GOBIERNO DE MÉXICO | TRABAJO
SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL

CENTRO FEDERAL DE CONCILIACIÓN Y REGISTRO LABORAL

POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES DEL CENTRO FEDERAL DE CONCILIACIÓN Y REGISTRO LABORAL

PRESENTACIÓN

Las presentes Políticas de Protección de Datos Personales del Centro Federal de Conciliación y Registro Laboral (CFCRL), se elaboraron en apego a lo previsto por el artículo 30, fracción II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), en el cual se prevé la creación de Políticas internas como uno de los mecanismos adoptados por quienes tratan datos, para dar cumplimiento al principio de responsabilidad, así como de acuerdo con lo establecido en el artículo 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, que establece que se deberán elaborar e implementar Políticas de protección de datos personales que tengan por objeto establecer los elementos y actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales.

Con la instrumentación de este mecanismo se posibilita a las áreas que integran el CFCRL, para realizar un tratamiento de datos personales, en estricto apego a los principios y deberes establecidos en la LGPDPPSO y demás disposiciones legales aplicables y se garantiza la adecuada protección y el ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición por parte de sus titulares.

INTRODUCCIÓN

Objetivo

Acreditar y asegurar el cumplimiento de los principios y deberes en materia de protección de datos personales, así como establecer los elementos y actividades de dirección, operación y control en los procesos en los que el CFCRL realice algún tratamiento de estos.

Alcance

Las presentes Políticas son de observancia general y obligatoria para todo el personal del CFCRL, involucrado en el tratamiento de datos personales.

La aplicación de estas Políticas se realizará por todas las áreas que tratan datos personales, de conformidad con la LGPDPPSO, los Lineamientos Generales y demás disposiciones aplicables en materia de protección de datos personales.

Cualquier controversia sobre la interpretación de sus alcances será analizada, discutida y, en su caso, resuelta por el Comité de Transparencia.

Marco Jurídico

- Constitución Políticas de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley Orgánica del Centro Federal de Conciliación y Registro Laboral.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Estatuto Orgánico del Centro Federal de Conciliación y Registro Laboral.
- Reglas de Integración y Funcionamiento de la Unidad de Transparencia y del Comité de Transparencia del Centro Federal de Conciliación y Registro Laboral.
- Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Documento Orientador del Programa de Protección de Datos.

GLOSARIO

- **CFCRL:** Centro Federal de Conciliación y Registro Laboral.
- **INAI:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- **LGPDPPSO:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

DEFINICIONES

- **Áreas:** Instancias que cuentan o puedan contar con la información de interés público; que estén previstas en el estatuto orgánico respectivo o equivalentes del Centro Federal de Conciliación y Registro Laboral.
- **Aviso de Privacidad:** Documento a disposición del titular 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.
- **Comité de Transparencia**: Autoridad máxima en materia de protección de datos personales al interior del Centro Federal de Conciliación y Registro Laboral.
- **Datos personales:** Cualquier 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.
- **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones Políticas y preferencia sexual.
- **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.
- **Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.
- **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.

- **Enlace:** Servidor público designado por cada unidad administrativa para fungir como enlace en materia de datos personales ante la Unidad de Transparencia y el Comité de Transparencia.

- **Lineamientos Generales**: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

CAPÍTULO I. De la implementación y acreditación de la Políticas de protección de datos personales del CFCRL

Designación de enlace

Artículo 1. Cada área designará a un servidor público que deberá contar como mínimo con el nivel de decisión de Director de Área, como enlace responsable de las actividades de protección de datos personales, con el fin de garantizar y evidenciar la operación y cumplimiento de esta Políticas ante el titular de los datos, el Comité de Transparencia y el Instituto.

Funciones de los enlaces

Artículo 2. Los enlaces contarán con las funciones siguientes:

I. Implementar y acreditar en su área, el cumplimiento de los principios y deberes de acuerdo con las directrices señaladas por esta Políticas y el Comité de Transparencia, en su calidad de autoridad máxima en materia de datos personales al interior del CFCRL.

II. Difundir las actividades de capacitación calendarizadas en el Programa Anual de Capacitación entre los servidores públicos adscritos a su área y que se encuentren involucrados directamente en el tratamiento de datos personales.

III. Participar en la integración y actualización de los documentos normativos exigidos por la ley y demás disposiciones aplicables.

IV. Conjuntar la información que se requiera a su área, en el ámbito de su competencia, para dar atención a los requerimientos en la materia.

V. Promover al interior de su área, la debida atención de solicitudes relativas al ejercicio de los Derechos de ARCO que sean presentadas ante la Unidad de Transparencia.

VI. Las demás que determinen las disposiciones normativas, el Instituto o, aquellas que deriven de las resoluciones emitidas por el Comité de Transparencia.

CAPÍTULO II. De los principios

Artículo 3. Las áreas del CFCRL responsables del tratamiento de datos personales observarán los principios rectores, siguientes:

I. Licitud.
II. Finalidad.

III. Lealtad.
IV. Consentimiento.
V. Información.
VI. Proporcionalidad.
VII. Calidad.
VIII. Responsabilidad.

Principio de Licitud

Artículo 4. El tratamiento de datos personales por parte de las áreas se sujetará a las atribuciones o facultades que les son conferidas en la normatividad que rige el actuar del CFCRL y, en estricto apego a lo dispuesto en la LGPDPPSO, los Lineamientos Generales, la presente Políticas y demás disposiciones legales aplicables en materia de protección de datos personales.

