Documento de Seguridad para el Tratamiento de Datos Personales del Instituto Mexicano del Seguro Social

I. Introducción

El concepto de privacidad se encuentra estrechamente vinculado a la intimidad, que es un derecho garantizado en los principales instrumentos interamericanos y universales de derechos humanos.

Con el vertiginoso desarrollo de las tecnologías de la comunicación e información, este concepto ha adquirido una nueva dimensión en un mundo tecnológicamente cada vez más cambiante y presenta complejos desafíos que exigen un equilibrio entre el derecho a la intimidad del individuo, el uso apropiado de la tecnología y el libre flujo de la información.

Tomado en consideración la constante evolución y desarrollo al que están sujetas la tecnología de la información y comunicaciones, no existen fronteras ni territorios que puedan garantizar el blindaje para proteger los datos personales, convergen intricados en los diversos documentos con que cuenta este Instituto Mexicano del Seguro Social, ya sea física, administrativa o tecnológicamente.

Ante la inminente evolución y la aparición de cada vez más amenazas, es que los miembros de la Organización de los Estados Americanos (OEA), han reafirmado la importancia de proteger los datos personales y el derecho a la privacidad, así como el derecho de toda persona a ser protegida contra injerencias indebidas, en congruencia con lo establecido en la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Declaración Americana de los Derechos y Deberes del Hombre y la Convención Americana sobre Derechos Humanos.

En la doctrina internacional, este concepto ha ido evolucionando hasta convertirse en el conjunto de derechos ARCO Acceso, Rectificación, Cancelación y Oposición como medios que deben estar al alcance de todos en la preservación de la identidad, la dignidad y la libertad, reconocidos en su conjunto como el derecho del individuo a la autodeterminación informativa.

Para tener una idea de la magnitud que reviste el tema y las implicaciones que trae aparejadas el acceso ilegítimo a los mismos, afectando entre otros, la tutela de la dignidad de la persona humana, el libre desarrollo de su personalidad y su intimidad, por lo que el uso indebido que haga un tercero de los archivos personales, imágenes, expedientes médicos, contraseñas de acceso a correos o cuentas bancarias, pueden ocasionar al individuo daños que abarcan múltiples facetas de su vida, entre ellas su

reputación, su honor, su integridad patrimonial, y su capacidad de acceder a ciertos servicios tales como los de índole crediticio o los relacionados con la salud.

Los sucesos a los que se ha hecho referencia han generado diversas reacciones en el ámbito gubernamental reflejadas en una mayor apertura y fomento a la cultura de la transparencia, dando pie a la implementación de políticas de protección de datos personales de los Sujetos Obligados, las cuales, inciden directamente en el actuar responsable de los diversos Servidores Públicos encargados del tratamiento de datos personales.

Así las cosas y como consecuencia causal es que el derecho de acceso y rectificación de los datos personales en el sector público federal se ha visto sustancialmente favorecido, tan es así que su acceso se encuentra debidamente regulado en la Ley Federal de Transparencia y Acceso a la información Pública Gubernamental publicada en 2002.

Aunado a la disposición legal referida en el párrafo que antecede, subsecuentemente se generaron diversas reformas en materia de Transparencia, Acceso a La Información y Protección de Datos Personales, contempladas en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos en 2009 y 2014, propiciando la emisión de diversa normatividad con el propósito de garantizar el ejercicio de este derecho humano.

En 2009 se reformó el artículo 16 constitucional el cual establece que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición al uso de su información personal, en los términos que fije la ley. Esta reforma dio cabida a la publicación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares en 2010, no obstante, es hasta la reforma del artículo 6° Constitucional en 2014, cuando se fijan las bases para la emisión de una Ley General para homologar los criterios en los tres niveles de gobierno respecto de la información en posesión de entes públicos.

En este contexto, 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, principios y procedimientos para garantizar el derecho que tiene toda persona física a la protección de sus datos personales en posesión de entes públicos de los tres órdenes de gobierno, con la cual, se definen las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el

ejercicio de los derechos de acceso, rectificación, cancelación y oposición mediante procedimientos sencillos y expeditos (Derechos ARCO).

A su vez, el 26 de enero de 2018, se publicaron los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales de Protección de Datos Personales)**,** en los que se desarrollan y concentran las obligaciones exigibles del derecho a la protección de datos personales en el sector público federal, para evitar la fragmentación o atomización de ordenamientos que puedan repercutir en el cumplimiento efectivo de la LGPDPPSO por parte de los responsables en el ámbito federal.

Finalmente el 12 de febrero de 2018, son publicados en el Diario Oficial de la Federación los Lineamientos que Establecen los Parámetros, Modalidades y Procedimiento para la Portabilidad de Datos Personales, con los que se hace frente a la nueva realidad que vivimos, pues la era digital será un tema de todos los días, teniendo la obligación y el deber de implementar acciones y mecanismos de control que nos permitan ejercer de manera libre y confiable el derechos de acceso a la información, pero sobre todo, que los responsables de su manejo y almacenamiento garanticen que la privacidad no será vulnerada, por ello es que el presente documento de seguridad representa para el Instituto Mexicano del Seguro Social la primicia que marca un antes y un después en el tema de tratamiento de datos personales, en un mundo en el que la tecnología se posesiona en primer plano de nuestras vidas.

Por ello es que debemos prepáranos y ponernos a la vanguardia, buscando cada vez mejores prácticas, para hacer frente a los avances de la ciencia en esta materia.

