Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

ACUERDO ACT-PUB/19/09/2018.06

ACUERDO MEDIANTE EL CUAL SE EMITEN LAS RECOMENDACIONES EN MATERIA DE ACCESO A LA INFORMACIÓN Y DATOS PERSONALES ANTE CAMBIOS DE TITULARES DE UNIDAD DE TRANSPARENCIA, DE COMITÉ DE TRANSPARENCIA Y DE SERVIDORES PÚBLICOS A CARGO DEL TRATAMIENTO DE DATOS PERSONALES.

Con fundamento en los artículos 6°, apartado A, fracción VIII, de la Constitución Política de los Estados Unidos Mexicanos; artículo 2, fracción VIII; 42, fracción XXI de la Ley General de Transparencia y Acceso a la Información Pública; 29, fracción I y 31, fracción XII, de la Ley Federal de Transparencia y Acceso a la Información Pública; 2, fracción VI, 83, párrafo segundo, 85 y 89, fracción XIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 6, 8, 12, fracción I , XXXV y XXXVII, 18, fracciones XIV, XVI y XXVI, 24, fracciones II y V del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, emite las siguientes:

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

1. Que el artículo 42, fracciones V, XX y XXI de la Ley General de Transparencia y Acceso a la Información Pública (Ley General), establece como atribuciones del Instituto, promover y difundir el ejercicio del derecho de acceso a la información; fomentar los principios de gobierno abierto, transparencia, rendición de cuentas y participación ciudadana; así como emitir recomendaciones a los sujetos obligados para diseñar, implementar y evaluar acciones de apertura gubernamental que permitan orientar las políticas internas en la materia.

2. Que el artículo 2, fracción III de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), establece como objetivo de la Ley favorecer la rendición de cuentas a los ciudadanos, de manera que puedan valorar el desempeño de los sujetos obligados.

3. Que el artículo 35, fracción V de la Ley Federal, establece como atribución del Pleno el establecer lineamientos, instrumentos, objetivos, indicadores, metas, estrategias, códigos de buenas prácticas, modelos y políticas integrales, sistemáticas, continuas y evaluables, tendientes a cumplir con los objetivos de dicha Ley.

4. Que el veintiséis de enero de dos mil diecisiete, fue publicada en el Diario Oficial de la Federación (DOF) la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), que en su artículo 2, fracción VI, establece como uno de

sus objetivos, garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales. Asimismo, en su artículo 83, párrafo segundo, señala que el Comité de Transparencia será la autoridad máxima en materia de protección de datos personales, y en el artículo 85 establece las funciones de la Unidad de Transparencia, entre las que se encuentra gestionar las solicitudes de ejercicio de los derechos vinculados con datos personales.

5. Que el artículo 131 de la Ley Federal establece que la Unidad de Transparencia será el vínculo entre los sujetos obligados y los solicitantes.

6. Que atento a lo señalado, resulta necesario asegurar la continuidad en el funcionamiento de las Unidades de Transparencia, en aquellos casos en que existan cambios en las y los Titulares de las mismas, pues con ello se garantizará el pleno goce se sus derechos a los particulares, mediante la expedición de las Recomendaciones en materia de Acceso a la Información y Datos Personales ante cambios de titulares de Unidad de Transparencia, de Comité de Transparencia y de servidores públicos a cargo del tratamiento de datos personales, conforme al documento anexo que forma parte integral del presente Acuerdo.

Por lo antes expuesto, en las consideraciones de hecho y de derecho, el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, expide el siguiente:

A C U E R D O

PRIMERO. Se aprueban las Recomendaciones en materia de Acceso a la Información y Datos Personales ante cambios de titulares de Unidad de Transparencia, de Comité de Transparencia y de servidores públicos a cargo del tratamiento de datos personales, conforme al documento anexo que forma parte integral del presente Acuerdo.

SEGUNDO. Se instruye a la Secretaría de Acceso a la Información para que, mediante las Direcciones Generales de Enlace, notifique el presente Acuerdo con su anexo correspondiente a los sujetos obligados de su competencia.

TERCERO. Se instruye a la Secretaría Técnica del Pleno para que, por conducto de la Dirección General de Atención al Pleno, realice las gestiones necesarias a efecto de que el presente Acuerdo se publique en el portal de Internet del Instituto.

CUARTO. Se instruye a la Dirección General de Asuntos Jurídicos para que realice las gestiones necesarias a efecto de que el presente Acuerdo se publique en el Diario Oficial de la Federación.

El presente acuerdo y su anexo pueden ser consultados en las direcciones electrónicas siguientes:
http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-09-2018.06.pdf
www.dof.gob.mx/2018/INAI/AcuerdosDelPleno-ACT-PUB-19-09-2018.06.pdf

Así lo acordó, por unanimidad de los Comisionados, el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en sesión ordinaria celebrada el diecinueve de septiembre de dos mil dieciocho. Los Comisionados firman al calce para todos los efectos a que haya lugar.

Francisco Javier Acuña Llamas
Comisionado Presidente

Carlos Alberto Bonnin Erales
Comisionado

Oscar Mauricio Guerra Ford
Comisionado

Blanca Lilia Ibarra Cadena
Comisionada

María Patricia Kurczyn Villalobos
Comisionada

Rosendoevgueni Monterrey Chèpov
Comisionado

Joel Salas Suárez
Comisionado

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

ACUERDO ACT-PUB/19/09/2018.06

Hugo Alejandro Córdova Díaz
Secretario Técnico del Pleno

Esta hoja pertenece al ACUERDO ACT-PUB/19/09/2018.06, aprobado por unanimidad en sesión del Pleno de este Instituto, celebrada el 19 de septiembre del 2018.

Recomendaciones en materia de Acceso a la Información y Datos Personales ante cambios de titulares de Unidad de Transparencia, de Comité de Transparencia y de servidores públicos a cargo del tratamiento de datos personales

VERSIÓN 10 DE SEPTIEMBRE DE 2018.

Contenido

GLOSARIO

Comité de Transparencia. La instancia a la que hacen referencia los artículos 43 de la Ley General de Transparencia y Acceso a la Información Pública; 83 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 64 de la Ley Federal de Transparencia y Acceso a la Información Pública.

Constitución. Constitución Política de los Estados Unidos Mexicanos.

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.

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

Dirección General de Enlace competente. Las Direcciones Generales de Enlace con Autoridades Laborales, Sindicatos, Universidades, Personas Físicas y Morales; de Enlace con la Administración Pública Centralizada y Tribunales Administrativos; de Enlace con Organismos Públicos Autónomos, Empresas Paraestatales, Entidades Financieras, Fondos y Fideicomisos; de Enlace con los Poderes Legislativo y Judicial, o de Enlace con Partidos Políticos, Organismos Electorales y Descentralizados, según corresponda, del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

DOF: El Diario Oficial de la Federación.

INAI o Instituto: El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Ley Federal de Transparencia: La Ley Federal de Transparencia y Acceso a la Información Pública.

Ley General de Protección de Datos Personales: La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Ley General de Transparencia: La Ley General de Transparencia y Acceso a la Información Pública.

Lineamientos Generales de Datos Personales: Los Lineamientos Generales de Protección de Datos Personales del Sector Público.

Recomendaciones: Las presentes Recomendaciones en materia de Acceso a la Información y Datos Personales ante cambios de titulares de Unidad de Transparencia, de Comité de Transparencia y de servidores públicos a cargo del tratamiento de datos personales.

Responsable: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, en el ámbito federal, que decida sobre el tratamiento de datos personales. Un Responsable es un sujeto obligado.

Sujetos obligados: Cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal.