Artículo 5. Las áreas identificarán el marco normativo que en el ámbito de sus funciones se encuentra relacionado con el tratamiento de datos personales, el tipo de datos objeto de tratamiento y las finalidades para ello.

Artículo 6. Para el cumplimiento del principio de licitud, las áreas incluirán en el Aviso de Privacidad Integral y en el Inventario, el fundamento legal que les faculta a tratar datos personales.

Principio de finalidad

Artículo 7. Todo tratamiento de datos personales efectuado por las áreas deberá estar justificado por finalidades concretas, licitas, explicitas y legítimas. Para tal efecto, se entenderá que las finalidades son:

I. **Concretas:** Cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.

II. **Explícitas:** Cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.

III. **Lícitas:** Cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable.

IV. **Legítimas:** Cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción a que se refiere la LGPDPPSO y la presente Políticas.

Artículo 8. Como consecuencia del principio de finalidad, las áreas que traten datos personales deberán:

I. Establecer detalladamente en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, las cuales serán acordes a las atribuciones o facultades que tienen encomendadas.

II. Tratar los datos personales, conforme a las finalidades concretas, lícitas, explícitas y legítimas,

expresadas en el aviso de privacidad.

III. Obtener el consentimiento de los titulares para el tratamiento de sus datos personales, salvo las excepciones establecidas en la LGPDPPSO y las presentes Políticas.

IV. Informar a los titulares, sobre el tratamiento de sus datos para finalidades distintas a las previstas en el aviso de privacidad, siempre y cuando se tenga facultades o atribuciones para ello y se recabe el consentimiento de éstos, con excepción de lo establecidos en la LGPDPPSO y las presentes Políticas.

V. Además, deberá considerarse lo siguiente:

   a. La expectativa razonable de privacidad del titular, consistente en la confianza depositada en el CFCRL para que los datos personales proporcionados sean tratados conforme a lo señalado en el aviso de privacidad.

   b. La naturaleza de los datos personales.

   c. Las consecuencias que, en su caso, se generen al titular con motivo del tratamiento posterior de los datos personales.

   d. Las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la LGPDPPSO.

Artículo 9. Para acreditar el cumplimiento del principio de finalidad, las áreas deberán:

I. Incluir en el inventario, las finalidades de cada tratamiento que se realice y verificar que estas sean específicas o determinadas y que sean acordes a las atribuciones o facultades del CFCRL y de su área.

II. Vigilar que los servidores públicos únicamente traten datos personales en términos de las finalidades informadas en el aviso de privacidad correspondiente.

III. Verificar que en los avisos de privacidad se informen todas las finalidades para las cuales se tratan los datos personales, y que éstas sean descritas de manera clara.

IV. Informar a los titulares sobre el tratamiento de los datos para finalidades distintas.

V. Recabar el consentimiento de los titulares, cuando este proceda.

Principio de Lealtad

Artículo 10. Las áreas del CFCRL se abstendrán de obtener y tratar datos personales a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

Artículo 11. Derivado del principio de lealtad los servidores públicos responsables del tratamiento de datos personales deberán:

I. Obtener y tratar los datos personales sin que medie dolo, mala fe o negligencia.

II. Privilegiar los intereses del titular y, evitar cualquier tipo discriminación, trato injusto o arbitrario en contra de éstos, con motivo del tratamiento de sus datos.

III. Respetar la expectativa razonable de privacidad.

Artículo 12. Para acreditar el cumplimiento del principio de lealtad, las áreas deberán:

I. Contar con avisos de privacidad que cumplan con lo establecido en la LGPDPPSO y las presentes Políticas.

II. Implementar instrumentos que permitan verificar que los tratamientos realizados no den lugar a discriminación, trato injusto o arbitrario en contra del titular.

III. Constatar que el tratamiento de datos personales sólo se lleve a cabo para los fines informados en el aviso de privacidad.

Principio de Consentimiento

Artículo 13. Previo al tratamiento de los datos personales, las áreas obtendrán el consentimiento del titular de manera libre, específica e informada, en términos de lo dispuesto en la Ley General, salvo que se actualice alguna de las causales de excepción siguientes:

I. Cuando una ley así lo disponga, en cuyo caso, los supuestos de excepción deberán ser acordes con las bases, principios y disposiciones establecidos en la LGPDPPSO que, en ningún caso, podrán contravenirla.

II. Cuando las transferencias que se realicen entre el CFCRL y otro sujeto responsable sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o acordes 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 del titular ante autoridad competente.

V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el CFCRL.

VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su 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 el titular de los datos personales sea una persona reportada como desaparecida en los

términos de la ley en la materia.

La actualización de alguno de los supuestos no exime al área y a los servidores públicos responsables del tratamiento de datos personales del cumplimiento de las demás obligaciones establecidas en la LGPDPPSO, los Lineamientos y las presentes
Políticas.

Por regla general, el consentimiento tácito será válido para llevar a cabo el tratamiento de datos personales, salvo aquellos supuestos en los cuales la LGPDPPSO o alguna disposición aplicable exija su obtención de forma expresa y, en su caso, por escrito, particularmente, cuando se refiera a datos sensibles.

Artículo 14. En términos de los alcances del principio de consentimiento, las áreas deberán:

I. Obtener el consentimiento del titular, previo al tratamiento de los datos, salvo que se actualice alguno de los supuestos de excepción descritos en el artículo anterior.

II. Recabar el consentimiento expreso y, en su caso, por escrito, a través de formatos claros y sencillos, acorde con el perfil del titular, en los cuales se distingan los datos y finalidades del tratamiento que requieren de la manifestación de su voluntad.