Sin duda, tenemos un camino largo que recorrer en el ámbito de la transparencia, en el que será fundamental la comunicación, la coordinación, así como intercambio de experiencias entre sujetos obligados, así como el sentir ciudadano, lo que nos permitirá tener una visión clara y caminar de la mano en la una misma dirección, con el único objetivo de cumplir cabalmente con lo que nos instruye nuestra Constitución Política y las Leyes Generales y Federales en la materia.

A partir de la publicación de la LGPDPPSO y de los Lineamientos Generales de Protección de Datos Personales, es que todas las dependencias y entidades, incluidos partidos políticos, al llevar a cabo el tratamiento de los datos personales de personas físicas, adquieren el carácter de "Responsable" y deberán tratar dichos datos conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

Con base en ello, adoptar medidas de seguridad en atención a los sistemas de datos que traten; plasmar en un documento de seguridad dichas medidas, garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, entre otras obligaciones previstas.

Considerando todo lo anterior, podemos dimensionar el impacto significativo que tiene en el ámbito de la Seguridad Social, entendida ésta como la más amplia expresión de solidaridad humana entre los trabajadores; institucionalizada con el propósito de proteger su salud, su vida y su nivel de ingreso y el de sus familias, frente a los riesgos inherentes de la vida misma: la incapacidad, la enfermedad y la muerte, tarea que corresponde principalmente al Instituto Mexicano del Seguro Social, fundado en 1943, por ser la institución con mayor presencia no solo en el territorio nacional, sino de todo Latinoamérica, y que la mayor parte de la información con la que trabaja tiene el carácter de personal, por demás vital que para llevar a cabo su encomienda, consistente en la investigación, la práctica y asistencia médica, así como el servicios previo cumplimiento de los requisitos legales y administrativos de las prestaciones económicas y sociales a las que se tiene derecho, cuya garantía está a cargo del Estado, motivos más que suficientes para que el Instituto Mexicano del Seguro Social cuente con un mecanismo eficaz que garantice el adecuado trato de todos los datos personales que están bajo su resguardo.

A manera de referencia, y para tener clara la importancia que reviste la adecuada utilización de los datos personales resulta por demás acertado hacer énfasis en la enseñanza y experiencia que nos dejó la reciente crisis sanitaria a la que se enfrentó el mundo a consecuencia del COVID-19, las circunstancias obligaron a la comunidad médica y científica a enfrentar un proceso de investigación clínica acelerada, en busca de lograr un control de la pandemia, basándose en el utilización de datos duros para realizar diversos tipos de análisis, siendo fundamental el procesamiento, filtración, selección, extracción de información sensible de personas físicas con características clínicas, sintomatología y estado de salud determinados en la busca de una solución al problema mayúsculo que tal situación se representó a nivel global.

Siendo el Instituto Mexicano del Seguro Social un Sujeto Obligado, de acuerdo con lo previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados el que debe implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la Ley y rendir cuentas sobre el tratamiento de datos personales en su posesión, tanto al titular de los mismos como al órgano garante, según corresponda, observando en todo momento lo previsto en la

Constitución Política de los Estados Unidos Mexicanos y los tratados Internacionales en los que el Estado Mexicano sea Parte.

En este orden de ideas, considerando que la protección de las personas físicas en relación con el tratamiento de sus datos personales es un derecho fundamental, nuestra Constitución ha incorporado el derecho de protección de datos personales, primero en posesión de sujetos obligados y recientemente en posesión de particulares; cuyo bien jurídico tutelado son la privacidad y la intimidad.

Así, entre los "Deberes" previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, está el de elaborar un documento de seguridad (artículo 35), en el que se describa y dé cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que poseen las distintas unidades administrativas que conforman este Instituto.

La coordinación para la elaboración de este documento corrió a cargo de la Unidad de Integridad y Transparencia (UIT), dependiente de la Dirección General, cuya creación fue autorizada por el H. Consejo Técnico del Instituto Mexicano del Seguro Social mediante acuerdo ACDO.AS2.HCT.070920/240.P.DA de fecha 07 de septiembre de 2020, como parte del programa institucional de combate a la corrupción y la impunidad encabezado por la Dirección General de este IMSS, cuyos ejes torales están enfocados en transparentar el fortalecimiento de una cultura de integridad y cumplimiento, apegada a valores como la ética y la eficiencia para fines públicos, así como la adopción del modelo institucional para la competitividad enfocado a mejorar el desempeño como método de trabajo cotidiano, teniendo entre sus líneas de acción la de transparentar información pública de interés para socializar acciones y decisiones institucionales que hagan cotidiana y constante la apertura de toda actividad institucional y facilite la identificación de actos irregulares e inhiba escenarios de comisión de actos indebidos, teniendo entre sus atribuciones la de eficientar y transparentar el desempeño institucional, garantizar la protección de los datos personales y el ejercicio de los Derechos ARCO por parte de sus titulares dentro del IMSS, así como la de presidir el Comité de Transparencia (CT), que en términos del artículo 83 de la LGPDPPSO es la autoridad máxima en materia de protección de datos personales.

A su vez, el CT tiene entre sus funciones, la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales

en la organización del responsable, de conformidad con las disposiciones previstas en la LGPDPPSO y demás disposiciones que resulten aplicables.

La coordinación en la elaboración del Documento de Seguridad consistió en llevar a cabo las siguientes actividades:

- Concentración de los requisitos suficientes con los que se debe contar, así como de la normatividad aplicable para arrancar con la elaboración de un primer borrador.