Sujetos obligados indirectos: Sujetos obligados que cumplen sus obligaciones a través del sujeto obligado responsable de coordinar su operación.

Titular: La persona física a quien corresponden los datos personales.

Tratamiento de datos personales: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Titular de la Unidad de Transparencia. Persona designada como responsable de la instancia a la que hacen referencia los artículos 45 de la Ley General de Transparencia y Acceso a la Información Pública; 85 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 61 de la Ley Federal de Transparencia y Acceso a la Información Pública.

PRESENTACIÓN

Con fundamento en los artículos 37 de la Ley General de Transparencia; 17 y 21, fracción VII, de la Ley Federal de Transparencia; y 89, fracciones I, XII y XIII de la Ley General de Protección de Datos Personales, el INAI pone estas recomendaciones a disposición de los sujetos obligados/Responsables que realicen cambios en el personal adscrito al Comité y Unidad de Transparencia o que estén a cargo de bases de datos personales, con el objetivo de que se identifiquen, por una parte, los elementos mínimos que permitan dar continuidad a la operación de estas instancias y, por otra, las acciones que resultan relevantes para que el tratamiento de datos personales ocurra de manera ordenada y conforme a lo que establece la ley, a fin de garantizar, en todo momento, el ejercicio de los derechos de acceso a la información y protección de datos personales, establecidos en los artículos 6 y 16 de la Constitución.

Resulta conveniente destacar que de conformidad con las funciones establecidas para el Comité y la Unidad de Transparencia, en los artículos 43, 44 y 45 de la Ley General de Transparencia; 61 y 65 de la Ley Federal de Transparencia, y 83, 84 y 85 de la Ley General de Protección de Datos Personales, el Comité de Transparencia es el responsable de coordinar y vigilar el cumplimiento de las obligaciones en materia de acceso a la información y protección de datos personales al interior de la organización del sujeto obligado/Responsable, y en particular la Unidad de Transparencia es el vínculo entre éste y los solicitantes o Titulares de los datos personales. De ahí la importancia de asegurar su debida operación a fin de que no se vea afectado el ejercicio de estos derechos humanos.

Las Recomendaciones están dirigidas tanto a los integrantes y servidores públicos que concluyen su función en el Comité o Unidad de Transparencia o a cargo de bases de datos personales, como a aquéllos que inicien sus funciones en estas áreas, con los siguientes objetivos:

1. Que los integrantes y servidores públicos de los sujetos obligados que concluyen su encargo como Titulares de las Unidades de Transparencia o como integrantes del Comité de Transparencia reconozcan sus obligaciones;
2. Que aquéllos que lo inician identifiquen la información que deberán recibir y las medidas que deberán tomar o solicitar para cumplir con las obligaciones en materia de acceso a la información y transparencia;
3. Que el manejo de los datos personales ocurra de manera adecuada en la entrega-recepción; y
4. Que no se interrumpa el ejercicio de los derechos de acceso a la información y de protección de datos personales.

En ese sentido, dado que su contenido se centra en los objetivos antes planteados, las Recomendaciones no abarcan de manera completa cada una de las obligaciones que establece la normativa de acceso a la información, ni la de datos personales.

No obstante, si desea conocer con mayor detalle las obligaciones que surgen de la Ley General de Protección de Datos Personales y los Lineamientos Generales de Datos Personales, así como las acciones que se reconocen como necesarias para su cumplimiento, lo invitamos a consultar el *Documento orientador para la elaboración del Programa de Protección de Datos Personales*, que se encuentra disponible en el portal de Internet del INAI (www.inai.org.mx), en la sección de "Protección de Datos Personales", subsección "Sector Público" (http://inicio.ifai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m4).

Asimismo, para conocer de las obligaciones que derivan de la Ley General y de la Ley Federal de Transparencia, se pone a su disposición la *Guía del Sistema de Portales de Obligaciones de Transparencia* (https://cevinai-snt.inai.org.mx/cursos/sipot_2.1/guia_sipot_v_2.html) y el documento denominado *Procedimiento para la Atención de Solicitudes de Acceso a la Información* (http://inicio.inai.org.mx/doc/SAI/Publicaciones/folleto.pdf).

Por otro lado, es necesario indicar que, en caso de que el sujeto obligado/Responsable tenga a su cargo a algún sujeto obligado indirecto, debe contemplar entregar la información que se presenta en estas recomendaciones, de manera separada por cada uno de este tipo de sujetos obligados, a fin de poder proporcionar las documentales de manera clara y precisa.

Para finalizar esta presentación, es importante señalar que estas recomendaciones tienen un carácter orientador, por lo que no son vinculantes o de observancia obligatoria.

1. Recomendaciones generales en materia de acceso a la información y protección de datos personales

El presente apartado tiene como objetivo identificar la información y documentos mínimos que se deberán entregar cuando haya cambios de personal adscrito al Comité o Unidad de Transparencia o de servidores públicos a cargo de bases de datos personales, los cuales pueden ser parte de los archivos y de la documentación soporte de los datos e información que se proporcionen en los informes y actas administrativas, y al estar relacionados con las facultades o atribuciones que por normatividad competan a la institución o, en su caso, al servidor público que concluye el empleo.

En primera instancia, es importante señalar que los titulares del Comité de Transparencia y de la Unidad de Transparencia que concluyan su encargo en dichas áreas deberán entregar, a quien reciba el encargo, todos los registros, documentación y archivos, en el medio en el que se encuentren (físico o electrónico), que tenga en su posesión y/o hayan generado con motivo de su designación.

La información deberá estar debidamente relacionada, ordenada y catalogada, y en aquellos casos en que ésta se encuentre clasificada como reservada o confidencial, tal circunstancia se deberá identificar de manera clara, mediante una carátula en donde se especifique que contiene partes o secciones reservadas o confidenciales, conforme a la normatividad aplicable.

Para que los registros, documentación y archivos que se entreguen estén completos y la información sea oportuna y accesible, se recomienda que se incluya, cuando menos, la siguiente información:

- Catálogo de la normatividad vigente en materia de transparencia, acceso a información pública y protección de datos personales, con un respaldo de los documentos en versión electrónica;
- Catálogo de la normatividad interna expedida en materia de transparencia, acceso a la información y protección de datos personales. (En caso de que se haya emitido este tipo de normatividad);
- Relación de usuarios y contraseñas para la operación de la Plataforma Nacional de Transparencia, del Sistema Infomex Gobierno Federal y de la Herramienta de Comunicación;
- Indicar si tiene a su cargo sujetos obligados indirectos y, en su caso, otorgar las claves de acceso que correspondan;
- Calendario, minutas y/o actas de las sesiones del Comité de Transparencia;
- Personal adscrito al Comité y Unidad de Transparencia y a las oficinas de atención al público;

- Responsables designados de cada área del sujeto obligado/Responsable ante la Unidad de Transparencia, con los datos de contacto institucional correspondientes, para atender los distintos asuntos de su competencia;
- Consultas o solicitudes realizadas al Instituto y que se encuentren en proceso de atenderse, señalando la fecha en que se realizó y ante quién se presentó;
- Indicar si se encuentra en proceso de auditoría, por parte del Órgano de Control Interno, instancia homóloga, o alguna entidad externa, y señalar los antecedentes, estado u observaciones realizadas a la auditoría en materia de transparencia;
- Proyectos interinstitucionales en materia de acceso a la información, protección de datos personales, transparencia y rendición de cuentas que se encuentran en proceso por parte del sujeto obligado/Responsable;
- Convenios de colaboración en materia de acceso a la información, protección de datos personales, transparencia y rendición de cuentas que haya celebrado el sujeto obligado/Responsable y que se encuentren vigentes;
- Relación de archivos de trámite, concentración e histórico, en su caso, a cargo del Comité o Unidad de Transparencia, según sea el caso;
- Direcciones de correos electrónicos institucionales, no asociados a un determinado integrante del sujeto obligado/Responsable, que se encuentren habilitados para dar atención al público, o bien, para recibir notificaciones ante el Instituto, así como las contraseñas para su acceso, y
- Cualquier otro asunto que se encuentre en trámite en materia de transparencia, políticas de acceso, gobierno abierto, acceso a la información y de protección de datos personales.

