DICONSA

Programa de Protección de Datos Personales de DICONSA, S.A DE C.V.

Contenido

I. Presentación

Con la reforma del artículo 60 Constitucional en 2014 se fijan las bases para la emisión de una Ley General respecto de la información en posesión de entes público.

El 26 de enero de 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), en la cual se establecen las bases, procedimientos, principios, deberes y obligaciones que rigen el tratamiento de información de carácter personal, así como los derechos que tienen los titulares a la protección de sus datos personales en posesión de los organismos de los poderes Ejecutivo, Legislativo y Judicial en los tres niveles de gobierno.

Asimismo, el 26 de enero de 2O18, se publicaron los Lineamientos Generales de Protección de Datos Personales para el Sector Publico, en los que se anuncian las obligaciones exigibles en el tratamiento de datos personales y el ejercicio de los derechos (ARCO), a partir de ambas publicaciones, todo aquel sujeto obligado obtiene la figura jurídica del "Responsable" que debe actuar de conformidad a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, además de adoptar medidas de seguridad (administrativas, físicas y técnicas) en el tratamiento de datos personales.

El 28 de septiembre de 2018, se publicó en el Diario Oficial de la Federación el decreto por el que se promulgan el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Dantos de Carácter Personal ("Convenio 1O8") y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos. Dicho decreto entró en vigor el día primero de octubre de este año, con lo cual el Convenio 108 y su Protocolo son vinculantes para México a partir de esa fecha, Asimismo, México ha suscrito diversas convenciones, tratados y acuerdos en la materia, y participa en diversas iniciativas, destacando la Red Iberoamericana de Protección de Datos (RIPD).

En tal tesitura, DICONSA, S.A DE C.V. es un sujeto obligado reconocido por la LGPDPPSO y tiene la obligación de cumplir con lo dispuesto en el marco normativo aplicable.

II. Marco Normativo

El derecho a la protección de datos personales, materia de este documento, tiene su fundamento en el marco jurídico siguiente:

- Constitución Política de los Estados Unidos Mexicanos.
- Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convento 108) y su Protocolo adicional.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Responsabilidades Administrativas de los Servidores Públicos.
- Ley Orgánica de la Administración Pública Federal.
- Ley General de Archivos
- Lineamientos Generales de Protección de Datos Personales en Sector Público.

El Programa de Protección de Datos Personales, es una herramienta de las acciones mínimas que deberá considerarse para la eficaz protección de Datos Personales recabados en atención a las atribuciones de cada unidad administrativa de la dependencia. Este conjunto de esfuerzos y acciones se ajustan a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y al marco normativo de la Entidad.

III. Alcance

El presente Programa de Datos Personales, es de observancia obligatoria de todas las Unidades Administrativas de DICONSA, S.A. de C.V. que en el cumplimiento de sus atribuciones recaban y tratan datos personales.

Es importante atender que también aplicará a todos los servidores públicos que por sus funciones realicen algún tipo de tratamiento de datos personales. En este caso, están obligados a conocer y aplicar las medidas de seguridad mínimas contempladas en la LGPDPPSO y sus Lineamientos Generales.

Se destaca que la responsabilidad de la tarea, implica no sólo tratar los datos personales con responsabilidad, sino también, guardar la debida confidencialidad y garantizar en todo momento la seguridad sobre la información a la que se tenga acceso.

IV. Objetivos

El programa tiene como objetivos:

1. Cumplir con las obligaciones que establecen la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados y los Lineamientos Generales, así como la normatividad que derive de los mismos.

2. Establecer las directrices y herramientas necesarias, para garantizar la protección de los datos personales en posesión de las unidades administrativas, por medio de la sensibilización, capacitación, implementación, operación, revisión, mantenimiento y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.

3. Promover la adopción de mejores prácticas en materia de Protección de Datos Personales al interior de DICONSA, así como proporcionar a la ciudadanía la certeza de que los datos personales en posesión de la dependencia están siendo tratados de conformidad con lo establecido en el marco normativo.

V. Líneas Estratégicas

Lo anterior, se logrará mediante la ejecución de las Líneas Estratégicas que a continuación se señalan:

1. Sensibilización.

Para aumentar el nivel de conocimiento de los servidores públicos de DICONSA sobre la protección de los datos personales, el área de Tecnologías de la Información, la Unidad de Transparencia, enviaran vía correo electrónico la difusión de sensibilización, promoción y difusión de la materia.

El incremento constante del conocimiento en la materia tiene como finalidad colocar en el dominio de las personas servidoras públicas los temas más básicos sobre la protección de los datos personales.

2. Desarrollo de Competencias

Para lograr la ejecución de esta línea estratégica el área de Tecnologías de la Información, realizará de manera constante al interior de DICONSA, campañas de promoción y difusión de diversos materiales sobre la protección de datos personales a través del correo electrónico institucional.

