** Usar, utilizar y emplear los datos personales a los que tenga acceso, en virtud de sus funciones, únicamente para el desempeño de la actividad laboral; Garantizar, custodiar, salvaguardar y cuidar tanto la información, como contenidos en el sistema tratamiento; reservar la confidencialidad de toda la información a la que tenga acceso; observar las medidas de seguridad indicadas por el administrador y establecidas en el documento de seguridad; abstenerse de borrar, destruir, dañar, alterar o modificar cualquier información relacionada con los datos personales contenidos en el sistema de tratamiento, salvo que cuente con la indicación y autorización expresa del administrador; abstenerse de realizar copias, transmisiones, comunicaciones o cesiones de cualquier información relacionada con los datos personales contenidos en el sistema de tratamiento, salvo que cuente con la indicación y autorización expresa del administrador; avisar al administrador sobre cualquier vulneración a la seguridad de los datos personales, sobre la ineficacia de una medida de seguridad adoptada, así como cualquier anomalía, error, imprecisión o fallo que detecte en los datos personales contenidos en el sistema de tratamiento de datos personales.

CAPÍTULO VIII
ESTABLECIMIENTO, ACTUALIZACIÓN, MONITOREO Y REVISIÓN DE LOS MECANISMOS Y MEDIDAS DE SEGURIDAD.

VIGÉSIMO SEXTO. El artículo 48 fracción VII de la LPDPPSOEP, establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.
Así mismo, de acuerdo el artículo 5I fracción VI, de la Ley, los mecanismos de monitoreo y revisión forman parte del documento de seguridad.

VIGÉSIMO SÉPTIMO. Las Unidades Administrativas, establecerán las medidas técnicas, físicas y administrativas para el control interno del tratamiento de datos personales, así como su actualización correspondiente, las cuales, en el ámbito de sus facultades y atribuciones, el Comité de Transparencia, la Unidad de Transparencia, el Oficial de Protección de Datos Personales, establecerán los mecanismos de monitoreo, vigilancia y revisión de dichas medidas, a través del Plan de Trabajo respectivo, con el objetivo de fortalecer, a través de un ciclo de mejora continua, la protección de los datos personales que se resguardan.

VIGÉSIMO OCTAVO. Las Unidades Administrativas deberán realizar revisiones periódicas a las medidas de seguridad establecidas, a efecto de detectar de manera preventiva posibles vulneraciones, y en su caso proponer acciones de mejora.

CAPÍTULO IX
MECANISMOS DE SUPERVISIÓN O REVISIÓN

VIGÉSIMO NOVENO. Además del monitoreo continuo de las medidas de seguridad, se deberá realizar una supervisión periódica de las medidas de seguridad, a través de revisiones internas a cargo del Oficial de Protección de Datos Personales, o externas mediante auditorías voluntarias que se someta este Sujeto Obligado ante el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Puebla.

TRIGÉSIMO. El Oficial de Protección de Datos Personales, someterá al Comité de Transparencia el Programa de Revisiones Internas a los Sistemas de Tratamiento de Datos Personales, para su aprobación.

CAPÍTULO X
VULNERACIONES

TRIGÉSIMO PRIMERO. La Unidad de Transparencia, deberá establecer los medios y procedimientos para que las áreas que realizan tratamientos de datos personales conozcan las acciones a seguir ante una vulneración de datos personales, así como las acciones correctivas que deben implementar de forma inmediata y definitiva.

CAPÍTULO XI
ATENCIÓN DE LAS SOLICITUDES DE DERECHOS ARCO

TRIGÉSIMO SEGUNDO. Este Sujeto Obligado, a través de la Unidad de Transparencia, deberá establecer los medios y procedimientos habilitados para atender las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO), en concordancia con lo establecido en la normatividad aplicable en la materia.

TRIGÉSIMO SEGUNDO. La Unidad de Transparencia será responsable de requerir a las unidades administrativas y dar respuesta a las solicitudes de datos personales, así como realizar todas las gestiones correspondientes a sus funciones y aquellas que el Comité le encomiende, durante la atención de las solicitudes y la sustanciación del recurso de revisión.