Asimismo, es importante que la Unidad de Transparencia cuente, en todo momento, con acceso a los sistemas administrados por el Instituto, para lo cual se recomienda que se notifique a la Dirección General de Enlace correspondiente, el nombramiento del nuevo Titular de la Unidad de Transparencia o, en su caso, el nombre de la persona encargada del despacho o designada en el periodo de transición.

Lo anterior a fin de que el Instituto pueda gestionar las nuevas claves de acceso del sujeto obligado/Responsable a los sistemas administrados por el INAI, y éste pueda proceder a cancelar las anteriores, para garantizar la seguridad en el acceso a los sistemas y por tanto de la información ahí contenida, de manera oportuna.

También, es recomendable que se notifique a la Dirección General de Enlace correspondiente del INAI cualquier cambio en la integración del Comité de Transparencia.

1.1 Solicitudes de acceso a la información y de datos personales

Con el objeto de garantizar la atención oportuna a las solicitudes presentadas ante los sujetos obligados/Responsables, es importante que se considere la entrega de una relación de las solicitudes electrónicas y manuales que se encuentren en proceso de atención, o bien, si se encuentran en plazo para ser impugnadas ante el INAI. En dicha relación es necesario que se

distinga si son en materia de información pública, o de acceso, rectificación, cancelación, oposición o portabilidad de datos personales.

Se recomienda que en la relación se señale, al menos, lo siguiente:

- Folio de la solicitud;
- Tipo de solicitud (acceso o datos personales);
- Tema de la solicitud (en su caso, resumen de la solicitud);
- Tipo de derecho ejercido, en el caso de datos personales (acceso, rectificación, cancelación, oposición o portabilidad);
- Fecha oficial de recepción;
- Estatus (Pendiente de respuesta / Con requerimiento de información adicional / En trámite / Con Prórroga / Terminada);
- Fecha límite de respuesta;
- Posibilidad de prórroga;
- Área o áreas a las que fue turnada para su atención, y
- Cualquier otro asunto relacionado.

1.2 Recursos de revisión ante el INAI

A efecto de atender oportunamente los medios de impugnación en trámite ante el Instituto, tanto en materia de acceso a la información, como de datos personales, se recomienda entregar un listado de los recursos interpuestos en contra del sujeto obligado/Responsable, en el cual se señale, por lo menos, la siguiente información:

- El número de expediente;
- La fecha oficial de notificación de la admisión;
- Fecha límite para remitir alegatos;
- El estado procesal en el que se encuentra;
- Ponencia bajo la cual se substancia el recurso;
- La materia sobre la que versa;
- El área o áreas responsables de darle seguimiento, así como a los servidores públicos responsables en lo específico;
- Los requerimientos realizados por el Instituto;
- La fecha límite para atender los requerimientos del Instituto;
- Fecha para celebración de audiencia (en caso de haberse señalado por la ponencia);
- Fecha de votación de resolución por parte del Pleno del Instituto;
- Estatus del cumplimiento;
- Fecha límite de cumplimiento;
- En los casos de incumplimientos, la fecha límite para dar atención a los requerimientos derivados de tal incumplimiento, y
- Cualquier otra información que se estime relevante.

Asimismo, se sugiere entregar un listado detallado sobre las medidas de apremio y sanciones impuestas por causas relacionadas con solicitudes de información y/o recursos de revisión, establecidas en la Ley General de Transparencia, Ley Federal de Transparencia y Ley General de Datos Personales, así como el estatus de cada una de ellas.

1.3 Informe anual

Se recomienda que la Unidad de Transparencia documente todos aquellos datos necesarios para que el Comité de Transparencia entregue al Instituto la información correspondiente para la elaboración del Informe Anual, de conformidad con lo establecido en los *Lineamientos para recabar la información de los sujetos obligados que permitan elaborar los informes anuales*, de conformidad con lo que establece el artículo 44 fracción VII de la Ley General de Transparencia.

1.4 Imposición de medidas de apremio y sanciones

Se recomienda entregar un listado de las medidas de apremio y sanciones impuestas por cualquier causa de sanción por incumplimiento de las obligaciones establecidas en la materia de la Ley General de Transparencia, Ley Federal de Transparencia y Ley General de Protección de Datos Personales, así como de aquellos procedimientos que se encuentren en trámite, precisando lo siguiente:

- Servidor Público o miembros del sujeto obligado encargado de cumplir con la resolución;
- Fecha de la resolución;
- Medida de apremio impuesta;
- Monto total de la multa (en su caso);
- Estatus del procedimiento;
- Sanciones determinadas;
- Causas de las sanciones o medidas de apremio;
- Servidores públicos o miembros del sujeto obligado apremiados o sancionados;
- Nombre de la autoridad competente a la que se denunció (en su caso);
- Última actuación del sujeto obligado y del Instituto; y
- Los requerimientos formulados y los pendientes de atención, notificados por parte del INAI.

2. Recomendaciones específicas en materia de Acceso a la Información

2.1 Obligaciones de transparencia

De conformidad con la Ley General de Transparencia y Ley Federal de Transparencia, los sujetos obligados pondrán a disposición del público y mantendrán actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, documentos y políticas que se señalan como obligaciones de transparencia comunes y específicas.

Con la finalidad de que la Unidad de Transparencia mantenga publicada y actualizada las obligaciones correspondientes, se sugieren las siguientes acciones:

a. Indicar la relación de obligaciones de transparencia que correspondan al artículo 70 de la Ley General de Transparencia, de conformidad con la Tabla de Aplicabilidad aprobada por el Pleno del Instituto, así como aquellas obligaciones de transparencia específicas que el sujeto obligado deba de cumplir, en términos de la normatividad aplicable, debiéndose señalar la fecha límite de la próxima actualización de la información por cada fracción.

b. Documentar el estado que guarda el cumplimiento de las obligaciones de transparencia establecidas tanto en la Ley General de Transparencia como en la Ley Federal de Transparencia, en la Plataforma Nacional de Transparencia y en su portal de Internet.

c. Informar si se cumple con las obligaciones de transparencia directamente en su portal de internet, o bien, si se cuenta con un vínculo de remisión al Sistema de Portales de Obligaciones de Transparencia de la Plataforma Nacional de Transparencia.

d. Señalar las obligaciones de transparencia que se encuentran asignadas a cada unidad administrativa para su cumplimiento en el Sistema de Portales Obligaciones de Transparencia en la Plataforma Nacional de Transparencia.

A. Verificación

Los Organismos garantes vigilarán que las obligaciones de transparencia que publiquen los sujetos obligados cumplan con lo dispuesto en la Ley General de Transparencia, en la Ley Federal de Transparencia y en los Lineamientos técnicos generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia, por lo que realizarán verificaciones que revisen y constaten el debido cumplimiento de la normatividad en la materia, por lo que la Unidad de

Transparencia deberá entregar el último reporte de cumplimiento a las Obligaciones de Transparencia, así como los resultados de las verificaciones emitidas por el INAI.

Se recomienda también que se indique si el INAI notificó alguna observación, recomendación o requerimiento respecto a alguna verificación que se encuentre en trámite, así como el plazo que se tiene para cumplir.