La Unidad de Transparencia, tomará en cuenta la oferta que brinda el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), para difundir a los servidores públicos la calendarización sobre los diversos temas de capacitación en materia de protección de datos personales, con la finalidad de que los servidores públicos estén debidamente capacitados en la normatividad de referencia.

Bajo ese contexto, los servidores públicos que participen y se involucren en los temas de capacitación que engloba la LGPDPPSO, podrán contar con información certera sobre el cumplimiento y atención de sus obligaciones en materia de protección de datos personales, dando cumplimiento a los deberes y principios previstos en la normatividad, dado que el tema de protección de datos personales es competencia de todos los servidores públicos que participen y se involucren en la protección de la información confidencial que obre en los archivos de la dependencia.

3. Implementación, operación, revisión, mantenimiento y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.

Es fundamental que las personas servidoras públicas tengan pleno dominio de las obligaciones, en cuanto a la elaboración de los inventarios de tratamiento, de avisos de privacidad y del documento de seguridad.

Este último, deberá ser desarrollado por el área de Tecnologías de la Información, con apoyo de cada unidad administrativa, entendiéndolo como el documento que da cuenta de las medidas técnicas, físicas y administrativas, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que obran en poder de las diversas unidades administrativas, asimismo en el Documento de Seguridad se contiene el inventario de datos personales.

VI. Desarrollo de Líneas Estratégicas

1) Sensibilización

El Diccionario de la lengua española, define el concepto sensibilizar, como "hacer sensible algo o a alguien", y efectivamente, el presente Programa aspira lograr sensibilizar a las personas públicas de la Entidad, es decir, contar con el conocimiento y compromiso de la profunda relevancia que tienen los datos personales.

Lo anterior, muestra que corresponde a todas las personas servidoras públicas de la Administración Pública Federal, y en particular de la Entidad, asumir el compromiso de velar en todo momento por el adecuado Tratamiento de los datos personales recabados.

Para lograrlo, en el Presente Programa de Protección de Datos Personales de la Entidad, encontrará el conjunto de actividades necesarias para concientizar a las personas servidoras públicas, respecto de los diferentes aspectos relativos a la protección de datos personales, vistos desde la trascendencia del respeto a los derechos fundamentales. El derecho a la autodeterminación informativa es un elemento que le permite al titular de los datos, decidir conscientemente con quién o qué organización desea compartir su información, así como tener la garantía que estarán adecuadamente protegidos, desde luego que también se debe atender a las excepciones determinadas por el marco normativo.

Este Programa, aspira a lograr sensibilizar a las personas servidoras públicas de DICONSA, es decir, crear conciencia acerca de la importancia de proteger, promover y difundir su derecho a la privacidad, así como destacar la importancia que tiene en la protección de datos personales como un derecho humano consagrado en la legislación mexicana y en diversos instrumentos internacionales.

La campaña de sensibilización aquí incluida, ofrece información específica que ayudará a los responsables de las unidades administrativas de la dependencia a delinear acciones particulares para el diseño de procesos orientados a la protección de datos personales.

En esta campaña, se busca eliminar aquellos obstáculos que impiden el conocimiento de los principales componentes del marco normativo, reforzando la referencia implícita o explícita de que resulta fundamental entender el compromiso que tenemos como ciudadanos y ciudadanas como servidoras y servidores públicos, asimismo, la campaña de sensibilización buscará atender a todos los elementos gráficos institucionales que, seguramente, podrán reforzar el sentimiento de pertenencia, identidad y comunidad con el movimiento nacional y global de marcos regulatorios, cada vez más exigentes en la protección de datos personales.

2) Desarrollo de competencias

DICONSA, S.A DE C.V., siempre busca cumplir con toda la normatividad aplicable, principalmente en la materia de protección de datos personales. En tal sentido, la Unidad de Transparencia se ha ocupado de sensibilizar y llevar a cabo capacitaciones a las diversas unidades administrativas vinculadas al tratamiento de datos personales para que deban elaborar avisos de privacidad, y/o atender solicitudes de ejercicio de derechos ARCO.

Asimismo, las unidades administrativas están en conocimiento de que cuentan con las asesorías necesarias en dicha materia por parte del INAI y la Unidad de Transparencia, para fortalecer y consolidar la asistencia a través del presente Programa, a efecto de que todas las unidades administrativas reciban la capacitación integral que les permita no sólo actualizar conocimientos en las tareas más relevantes de la protección de los datos personales, sino también identificar las buenas prácticas sobre la materia.

Es importante señalar que la capacitación respecto de los alcances del marco normativo en materia de protección de datos personales, así como de la identificación de las buenas prácticas institucionales, permitirán actualizar y sensibilizar al personal de las unidades administrativas, generando una conciencia institucional sobre la trascendencia del tratamiento y la protección de los datos personales que obran en las bases de datos o documentos institucionales.

Lo anterior, se refiere a los procedimientos físicos, automatizados o aplicados a los datos personales relacionadas, de manera enunciativa más no limitativa, con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, transferencia y en general cualquier uso o disposición de datos personales.