III. Implementar medios sencillos y gratuitos para la obtención del consentimiento, independientemente de la modalidad en que éste se requiera.

IV. En su caso, habilitar en el aviso de privacidad casillas y/o espacios para que el titular exprese su consentimiento, respecto de cada una de las finalidades para las cuales son tratados sus datos.

Artículo 15. Para acreditar el cumplimiento del principio de consentimiento, las áreas deberán:

I. Identificar en el aviso de privacidad, aquellos datos y finalidades que requieren del consentimiento del titular, para su tratamiento.

II. Mantener bajo su resguardo una copia del documento en el cual se haya manifestado el consentimiento del titular para el tratamiento de sus datos, cuando éste proceda.

III. Documentar la puesta a disposición del aviso de privacidad al titular, en aquellos casos en los cuales sea válido el consentimiento tácito.

Principio de Información

Artículo 16. Independientemente de que se requiera o no el consentimiento del titular para el tratamiento de sus datos personales, las áreas del CFCRL informarán a los titulares sobre la existencia y las características principales del tratamiento al que serán sometidos sus datos personales.

Las áreas que traten datos personales, sin importar la función con la que se vincule, elaborarán y pondrán a disposición los avisos de privacidad simplificados e integrales que correspondan a los tratamientos llevados a cabo, en los términos establecidos por la LGPDPPSO, los Lineamientos Generales, así como en las presentes Políticas.

Artículo 17. Para dar atención al principio de información, las áreas que traten datos personales

deberán:

I. Redactar las modalidades de avisos de privacidad, integral y simplificado que se requieran, conforme a los tratamientos que se lleven a cabo.

II. Poner gratuitamente a disposición de los titulares el aviso de privacidad en los términos que fije la LGPDPPSO y los Lineamientos Generales, aunque no se requiera el consentimiento de los titulares para el tratamiento de los datos personales.

III. Elaborar los avisos de privacidad con todos los elementos informativos que resulten aplicables, de manera clara, comprensible, así como con una estructura y diseño que facilite su entendimiento, considerando su accesibilidad para personas con algún tipo de discapacidad.

IV. Difundir el aviso de privacidad por medios electrónicos y físicos.

V. Ubicar el aviso de privacidad en un lugar visible y que facilite su consulta, con independencia del medio de difusión o reproducción que se utilice.

VI. Promover que los avisos de privacidad sean redactados de conformidad con lo establecido por la LGPDPPSO y los Lineamientos.

VII. Comunicar el aviso de privacidad a quienes se transfieran datos personales.

VIII. Prever la implementación de medidas compensatorias, en términos de lo dispuesto en la LGPDPPSO y demás disposiciones aplicables, para dar a conocer los avisos de privacidad a través de medios masivos de difusión (periódico oficial, página de Internet, carteles o cápsulas informativas u otro similar), cuando resulte imposible hacerlo de manera directa al titular o, ello exija esfuerzos desproporcionados.

Artículo 18. En aras de acreditar el cumplimiento del principio de información, las áreas realizarán las acciones siguientes:

I. Contar con los avisos de privacidad integral y simplificado por cada proceso de tratamiento de datos personales que se lleve a cabo.

II. Implementar un procedimiento gratuito para la puesta de disposición del aviso de privacidad.

III. Realizar las gestiones para que los avisos de privacidad, en sus modalidades simplificada e integral, sean publicados en el portal de Internet del CFCRL, en la sección que se destine para ello, a fin de que se difunda por medios electrónicos.

IV. Incluir en el inventario los lugares y medios en los que se difunden y colocan los avisos de privacidad.

V. Documentar la comunicación realizada del aviso de privacidad a terceros a los que se transfieran los datos personales.

Principio de Proporcionalidad

Artículo 19. Las áreas del CFCRL recabarán aquellos datos personales que resulten adecuados,

relevantes y necesarios para la finalidad que justifica su tratamiento.

Se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas a las áreas del CFCRL.

Artículo 20. Para el cumplimiento del principio de proporcionalidad los servidores públicos responsables del tratamiento de datos personales deberán:

I. Recabar y tratar sólo aquellos datos personales necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

II. Realizar esfuerzos razonables para actualizar la normativa y formatos internos, con el fin de limitar los datos personales tratados al mínimo necesario, considerando las finalidades que motivan su tratamiento.

III. Limitar al mínimo posible el periodo de tratamiento de datos personales.

Artículo 21. En aras de acreditar el cumplimiento del principio de proporcionalidad, las áreas realizarán, al menos, las acciones siguientes:

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

II. Promover que en su área se requiera el mínimo posible de datos personales para lograr las finalidades para las cuales se tratan.

III. Promover prácticas que minimicen la obtención de datos personales y el periodo de su tratamiento, así como señalarlas en el documento de seguridad.

Principio de Calidad

Artículo 22. Las áreas adoptarán las medidas señaladas en el documento de seguridad para mantener los datos personales exactos, correctos, completos y actualizados, a fin de que no se altere la veracidad de éstos.

Se entenderá que los datos personales son:

I. **Exactos y correctos:**

- Cuando los datos personales no presentan errores que pudieran afectar su veracidad.
- Cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y las atribuciones del responsable.

II. **Actualizados:**

Cuando los datos personales responden fielmente a la situación actual del titular. Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

Cuando los datos personales se hayan obtenido indirectamente del titular, las áreas adoptarán las medidas referidas en el documento de seguridad para garantizar que éstos respondan al principio de calidad, de acuerdo con la categoría de datos personales, así como las condiciones y medios del tratamiento.