Asimismo, resulta importante que se proporcione un listado con los usuarios y áreas al interior que tienen asignada cada una de las fracciones aplicables que le corresponde al sujeto obligado.

B. Denuncia

De conformidad con los artículos 89 de la Ley General de Transparencia y 81 de la Ley Federal de Transparencia, cualquier persona podrá denunciar las violaciones a las disposiciones relativas a las obligaciones de transparencia previstas en los artículos 70 a 83 de la Ley General de Transparencia y 68 a 76 de la Ley Federal de Transparencia.

En este sentido, se sugiere entregar una relación de las denuncias en trámite presentadas ante el sujeto obligado por incumplimiento a las obligaciones de transparencia, en la que se señale, al menos, lo siguiente:

- Número de la denuncia;
- Incumplimiento denunciado, señalando artículo fracción y/o en su caso criterio;
- Fecha oficial de recepción;
- Estado procesal incluyendo la Dirección General responsable del trámite;
- Fecha límite para atender los requerimientos realizados por el Instituto;
- Área o áreas turnada para su atención;
- Fecha de votación;
- Estatus de cumplimiento;
- Fecha límite para su cumplimiento;
- Precisar si alguna denuncia se notificó al superior jerárquico del área responsable, y
- Cualquier otro asunto relacionado.

C. Incumplimiento a las obligaciones de transparencia

Entregar un listado de los procedimientos por incumplimiento a las obligaciones de transparencia que se encuentren en proceso de cumplimiento, en el que se señale, al menos, lo siguiente:

- Precisar el procedimiento que derivó en incumplimiento (Denuncia / Verificación);
- Número de expediente;

- Fecha oficial de recepción;
- Estado procesal;
- Fecha límite para atender los requerimientos o cumplimientos realizados por el Instituto;
- Área o áreas a las que se turnó para su atención, y
- Cualquier otro asunto relacionado.

Asimismo, se deberá entregar un listado de las medidas de apremio y sanciones impuestas por causas relacionadas con publicación de obligaciones de transparencia, establecidas en la Ley General de Transparencia y Ley Federal de Transparencia.

2.2 Índice de Expedientes Clasificados como Reservados

De conformidad con los artículos 102 de la Ley General de Transparencia y 101 de la Ley Federal de Transparencia, cada área de los sujetos obligados elaborará un índice de los expedientes clasificados por el Comité de Transparencia como reservados, por área responsable de la información y tema, mismo que deberá elaborarse semestralmente y publicarse en Formatos Abiertos al día siguiente de su elaboración.

En este sentido, deberá entregarse el soporte documental del Índice de Expedientes Clasificados como Reservados reportados al Instituto del semestre inmediato anterior; así como del reporte del estado que guarda la información en el mismo por área, de acuerdo con las características que señalan los *Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas*, mismas que se mencionan a continuación:

- El área que generó, obtuvo, adquirió, transformó y/o conserve la información;
- El nombre del documento;
- Fracción de la ley que da origen a la reserva;
- La fecha de clasificación;
- Razones y motivos de la clasificación;
- Señalar si se trata de una clasificación completa o parcial;
- En caso de ser parcial, las partes del documento que son reservadas;
- En su caso, la fecha del acta en donde el Comité de Transparencia confirmó la clasificación;
- El plazo de reserva y si se encuentra o no en prórroga;
- La fecha en que culmina el plazo de la clasificación, y
- Las partes o secciones de los expedientes o documentos que se clasifican.

3. Recomendaciones en materia de Datos Personales[1]

3.1 Documentos generados a partir de las obligaciones específicas en materia de datos personales

La Ley General de Protección de Datos Personales y los Lineamientos Generales de Datos Personales establecen como parte de las obligaciones de los Responsables la elaboración de diversos documentos o la realización de acciones que deben estar documentadas, encaminados a garantizar un tratamiento adecuado de los datos personales.

En esta sección se identifican los documentos principales que se generan en cumplimiento de la normatividad en materia de datos personales, a fin de que sean considerados en los registros y archivos del acta de entrega-recepción del Comité y Unidad de Transparencia y de las áreas que tienen a su cargo bases de datos personales.

De manera previa, se considera importante enlistar los instrumentos que regulan este derecho en el sector público federal, a fin de identificarlos como parte del marco normativo aplicable a las dependencias, entidades y empresas productivas del Estado:

1. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el DOF el 26 de enero de 2017;
2. Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el DOF el 26 de enero de 2018;
3. Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal, publicados en el DOF el 23 de enero de 2018;
4. Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, publicadas en el DOF el 23 de enero de 2018, y
5. Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, publicados en el Diario Oficial de la Federación el 12 de febrero de 2018.

Asimismo, los Responsables pudieron haber generado normatividad interna específica para regular los procesos propios de la institución en materia de datos personales, la cual, en caso de haberse generado, también deberá tomarse en cuenta e incluirse como parte del marco normativo aplicable a la institución.

[1] Es importante señalar que, de conformidad con el párrafo sexto del artículo primero de la Ley General de Protección de Datos Personales, los sindicatos serán responsables de los datos personales de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares, por lo que este apartado no le es aplicable.

Dicho lo anterior, a continuación, se describirán los documentos básicos que se generan en cumplimiento de la Ley General de Protección de Datos Personales y los Lineamientos Generales de Datos Personales.

A. Obligaciones específicas del Comité y de la Unidad de Transparencia

De conformidad con el artículo 83 de la Ley General de Protección de Datos Personales, el Comité de Transparencia es la máxima autoridad en materia de protección de datos personales al interior de la organización del Responsable, y -de conformidad con el artículo 84 de la Ley en cita- tiene a su cargo las siguientes funciones:

I. Coordinar, supervisar y realizar 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 esa ley y en aquellas disposiciones que resulten aplicables en la materia;
II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
III. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;
IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de esa ley y en aquellas disposiciones que resulten aplicables en la materia;
V. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;
VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto;
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; particularmente en casos relacionados con la declaración de inexistencia que realicen los Responsables.

Por su parte, de acuerdo con lo establecido en el artículo 85 de la Ley General de Protección de Datos Personales, la Unidad de Transparencia es la encargada de coordinar lo relativo a las solicitudes de ejercicio de los derechos ARCO y, en ese sentido, tiene las siguientes funciones:

I. Auxiliar y orientar al Titular 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 solo 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, y
VII. Asesorar a las áreas adscritas al Responsable en materia de protección de datos personales.

En algunos casos, el Responsable pudo haber designado a un oficial de protección de datos personales, especializado en la materia, quien estaría a cargo de las funciones de la Unidad de Transparencia y formaría parte de ésta.

Asimismo, el artículo 85, último párrafo, de la Ley en cita señala que los sujetos obligados promoverán acuerdos con instituciones públicas especializadas que pudieran auxiliarles a la recepción, trámite y entrega de las respuestas a solicitudes de información, en la lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente.

A partir de lo anterior, se advierte que en la entrega de la información relativa al Comité de Transparencia se tendría que incluir, al menos, lo siguiente:

1. Procedimientos internos que en su caso se hubieran desarrollado para atender con mayor eficiencia las solicitudes de ejercicio de los derechos ARCO y de portabilidad;
2. Actas de las sesiones del Comité en las que haya confirmado, modificado o revocado la inexistencia de los datos personales solicitados o la negativa de ejercicio de alguno de los derechos ARCO o portabilidad;
3. Los criterios específicos que en su caso se hayan desarrollado para una mejor observancia de la normatividad de datos personales;
4. La documentación generada en las actividades que en su caso se hubieran realizado para vigilar el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;
5. La documentación generada en torno al seguimiento y cumplimiento de las resoluciones que en su caso haya emitido el INAI;
6. Los programas de capacitación y actualización de los servidores públicos en materia de datos personales, así como la evidencia de implementación de los mismos, y
7. Las vistas que haya dado al Órgano Interno de Control o instancia equivalente por presuntas irregularidades en el tratamiento de datos personales.