TRIGÉSIMO TERCERO. La Unidad de Transparencia deberá tener a disposición del titular de los datos personales y, en su caso, de su representante, los datos personales en el medio de reproducción solicitada, durante un plazo máximo de sesenta días contados a partir del día siguiente en que se hubiere notificado la respuesta de procedencia al titular. Transcurrido dicho plazo, la Unidad de Transparencia deberá dar por concluida la atención a la solicitud para el ejercicio de los derechos ARCO y proceder a la destrucción del material en el que se reprodujeron los datos personales o de las constancias que acrediten el ejercicio efectivo de los derechos ARCO.

TRIGÉSIMO CUARTO. Los plazos y formas de atención de las solicitudes de derechos ARCO, se encuentran establecidos en la Ley de la materia, mismos que, las Unidades Administrativas y la Unidad de Transparencia, deberán cumplir en el ámbito de sus facultades y atribuciones.

Diagrama 2
PLAZOS DE ATENCIÓN SOLICITUDES DE DERECHOS ARCO

Diagrama 3
INICIO SOLICITUDES PARA EL EJERCICIO DE LOS DERECHOS ARCO

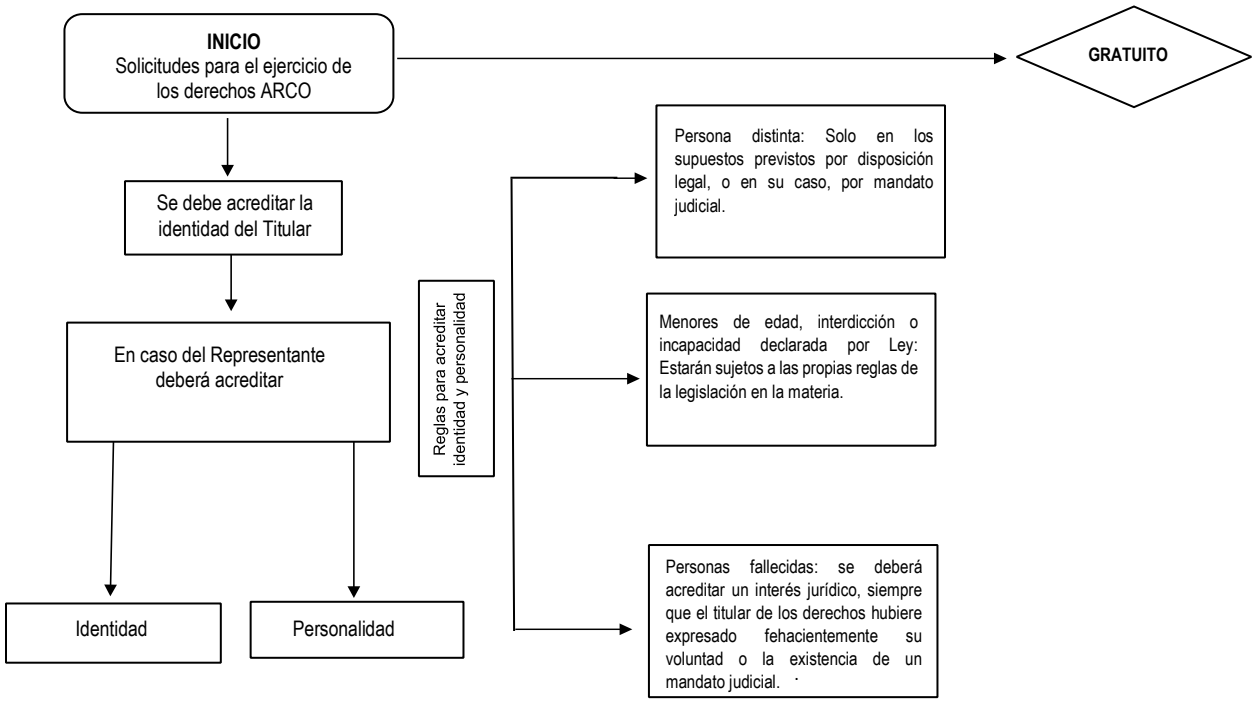


Diagrama 4
PLAZOS DE RESPUESTA SOLICITUDES DE DERECHOS ARCO

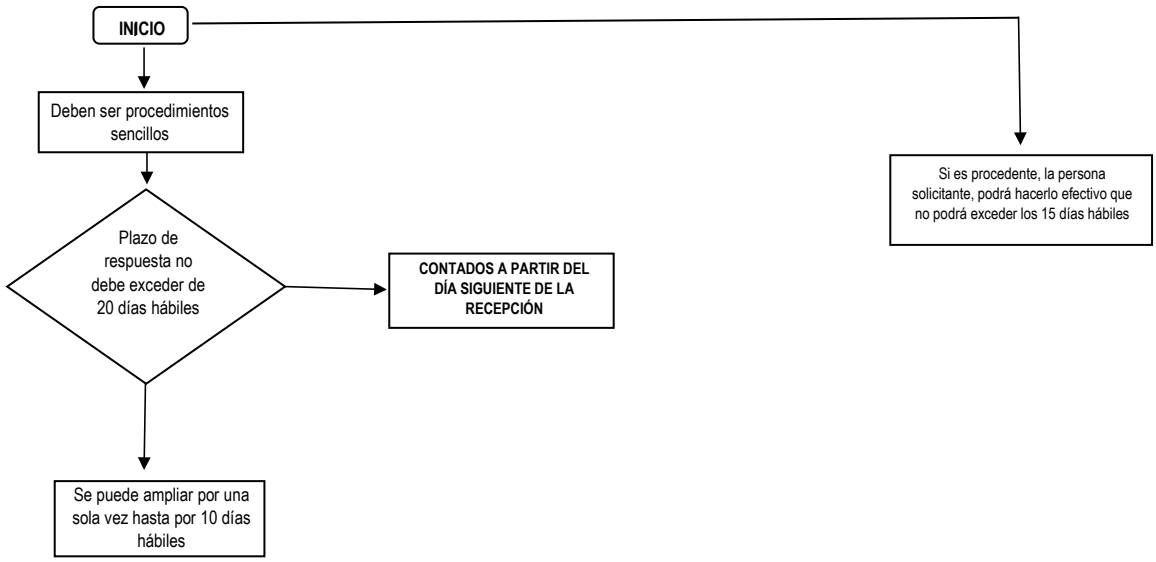


Diagrama 5
INICIO SOLICITUDES PARA EL EJERCICIO DE LOS DERECHOS ARCO

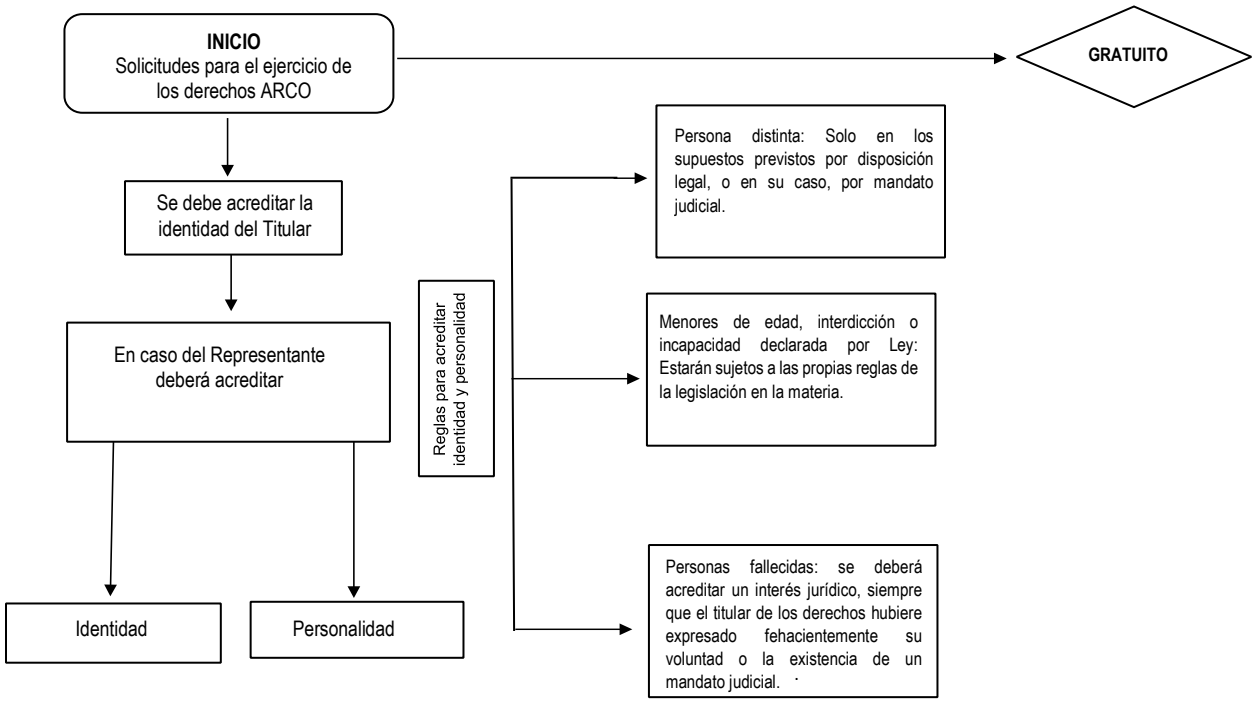