En el supuesto de que los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones aplicables, serán suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de éstos, en los términos previstos en el inventario que se integra al documento de seguridad.

Artículo 23. Para el cumplimiento del principio de calidad, las áreas que traten datos personales deberán:

I. Implementar medidas para que las actualizaciones efectuadas, tengan impacto inmediato en las distintas bases de datos en las cuales obre la información del titular.

II. Establecer plazos de conservación de la información, conforme a las disposiciones legales aplicables en materia archivística.

III. Elaborar procedimientos para la conservación, bloqueo y supresión de los datos personales.

Artículo 24. Para acreditar el cumplimiento del principio de calidad, las áreas deberán realizar lo siguiente:

I. Generar una relación de todas las bases de datos con que cuentan y el tipo de información personal tratada en cada una de ellas que, en su caso, permita vincularlas.

II. Documentar las actualizaciones y supresiones realizadas.

III. Contar con los procedimientos para la conservación, bloqueo y supresión de los datos personales.

Principio de Responsabilidad

Artículo 25. Conforme al principio de responsabilidad, el CFCRL velará por el cumplimiento del resto de los principios; promoverá la adopción de medidas necesarias para su aplicación y, demostrará ante titulares y el organismo garante, que se cumplen con las obligaciones en torno a la protección de los datos personales.

Artículo 26. Para dar cumplimiento al principio de responsabilidad, las áreas realizarán lo siguiente:

I. Establecer entre su personal la obligatoriedad y exigibilidad del programa de protección de datos personales que apruebe el Comité de Transparencia.

II. Prever recursos para la instrumentación de las presentes Políticas y del programa de protección de datos, en su caso.

III. Incentivar la capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.

IV. Revisar periódicamente el programa de protección de datos personales y el documento de seguridad para determinar las modificaciones que se requieran.

V. Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

VI. Observar lo previsto en el programa de protección de datos personales, así como los servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología con que cuente y que implique el tratamiento de datos personales y en su caso, proponer modificaciones a estos para que desde el inicio cumplan por diseño con las obligaciones previstas en la LGPDPPSO, los Lineamientos Generales y las presentes Políticas.

Artículo 27. Para acreditar el cumplimiento al principio de responsabilidad, las áreas deberán:

I. Contar con las constancias de capacitación de su personal en temas relacionados con la materia de protección de datos personales.

II. Llevar un registro de las dudas y quejas de los titulares.

III. Documentar la comunicación hacia su personal de las presentes Políticas y del programa de protección de datos que al efecto sea aprobado.

IV. Guardar evidencia del cumplimiento a las presentes Políticas.

CAPÍTULO III. De los deberes

Artículo 28. Además de los principios señalados en el Capítulo anterior, las áreas cumplirán con lo siguiente:

I. Deber de confidencialidad.

II. Deber de seguridad.

Deber de Confidencialidad

Artículo 29. Las áreas establecerán controles o mecanismos de observancia obligatoria para los servidores públicos que intervengan en cualquier fase del tratamiento, con la finalidad de que éstos guarden confidencialidad de los datos personales, obligación que subsistirá aún después de finalizar su relación laboral con el CFCRL y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

Artículo 30. Para el debido cumplimiento del deber de confidencialidad, las áreas deberán:

I. Prever controles mediante los cuales se garantice la confidencialidad de los datos personales que son tratados.

II. Establecer cláusulas en los contratos para que los sujetos obligados del ámbito público o

privado a los cuales les sean transferidos o remitidos datos personales se obliguen a la confidencialidad de éstos durante y posterior a la vigencia del instrumento jurídico.

III. Implementar campañas de sensibilización para los servidores públicos, sobre la importancia de la confidencialidad de los datos personales.

IV. Proponer la implementación de mejores prácticas al interior del CFCRL, para garantizar la secrecía de los datos personales.

Artículo 31. Para acreditar el cumplimiento del deber de confidencialidad, las áreas realizarán, al menos, lo siguiente:

I. Incluir en el documento de seguridad, los controles y medidas de seguridad implementadas para garantizar la secrecía de los datos personales.

II. Generar la evidencia de los controles implementados para garantizar la confidencialidad de los datos.

III. Contar con los contratos en los cuales se establezcan las cláusulas de confidencialidad de datos, respecto de transferencias o remisiones.

IV. Tener la evidencia documental de los cursos, talleres, seminarios o similar en los que haya participado el personal de las áreas y se encuentre relacionado con la materia de protección de datos personales.

V. Documentar la implementación de mejores prácticas que garanticen la confidencialidad de los datos tratados.

Deber de Seguridad

Artículo 32. Las áreas adoptarán e instrumentarán las medidas de seguridad físicas, técnicas y administrativas a través de las cuales garantice la protección de los datos personales tratados, a fin de evitar cualquier afectación a estos y su titular.

Artículo 33. Para el debido cumplimiento del deber de seguridad, las áreas llevarán a cabo, al menos, lo siguiente:

I. Generar e implementar Políticas de gestión, en las cuales se considere el tipo de datos personales recabados, el tratamiento que se les dará y el ciclo de vida de estos.

II. Establecer los servidores públicos que podrán intervenir en el tratamiento de los datos personales y definir las funciones y obligaciones que estos tendrán.

III. Realizar un análisis de riesgo de los datos personales tratados, así como de los sistemas físicos y/o electrónicos en el cual se desarrolle dicho tratamiento.