En cuanto a la Unidad de Transparencia, se pude observar que en la entrega correspondiente se tendría que incluir, al menos, la siguiente información:

1. Los documentos generados en torno a las gestiones de las solicitudes de ejercicio de derechos ARCO y portabilidad;
2. Los procedimientos internos que en su caso se hayan desarrollado para una mayor eficiencia en la gestión de las solicitudes de derechos ARCO y portabilidad, así como los mecanismos para garantizar que los datos personales se entreguen sólo a su titular o representante;
3. Los instrumentos desarrollas para evaluar la calidad sobre la gestión de las solicitudes, así como los resultados de las evaluaciones que en su caso se hayan practicado;
4. La designación, en su caso, del oficial de protección de datos personales;
5. Los acuerdos que en su caso se hayan firmado con instituciones públicas especializadas que pudieran auxiliarles a la recepción, trámite y entrega de las respuestas a las solicitudes en lengua indígena, braille o cualquier otro formato accesible, y
6. Información respecto de las asesorías que, en su caso, haya prestado a las unidades administrativas del sujeto obligado.

B. Inventario de datos personales

La protección integral de los datos personales requiere que el Responsable tenga documentado e identificado el ciclo de vida de los datos personales, así como las principales acciones que ocurren en sus distintas etapas.

Este inventario sirve de diagnóstico sobre los distintos tratamientos de datos personales que ocurren al interior de una organización.

Por "inventario" entenderemos el control documentado que se llevará del tratamiento que realizan las unidades administrativas dentro de los procesos o procedimientos que realicen en ejercicio de sus atribuciones.

El inventario de datos personales está previsto en los artículos 33, fracción III, 35, fracción I de la Ley General, y 58 de los Lineamientos Generales, que establecen lo siguiente:

Ley General:

> *Artículo 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *[...]*
> *III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;*
> *[...]*
>
> *Artículo 35. De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*
> *I. El inventario de datos personales y de los sistemas de tratamiento;*
> *[...]*

Lineamientos Generales:

Inventario de datos personales
Artículo 58. Con relación a lo previsto en el artículo 33, fracción III de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:

I. *El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;*
II. *Las finalidades de cada tratamiento de datos personales;*
III. *El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;*
IV. *El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;*
V. *La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;*
VI. *En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y*
VII. *En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.*

Este inventario identifica y documenta información clave sobre el tratamiento de datos personales, entre ella:

- ¿Qué tratamientos de datos personales realiza la unidad administrativa?
- ¿Qué unidad administrativa está a cargo de estos procesos y que por tanto sea la administradora de las bases de datos o archivos que se generen con motivo de dichos tratamientos?
- ¿Cómo se obtienen los datos personales?
- ¿Qué tipo de datos personales se tratan? ¿son sensibles?
- ¿Dónde se almacenan y realiza el tratamiento de los datos personales?
- ¿Para qué finalidades se utilizan los datos personales?
- ¿Quién tiene acceso a la base de datos o archivos (sistemas de tratamiento) y a quién se comunican los datos personales al interior de la organización del Responsable?
- ¿Intervienen Encargados en el tratamiento de los datos personales?
- ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?
- ¿Se difunden los datos personales?
- ¿Cuál es el plazo de conservación de los datos personales?

En ese sentido, el inventario de datos personales es uno de los documentos principales para conocer los tratamientos de datos personales que realiza cada Responsable, así como sus características generales. A partir del diagnóstico o radiografía que ofrece el inventario, el Responsable puede desarrollar un programa para cumplir con las distintas obligaciones que tiene en materia de protección de datos personales y elaborar otros documentos como los avisos de privacidad y el documento de seguridad.

Es por ello que resulta de suma importancia que el inventario de datos personales se incluya entre la información a entregar por parte del titular del Comité de Transparencia, en caso de que dicho titular concluya su encargo.

C. Avisos de privacidad y medidas compensatorias

De conformidad con los artículos 26 de la Ley General de Protección de Datos Personales y 26 de los Lineamientos Generales de Datos Personales, los Responsables deben informar al Titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, con independencia de que se requiera o no el consentimiento para que éste ocurra.

Asimismo, los Responsables deben elaborar los avisos de privacidad en su versión integral y simplificada, con la información que señalan los artículos 27 y 28 de la Ley General de Protección de Datos Personales, los Lineamientos Generales de Datos Personales y el artículo 11 de los Lineamientos que Establecen los Parámetros, Modalidades y Procedimientos para la Portabilidad de Datos Personales, y ponerlos a disposición en medios físicos y electrónicos.

Los avisos de privacidad son otros de los documentos fundamentales que se generan en torno a las obligaciones de protección de datos personales, ya que a través de éstos se pueden conocer las condiciones bajo las cuales el Titular y el Responsable acordaron el tratamiento de los datos personales, por lo que éstos deberían ser incluidos en las actas entrega-recepción de los servidores públicos que concluyan su empleo y que hayan tenido a su cargo la administración de bases de datos personales.

Es importante señalar que los avisos de privacidad se generan por cada uno de los tratamientos que realiza el Responsable, por lo que una misma dependencia, entidad o empresa productiva del Estado puede tener más de un aviso de privacidad. Asimismo, dado que los avisos de privacidad describen de manera general las características del tratamiento al que refieren, lo deseable y común es que sean elaborados por las unidades administrativas que están a cargo del proceso o procedimiento bajo el cual se tratan los datos personales.

Por ello, se considera conveniente que los avisos de privacidad sean incluidos en la entrega del servidor público que concluye el empleo y que tuvo a su cargo el tratamiento de datos personales como ejercicio de sus atribuciones.

Lo anterior con independencia de que el Comité de Transparencia pueda entregar una relación o la totalidad de avisos de privacidad con que cuenta el Responsable, en caso de que hubiera cambio en alguno de su titular y de que cuente con dicha información.

En cuanto a las medidas compensatorias, el artículo 26, último párrafo, de la Ley General de Protección de Datos Personales establece que cuando resulte imposible dar a conocer al Titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, el Responsable podrá instrumentar medidas compensatorias de comunicación masiva de

acuerdo con los criterios que para tal efecto emita el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Al respecto, en caso de que el Responsable haya aplicado medidas compensatorias o solicitado al INAI la autorización para su implementación, sería conveniente que incluya la documentación correspondiente en la entrega del servidor público a cargo del tratamiento de datos personales.

Lo anterior con independencia de que el Comité de Transparencia pueda entregar una relación o la totalidad de medidas compensatorias con que cuenta el Responsable, en caso de que hubiera cambio en su titular y de que cuente con dicha información.

Por último, es importante señalar que de conformidad con el artículo 45 de los Lineamientos Generales de protección de datos personales, la carga de la prueba para acreditar la puesta a disposición del aviso de privacidad recaerá en el Responsable, por lo que resulta también importante que en caso de que esto se encuentre documentado, se incluya en la entrega correspondiente del servidor público a cargo del tratamiento que concluye su empleo.

D. Documento de seguridad

De conformidad con el artículo 35 de la Ley General de Protección de Datos Personales, los Responsables deberán elaborar un documento de seguridad que contenga, al menos, 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, y
VII. El programa general de capacitación.