Diagrama 6
PLAZO DE RESPUESTA

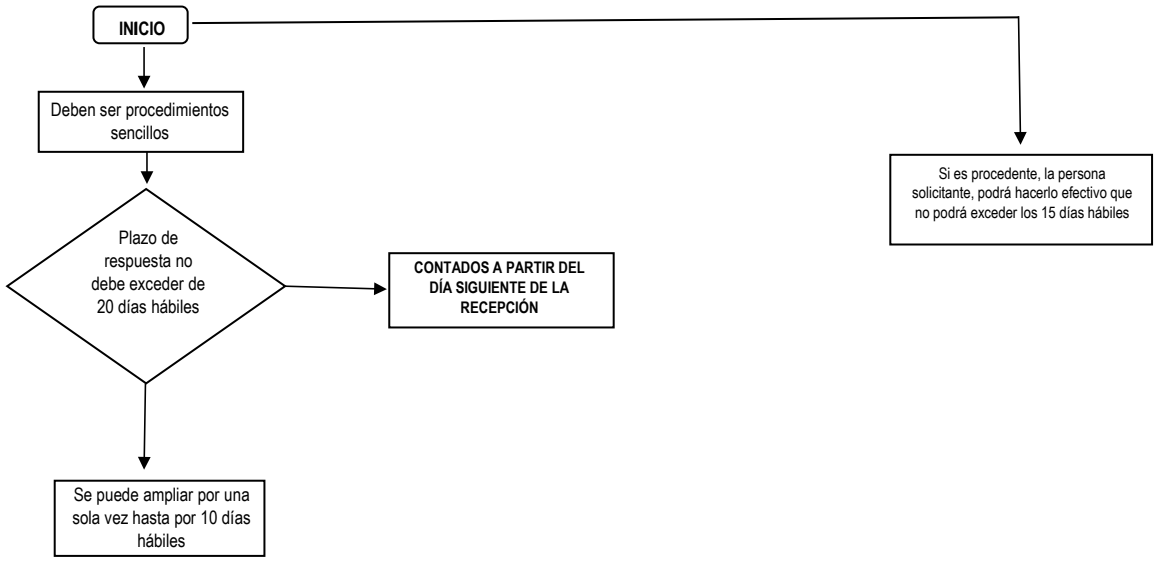


Diagrama 7
PREVENCIÓN

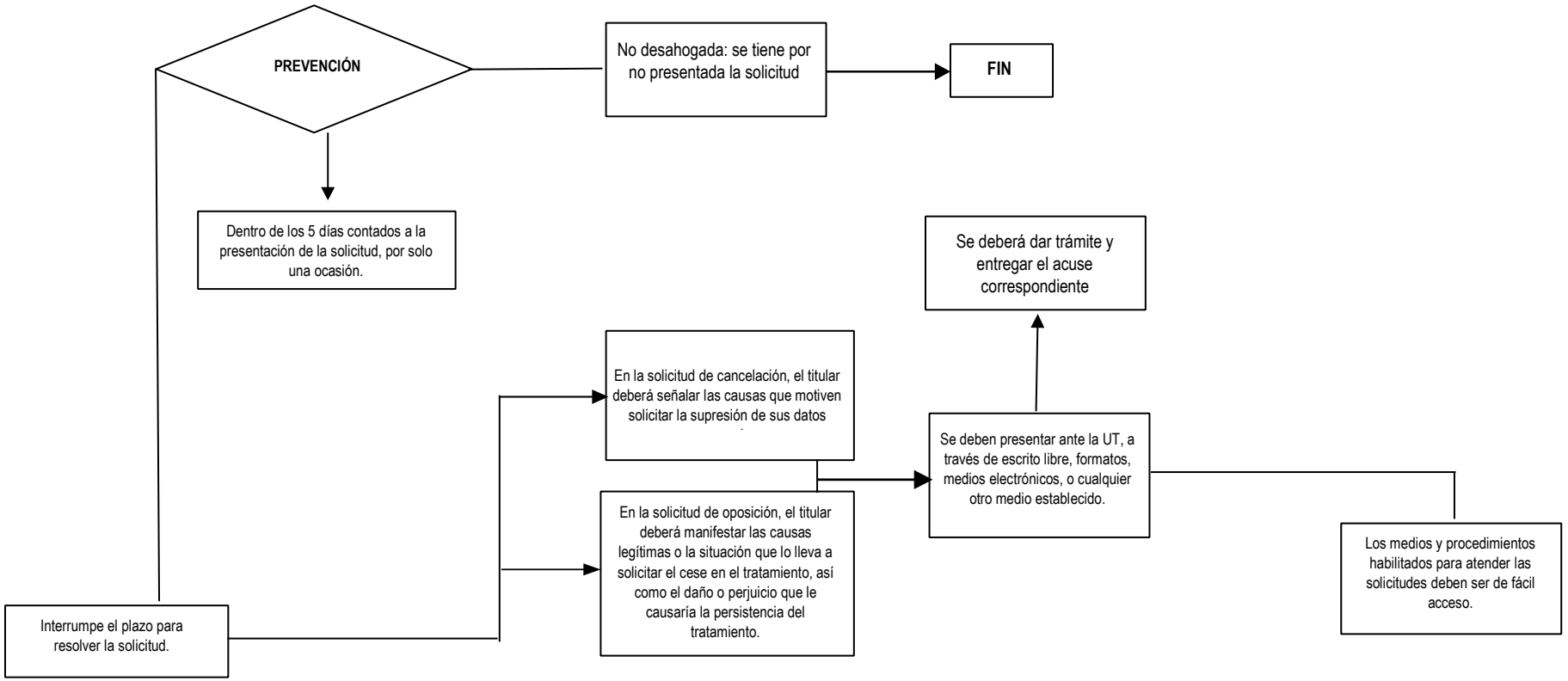


Diagrama 8
NO COMPETENCIA, INEXISTENCIA, RECONDUCCIÓN, TRÁMITE O PROCEDIMIENTO ESPECÍFICO

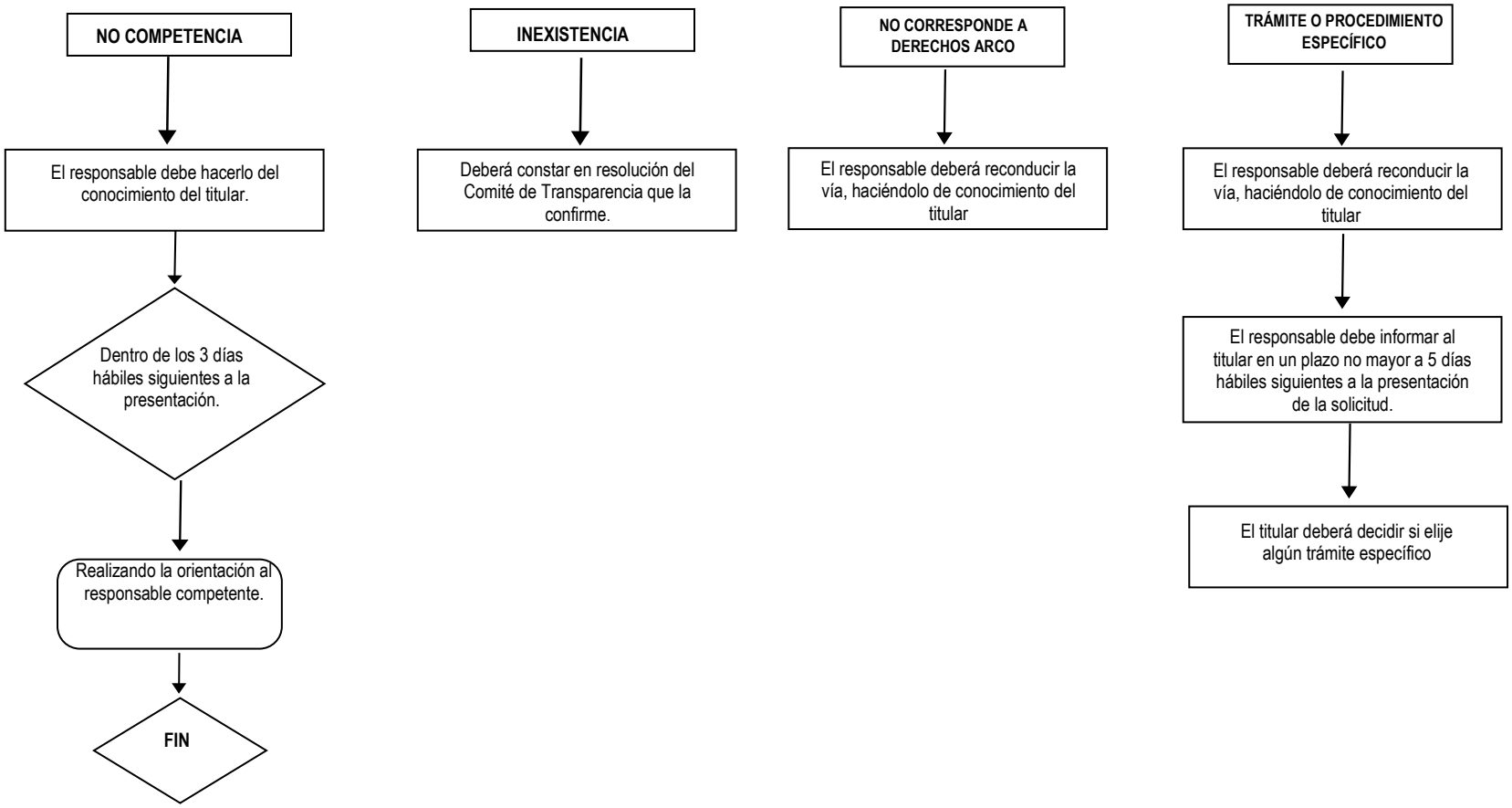
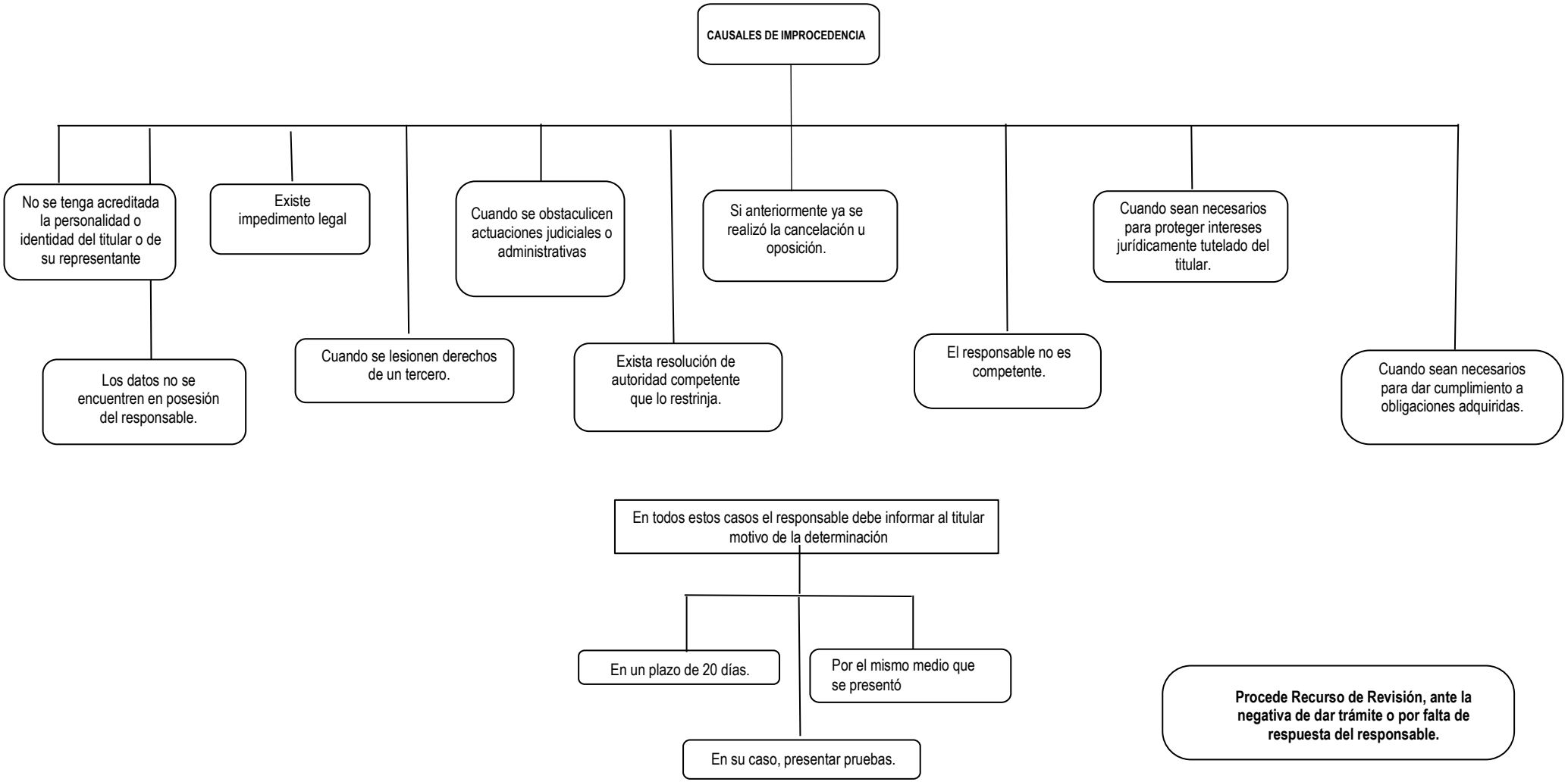