IV. Desarrollar acciones de prevención y mitigación de amenazas o vulneraciones de datos personales.

V. Monitorear y revisar de las medidas de seguridad adoptadas para garantizar la protección de

datos.

VI. Incentivar la capacitación de los servidores públicos involucrados en el tratamiento de datos personales, conforme al nivel de responsabilidad que éstos tengan asignado.

Artículo 34. Para acreditar el cumplimiento del deber de seguridad, las áreas realizarán, al menos, lo siguiente:

I. Contar con un inventario de datos y de los sistemas de tratamiento.

II. Comunicar al personal las Políticas implementadas para la protección de datos y guardar evidencia de ello.

III. Llevar una bitácora en la cual se asiente cualquier amenaza o vulneración de datos personales suscitada, así como de las acciones realizadas para su mitigación.

IV. Instrumentar las medidas de seguridad físicas, técnicas y administrativas adoptadas para garantizar el tratamiento de los datos recabados, así como las acciones de monitoreo, análisis y revisión a implementar, a fin de mantenerlas actualizadas y, en su caso, detectar áreas de oportunidad para su desarrollo y ejecución.

V. Tener la evidencia documental de los cursos, talleres, seminarios o similar en los que haya participado el personal de las áreas y se encuentre relacionado con la materia de protección de datos personales.

CAPÍTULO IV. Programa de Protección de Datos Personales

Artículo 35. El CFCRL contará con un programa de protección de datos personales, aprobado por el Comité de Transparencia, cuyo objetivo es determinar las pautas generales bajo las cuales se llevarán a cabo las tareas institucionales orientadas a mantener la observancia en el cumplimiento de los principios y deberes, así como a garantizar el derecho a la protección de datos personales al interior de este sujeto obligado

Artículo 36. El programa tendrá una vigencia sexenal, a fin de garantizar el desarrollo ininterrumpido de actividades, sin demerito de que podrá ser sometido a su revisión, ajuste o actualización por parte del Comité de Transparencia, de conformidad con las facultades y atribuciones que le establece la normativa aplicable, en caso de estimarse necesario.

Artículo 37. La Unidad de Transparencia del CFCRL elaborará la propuesta de ajustes o actualizaciones al programa de protección de datos personales del CFCRL, las cuales serán presentada al Comité de Transparencia para su revisión y, en su caso, aprobación. Cualquier modificación y actualización se sujetará a los términos señalados en el párrafo anterior.

Artículo 38. El Programa de Protección de Datos Personales del CFCRL deberá contener al menos:

I. La vigencia del programa.

II. Un diagnóstico sobre los problemas, necesidades o áreas de oportunidad detectadas para el

debido cumplimiento de los principios y deberes en materia de protección de datos personales dentro del CFCRL.

III. Las actividades propuestas, su viabilidad, así como los objetivos que se persiguen, los cuales estarán vinculados a la atención de los problemas, necesidades o áreas de oportunidad previamente detectadas.

IV. Los indicadores a través de los cuales se medirá el cumplimiento de las actividades propuestas.

Artículo 39. Corresponde al Comité de Transparencia dar seguimiento al cumplimiento de los indicadores comprometidos en el programa de protección de datos personales y sus resultados.

CAPÍTULO V. Documento de Seguridad

Artículo 40. El CFCRL cuenta con un Documento de Seguridad como parte de los mecanismos implementados para asegurar el cumplimiento al deber de seguridad, cuyo objeto es establecer, de manera general, las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales tratados.

Artículo 41. El Documento de Seguridad deberá contener como mínimo, lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento.

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

III. El análisis de riesgos.

IV. El análisis de brecha.

V. El plan de trabajo.

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

VII. El programa general de capacitación.

Artículo 42. En las actualizaciones que se realicen al Documento de Seguridad deberán participar todas las áreas, a través de sus enlaces a que se hacen referencia las presentes Políticas, quienes en todo momento observarán los principios y deberes a que se refiere la LGPDPPSO, los Lineamientos Generales y demás disposiciones legales aplicables.

Para la formulación de propuestas de actualización del Documento de Seguridad, la Unidad de Transparencia del CFCRL elaborará formatos, cuestionarios o cualquier otro instrumento de apoyo, que resulte útil para el cumplimiento de estas Políticas y demás disposiciones aplicables en la materia.

Acorde con lo dispuesto en la LGPDPPSO, el Documento de Seguridad se actualizará en los supuestos siguientes:

I. Se produzcan modificaciones sustanciales al tratamiento de los datos personales que deriven en un cambio de nivel de riesgo.

II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión con que se cuente.

III. Derivado de un proceso de mejora para mitigar el impacto de vulneración a la seguridad ocurrida.

IV. Con motivo de la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Con independencia de los supuestos anteriores, el Documento de Seguridad podrá ser actualizado cada seis años.

Artículo 43. Cuando alguna de las áreas se encuentre en alguno de los supuestos referidos, el enlace responsable solicitará por escrito al Comité de Transparencia las actualizaciones conducentes, quien resolverá lo conducente.

Los enlaces responsables podrán solicitar orientación técnica a la Unidad de Transparencia, para la integración o cualquier acto relacionado con los alcances del Documento de Seguridad.

Artículo 44. Corresponde al titular de cada área y al personal de mando superior la supervisión de las Políticas internas para la gestión y tratamiento de datos personales. El titular de la UA podrá solicitar en cualquier momento a su enlace responsable, los informes que se requieran sobre las acciones contenidas en el documento de seguridad, mismo que deberán integrarse en coordinación con el servidor público de mando que corresponda, de acuerdo con su ámbito de competencia.