En ese sentido, en caso de que existiera un cambio de titular del Comité de Transparencia, sería conveniente que incluyera en su entrega el documento de seguridad del Responsable con cada uno de los siete elementos antes señalados, así como sus actualizaciones en caso de que éstas existieran.

E. Bitácora y notificación de vulneraciones

De conformidad con el artículo 39 de la Ley General de Protección de Datos Personales, los Responsables deberán llevar una bitácora de las vulneraciones a la seguridad que hayan ocurrido, en la que se describan en qué consistió la vulneración, la fecha en la que ocurrió, el motivo o causa de la vulneración, y las acciones correctivas implementadas de forma inmediata y definitiva.

Asimismo, el artículo 40 de la Ley General de Protección de Datos Personales señala que los Responsables deberán informar al Titular y al Instituto las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales.

En ese sentido, en caso de que hubieran ocurrido vulneraciones a la seguridad de los datos personales en la organización del Responsable, por una parte, el Comité de Transparencia tendría que incluir en su entrega las bitácoras correspondientes y el servidor público que estuvo a cargo de la base de datos vulnerada que concluya el encargo, tendrían que incluir en su entrega las constancias de las notificaciones a los Titulares y al INAI.

La creación de bitácoras y la notificación de vulneraciones no deberían ser procesos aislados, sino formar parte del plan de respuesta a incidentes de la organización, por ello, es aconsejable consultar las Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales, elaboradas por el INAI y disponibles en: http://inicio.ifai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

F. Procedimientos para el bloqueo, supresión y conservación de datos personales

De acuerdo con los artículos 24 de la Ley General de Protección de Datos Personales y 23 de los Lineamientos Generales de Datos Personales, los Responsables deberán establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleven a cabo, en los cuales se incluyan los periodos de conservación de los mismos.

En ese sentido, el Comité de Transparencia tendría que incluir en su entrega los procedimientos de conservación, bloqueo y supresión de los datos personales, con el periodo de conservación respectivo.

G. Consentimientos otorgados y revocaciones

De conformidad con el artículo 20 de la Ley General de Protección de Datos Personales, cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de dicha ley, el Responsable deberá contar con el consentimiento previo del Titular para el tratamiento de los datos personales.

Asimismo, el artículo 65 de la Ley General de Protección de Datos Personales establece que las transferencias de datos personales, nacionales e internacionales, están sujetas al consentimiento del Titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de esa ley.

El consentimiento para el tratamiento y transferencias podrá otorgarse de forma tácita o explícita, según los datos personales que se vayan a tratar, es decir, si son sensibles o no.

El consentimiento será tácito cuando habiéndose puesto a disposición del Titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario. En ese sentido, lo que se

documenta en este caso es la negativa del consentimiento o la puesta a disposición del aviso de privacidad.

El consentimiento será expreso cuando la voluntad del Titular se manifieste de forma verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología. En este caso lo que se documenta es el consentimiento mismo otorgado por el Titular.

En ese sentido, en caso de que alguno de los tratamientos o transferencias que realice el Responsable requiera el consentimiento de los Titulares, la obtención del mismo debió ser documentada y por tanto debe incluirse en la entrega del servidor público que tuvo a su cargo el tratamiento respectivo, a fin de que el servidor público que asuma el encargo pueda realizar el tratamiento de los datos personales conforme a lo que establece la norma.

Por su parte, el artículo 20 de los Lineamientos Generales de Datos Personales señalan que, en cualquier momento, el Titular podrá revocar el consentimiento que ha otorgado para el tratamiento de sus datos personales sin que se le atribuyan efectos retroactivos a la revocación, a través del ejercicio de los derechos de cancelación y oposición.

De igual forma, es importante que las revocaciones del consentimiento estén debidamente documentadas y se entreguen en el acta respectiva.

Tanto lo relativo al consentimiento como a su revocación se considera que deben ser reportados por el servidor público que estuvo a cargo del tratamiento respectivo, pues se asume que la unidad administrativa o área a su cargo debió recabar los consentimientos requeridos por la norma, para operar el programa, actividad o política pública correspondiente.

H. Transferencias de datos personales

Por transferencia se entiende toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del Responsable o del Encargado. Las transferencias no abarcan las remisiones de datos personales, que son las comunicaciones de datos personales realizadas exclusivamente entre el Responsable y Encargado, dentro o fuera del territorio mexicano, ni incluye el intercambio de información entre las unidades administrativas del propio sujeto obligado.

De acuerdo con lo dispuesto por el artículo 66 de la Ley General de Protección de Datos Personales, toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al Responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes, salvo las propias excepciones que establece el artículo en mención.

En ese sentido, otro de los documentos a entregar por parte de los servidores públicos que concluyan en su empleo y que hayan tenido a su cargo tratamientos de datos personales, son los instrumentos mediante los cuales se hayan formalizado las transferencias de datos personales nacionales e internacionales, en caso de que éstos existan por no actualizarse las causales de excepción previstas en el último párrafo del artículo 66 de la Ley General de Protección de Datos Personales.

Lo anterior con independencia de que el Comité de Transparencia pueda entregar una relación o la totalidad de instrumentos de transferencias con que cuenta el Responsable, en caso de que hubiera cambio en su titular y de que éste cuente con dicha información.

I. Relación con Encargados

La fracción XV del artículo 3 de la Ley General de Protección de Datos Personales define al Encargado como la persona física o moral, 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.

En cuanto a la relación entre el Responsable y el Encargado, la Ley General de Protección de Datos Personales establece en su artículo 59 que ésta deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el Responsable, de conformidad con la normativa que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido.

En el contrato o instrumento jurídico que decida el Responsable se deberán prever, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el Encargado:

I. Realizar el tratamiento de los datos personales conforme a las instrucciones del Responsable;
II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Responsable;
III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
IV. Informar al Responsable 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 Responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y
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.

Asimismo, el artículo 64 de la Ley General de Protección de Datos Personales establece una serie de condiciones para el tratamiento de datos personales en servicios, aplicaciones e

infraestructura de cómputo en la nube y otras materias, en los que el Responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación.

A partir de lo anterior, el servidor público que haya estado a cargo de tratamientos en los que exista una relación con Encargados, y aquél a cargo de la contratación de servicios de cómputo en la nube en la organización del Responsable, que vayan a terminar su encargo, tendrían que incluir en su entrega la relación de los instrumentos jurídicos que regulan la relación con los Encargados y, en su caso, los documentos mismos.

Lo anterior con independencia de que el Comité de Transparencia pueda entregar una relación o la totalidad de los instrumentos que regulan las relaciones con Encargados con que cuenta el Responsable, en caso de que hubiera cambio en su titular y de que éste cuente con dicha información.

J. Programa y políticas internas de protección de datos personales

De conformidad con el artículo 30, fracción II, y 33, fracción I de la Ley General de Protección de Datos Personales, los Responsables deberán elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de su organización.

Por su parte, el segundo párrafo del artículo 47 de los Lineamientos Generales de Datos Personales señala que estas políticas y programas deberán ser aprobados, coordinados y supervisados por su Comité de Transparencia.

Asimismo, el artículo 56 de los Lineamientos Generales de Datos Personales define el contenido de estas políticas y programas internos, de la siguiente forma:

I. El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General y los Lineamientos generales;
II. Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen;
III. Las sanciones en caso de incumplimiento;
IV. 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;
V. El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales, y
VI. El proceso general de atención de los derechos ARCO.

En ese sentido, en caso de que hubiera un cambio en el titular del Comité de Transparencia, éste tendría que incluir en su entrega el programa o política de protección de datos personales de la dependencia, entidad o empresa productiva del Estado que corresponda.