- Celebración de reuniones de trabajo con la Dirección de Innovación y Desarrollo Tecnológico; (DIDT), por ser la encargada de brindar auxilio a sus homólogas en cuanto al diseño, contenido y cuidado tecnológico de los diversos sistemas institucionales, así como con las que por la naturaleza de sus funciones tienen a cargo procedimientos en los que existe una significativa carga de datos personales, ello con el objeto de conocer el número de Sistemas con los que se cuenta, así como las características de las medidas de seguridad y soporte electrónico, infraestructura tecnológica y de comunicaciones establecidas en el Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información (MAAGTICSI).

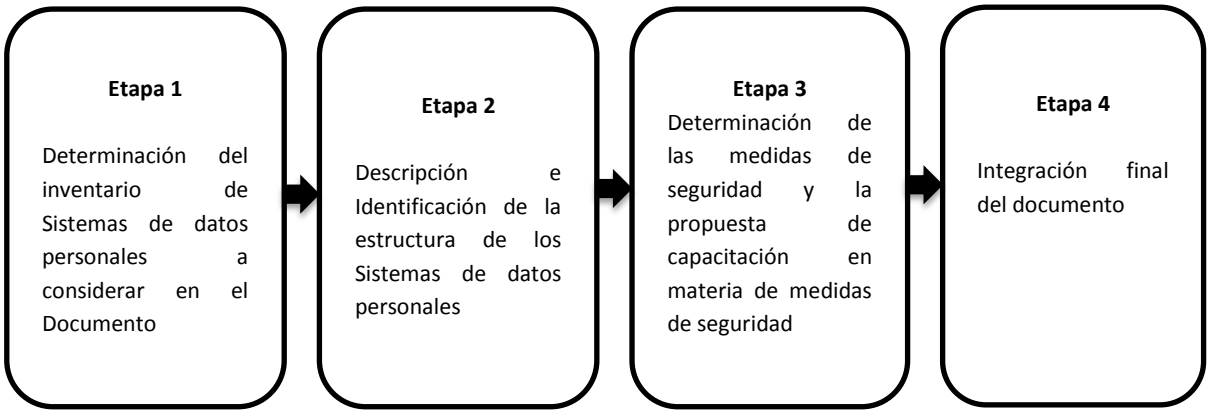
Con base en las acciones antes descritas se procedió a lo siguiente:

- Se desarrolló la metodología y un ejemplo de un Sistema de Tratamiento de Datos Personales.

- Se realizó reunión de trabajo con integrantes de la UIT, para presentar la estructura del documento y la metodología para recopilar la información de las unidades administrativas.

- Se celebraron diversas reuniones de trabajo con la DIDT, facilitándoles el borrador del documento inicial, a efecto de enriquecerlo con sus aportaciones por ser el área especialista en el manejo de las tecnologías de la información.

A partir de estas actividades, se definió un plan de trabajo en el cual se determinó incluir para cada etapa una reunión con personal de las unidades administrativas del IMSS para sensibilizar sobre la obligación correspondiente a la elaboración del Documento de Seguridad, definiendo los requisitos normativos para su integración, así como la metodología para entregar la información sobre los distintos sistemas de tratamiento de datos personales como sigue a continuación:



Es así como las distintas unidades administrativas que cuentan con sistemas en los que se manejan datos personales hicieron llegar su informe acorde con la metodología propuesta, para su análisis e integración del Documento de Seguridad en tres momentos distintos, como a continuación se explica:

- Identificar los sistemas de tratamiento de datos con los que cuentan, describir su objetivo y el fundamento normativo que los sustenta para llevar a cabo dicho tratamiento.

- Describir la estructura de los sistemas que involucran el tratamiento de datos personales, su idoneidad, la manera en que se obtienen, así como la identificación de quienes fungen como administradores, operadores y usuarios, el tipo de soporte en que se encuentran, las características del lugar en que se localizan, si es posible su portabilidad, si existe transferencia y si hay encargados.
-

- Detallar las medidas de seguridad existentes con la que cuenta cada sistema, detección de riesgos, análisis de brechas, con base en ello la elaboración del plan de trabajo, estableciendo mecanismos de monitoreo y generar acciones que permitan fortalecer las medidas de seguridad existentes y creación de nuevas.

Es de esta manera como se estructuró e integró el presente Documento de Seguridad, sustentado con la información proporcionada por las distintas Unidades Administrativas.

Es oportuno considerar que de conformidad con el artículo 89, fracciones XII y XIII de la LGDPPSO, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) está facultado para proporcionar apoyo técnico a los responsables, para el cumplimiento de las obligaciones establecidas en dicha Ley, así como para divulgar y emitir las recomendaciones, estándares y mejores prácticas en las materias reguladas por la misma.

I. MARCO NORMATIVO

Para efectos del presente documento, la normatividad aplicable es la siguiente:

- Artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017.
- Ley del Seguro Social
- Ley Orgánica de la Administración Pública Federal, cuya última reforma fue publicada en el Diario Oficial de la Federación el 24 de abril de 2018.
- Reglamento Interior del Instituto Mexicano del Seguro Social, cuya última reforma fue publicada en el Diario Oficial de la Federación el 23 de agosto de 2012.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público 19/12/2017 DOF.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018.

- Lineamientos que Establecen los Parámetros, Modalidades y Procedimiento para la Portabilidad de Datos Personales, publicados en el Diario Oficial de la Federación el 12 de febrero de 2018.

- Metodología de Análisis de Riesgo BAA.- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Junio 2015.

II. ABREVIATURAS Y DEFINICIONES

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.

IMSS: Instituto Mexicano del Seguro Social

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017.

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

UIT: Unidad de Integridad y Transparencia

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

Datos Personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos Personales Sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico,

estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

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.

Responsable: Los sujetos obligados del ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, a que se refiere el artículo 1 de la Ley que deciden sobre el tratamiento de datos personales.