Artículo 45. En términos de lo previsto en la LGPDPPSO, se consideran vulneraciones a la seguridad de los datos, las siguientes:

I. La pérdida o destrucción no autorizada.

II. El robo, extravío o copia no autorizada.

III. El uso, acceso o tratamiento no autorizado.

IV. El daño, la alteración o modificación no autorizada.

Artículo 46. Cuando las vulneraciones afecten de forma significativa los derechos patrimoniales o morales de los titulares, las áreas involucradas, deberán generar un informe detallado que contenga al menos lo siguiente:

I. La naturaleza del incidente.

II. Los datos personales comprometidos.

III. Las recomendaciones al titular acerca de las medidas que éste puede adoptar para proteger sus intereses.

IV. Las acciones correctivas implementadas para mitigar la vulneración.

V. Los datos de contacto del enlace responsable o personal al cual puede acudir el titular para obtener más información al respecto.

El referido informe será remitido a la Unidad de Transparencia en un plazo no mayor a dos días naturales posteriores a que se haya confirmado la vulneración, para que ésta lo haga del conocimiento de los titulares de datos involucrados y del Comité de Transparencia.

Adicionalmente, las áreas deberán prever en el informe a notificarse al Instituto por parte de la Unidad de Transparencia, lo siguiente:

1) La hora y fecha de la identificación de la vulneración.

2) La hora y fecha del inicio de la investigación sobre la vulneración.

3) La naturaleza del incidente o vulneración ocurrida.

4) La descripción detallada de las circunstancias en torno a la vulneración ocurrida.

5) Las categorías y número aproximado de titulares afectados.

6) Los sistemas de tratamiento y datos personales comprometidos.

7) La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida.

8) Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

Artículo 47. Conforme a lo previsto en los Lineamientos Generales, se entenderá que afectan los derechos patrimoniales del titular, cuando la vulneración esté relacionada con sus bienes, información fiscal, historial crediticio, ingresos o egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados u otros similares.

Para el caso de los derechos morales, se entenderán aquellos relacionados, de manera enunciativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, aspecto físico o menoscabe ilegalmente la libertad, integridad física o psíquica del titular de los datos.

Artículo 48. En aquellos casos en los cuales no sea posible notificar directamente a los titulares de los datos el informe a que hace referencia las presentes Políticas o ello implique esfuerzos desproporcionados, las áreas instrumentarán medidas compensatorias de comunicación para tal efecto, como son: la publicación en periódico oficial, página de Internet, carteles o cápsulas informativas u otro similar.

Artículo 49. El Comité de Transparencia podrá determinar la implementación de acciones adicionales a las realizadas por las áreas para evitar futuras vulneraciones y reforzar las medidas de seguridad aplicables.

Para tal efecto, el Comité de Transparencia podrá auxiliarse de la asesoría, orientación o apoyo de otras áreas del CFCRL, proponer la suscripción de convenios de colaboración o solicitar la

contratación de especialistas en la materia, siempre y cuando exista la suficiencia presupuestal para ello.

CAPÍTULO VI. Avisos de Privacidad

Artículo 50. Como parte de las acciones para cumplir con el principio de información y, con independencia de que no se requiera del consentimiento del titular para el tratamiento de sus datos personales, en el CFCRL se contará con un aviso de privacidad integral y su correlativo aviso de privacidad simplificado, por cada proceso en los que se traten datos personales.

Excepcionalmente, cuando dos o más procesos de tratamiento de datos personales, atiendan a una misma finalidad o función, se podrá contar con un mismo aviso de privacidad, en sus dos modalidades, siempre y cuando sea posible expresar con precisión y claridad las finalidades del tratamiento de datos personales, de tal suerte que no dé lugar a incertidumbre o ambigüedad a sus titulares.

Artículo 51. Los formatos para la elaboración de los avisos de privacidad integral y simplificado serán acordes con los elementos que establece la LGPDPPSO, los Lineamientos Generales y demás normatividad que resulte aplicable.

Artículo 52. En la integración y elaboración de los avisos de privacidad, las áreas preverán un diseño que facilite su entendimiento por parte de los titulares de los datos. De ser el caso, la Unidad de Transparencia podrá elaborar las propuestas de formatos que faciliten su integración o actualización, manteniendo la homogeneidad de los elementos.

Artículo 53. Las áreas se asegurarán de que la información asentada en los avisos de privacidad se encuentre redactada en un lenguaje sencillo, claro y comprensible, considerando en todo momento el perfil del titular al cual vaya dirigido, por lo que se abstendrán de:

I. Usar frases inexactas, ambiguas o vagas.

II. Incluir textos que induzcan a los titulares a elegir una opción en específico.

III. Marcar previamente casillas, en caso de que éstas se incluyan, para que los titulares otorguen su consentimiento, o bien, incluir declaraciones orientadas a afirmar que el titular ha consentido el tratamiento de sus datos personales sin manifestación alguna de su parte.

IV. Remitir a textos o documentos que no estén disponibles para los titulares.

Artículo 54. Para la elaboración o actualización de los avisos de privacidad, los enlaces podrán en todo momento, solicitar orientación técnica a la Unidad de Transparencia.