En este sentido, el presente Programa de protección de datos personales ha sido aprobado por el Comité de Transparencia de DICONSA.

Las personas servidoras públicas responsables de los sistemas de tratamiento de datos personales que poseen, deberán de adoptar las medidas necesarias para evitar que se vulneren los mismos, respetando los principios de la protección de datos que constituyen el pilar mediante el cual se articula este derecho y son de observancia obligatoria para todo aquél que interviene en el tratamiento de datos personales desde el momento de la obtención hasta la destrucción de los mismos. Desde la perspectiva de lo anterior, se describen los siguientes Principios:

a) P R I N C I P I O S

a.1) Principio de licitud

El principio de licitud significa que las personas servidoras y servidores públicos deberán de asumir un comportamiento ético y responsable, en el tratamiento de los datos personales que poseen en sus unidades administrativas, sujetándose a las atribuciones o facultades que la normatividad aplicable les confiera.

a.2) Principio de Lealtad

De acuerdo con el principio de lealtad, las personas servidoras públicas no podrán usar medios engañosos, ni fraudulentos, lo que implica que:

- No se recaben datos personales con dolo, mala fe o negligencia;
- No se traten los datos que generen discriminación o un trato injusto contra los titulares.
- No se vulnere la confianza del titular con relación a que sus datos personales.
- Se informen todas las finalidades del tratamiento en el aviso de privacidad.

a.3) Principio del consentimiento

Como regla general, las personas servidoras y servidores públicos deberán contar con el consentimiento del titular para el tratamiento de los datos personales. Para obtener el consentimiento tácito, expreso o expreso por escrito, y dependiendo del tipo de datos personales, la solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general.

Aunado a ello, el consentimiento debe ser informado, por lo que previo a su obtención, es necesario que el titular conozca el aviso de privacidad, además de que debe ser libre tal y como lo refiere la LGPDPPSO, en el sentido que no medie error, mala fe, violencia o dolo que afecten la voluntad del titular.

a.4) Principio de información

Por virtud de este principio, las personas servidoras públicas se encuentran obligadas a informar a los titulares, las características principales del tratamiento al que será sometida su información personal, lo que se materializa a través del aviso de privacidad.

A fin de que los titulares puedan tomar decisiones informadas al respecto, y puedan ejercer el derecho a la protección de su información personal. En ese sentido, toda área que trate datos personales, sin importar la actividad que realice, requiere elaborar y poner a disposición los avisos de privacidad que correspondan en los tratamientos que lleven a cabo.

Es importante tomar en cuenta que con independencia de que se requiera o no el consentimiento del titular para el tratamiento de sus datos personales, el responsable está obligado a poner a su disposición el aviso de privacidad.

a.5) Principio de Proporcionalidad

El principio de proporcionalidad establece la obligación que las personas servidoras públicas tratarán que sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron. De acuerdo con lo antes expuesto, las unidades tienen las siguientes obligaciones en torno al principio de proporcionalidad:

- Tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron;
- Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles; y
- Crear bases de datos con datos personales sensibles sólo cuando se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de la Ley General en la materia.

Atendiendo a lo anterior las personas servidoras públicas deberán de realizar el esfuerzo para que los datos personales tratados sean los mínimos necesarios para lograr la o las finalidades para las cuales se obtuvieron, mismas que deben ser acordes con las atribuciones conferidas al responsable y señaladas en el aviso de privacidad.

a.6) Principio de Finalidad

Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales, y solo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste.

Las finalidades deben ser concretas, explicitas, licitas y legítimas, siendo importante que las personas servidoras públicas consideren las siguientes características:

- 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.
- Explícitas: Tienen lugar cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.
- 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.

- 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 previstas en el artículo 22 de la Ley General.

La finalidad o finalidades del tratamiento de datos personales deberán ser determinadas, es decir, las personas servidoras públicas están obligadas a especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad.

A manera de ejemplo, una finalidad es cuando un responsable, para contribuir a realizar un trámite solicitado por un titular, señala que las finalidades del tratamiento de los datos personales que solicita son:

- Creación de un Expediente
- Atención y Seguimiento del Trámite
- Generación de datos estadísticos entre los responsables.

a.7) Principio de Calidad

El principio de calidad significa que, conforme a las finalidades para las que se vayan a tratar los datos personales, éstos deben ser exactos, correctos, completos y actualizados.

Las personas servidoras públicas están obligadas a:

- Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación;
- Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo;
- Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales;
- Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación de conformidad con lo establecido por la Ley General de Archivos;
- Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales.

A efecto de cumplir con el principio de calidad, es necesario tomar en consideración los siguientes aspectos:

✓ Conservación de los Datos Personales

El plazo de conservación de los datos personales no debe exceder el tiempo estrictamente necesario para llevar a cabo las finalidades que justificaron el tratamiento, ni aquél que se requiera para cumplir con:

- ❖ Las disposiciones legales establecidas en la Ley General de Archivos.
- ❖ Las disposiciones aplicables en la materia de que se trate.
- ❖ Los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.
- ❖ El periodo de bloqueo.