Titular: La persona física a quien corresponden los datos personales. Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona 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.

III. Ámbito de Aplicación y Observaciones Generales

En atención a los Deberes a que se refiere la LGPDPPSO, el presente documento, es aplicable para todos los servidores públicos adscritos a las distintas Unidades Administrativas del Instituto Mexicano del Seguro Social que, en el ejercicio de sus atribuciones y funciones, administren bases de datos en sistemas de tratamiento de datos personales, ya sea que obren en soportes físicos y/o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento, almacenamiento y organización. Los datos personales podrán ser expresados en forma numérica, alfabética, grafica, alfanumérica, fotográfica, acústica o en cualquier otro formato.

Todos los servidores públicos, no importando las funciones que tengan encomendadas, están obligados a conocer y aplicar las medidas de seguridad propias de cada Sistema o mecanismo físico o Administrativo en el que se concentren datos personales, por lo que el documento de seguridad es aplicable en todas las Unidades Administrativas, Médicas y Operativas con las que cuente el Instituto Mexicano del Seguro Social, así como cada una de las fases de tratamiento de los datos personales, iniciando desde la obtención de estos y finalizando con su eliminación.

Cabe mencionar que, la obligación de confidencialidad debe subsistir aún después de que los involucrados hayan finalizado su empleo, cargo o comisión, o bien su participación directa en el tratamiento de los datos personales, sea por cambio de funciones o conclusión de la relación laboral con el Instituto.

Con independencia de su empleo, cargo a comisión que desempeñe, todo servidor público adscrito al Instituto Mexicano del Seguro Social tiene la obligación de guardar y hacer guardar los principios de legalidad, objetividad, profesionalismo, honradez,

lealtad, imparcialidad, eficiencia, eficacia, equidad, transparencia, economía, integridad y competencia por mérito que rigen el servicio público, debiendo conducirse de la siguiente manera:

Funciones Genéricas en Cualquier Nivel de Tratamiento.

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se haya establecido para tal fin.
- Regular su actuación de acuerdo con los principios de protección de datos personales: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.
- Guardar confidencialidad sobre la información que conozcan en el desarrollo de sus actividades.
- Estar capacitado en materia de tratamiento de datos personales.
- Dar aviso a los superiores jerárquicos, ante cualquier acción que pueda poner en riesgo los datos personales, y en general que puedan vulnerar la seguridad de los datos personales.

De manera particular y de conformidad con los cargos, encargos y/o designaciones de los servidores públicos, se definen cuatro roles básicos en el tratamiento de los datos personales:

- Responsable del Sistema
- Administrador del Sistema
- Operadores y
- Enlace de datos personales

Sus funciones son las siguientes:

- **Responsable del Sistema**: Siempre será el titular de la Unidad Administrativa donde se administre el sistema de que se trate. Deberá:

  ✔ Dar aviso a la Unidad de Transparencia de los Sistemas que involucren tratamiento de datos personales, a cargo de dicha Unidad Administrativa.

  ✔ Designar al Administrador del Sistema

✔ Validar que la información entregada por los titulares de los datos personales, sea la estrictamente necesaria para cumplir con los fines legales para los cuales se hubieran recabado.

- **Administrador del Sistema**: Será el servidor público a quien designe de manera expresa el Titular de la Unidad Administrativa. Tiene a su cargo la responsabilidad de la administración del sistema y de los operadores. Deberá:

  ✔ Mantener actualizado el Sistema
  ✔ Determinar los servidores públicos que deben tener acceso a los datos personales en función del tratamiento que debe aplicarse a los mismos.
  ✔ Autorizar los accesos de los servidores públicos, determinar los privilegios y limitantes y llevar un registro de los mismos.
  ✔ Implementar las medidas de seguridad con la finalidad de evitar vulneraciones de la información.

- **Operador (es)**

  ✔ Sus funciones quedan determinadas de acuerdo al perfil que se haya asignado en el tratamiento de los datos personales de cada uno de los sistemas.

- **Enlace de datos personales**

  ✔ Conocer el inventario de Sistemas que involucren tratamiento de datos personales y por cada uno, conocer el tipo de datos personales que se recaban y el nombre del Encargado por cada Sistema.
  ✔ Dar seguimiento a las acciones de capacitación para los servidores públicos involucrados en el tratamiento de los datos personales.
  ✔ Atender a los requerimientos de información que solicite la DGT.

En cumplimiento a lo establecido en el Documento de Seguridad, así como por la LGPDPPSO y los Lineamientos Generales de Protección de Datos Personales, causará la aplicación de medidas de apremio y/o sanciones, que se detallan en dichos instrumentos normativos.

En caso de existir figura de “Encargado”, en la formalización de la presentación del servicio que implique la trasferencia de datos para su tratamiento, deberá atenderse a lo previsto en el artículo 59 de la LGPDPPSO y los artículos correspondientes de los

Lineamientos Generales de Protección de Datos Personales, que se refieren a la existencia de algún instrumento jurídico que incluya cláusulas sobre el tratamiento de datos personales conforme a las instrucciones del responsable, que prevean que los datos no se tratarán para finalidades distintas a las previstas, que establezcan que se implementarán medidas de seguridad, que se informará al responsable en caso de vulneración, que se guardará confidencialidad respecto de los datos personales, que éstos se suprimirán o devolverán al concluir la relación jurídica en atención a las normas jurídicas sobre su conservación y que se abstendrán de transferirlos salvo determinación del responsable en atención a la normatividad y el aviso de privacidad correspondiente.