Artículo 55. En sustitución de los avisos de privacidad ya existentes, los servidores públicos responsables, considerarán la elaboración de un nuevo aviso de privacidad, en sus dos modalidades, cuando:

I. Por disposición de alguno de los ordenamientos aplicables al Centro Federal de Conciliación y Registro Laboral, el proceso de tratamiento de datos personales se traslade a una nueva área o

ésta cambie su denominación.

II. Se requieran recabar datos sensibles adicionales a aquellos informados en el aviso de privacidad original, los cuales no se obtengan de manera directa del titular y se requiera de su consentimiento para el tratamiento de estos.

III. Cambien las finalidades señaladas en el aviso de privacidad original, o

IV. Se modifiquen las condiciones de las transferencias de datos personales o se pretendan realizar otras no previstas inicialmente y, el consentimiento del titular sea necesario.

CAPÍTULO VII. Programa de Capacitación y Actualización

Artículo 56. El CFCRL contará con un Programa de Capacitación y Actualización en materia de protección de datos personales, como uno de los mecanismos a través de los cuales se cumple con el principio de responsabilidad, el cual considerará los niveles de capacitación atendiendo a los roles y responsabilidades de los servidores públicos que tratan la información personal.

Artículo 57. El Comité de Transparencia será el órgano encargado de aprobar el programa de capacitación y actualización en la materia, con base en la propuesta que sea presentada por la Unidad de Transparencia, en la cual se consideren las necesidades de capacitación de las áreas y la oferta educativa del INAI.

Artículo 58. En caso de que los cursos y actividades de capacitación corresponda a contenidos ofertados por el INAI, la Unidad de Transparencia será la encargada de dar seguimiento al programa respectivo, con la colaboración de los enlaces.

CAPÍTULO VIII. Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO)

Artículo 59. Para efectos de este procedimiento, se considera que los derechos ARCO comprenden:

I. **Acceso:** Derecho del titular para acceder a sus datos personales en posesión del CFCRL, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.

II. **Rectificación:** Derecho del titular para solicitar al CFCRL la corrección de sus datos personales, cuando estos resulten inexactos, incompletos o no se encuentren actualizados.

III. **Cancelación:** Derecho del titular para solicitar al CFCRL que sus datos personales sean bloqueados y, posteriormente, suprimidos de los archivos, registros, expedientes y sistemas institucionales del CFCRL, a fin de que los mismos no se encuentren más en su posesión y, por lo tanto, dejen de ser tratados.

IV. **Oposición:** Derecho del titular para solicitar a el CFCRL que se abstenga de utilizar información personal para ciertos fines o de requerir que se concluya su uso, a fin de evitar un daño o

afectación a su persona.

Artículo 60. La presentación de solicitudes de derechos ARCO podrá realizarse a través de los medios de recepción siguientes:

I. Directamente en la oficina de la Unidad de Transparencia del CFCRL.

II. Correo electrónico: transparencia@centrolaboral.gob.mx

III. Plataforma Nacional de Transparencia: http://www.plataformadetransparencia.org.mx/

Artículo 61. La Unidad de Transparencia será la responsable de turnar las solicitudes de ejercicio de derechos ARCO que sean presentadas a el CFCRL a aquellas áreas que conforme a sus atribuciones, competencias o funciones puedan o deban poseer los datos personales se pronuncien, para dar atención a estas en los plazos y términos establecidos en la LGPDPPSO, los Lineamientos Generales y demás disposiciones aplicables en la materia.

Artículo 62. Las áreas llevarán a cabo las acciones pertinentes para garantizar el efectivo ejercicio de los Derechos ARCO de los titulares, acorde con los principios, obligaciones y deberes en materia de protección de datos personales.

Artículo 63. Las áreas trabajarán en conjunto con la Unidad de Transparencia para la atención de las solicitudes y, en su caso, de los recursos de revisión interpuestos en términos de la LGPDPPSO, con motivo de las respuestas otorgadas.

Artículo 64. Las resoluciones que emita el INAI son vinculantes para el CFCRL y, una vez recibidas, la Unidad de Transparencia llevará a cabo las gestiones que resulten necesarias ante las unidades administrativas competentes para dar cumplimiento a lo instruido.

CAPÍTULO IX. De las remisiones y transferencias de los datos personales en posesión del CFCRL

Artículo 65. La remisión es toda aquella comunicación de datos personales realizada exclusivamente entre responsables (CFCRL) y encargado, dentro o fuera del territorio mexicano.

Artículo 66. El CFCRL podrá encargar el tratamiento de datos personales a personas físicas o morales ajenas a la institución, únicamente cuando sea consecuencia de la existencia de una relación formalizada mediante un instrumento jurídico suscrito por los servidores públicos facultados para ello.

Artículo 67. El encargado tratará los datos personales a nombre y por cuenta del CFCRL dentro del ámbito de actuación de la prestación del servicio debidamente formalizado y sin ostentar poder alguno de decisión sobre el alcance y contenido del tratamiento, limitando en ese sentido, sus actuaciones a los términos fijados por el CFCRL.

Artículo 68. Cualquier acuerdo alcanzado y debidamente formalizado entre el CFCRL y el encargado se efectuará con base en lo previsto por la LGPDPPSO, los Lineamientos Generales, las presentes Políticas y el aviso de privacidad puesto a disposición de los titulares de los datos en el cual quedaron

definidas previamente las condiciones del tratamiento de los datos personales.

Artículo 69. Acorde con lo dispuesto en la LGPDPPSO y los Lineamientos Generales, el instrumento jurídico por el cual se formalice la relación jurídica entre el CFCRL y el encargado deberá incluir al menos las siguientes obligaciones para este:

I. Realizar el tratamiento de los datos personales conforme a las instrucciones del CFCRL.

II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el CFCRL.