K. Evaluaciones de impacto en la protección de datos personales

De conformidad con el artículo 74 de la Ley General de Protección de Datos Personales, cuando el Responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esa ley impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una Evaluación de impacto en la protección de datos personales, y presentarla ante el Instituto, en los términos establecidos en las *Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales*, el cual podrá emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

En ese sentido, en caso de que se hubiera realizado una Evaluación de impacto en la protección de datos personales, el Comité de Transparencia o el servidor público a cargo del tratamiento respectivo que concluya el encargo, según se haya establecido en el procedimiento interno en la organización del Responsable, tendrían que incluir en su entrega la documentación generada en torno a la evaluación en cuestión.

L. Esquemas de mejores prácticas

El artículo 72 de la Ley General de Protección de Datos Personales señala que, para el cumplimiento de las obligaciones previstas en esa ley, el Responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros Responsables, Encargados u organizaciones, esquemas de mejores prácticas.

En ese sentido, en caso de que el Responsable hubiera desarrollado esquemas de mejores prácticas, el Comité de Transparencia o el servidor público a cargo del tratamiento respectivo que concluya el encargo, según se haya establecido en el procedimiento interno en la organización del Responsable, tendrían que incluir en su entrega la documentación generada en torno a los esquemas de mejores prácticas.

M. Auditorías voluntarias

El artículo 151, primer párrafo, de la Ley General de Protección de Datos Personales señala que los Responsables podrán voluntariamente someterse a la realización de auditorías por parte del Instituto, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en dicha ley y demás normativa que resulte aplicable.

En ese sentido, en caso de que el Responsable hubiera desarrollado esquemas de mejores prácticas, el Comité de Transparencia o el servidor público a cargo del tratamiento respectivo que concluya el encargo, según se haya establecido en el procedimiento interno en la organización del Responsable, tendrían que incluir en su entrega la documentación generada en torno a las auditorías voluntarias practicadas.

N. Sanciones y medidas de apremio

La Ley General de Protección de Datos Personales prevé, en su Título Décimo Primero, medidas de apremio y sanciones, las primeras para asegurar el cumplimiento de las resoluciones del INAI y los organismos garantes, y las segundas por incumplimiento de las obligaciones establecidas en dicha ley.

En ese sentido, en caso de que servidores públicos del Responsable hubieran sido sujetos a medidas de apremio o sanciones en materia de datos personales, se sugiere que el Comité de Transparencia entregue, en caso de cambios en su titular, una relación de los servidores públicos involucrados y la documentación soporte.

Por otra parte, es importante tener en cuenta que en materia de protección de datos personales existen otros procedimientos ante el INAI, además del recurso de revisión, respecto de los cuales también tendría que entregarse la documentación que se haya generado en seguimiento y cumplimiento a los mismos. Estos procedimientos son los siguientes:

1. Procedimiento de investigación y verificación, y
2. Imposición de medidas de apremio.

Sumario

A partir de lo establecido en este apartado sobre documentos generados con motivo de las obligaciones específicas en materia de datos personales, se puede advertir que en caso de que haya cambios en el titular del Comité de Transparencia de un sujeto obligado, resulta conveniente que se incluya en su entrega, al menos, la siguiente información y documentos:

1. Los procedimientos internos que en su caso se hubieran desarrollado para atender con mayor eficiencia las solicitudes de ejercicio de los derechos ARCO y de portabilidad;
2. Las determinaciones en las que haya confirmado, modificado o revocado la inexistencia de los datos personales solicitados o la negativa de ejercicio de alguno de los derechos ARCO o portabilidad;
3. Los criterios específicos que en su caso se hayan desarrollado para una mejor observancia de la normatividad de datos personales;
4. La documentación generada en las actividades que en su caso se hubieran realizado para vigilar el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;
5. La documentación generada en torno al seguimiento y cumplimiento de las resoluciones que en su caso haya emitido el INAI;
6. Los programas de capacitación y actualización de los servidores públicos en materia de datos personales;
7. La evidencia de la implementación de los programas de capacitación y actualización de los servidores públicos en materia de datos personales;
8. El inventario de datos personales de la organización del Responsable;

9. El documento de seguridad con los elementos que establece la norma y sus actualizaciones, en caso de que éstas existan;
10. Las bitácoras y notificaciones de las vulneraciones ocurridas a las bases de datos del Responsable, en caso de que se hayan presentado;
11. Los procedimientos para el bloqueo, supresión y conservación de los datos personales;
12. Los programas y políticas internas de protección de los datos personales;
13. Las evaluaciones de impacto en la protección de datos personales, en su caso;
14. Los esquemas de mejores prácticas que se hubieran implementado de manera horizontal en la organización del Responsable;
15. Las auditorías voluntarias que hubiera promovido;
16. Las vistas que haya dado al Órgano Interno de Control o instancia equivalente por presuntas irregularidades en el tratamiento de datos personales;
17. La relación de servidores públicos sujetos a medidas de apremio o sanciones por incumplimientos en materia de protección de datos personales, y
18. Los expedientes vinculados con procedimientos ante el INAI: recursos de revisión y verificaciones.

Asimismo, es recomendable que el titular del Comité de Transparencia que concluya su encargo en esta área incluya en su entrega cualquier otra información o documento que obre en sus archivos con motivo del cumplimiento de sus funciones como autoridad máxima en materia de datos personales al interior de la organización del Responsable.

En cuanto a la Unidad de Transparencia de un sujeto obligado, en caso de que exista cambio en su titular, resulta conveniente que se incluya en su entrega, al menos, la siguiente información y documentos:

1. Los documentos generados en torno a las gestiones de las solicitudes de ejercicio de derechos ARCO y portabilidad;
2. Los procedimientos internos que en su caso se hayan desarrollado para una mayor eficiencia en la gestión de las solicitudes de derechos ARCO y portabilidad, así como los mecanismos para garantizar que los datos personales se entreguen sólo a su titular o representante;
3. Los instrumentos desarrollas para evaluar la calidad sobre la gestión de las solicitudes, así como los resultados de las evaluaciones que en su caso se hayan practicado;
4. La designación, en su caso, del oficial de protección de datos personales, y
5. Los acuerdos que en su caso se hayan firmado con instituciones públicas especializadas que pudieran auxiliarles a la recepción, trámite y entrega de las respuestas a las solicitudes en lengua indígena, braille o cualquier otro formato accesible.

Por su parte, cuando un servidor público, con nivel de dirección de área o del que por normatividad esté obligado a presentar un acta de entrega-recepción, haya tenido a su cargo

el tratamiento de datos personales y concluya su encargo, es conveniente que incluya en su entrega, al menos, la siguiente información y documentos:

1. Los avisos de privacidad relacionados con los tratamientos a su cargo y las constancias de su puesta a disposición, así como, en su caso, las medidas compensatorias que hubiera implementado;
2. Los consentimientos otorgados por los Titulares de los datos personales, en caso de que éstos se hayan requerido para el tratamiento a su cargo, así como las revocaciones que se hubieran solicitado por parte de los Titulares;
3. La relación de las categorías o descripciones genéricas de transferencias de datos personales que se realizan en los tratamientos, del 27 de enero de 2017 a la fecha de la entrega recepción, en su caso;
4. Los instrumentos jurídicos en los cuales se hayan formalizado las transferencias ocurridas en el tratamiento a su cargo, en caso de que así lo requiera la ley; los consentimientos de los Titulares para estas transferencias, de no actualizarse las excepciones previstas por la norma, y las constancias de la puesta a disposición del aviso de privacidad a los terceros receptores de los datos personales;
5. Los instrumentos jurídicos mediante los cuales se haya formalizado la relación con Encargados del tratamiento de datos personales a su cargo, en caso de que éstos existan;
6. Las evaluaciones de impacto en la protección de datos personales que se hubieran realizado con relación a los tratamientos a su cargo, en su caso;
7. Los esquemas de mejores prácticas que hubiera implementado de manera directa.
8. Las auditorías voluntarias que hubiera promovido de manera directa a los tratamientos a su cargo, y
9. Las notificaciones de las vulneraciones a los Titulares y al INAI que en su caso hubieran ocurrido a las bases de datos personales a su cargo.