Asimismo, el Comité de Transparencia es el área responsable de dar a conocer a los servidores públicos del IMSS el Programa de Protección de Datos Personales, que se basa en un sistema de gestión, a fin de que el personal conozca sus funciones para el cumplimiento del sistema de gestión y las consecuencias de su incumplimiento.

IV. DESARROLLO

1. Inventario de Sistemas de Tratamiento de Datos Personales.

Los sistemas que se detallan en el presente documento son aquellos que contienen datos personales, que se encuentran tanto en soporte electrónico como físico:

1	**DataMart Cobranza (Repositorio de Información)**
2	**DataMart Información IMSS-SAT (Repositorio de Información)**
3	**DataMart Afiliación (Repositorio de Información).**
4	**Sistema de Datos Personales de Registro de Beneficiaros (ACCEDER UNIFICADO).**
5	**Sistema de Clasificación de Empresas Riesgos de Trabajo.**
6	**Consulta de Riesgos de Trabajo Terminados**
7	**Programa Especial del Control del Artículo 43 (PEC-A43RI).**
8	**MAC Presencial - Modulo de Actualización de la Clasificación**
9	**MAC II IMSS DIGITAL (Gestión de Clasificación de Empresas)**
10	**Automatización del PAC.**
11	**Movimientos Patronales (escritorio virtual).**
12	**Consulta de Riesgos de Trabajo Terminados**
13	**Servicio Integral de Obras de Construcción (SIROC).**
14	**Sistema de Corrección en Línea (SISCONET)**
15	**Sistema de Automatizada de Pensiones (SC01),**

16	Sistema de Certificación de Incapacidad de Riesgo de Trabajo
17	Sistema de Certificación Manual de Incapacidades (SC 20)
18	Servicio web de Certificación de Inactividad para el Pago de Parcialidades (Trámite, Retiro por Desempleo)
19	Web Service de Certificación del derecho al Retiro por Desempleo
20	Sistema Integral de Semanas Cotizadas (SISEC).
21	Sistema de Verificación de Pagos (SIVEPA)
22	Sistema IMSS Convenios
23	Sistema de Cobranza (SISCOB)
24	Sistema de Fianzas y Garantías
25	Sistema de Devoluciones de Cuotas Obrero Patronales (SIDECO)
26	Sistema Integral para el Control de Actos de Fiscalización
27	Programa de Monitoreo de la Casuística
28	Alta Patronal presencial para Personas Físicas
29	Alta Patronal Persona Física NO Presencial del IMSS Digital
30	Asignación de NSS en Ventanilla Subdelegacional
31	Régimen de Incorporación de la Seguridad Social
32	Catálogo Nacional de Asegurados
33	Actualización de dato CURP
34	Corrección de Datos del Asegurado
35	Certificados IMSS Número Patronal del Identificación Electrónica (NPIE)
36	Consulta de Movimientos Afiliatorios
37	Inscripción a la Continuación Voluntaria al Régimen Obligatorio
38	DataMart Afiliación (AFICOB)
39	Emisión Bimestral Anticipada
40	Emisión Mensual Anticipada
41	Emisión de Seguros Especiales
42	IMSS DESDE SU EMPRESA
43	Incorporación al Seguro de Salud para la Familia
44	Incorporación Voluntaria al Régimen Obligatorio
45	Eliminación de Registro por Homonimia
46	Incorporación de las personas trabajadoras del hogar
47	Personas Trabajadoras Independientes
48	Captura de Movimientos Afiliatorios recibidos a través de ventanilla Subdelegacional.
49	Administración de Usuarios de los Servicios Digitales
50	Almacenes de Datos de Operación
51	Seguridata

52	Sistema de Incorporación de Mexicanos en el Extranjero.
53	Sistema Integral de Derechos y Obligaciones para Asegurados, Patrones y Municipios.
54	Sistema de Registro de Movimientos Afiliatorios para Productores Eventuales del Campo.
55	Sistema de Registro de Movimientos Afiliatorios para Productores de caña de Azúcar.
56	Sistema Único de Autodeterminación
57	Sistema Único de Emisiones
58	Visor de solicitudes de IMSS Digital
59	Alta Patronal Presencial
60	Alta Patronal Persona Moral NO Presencial
61	Alta Patronal Persona Moral
62	Sistema de Dictamen Electrónico del IMSS (SIDEIMSS).
63	Sistema de Investigación de Mercados.
64	SIAP_CGRH_DRL_Gestión nómina jubilados pensionados IMSS
65	SIAP_CGRH_DSPNC_Integración expediente histórico
66	SIAP_CGRH_DPP_RH200_Administración prestaciones
67	SIAP_CPGGSP_Control del proceso
68	SIAP_CRL_Pago de finiquitos
69	SICAVI_CA_Impartición cursos capacitación
70	SIAP_DANM_Contratación serv públicos mando
71	FacE Sistema de Emisión de Facturación Electrónica
72	Servicio digital de recepción de facturas para proveedores.
73	Sistema de Administración de Siniestros
74	Nombre del Sistema. Sistema de Salud en el Trabajo (SISAT)
75	Sistema de Información de Prestaciones Sociales Institucionales (SIPSI).
76	Sistema de Trámite de Inscripción a Guarderías por Internet
77	Sistema de Administración Hotelero para Centros Vacacionales
78	Sistema SSC
79	FORMATO CAICE
80	FORMATO SIQUEM
81	SIADE
82	SSCC
83	Vacunas COVID 19

2. Descripción y Estructura de los Sistemas de Tratamiento de Datos Personales

En la descripción de cada sistema de tratamiento de datos personales se señala el objetivo, fundamento legal, servidor público que administra el sistema, operador (es) y usuarios de éste y el tipo de datos personales que se tratan en los sistemas que a continuación se enlistan:

1	**DataMart Cobranza (Repositorio de Información)**
2	**DataMart Información IMSS-SAT (Repositorio de Información)**
3	**DataMart Afiliación (Repositorio de Información).**
4	**Sistema de Datos Personales de Registro de Beneficiaros (ACCEDER UNIFICADO).**
5	**Sistema de Clasificación de Empresas Riesgos de Trabajo.**
6	**Consulta de Riesgos de Trabajo Terminados**
7	**Programa Especial del Control del Artículo 43 (PEC-A43RI).**
8	**MAC Presencial - Modulo de Actualización de la Clasificación**
9	**MAC II IMSS DIGITAL (Gestión de Clasificación de Empresas)**
10	**Automatización del PAC.**
11	**Movimientos Patronales (escritorio virtual).**
12	**Consulta de Riesgos de Trabajo Terminados**
13	**Servicio Integral de Obras de Construcción (SIROC).**
14	**Sistema de Corrección en Línea (SISCONET)**
15	**Sistema de Automatizada de Pensiones (SC01),**
16	**Sistema de Certificación de Incapacidad de Riesgo de Trabajo**
17	**Sistema de Certificación Manual de Incapacidades (SC 20)**
18	**Servicio web de Certificación de Inactividad para el Pago de Parcialidades (Trámite, Retiro por Desempleo)**
19	**Web Service de Certificación del derecho al Retiro por Desempleo**
20	**Sistema Integral de Semanas Cotizadas (SISEC).**
21	**Sistema de Verificación de Pagos (SIVEPA)**
22	**Sistema IMSS Convenios**
23	**Sistema de Cobranza (SISCOB)**
24	**Sistema de Fianzas y Garantías**
25	**Sistema de Devoluciones de Cuotas Obrero Patronales (SIDECO)**
26	**Sistema Integral para el Control de Actos de Fiscalización**
27	**Programa de Monitoreo de la Casuística**
28	**Alta Patronal presencial para Personas Físicas**
29	**Alta Patronal Persona Física NO Presencial del IMSS Digital**
30	**Asignación de NSS en Ventanilla Subdelegacional**
31	**Régimen de Incorporación de la Seguridad Social**

32	**Catálogo Nacional de Asegurados**
33	**Actualización de dato CURP**
34	**Corrección de Datos del Asegurado**
35	**Certificados IMSS Número Patronal del Identificación Electrónica (NPIE)**
36	**Consulta de Movimientos Afiliatorios**
37	**Inscripción a la Continuación Voluntaria al Régimen Obligatorio**
38	**DataMart Afiliación (AFICOB)**
39	**Emisión Bimestral Anticipada**
40	**Emisión Mensual Anticipada**
41	**Emisión de Seguros Especiales**
42	**IMSS DESDE SU EMPRESA**
43	**Incorporación al Seguro de Salud para la Familia**
44	**Incorporación Voluntaria al Régimen Obligatorio**
45	**Eliminación de Registro por Homonimia**
46	**Incorporación de las personas trabajadoras del hogar**
47	**Personas Trabajadoras Independientes**
48	**Captura de Movimientos Afiliatorios recibidos a través de ventanilla Subdelegacional.**
49	**Administración de Usuarios de los Servicios Digitales**
50	**Almacenes de Datos de Operación**
51	**Seguridata**
52	**Sistema de Incorporación de Mexicanos en el Extranjero.**
53	**Sistema Integral de Derechos y Obligaciones para Asegurados, Patrones y Municipios.**
54	**Sistema de Registro de Movimientos Afiliatorios para Productores Eventuales del Campo.**
55	**Sistema de Registro de Movimientos Afiliatorios para Productores de caña de Azúcar.**
56	**Sistema Único de Autodeterminación**
57	**Sistema Único de Emisiones**
58	**Visor de solicitudes de IMSS Digital**
59	**Alta Patronal Presencial**
60	**Alta Patronal Persona Moral NO Presencial**
61	**Alta Patronal Persona Moral**
62	**Sistema de Dictamen Electrónico del IMSS (SIDEIMSS).**
63	**Sistema de Investigación de Mercados.**
64	**SIAP_CGRH_DRL_Gestión nómina jubilados pensionados IMSS**
65	**SIAP_CGRH_DSPNC_Integración expediente histórico**

66	**SIAP_CGRH_DPP_RH200_Administración prestaciones**
67	**SIAP_CPGGSP_Control del proceso**
68	**SIAP_CRL_Pago de finiquitos**
69	**SICAVI_CA_Impartición cursos capacitación**
70	**SIAP_DANM_Contratación serv públicos mando**
71	**FacE Sistema de Emisión de Facturación Electrónica**
72	**Servicio digital de recepción de facturas para proveedores.**
73	**Sistema de Administración de Siniestros**
74	**Nombre del Sistema. Sistema de Salud en el Trabajo (SISAT)**
75	**Sistema de Información de Prestaciones Sociales Institucionales (SIPSI).**
76	**Sistema de Trámite de Inscripción a Guarderías por Internet**
77	**Sistema de Administración Hotelero para Centros Vacacionales**
78	**Sistema SSC**
79	**FORMATO CAICE**
80	**FORMATO SIQUEM**
81	**SIADE**
82	**SSCC**
83	**Vacunas COVID 19**

3. Medidas de Seguridad

Las medidas de seguridad deben conjugarse con el nivel de protección que requieren las bases de datos. Por ejemplo, el nivel de protección será mayor cuando se trate de bases de datos que resguarden datos personales sensibles y/o almacenen información de una gran cantidad de titulares de acuerdo con la siguiente clasificación:

– **Datos identificativos**: El nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Matrícula, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, demás análogos;

– Datos electrónicos: 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 u otra red de comunicaciones electrónicas;

– Datos laborales: Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio, demás análogos;

– Datos patrimoniales: Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales, demás análogas;

– Datos académicos*:* Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos, demás análogos;

– Datos sobre la 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, y demás análogos;

– Datos biométricos*:* huellas dactilares, ADN, geometría de la mano, características de iris y retina, demás análogos; y,

– Datos especialmente protegidos (sensibles): en algunos casos los datos biométricos arriba señalados, origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual; así como los datos de niños y niñas y demás análogos.