III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.

IV. Informar a el CFCRL cuando ocurra una vulneración a los datos personales que trata por sus instrucciones.

V. Guardar confidencialidad respecto de los datos personales tratados.

VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el CFCRL, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

VII. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

VIII. Permitir al Instituto o a el CFCRL, realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales.

IX. Colaborar con el INAI en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la LGPDPPSO y los Lineamientos Generales, proporcionando la información y documentación que se estime necesaria para tal efecto.

X. Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de las obligaciones señaladas en este artículo.

Artículo 70. La subcontratación de servicios que impliquen el tratamiento de los datos personales previamente remitidos por el CFCRL sólo podrá llevarse a cabo cuando en el instrumento jurídico suscrito por el CFCRL y el encargado se contemple dicha situación, debiendo el encargado formalizar, a su vez, la relación jurídica con el subcontratado a través de cualquier instrumento jurídico que permita acreditar su existencia, alcance y contenido, en términos de las disposiciones legales aplicables.

En el instrumento jurídico de subcontratación, además de prever las cláusulas establecidas en el artículo anterior, se establecerá que la persona física o moral subcontratada asumirá las mismas obligaciones establecidas para el encargado.

Artículo 71. El CFCRL podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice las condiciones y cuente con los mecanismos establecidos

en la LGPDPPSO.

Para dichos efectos, el área contratante deberá solicitar dictamen técnico al área que, de conformidad con las atribuciones establecidas en la normativa interna, cuente con la atribución de establecer normas y emitir las Políticas en materia de tecnología de la información, comunicación y seguridad informática en el CFCRL.

CAPÍTULO X. De las Transferencias de Datos Personales

Artículo 72. El CFCRL podrá llevar a cabo transferencias nacionales o internacionales a terceros, de los datos personales en su posesión, en los términos y bajo las condiciones que determina la LGPDPPSO.

Las comunicaciones de los datos personales que lleve a cabo el CFCRL a los encargados, no serán consideradas como transferencias.

Artículo 73. Toda transferencia de datos personales que lleve a cabo el CFCRL se encuentra sujeta al consentimiento de su titular. Para tal efecto, las áreas del CFCRL por medio del aviso de privacidad correspondiente informarán al titular de los datos personales, las finalidades de la transferencia, así como su destinatario.

En caso de ser una transferencia que requiera de consentimiento, se habilitarán los mecanismos para que el titular manifieste la voluntad correspondiente. El CFCRL no estará obligada a requerir el consentimiento del titular para llevar a cabo la transferencia de sus datos, en los casos previstos por la LGPDPPSO.

La actualización de alguna de las excepciones previstas en las disposiciones previamente citadas no exime a las unidades administrativas del CFCRL a cumplir con las obligaciones previstas en la LGPDPPSO y las presentes Políticas.

Artículo 74. En toda transferencia de datos personales, los servidores públicos responsables comunicarán el aviso de privacidad respectivo, al tercero receptor de las transferencias, debiendo documentar detalladamente dicha comunicación.

Artículo 75. Acorde con lo previsto en la LGPDPPSO, toda transferencia de datos personales que realicen las unidades administrativas del CFCRL deberá formalizarse mediante la suscripción de un instrumento jurídico que demuestre el alcance de su tratamiento, así como las obligaciones y responsabilidades contraídas por las partes.

La formalización referida no resultará aplicable en los siguientes casos:

I. Cuando la transferencia sea nacional y se realice en virtud del cumplimiento de una disposición legal o del ejercicio de las atribuciones expresamente conferidas.

II. Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México; se realice derivado de una petición de la autoridad extranjera u organismo internacional competente en su carácter de receptor; cuando las facultades entre el CFCRL y el responsable receptor sean homólogas; o cuando las finalidades que motivan la

transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento por parte del CFCRL.

Artículo 76. Cuando la comunicación de datos personales se realice fuera del territorio nacional, previo a su transferencia, el CFCRL se asegurará que el tercero receptor se obligue a proteger los datos personales conforme a los principios, deberes y obligaciones similares o equiparables a las previstas en la LGPDPPSO y demás normatividad mexicana aplicable en la materia, así como a los términos previstos en el aviso de privacidad que le será comunicado por el CFCRL.

En todo caso, el CFCRL podrá solicitar al INAI opinión respecto de las transferencias internacionales que se le susciten, en términos de lo dispuesto en los Lineamientos Generales.

ARTÍCULOS TRANSITORIOS

Artículo Primero. Las presentes Políticas entrará en vigor al día siguiente de su aprobación por el Comité de Transparencia.

Artículo Segundo. Se instruye a la Unidad de Transparencia, para que realice las acciones pertinentes a fin de que la Políticas sea publicada en el micrositio de Protección de Datos de la página de Internet del CFCRL.

Artículo Tercero. La presente Políticas deberá hacerse del conocimiento del personal de las áreas dentro de los treinta días naturales siguientes a la entrada en vigor de las presentes Políticas, a través de los medios físicos o electrónicos institucionales que estime pertinentes cada titular o el enlace designado y remitir las constancias de ello a la Unidad de Transparencia.

El presente documento fue aprobado por el Comité de Transparencia, en la Trigésima Tercera Sesión Extraordinaria 2022, de fecha treinta de junio de dos mil veintidós, mediante acuerdo CFCRL/CT/SE/33/03/2022.----------
---