Diagrama 9
IMPROCEDENCIA



CAPÍTULO XII
DUDAS Y DENUNCIAS

TRIGÉSIMO QUINTO. A la Unidad de Transparencia, en el ámbito de sus facultades y atribuciones corresponderá a la atención de dudas, orientación y/o asesoría a las personas para el efectivo ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad al tratamiento de los datos personales ante la Secretaría.

Se entenderá indistintamente como duda o consulta la petición de orientación, asesoría o servicio formulada por una persona, sobre el ejercicio de los derechos ARCO y sobre el ejercicio del derecho a la protección de datos personales tanto de Titulares, como de particulares.

TRIGÉSIMO SEXTO. Para el trámite de quejas o denuncias por actos u omisiones que pudieran constituir faltas administrativas por parte de las Personas Servidoras Públicas adscritas a la Secretaría de Trabajo, lo podrán hacer a través de los siguientes medios:

i **Escrito:** Al documento en formato libre o formato de denuncia, presentado por el Denunciante en la Oficinas de la Unidad de Transparencia
ii **Presencial:** Manifestación personal de la denuncia presentada por el Denunciante, ante Unidad de Transparencia, quien dará cuenta de los hechos mediante un acta circunstanciada.
iii **Electrónico:** Mediante correo electrónico oficial unidaddetransparencia@puebla.gob.mx

TRIGÉSIMO SÉPTIMO. Para hacer efectivo el trámite de quejas o denuncias deberá contener al menos la siguiente información:

I. Datos del Denunciante:
a) Nombre, respetando el derecho a presentar denuncias de manera anónima, y
b) Datos de contacto, como puede ser dirección, teléfono, correo electrónico.
c) Datos de Notificación, como correo electrónico y domicilio.

II. Datos de Identificación de la persona servidora pública denunciada:
a) Nombre;
b) Cargo que desempeña;
c) De no contar con los datos anteriores, proporcionar cualquier otro dato que facilite su identificación, como media filiación, que podrá consistir en sexo, estatura, complexión, edad aproximada, color de ojos, piel, cabello, tipo de boca, nariz y señas particulares.

III. Trámite o servicio que originó la denuncia.
IV. Narración de los hechos, se redactará en primera persona, evitando incluir apreciaciones subjetivas, vagas e imprecisas.
V. Cualquier medio de prueba que sea proporcionado por el Denunciante, que permita advertir la presunta responsabilidad administrativa por la comisión de faltas administrativas.

TRIGÉSIMO OCTAVO. La Unidad de Transparencia deberá dar vista al ITAIPUE y al Órgano Interno de Control, respectivamente, de cualquier responsabilidad administrativa atribuible a las personas servidoras públicas por incumplimiento de las obligaciones previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados y Lineamientos, para que el ámbito de sus competencias, resuelvan lo conducente.