Es importante señalar que, en particular, el artículo 24 de la Ley General, establece que se deben documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales respecto de cada tratamiento que se efectúe por las unidades administrativas.

✓ Conclusión del plazo de conservación

Una vez concluido el plazo de conservación, y siempre que no exista disposición legal o reglamentaria que establezca lo contrario, las unidades administrativas deben proceder a la supresión de los datos personales. En este caso, deberán de informarlo a la Unidad de Transparencia, quien lo hará del conocimiento del Comité de Transparencia, a efecto de que determine lo conducente. Es importante recordar que el plazo de conservación debe incluir un periodo de bloqueo, ya que los datos personales deben ser bloqueados antes de que sean eliminados o suprimidos.

Además, en cuanto a los datos personales sensibles, el responsable debe realizar esfuerzo razonable para limitar el periodo de tratamiento al mínimo indispensable.

✓ Bloqueo de los datos personales

El bloqueo se define como la acción que tiene por objeto impedir el tratamiento de los datos personales para cualquier finalidad, con excepción de su almacenamiento y acceso para determinar posibles responsabilidades en relación con el tratamiento de los datos personales, hasta el plazo de prescripción correspondiente. Las personas servidoras públicas están obligadas a:

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

Concluido dicho periodo se deberá proceder a su supresión.

DICONSA, S.A DE C.V. tendría que bloquear los datos personales después de transcurridos los 15 años del tratamiento (10 años en que el titular tuvo una relación con ésta más 5 años que establecía la norma). El tiempo en que los datos personales deberán estar bloqueados depende de los plazos legales que establezca la legislación de índole archivística para determinar posibles responsabilidades en relación con el tratamiento de los datos personales, lo cual dependerá, a su vez, de la materia de que se trate. Concluido el periodo de bloqueo, el responsable deberá suprimir los datos personales.

a.8 Principio de Responsabilidad

El principio de responsabilidad cierra el círculo con relación a los principios que regulan la protección de los datos personales. Este principio establece la obligación de las unidades de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y el órgano garante, que cumple con sus obligaciones en torno a la protección de los datos personales. Bajo este principio, las personas servidoras públicas responsables del tratamiento están obligados a velar por la protección de los datos personales, aún y cuando los datos estén siendo tratados por encargados.

Asimismo, este principio supone que se tomen las medidas suficientes para que los términos establecidos en el aviso de privacidad sean respetados por aquéllos con los que mantenga una relación jurídica, así como al momento de realizar transferencias nacionales o internacionales de datos personales. Finalmente, han quedado expuestos los principios que deberán de considerar las unidades administrativas para dar cumplimiento al marco normativo.

b) CONFIDENCIALIDAD Y SEGURIDAD.

La protección de los datos personales además de principios y obligaciones encuentra base en dos deberes:

b.1) Deber de Confidencialidad

Por confidencialidad, se entiende que se deben de establecer controles o mecanismos que tengan por objeto que todas aquellas personas servidoras públicas que traten datos personales, en cualquier fase del tratamiento, mantengan en secreto la información, así como evitar que la información sea revelada a personas no autorizadas y prevenir la divulgación no autorizada de la misma.

Las personas servidoras públicas tienen obligación de guardar la debida confidencialidad respecto de los datos personales que son tratados en sus unidades administrativas, para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información y hacer mal uso de esta.

b.2) Deber de Seguridad

Para una efectiva protección de los datos personales es necesaria la implementación de un Sistema de Gestión de Seguridad de Datos Personales (Sistema de Gestión), que permita planificar, implementar, monitorear y mejorar las medidas de seguridad de carácter administrativo, físico y técnico, a través de una serie de actividades interrelacionadas y documentadas tomando en consideración los estándares nacionales e internacionales, en materia de protección de datos personales y seguridad.

En este sentido, las personas servidoras públicas con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectué, deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad de los datos de carácter personal que conozca y a los que tenga acceso durante la relación laboral que se mantenga, debiendo subsistir esta obligación después de finalizar sus relaciones laborales.

Es importante recordar que un dato personal es cualquier información correspondiente a una persona física identificada o cuya identidad se pueda conocer a través de esa información, por ejemplo, nombre, apellidos, CURP, número de pasaporte, número de teléfono, dirección de correo electrónico, número de tarjeta de crédito, datos profesionales, laborales o académicos, salario, entre otros.

A continuación, se describen las siguientes categorías de datos personales y sus niveles:

Datos identificativos: Nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Clave de elector, Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía y demás análogos. Nivel: (básico).

Datos electrónicos: Las direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona, para su identificación en Internet, acceso a sistemas de información u otra red de comunicaciones electrónicas; Nivel: (básico).

Datos laborales: Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio y demás análogos. Nivel: (básico).