Es necesario advertir que algunos tipos de datos arriba mencionados son susceptibles de hacerse públicos, cuando por ley exista una obligación de difundirlos y/o se trate de servidores públicos, tal es el caso de algunos datos identificativos, patrimoniales, laborales, académicos.

Como parte de las acciones realizadas por las Unidades Administrativas en las que se tiene tratamiento de datos personales se procedió a la elaboración de

una ficha técnica por cada sistema en la que se describen las medidas de seguridad con las que cuentan para reducir su vulnerabilidad ante un posible riesgo:

1	**DataMart Cobranza (Repositorio de Información)**
2	**DataMart Información IMSS-SAT (Repositorio de Información)**
3	**DataMart Afiliación (Repositorio de Información).**
4	**Sistema de Datos Personales de Registro de Beneficiaros (ACCEDER UNIFICADO).**
5	**Sistema de Clasificación de Empresas Riesgos de Trabajo.**
6	**Consulta de Riesgos de Trabajo Terminados**
7	**Programa Especial del Control del Artículo 43 (PEC-A43RI).**
8	**MAC Presencial - Modulo de Actualización de la Clasificación**
9	**MAC II IMSS DIGITAL (Gestión de Clasificación de Empresas)**
10	**Automatización del PAC.**
11	**Movimientos Patronales (escritorio virtual).**
12	**Consulta de Riesgos de Trabajo Terminados**
13	**Servicio Integral de Obras de Construcción (SIROC).**
14	**Sistema de Corrección en Línea (SISCONET)**
15	**Sistema de Automatizada de Pensiones (SC01),**
16	**Sistema de Certificación de Incapacidad de Riesgo de Trabajo**
17	**Sistema de Certificación Manual de Incapacidades (SC 20)**
18	**Servicio web de Certificación de Inactividad para el Pago de Parcialidades (Trámite, Retiro por Desempleo)**
19	**Web Service de Certificación del derecho al Retiro por Desempleo**
20	**Sistema Integral de Semanas Cotizadas (SISEC).**
21	**Sistema de Verificación de Pagos (SIVEPA)**
22	**Sistema IMSS Convenios**
23	**Sistema de Cobranza (SISCOB)**
24	**Sistema de Fianzas y Garantías**
25	**Sistema de Devoluciones de Cuotas Obrero Patronales (SIDECO)**
26	**Sistema Integral para el Control de Actos de Fiscalización**
27	**Programa de Monitoreo de la Casuística**
28	**Alta Patronal presencial para Personas Físicas**
29	**Alta Patronal Persona Física NO Presencial del IMSS Digital**
30	**Asignación de NSS en Ventanilla Subdelegacional**
31	**Régimen de Incorporación de la Seguridad Social**

32	**Catálogo Nacional de Asegurados**
33	**Actualización de dato CURP**
34	**Corrección de Datos del Asegurado**
35	**Certificados IMSS Número Patronal del Identificación Electrónica (NPIE)**
36	**Consulta de Movimientos Afiliatorios**
37	**Inscripción a la Continuación Voluntaria al Régimen Obligatorio**
38	**DataMart Afiliación (AFICOB)**
39	**Emisión Bimestral Anticipada**
40	**Emisión Mensual Anticipada**
41	**Emisión de Seguros Especiales**
42	**IMSS DESDE SU EMPRESA**
43	**Incorporación al Seguro de Salud para la Familia**
44	**Incorporación Voluntaria al Régimen Obligatorio**
45	**Eliminación de Registro por Homonimia**
46	**Incorporación de las personas trabajadoras del hogar**
47	**Personas Trabajadoras Independientes**
48	**Captura de Movimientos Afiliatorios recibidos a través de ventanilla Subdelegacional.**
49	**Administración de Usuarios de los Servicios Digitales**
50	**Almacenes de Datos de Operación**
51	**Seguridata**
52	**Sistema de Incorporación de Mexicanos en el Extranjero.**
53	**Sistema Integral de Derechos y Obligaciones para Asegurados, Patrones y Municipios.**
54	**Sistema de Registro de Movimientos Afiliatorios para Productores Eventuales del Campo.**
55	**Sistema de Registro de Movimientos Afiliatorios para Productores de caña de Azúcar.**
56	**Sistema Único de Autodeterminación**
57	**Sistema Único de Emisiones**
58	**Visor de solicitudes de IMSS Digital**
59	**Alta Patronal Presencial**
60	**Alta Patronal Persona Moral NO Presencial**
61	**Alta Patronal Persona Moral**
62	**Sistema de Dictamen Electrónico del IMSS (SIDEIMSS).**
63	**Sistema de Investigación de Mercados.**
64	**SIAP_CGRH_DRL_Gestión nómina jubilados pensionados IMSS**
65	**SIAP_CGRH_DSPNC_Integración expediente histórico**