CAPÍTULO XIII
SANCIONES

TRIGÉSIMO NOVENO. Serán causas de sanción por incumplimiento de las obligaciones en materia de protección de datos personales por parte de las autoridades competentes, el actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes; incumplir plazos de atención previstos en la Ley; usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida Datos Personales; no contar con los avisos de privacidad correspondientes; clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables: incumplir con el deber de confidencialidad, entre otras causales establecidas en el artículo 188 de la LPDPPSOEP.

TRANSITORIOS

PRIMERO. Las presentes Políticas entrarán en vigor el día de su aprobación por parte del Comité de Transparencia de la Secretaría.

SEGUNDO. Las presentes Políticas se difundirán vía correo electrónico oficial y se publicarán en la página oficial de la Secretaría.

ANEXO ÚNICO

CARTA COMPROMISO DE CONFIDENCIALIDAD Y RESPONSABILIDAD DE GESTIÓN DE LA INFORMACIÓN Y DATOS PERSONALES QUE SE TRATAN EN (nombre del tratamiento de datos) DE LA (Unidad Administrativa responsable del tratamiento) DE LA SECRETARÍA.

"Cuatro Veces Heroica Puebla de Zaragoza", a xx de xxxxx del 2024

El/la que suscribe (nombre completo de la persona Servidora Pública), con número de expediente ___, desempeñándome como ___ del (área administrativa), adscrito/a la (Unidad Administrativa) de la Secretaría.

Se hace constar que se me otorgó por parte de la (Unidad Administrativa responsable), la "Política Interna para la Gestión y Tratamiento de Datos Personales en posesión de la Secretaría de Trabajo", en la que consta que todas las personas servidoras públicas, así como personal externo, debemos cumplir estrictamente con dicha Política, y con la normativa en materia de protección de datos personales.

Para efectos de lo anterior, tomo conocimiento de que queda estrictamente prohibido, de manera enunciativa más no limitativa, acceder, robar, copiar sin autorización, alterar o modificar, divulgar, transferir, publicar, prestar la información para fines ajenos a mis atribuciones y facultades, atendiendo en todo momento y aún después de mi comisión o encargo para conocerlos, de conformidad con los principios y directrices que rigen la actuación de los Servidores Públicos. Lo anterior con fundamento en los artículos 7 fracciones I, II, V y VI de la Ley General de Responsabilidades Administrativas, y 108 fracciones I, III, IV y VII de la Ley de Archivos del Estado de Puebla.

Por su parte, en cumplimiento a los principios y deberes en materia de protección de datos personales, me comprometo a:

1. Utilizar la documentación, información y datos personales en mi posesión que tenga bajo mi responsabilidad, por razones de mi empleo y que sean generados, obtenidos, adquiridos con motivo de mi encargo o comisión.
2. Garantizar, custodiar, salvaguardar y cuidar la documentación, información y datos personales en mi posesión que tenga bajo mi responsabilidad, por razones de mi empleo y que sean generados, obtenidos o adquiridos con motivo de mi encargo o comisión.

3. Impedir o evitar el mal uso, divulgación, transferencia, sustracción, destrucciones o inutilización, total o parcial, de la documentación, información y datos personales en mi posesión bajo mi responsabilidad, por razones de mi empleo y que sean generados, obtenidos o adquiridos con motivo de mi encargo o comisión.
4. Adquirir y actualizar los conocimientos necesarios en materia de protección de datos personales y seguridad de la información.
5. Actuar conforme a los principios y directrices que rigen la actuación de los Servidores Públicos establecidos en la Ley General de Responsabilidades Administrativas, el Código de Ética para las Personas Servidoras Públicas de la Administración Pública Estatal, el Código de Conducta de las Personas Servidoras Públicas de la Secretaría de Trabajo, y demás leyes normativas aplicables.

Por último, me doy por enterada/o de que en caso de incurrir en alguna violación o incumplimiento de cualquiera de los supuestos establecidos en los párrafos anteriores se podrá iniciar un procedimiento correspondiente de conformidad con lo establecido en la normatividad aplicable.

Una vez leída la presente carta de confidencialidad y responsabilidad, y enterada/o de su contenido y alcances legales, firmo y acepto a su entera satisfacción y conformidad.

(Nombre completo, cargo y firma)