Datos académicos: Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos y demás análogos. Nivel: (básico).

Datos de salud: El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona. Nivel: (alto).

Datos patrimoniales: Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales y demás análogos. Nivel: (medio).

Datos sobre procedimiento administrativos: La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho. Nivel: (medio).

Datos de tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria. Nivel: (básico).

Datos biométricos: huellas dactilares, ADN, geometría de la mano, características de iris y retina y demás análogos. Nivel: (alto).

Datos sensibles: origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas, la pertenencia a sindicatos, la salud y preferencia sexual. Nivel: (alto).

Datos personales de naturaleza pública: Aquellos que por mandato legal sean accesibles al público. Nivel: (básico).

Se deberán de considerar los siguientes atributos y los medios de almacenamiento, físicos y/o Electrónicos en los que se encuentren los datos personales:

- **Irreversibilidad:** Que el proceso utilizado no permita recuperar los datos personales.
- **Seguridad y confidencialidad:** Que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la Ley General y los
- **Lineamientos Generales.**
- **Favorable al medio ambiente:** Que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.

A mayor abundamiento, cuando los datos personales hayan dejado de ser necesitados para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso.

Una vez que concluya el plazo de conservación de los mismos. Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

c) Inventario de Datos Personales y Sistema de Tratamiento

Este último, deberá ser desarrollado por el área de Tecnologías de la Información, con apoyo de cada unidad administrativa, en el documento de seguridad, entendiendo este último, como el documento que da cuenta de las medidas técnicas, físicas y administrativas, para garantizar la confidencialidad, integridad y disponibilidad de datos personales que obran en poder de las diversas unidades administrativas, asimismo, en el documento de seguridad se contiene el inventario de datos personales.

d) Aviso de Privacidad

El aviso de privacidad es el documento que las unidades administrativas deberán poner a disposición del titular de forma física, electrónica o en cualquier formato, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

La puesta a disposición del aviso de privacidad implica que éste se publique en un lugar visible, accesible y gratuito, en el cual el titular, de manera informada, cuente con la posibilidad de conocer el tratamiento que se les dará a sus datos personales. En todo caso, el aviso de privacidad deberá estar ubicado en un lugar visible y que facilite su consulta, los que se encuentran disponibles en la página institucional.

Lo anterior, con el propósito de que las personas servidoras públicas, tengan conocimiento sobre el tratamiento de datos personales que serán transferidos con motivo de algún curso, taller, capacitación que realicen las unidades administrativas, atendiendo a las atribuciones señaladas en el reglamento interior.

Finalmente, las personas servidoras públicas con apoyo de los enlaces designados en la materia, deberán considerar que los avisos de privacidad, se harán del conocimiento al Comité de la Transparencia de conformidad con lo establecido en el artículo 84 de LGPDPPSO, por ser la máxima autoridad en la materia de protección de datos personales.

d.1) Modalidades del Aviso de Privacidad

Existen dos modalidades del aviso de privacidad: Simplificado e Integral. El simplificado debe contener lo siguiente:

- ✓ La denominación del responsable;
- ✓ Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular;
- ✓ Cuando se realicen transferencias de datos personales que requiera consentimiento, se deberá informar:
- ✓ Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales.
- ✓ Las finalidades de estas transferencias.
- ✓ Los mecanismos y medios disponibles para que el titular, en su caso, puede manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular, y
- ✓ El sitio donde se podrá consultar el aviso de privacidad integral.
- ✓ Por otra parte, el aviso de privacidad integral deberá contener, además de lo citado con anterioridad, al menos, la información siguiente:
- ✓ El domicilio del responsable;
- ✓ Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;
- ✓ El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;
- ✓ Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular;
- ✓ Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;
- ✓ El domicilio de la Unidad de Transparencia, y
- ✓ Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

Finalmente, para conocer los formatos de aviso de privacidad que deberán utilizar las unidades administrativas, se agregan al presente un Programa las plantillas de los avisos de privacidad simplificado e integral.

d.2) Medidas Compensatorias

Las medidas compensatorias son los mecanismos alternos para dar a conocer a los titulares el aviso de privacidad simplificado, a través de su difusión por medios de comunicación masiva u otros mecanismos de amplio alcance.

Para dar a conocer a los titulares el aviso de privacidad simplificado, a través de su difusión por medios masivos de comunicación u otros mecanismos de amplio alcance, como los siguientes:

- Diario Oficial de la Federación o diarios de circulación nacional;
- Página de Internet o cualquier otra plataforma o tecnología oficial del responsable;
- Carteles informativos;
- Cápsulas informativas radiofónicas, o
- Cualquier otro medio alterno de comunicación masivo

Ahora bien, de conformidad con el artículo 2 de los Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal, se entiende por imposibilidad, esfuerzos desproporcionados y obtención directa, lo siguiente:

- Imposibilidad de dar a conocer al titular el aviso de privacidad de forma directa: se presenta cuando el responsable no cuenta con los datos personales necesarios que le permitan tener un contacto directo con el titular, ya sea porque no existen en sus archivos, registros, expedientes, bases o sistemas de datos personales, o bien, porque los mismos se encuentran desactualizados, incorrectos, incompletos o inexactos.
- Esfuerzos desproporcionados para dar a conocer al titular el aviso de privacidad de forma directa: cuando el número de titulares sea tal, que el hecho de poner a disposición de cada uno de éstos el aviso de privacidad, de manera directa, le implique al responsable un costo excesivo atendiendo a su suficiencia presupuestaria, o comprometa la viabilidad de su presupuesto programado o la realización de sus funciones o atribuciones que la normatividad aplicable le confiera; o bien, altere de manera significativa aquellas actividades que lleva a cabo cotidianamente en el ejercicio de sus funciones o atribuciones.
- Obtención directa de los datos personales: cuando el titular proporciona personalmente sus datos personales a quien representa al responsable o a través de algún medio que permita su entrega directa como podrían ser sistemas o medios electrónicos, ópticos, sonoros, visuales, vía telefónica, internet o cualquier otra tecnología o medio físico.

Los avisos de privacidad serán actualizados o, en su caso, elaborados por cada unidad administrativa que trate datos personales, según sus atribuciones.

d.3) Consentimiento

Las personas servidoras públicas deberán de contar con el consentimiento del titular de los datos personales, salvo que se actualice alguna de las excepciones de los artículos 22, 66 y 70 de la LGPDPPSO. Antes de poner a disposición del titular el aviso de privacidad, la unidad administrativa deberá observar lo siguiente:

- ✓ Elaborar su respectivo aviso de privacidad, revisando la necesidad y legalidad de su tratamiento para cumplir con la finalidad de que se trate, a fin de que quede debidamente justificada la obtención y uso de los datos personales.
- ✓ Identificar las finalidades para las cuales se requiere el consentimiento de los titulares.
- ✓ En caso de que las finalidades o tratamiento establecidos en el aviso de privacidad, encuadre en las hipótesis de los artículos 22, 66 y 70 de la LGPDPPSO, la unidad administrativa estará exenta de solicitar al usuario su consentimiento.
- ✓ Una vez que se ponga a disposición del titular el aviso de privacidad, las unidades administrativas deberán observar los casos en los que se requiera consentimiento tácito o expreso, dependiendo el tipo de datos personales.

c) Derechos de ARCO

El acrónimo ARCO está conformado por las iniciales de los derechos de Acceso, Rectificación, Cancelación y Oposición de los datos personales, derechos reconocidos por la legislación mexicana y que los titulares pueden ejercer, consisten en:

- ❖ **Derecho de Acceso:** Es el derecho que tiene el titular de solicitar el acceso a sus datos personales que se encuentran en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacena o utiliza, así como de conocer información relacionada con el tratamiento que se da a su información personal.
- ❖ **Derecho de Rectificación:** Es el derecho que tiene el titular de solicitar la rectificación o corrección de sus datos personales, cuando éstos sean inexactos o incompletos o no se encuentren actualizados. En otras palabras, puede solicitar a quien posea o utilice sus datos personales que los corrija cuando los mismos sean incorrectos, desactualizados o inexactos.
- ❖ **Derecho de Cancelación:** Es el derecho que tienen los titulares de solicitar que sus datos personales se eliminen de los archivos, registros, expedientes, sistemas, bases de datos del responsable que los trata. Aunque hay que tomar en cuenta que no en todos los casos se podrán eliminar sus datos personales, principalmente cuando sean necesarios por alguna cuestión legal o para el cumplimiento de obligaciones.

- **Derecho de Oposición:** Es el derecho que tiene el titular de solicitar que sus datos personales no se utilicen para una determinada finalidad, no para la totalidad de estas. También en este caso, como en el anterior, no siempre se podrá impedir el uso de los datos, cuento estos sean necesarios por motivos legales o para el cumplimiento de obligaciones.

  Las personas servidoras públicas, deben tener conocimiento que, como cualquier otro derecho, el de protección de datos personales tiene límites, por lo que bajo ciertas circunstancias los derechos ARCO no podrán ejercerse o su ejercicio se verá limitado por cuestiones de seguridad nacional; orden, seguridad y salud públicos, así como por derechos de terceros.

  Las causas por las que el responsable puede negar el ejercicio de los derechos ARCO son:

  - El titular de los datos personales o su representante no hayan acreditado su identidad;
  - El responsable no es competente para atender la solicitud.
  - Existe un impedimento legal;
  - Se pueda afectar los derechos de terceras personas;
  - Cuando el ejercicio de los derechos ARCO pudiera obstaculizar procesos judiciales o administrativos;
  - Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular;
  - Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;
  - Cuando los datos sean parte de información de las entidades sujetas a regulación y supervisión
  - Financiera del sujeto obligado, o
  - Cuando en función de sus atribuciones del sujeto obligado, el uso, resguardo y manejo sean necesarios para mantener la integridad, estabilidad y permanencia del Estado mexicano.