En el caso de la información relacionada con los tratamientos de datos personales que hubieran realizado los servidores públicos como parte del ejercicio de sus atribuciones, se recomienda que ésta no se entregue por separado, sino en los propios expedientes de los asuntos o proyectos a cargo del servidor público que concluye el empleo y que está reportando en su entrega, en una subsección en la que se incluya la información relativa a este tema.

Por ejemplo, supongamos que el servidor público A estuvo a cargo del programa social B, cuyo expediente se incluye en la entrega del servidor público por referir a un asunto a su cargo. En dicho programa social se efectuó el tratamiento de datos personales, por lo que en el expediente del programa, en una subsección especial sobre cumplimiento de obligaciones en materia de datos personales, se tendría que incluir, al menos, lo siguiente: el o los avisos de privacidad vinculados con el tratamiento llevado a cabo con motivo del programa; en su caso, las medidas compensatorias implementadas; los consentimientos otorgados si éstos fueron necesarios conforme a la ley y, en su caso, las revocaciones que hubieran existido; lo relativo a las transferencias si en el programa en cuestión se realizaron; la documentación soporte de

la relación con los Encargados si esta figura existió dentro del tratamiento; si este programa implicó una evaluación de impacto a la protección de datos personales tendría que incluirse la información relacionada con la misma; si en el programa se desarrollaron esquemas de mejores prácticas también tendría que incluir dicha información; de igual forma, si se hubiera llevado a cabo una auditoría voluntaria con relación al tratamiento de datos personales ocurrido en el programa, en el expediente en cuestión tendría que incluirse dicha información, y si la base de datos personales generada con motivo de este programa hubiera sufrido alguna vulneración, tendrían que incluirse las notificaciones a los Titulares y al INAI.

3.2. Medidas de seguridad específicas para la entrega de bases de datos personales y deber de confidencialidad

La Ley General de Protección de Datos Personales establece como una de las obligaciones principales de los Responsables la implementación y mantenimiento de medidas de seguridad físicas, técnicas y administrativas, para proteger los datos personales contra daño, pérdida, alteración, destrucción o de un uso, acceso o tratamiento no autorizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

En ese sentido, además de las medidas de seguridad que tenga implementadas el Responsable en el tratamiento cotidiano de los datos personales, se estiman convenientes los siguientes controles de seguridad para la etapa de transición o entrega de las bases de datos:

1. Se sugiere mantener medidas de seguridad en las bases de datos personales en formato físico, tales como gestión de privilegios de acceso y uso, libros de registro o bitácoras, gestión documental, y restricción de copiado o digitalización. Para las bases de datos en formato electrónico, se pueden considerar medidas tales como administración de usuarios y contraseñas, cifrado, gestión de privilegios de acceso y uso, bitácoras o *logs* y restricción de impresión. Las medidas anteriores permiten minimizar el riesgo de que se obtengan copias no autorizadas de las bases de datos, se utilicen de manera indebida, se destruyan, o se bloquee su acceso de manera irregular.
2. Si el acceso a la base de datos correspondiente requiere del registro de usuario y contraseña, se recomienda dar de baja los datos del servidor público que concluye el empleo y sus privilegios de acceso, a fin de evitar accesos posteriores no autorizados. Asimismo, se recomienda revisar, periódicamente, las bitácoras de acceso a los sistemas de tratamiento, para identificar, en su caso, usuarios que debieran estar dados de baja, y si han tenido acceso a las bases de datos.
3. Se debe asegurar que los servidores públicos entreguen llaves, identificaciones, tarjetas de proximidad, y cualquier elemento que les proporcione acceso físico a los sistemas de tratamiento y bases de datos a las que ya no están autorizados utilizar. En su caso, también se debe dar de baja toda información que sirva de acceso a los sistemas de tratamiento de datos personales, o a sus sitios de resguardo físico (por ejemplo, un *pin* o la huella dactilar).

4. Se recomienda evitar copias innecesarias de las bases de datos personales. En particular, se debe gestionar la información que respalda un servidor público cuando entrega un equipo de cómputo, procurando eliminar todas aquellas copias parciales o totales de las bases de datos a las cuales ya no tiene autorización de acceder.
5. Cualquier dispositivo proporcionado por la dependencia al servidor público, deberá ser objeto de un escrupuloso inventario: teléfonos inteligentes, computadoras portátiles, discos duros, entre otros.
6. A fin de contar con elementos que puedan ayudar en caso de que se presente una vulneración a la seguridad de los datos personales, se recomienda conservar junto con los respaldos que haga al equipo de cómputo de la persona involucrada en la vulneración, una copia del buzón de su correo electrónico, y en la medida de lo posible el disco duro o la imagen forense, según las capacidades técnicas de la organización. Todos los elementos mencionados anteriormente deberán estar resguardados adecuadamente para evitar un acceso no deseado por un tercero.
7. Se sugiere mantener una cadena de custodia sobre los entregables, es decir, se debe contar con una lista de todo lo que entrega un servidor público. En este sentido, la primera tarea de quien recibe un cargo, sería revisar que la documentación que entregó su predecesor esté completa. Esta revisión también puede involucrar, en el ámbito de sus competencias, a otras áreas, como sistemas o recursos humanos.
8. En caso de que haya concluido el plazo de conservación de los datos personales y sea necesaria su eliminación, es importante que la misma se realice por medios seguros. Para ello, se recomienda consultar la Guía para el Borrado Seguro de Datos Personales, elaborada por el INAI y disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf

Las medidas de seguridad que se adopten deberán estar registradas en el documento de seguridad que se describió en el apartado anterior y que se señaló deberá ser entregado como parte del acta correspondiente.

Por otra parte, salvo la información que deba ser pública en cumplimiento de las obligaciones de transparencia previstas en la Ley General y Federal de transparencia, los Responsables deberán cumplir con el deber de confidencialidad previsto en el artículo 42 de la Ley General de Protección de Datos Personales, por lo que se sugiere evitar la difusión de datos personales que no pertenezcan a las obligaciones de transparencia, en las memorias, libros blancos e informes institucionales.

No obstante, la confidencialidad no aplica en la comunicación de datos personales a los servidores públicos que reciben el encargo, cuando éstos estén facultados para tener acceso a los mismos, por lo que en esos casos los servidores públicos que entregan el cargo no podrán negar el acceso a las bases de datos aludiendo al deber de confidencialidad.

En todo caso, es importante que los servidores públicos tengan presente que la Ley General de Protección de Datos Personales prevé sanciones por incumplimiento de los deberes en materia de protección de datos personales.

Una de las causas de sanción, de acuerdo con el artículo 163, fracción III, de la Ley General de Protección de Datos Personales, es usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.

En ese sentido, los servidores públicos que concluyan su encargo deberán evitar sustraer bases de datos personales cuando no haya autorización para ello o justificación normativa que lo avale.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Instituto Nacional de Transparencia, Acceso a la Información
y Protección de Datos Personales
Insurgentes Sur No. 3211
Col. Insurgentes Cuicuilco, Delegación Coyoacán,
C.P. 04530
www.inai.org.mx