Cabe resaltar, aunque no proceda el ejercicio de derechos ARCO, las unidades administrativas están obligadas a responder la solicitud e informar las causas de improcedencia.

Luego entonces, el derecho a la protección de datos personales es un derecho personalísimo, solamente los titulares o sus representantes podrán solicitar el ejercicio delos derechos ARCO, por lo que es indispensable acreditarla identidad.

d) Transferencias

Las personas servidoras públicas responsables del tratamiento de los datos personales deberán de comprender que la transferencia es toda comunicación de datos personales, dentro o fuera del territorio nacional, a persona distinta del titular, del responsable o del encargado.

Es decir, la comunicación de datos entre el responsable y el encargado, NO se considera transferencia.

A ese tipo de comunicaciones se les llama "remisiones". Es importante señalar que los responsables no están obligados a solicitar el consentimiento de los titulares para la realización de remisiones, ni informarlas en el aviso de privacidad, contrario a lo que ocurre con las transferencias, como se verá más adelante.

Para que las unidades administrativas transfieran los datos personales dentro o fuera de México, es necesario que se ajusten a lo siguiente:

- Se informe al titular en el aviso de privacidad al destinatario de las transferencias ya sea en el ámbito público como privado, además deberá señalar las finalidades de estas transferencias. En caso de ser una transferencia que requiera consentimiento, deberá habilitar los mecanismos correspondientes.
- El titular haya otorgado su consentimiento para que la transferencia se realice, salvo los casos de excepción previstos en el artículo 22, 66 y 70 de la Ley General (este tipo de transferencias es opcional incluirlas en el aviso de privacidad integral).

No se requerirá el consentimiento de los titulares para realizar transferencias, cuando:

- Una ley así lo disponga;
- Las transferencias que se realicen entre responsables, para el ejercicio de facultades propias, sean compatibles o análogas con la finalidad que motivó el tratamiento;
- Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
- Para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica;
- Cuando exista una situación de emergencia;
- Asistencia sanitaria;
- Los datos se encuentren en fuentes de acceso público;
- Los datos personales sean sometidos a un procedimiento de disociación;
- El titular de los datos sea una persona reportada como desaparecida;

- Transferencia sea nacional o internacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en cumplimiento en una ley o tratado internacional suscrito y ratificado por el estado mexicano;
- A petición de una autoridad u organismo extranjero, competente en su carácter de receptor, cuyas facultades sean homologas;
- La Transferencia sea necesaria por un contrato celebrado o por celebrar en interés del titular;
- La transferencia sea necesaria por razones de seguridad.

Finalmente, resulta indispensable que las personas servidoras públicas responsables del tratamiento de datos personales den cabal cumplimiento a las obligaciones que se deriven de las transferencias a nivel nacional o internacional, con motivo de sus atribuciones.

e) Documento de Seguridad

El documento de seguridad es el 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.

Para su elaboración resulta indispensable la participación de las personas servidoras publicas responsables del tratamiento de los datos personales de todas las unidades administrativas, en el ámbito de su competencia quienes, para este fin, serán coordinadas por el personal de la Unidad de Transparencia quien orientará y verificará la integración del documento, mismo que se conformará por lo siguiente:

- El Inventario de Datos Personales;
- Las Funciones de las personas que tratan datos;
- El Análisis de Riesgo.
- El Análisis de Brecha;
- El Plan de Trabajo;
- Los Mecanismos de Monitoreo y Revisión
- El Programa de Capacitación

El documento de seguridad podrá sufrir actualizaciones considerando los siguientes eventos:

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

II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;

III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida.

IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Es importante destacar que la seguridad de los datos personales deberá observarse durante todo su ciclo de vida, desde su obtención hasta su eliminación.

f) Vulneraciones

La vulneración de datos personales además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

- La pérdida o destrucción no autorizada;
- El robo, extravío o copia no autorizada;
- El uso, acceso o tratamiento no autorizado, o
- El daño, la alteración o modificación no autorizada

Las personas servidoras públicas responsables de los sistemas de gestión de los datos personales deberán notificar inmediatamente a sus respectivos enlaces de protección de datos personales, cuando se actualice alguno de los puntos considerados anteriormente, debiendo contener lo siguiente:

- La naturaleza del incidente o vulneración ocurrida;
- Los datos personales comprometidos;
- Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
- Las acciones correctivas realizadas de forma inmediata;
- Los medios donde puede obtener más información al respecto;
- La descripción de las circunstancias generales entorno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y
- Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

VII. Acciones de Mejora

Con la finalidad de comprobar el cumplimiento del programa, el Comité de Transparencia realizará las siguientes acciones:

- Requerirá al área de Tecnologías de la Información y a la Unidad de Transparencia el informe de resultados de los programas de sensibilización y desarrollo de competencias diseñadas para el adecuado tratamiento y la seguridad de los datos personales, es decir, el número de difusiones realizadas por correo electrónico y los resultados de capacitación, en cada sesión ordinaria.
- A través de la Unidad de Transparencia, se requerirá a las unidades administrativas que así lo requieran la elaboración del aviso de privacidad integral y/o simplificada cuando de acuerdo con sus actividades, funciones y atribuciones realicen tratamiento de datos personales y se cargará en la página institucional.
- El área de Tecnologías de la Información, tomará en cuenta las áreas de oportunidad para las medidas de seguridad físicas, administrativas y técnicas, las que quedarán establecidas en el correspondiente "documento de seguridad", que les compete elaborar y mantener permanentemente actualizado, y del que dan cuenta al Comité de Transparencia en cada sesión Ordinaria.
- Con las acciones señaladas, se ensaya el nivel de cumplimiento de las disposiciones establecidas en el presente programa y la emisión de recomendaciones por parte del Comité de Transparencia para dar cumplimiento a las obligaciones que en materia de protección de datos personales que establece el marco normativo.

El Comité de Transparencia, realizará las recomendaciones que estime conveniente en materia de protección de datos personales, teniendo como finalidad fundamental que las unidades administrativas adopten acciones preventivas y correctivas:

1. **Acciones preventivas** que deberán documentarse: Son aquellas encaminadas a evitar cualquier "incumplimiento" a lo establecido en el presente Programa.

Para las *acciones preventivas* se podrán llevar las siguientes actividades:

a) Analizar y revisar las posibles causas de incumplimiento;

b) Determinar qué otras causas de incumplimiento podría desencadenarse a partir de ciertas situaciones de riesgo para el tratamiento de datos personales;

c) Evaluar las acciones necesarias para evitar que el incumplimiento ocurra;

d) Determinar e implementar estas acciones;

e) Documentar los resultados de las acciones tomadas, y

f) Revisar la eficacia de las acciones preventivas tomadas.

2. **Acciones correctivas** que deberán documentarse son las encaminadas a eliminar las causas de incumplimiento con relación a lo previsto en el presente Programa.

Para las *acciones preventivas* se podrán llevar a cabo las siguientes actividades:

a) Analizar y revisar el incumplimiento;

b) Determinarlas causas que dieron origen al incumplimiento;

c) Evaluar las acciones necesarias para evitar que el incumplimiento vuelva a ocurrir;

d) Proponer acciones correctivas y establecer un plazo para su cumplimiento;

e) Documentar resultados de las acciones tomadas, y

f) Revisar la eficacia de las acciones correctivas tomadas.

Resulta trascendental tener presente que el objetivo de las acciones denominadas correctivas, es eliminar las causas que generaron el incumplimiento a lo establecido en el presente programa, o bien, reducir su grado de prevalencia.

VIII. Sanciones

Cuando la Unidad de Transparencia, tenga conocimiento del incumplimiento de alguna obligación prevista en este Programa, deberá informarlo al Comité de Transparencia de DICONSA para que éste realice a la unidad administrativa correspondiente un exhorto para que lleve a cabo las acciones que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo para los datos personales.

De manera adicional, es importante que las personas servidoras públicas que están a cargo del tratamiento de datos personales tengan presente que de conformidad con el artículo 163 de la LGPDPPSO serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha ley, mismas que son las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;

II. Incumplir los plazos de atención previstos en la LGPDPPSO para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;

III. 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;

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGPDPPSO;

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la LGPDPPSO, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;

VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la LGPDPPSO;

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la LGPDPPSO;

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;

XI. Obstruir los actos de verificación de la autoridad;

XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO;

XIII. No acatar las resoluciones emitidas por el Instituto, y

XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves.

Asimismo, de conformidad con el artículo 105 de los Lineamientos Generales, cuando alguna unidad administrativa se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta dará aviso al superior jerárquico para que le ordene realizar sin demora las acciones conducentes.

Si persiste la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia para que, a su vez, dé vista al Órgano Interno de Control, y en su caso, se inicie este procedimiento de responsabilidad Administrativo respectivo. Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos. Las responsabilidades que resulten de los procedimientos administrativos correspondientes, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

El Comité de Transparencia tomará las medidas necesarias para que las personas servidoras públicas del sujeto obligado conozcan esta información.

IX. Glosario de Términos

Activo: La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización.

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Bases de datos: Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabadas, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

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, morales y opiniones.

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: 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.

Fuentes de acceso público: Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás normativa aplicable;

Instituto o 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.

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

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

e) Programa de Protección de Datos Personales.

Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

Responsable: Sujeto obligado de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que decide sobre el tratamiento de los datos personales.

Revisión: Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa.

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

Sujeto obligado: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal.

Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Titular: Persona física a quien corresponden los datos personales.

Transferencias: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada apersona distinta del titular, del responsable o del encargado.

Tratamiento: 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.

Unidad Administrativa: Área a la que se le confiere atribuciones específicas en el Reglamento Interior.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.