66	**SIAP_CGRH_DPP_RH200_Administración prestaciones**
67	**SIAP_CPGGSP_Control del proceso**
68	**SIAP_CRL_Pago de finiquitos**
69	**SICAVI_CA_Impartición cursos capacitación**
70	**SIAP_DANM_Contratación serv públicos mando**
71	**FacE Sistema de Emisión de Facturación Electrónica**
72	**Servicio digital de recepción de facturas para proveedores.**
73	**Sistema de Administración de Siniestros**
74	**Nombre del Sistema. Sistema de Salud en el Trabajo (SISAT)**
75	**Sistema de Información de Prestaciones Sociales Institucionales (SIPSI).**
76	**Sistema de Trámite de Inscripción a Guarderías por Internet**
77	**Sistema de Administración Hotelero para Centros Vacacionales**
78	**Sistema SSC**
79	**FORMATO CAICE**
80	**FORMATO SIQUEM**
81	**SIADE**
82	**SSCC**
83	**Vacunas COVID 19**

Las medidas de seguridad que deberán adoptarse por el responsable serán con base en el nivel de riesgo que presenta cada tratamiento de datos personales. Para ello, es necesario calcular los factores de riesgo por tipo de dato, por tipo de acceso y por entorno desde el cual se realizan los tratamientos de los datos personales.

A partir del tipo de dato es posible reconocer el factor de riesgo inherente, por lo que a continuación abordaremos las medidas de seguridad de acuerdo con su naturaleza: Administrativas, Físicas y Técnicas.

Medidas de Seguridad de Tipo Administrativo

Se tienen establecidos procedimientos que permiten fortalecer el resguardo y custodia de los sistemas de información que resguardan datos personales, lo anterior a través de cartas de responsabilidad en las cuales se especifican las condiciones de uso y acceso a la información.

Para el caso de los sistemas en soporte electrónico administrados por un Encargado, se atiende a las medidas de seguridad establecidas en el instrumento jurídico que se haya formalizado y que deben ser equivalentes con las previstas en el Documento de Seguridad para cada sistema de tratamiento.

El artículo 33, fracciones IV, V y VI de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la realización del análisis de riesgo, análisis de brecha y plan de trabajo, en los siguientes términos:

> *"... 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:*
>
> *I. [...]*
>
> *IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;*
>
> *V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*
>
> *VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales; [...]*

Medidas de Seguridad de Tipo Físico.

De acuerdo con la información Proporcionada por todas y cada una de las Unidades Administrativas en las que se manejan datos personales, el Instituto Mexicano del Seguro Social cuenta con las siguientes medidas de seguridad:

Para la prevención del acceso no autorizado al perímetro institucional, tales como instalaciones físicas, áreas críticas, recursos e información, se cuenta con un contrato de prestación de servicios de seguridad y vigilancia que tiene por objeto proteger las instalaciones, bienes y personas en los distintos inmuebles con que se cuenta, ello para tener capacidad de respuesta inmediata y oportuna ejecución de las medidas de prevención, contención, neutralización y mitigación de cualquier amenaza, lo que se traduce en resguardar las instalaciones físicas, áreas críticas, recursos e información de manera permanente, mediante control de accesos y uso obligatorio de gafetes, control de recepción, vigilancia en sótanos, control en estacionamiento y apoyo en vialidad periférica.

Se cuenta con Normas, Procedimientos y medidas de seguridad contemplados en el Programa Interno de Protección Civil que contienen el diseño y establecimiento de lineamientos de salvaguarda aplicables al interior de los inmuebles, con el propósito de reducir al mínimo la incidencia de riesgos como: protocolo de acceso a las áreas estratégicas, ante posibles sabotajes, manifestaciones, amenazas de bomba, de sismos y de incendio.

El IMSS cuenta también con acciones y mecanismos que permiten proteger e identificar los equipos móviles y portátiles; mobiliario, documentos y materiales mediante controles de entrada y salida, como son: control en el uso de aparatos electrónicos y eléctricos, control en el ingreso y egreso de aparatos, equipos, mobiliarios, documentos y materiales mediante pase de salida autorizado por un Servidor público habilitado y cuya firma se encuentra autorizada y registrada en todos los puntos de acceso.

Los equipos de cómputo de escritorio y portátiles que la Dirección de Innovación y Desarrollo Tecnológico asigna a los servidores públicos y unidades administrativas para el cumplimiento de sus funciones, así como los equipos destinados al procesamiento, almacenamiento, transmisión y respaldo de la información relacionada a los Sistemas de información instalaciones, cuentan con un número de inventarios, así como con paquetería autorizada y con licencia de uso vigente, que son sometidos de manera programada y oportuna al mantenimiento correspondiente por personal especializado o bien, por el fabricante de los equipos.

Medidas de Seguridad de Tipo Técnico.

Los sistemas de información que son operados en las distintas Unidades Administrativas del Instituto Mexicano del Seguro Social, contemplan controles de acceso lógico conforme lo siguiente:

Prevención contra acceso no autorizado, detección de amenaza y antidenegación de servicios, Cifrado de información de tránsito, Almacenamiento y respaldos de información, Supervisión contra actividad sospechosa o anómala, Redundancia de componentes de comunicaciones y seguridad. Monitoreo de sistemas de información, Pruebas de seguridad para prevenir vulneración por defectos de software.

El acceso a los repositorios de datos se controla a través de cédulas de registro que la Dirección de Innovación y Desarrollo Tecnológico, gestiona por solicitud de área de

negocio correspondiente, así mismo se tiene debidamente identificado al personal de áreas técnicas que controla y tiene funciones de operar dichos sistemas de información. Las funciones del usuario de los sistemas de información institucionales son definidas por las áreas responsables de los procesos respectivos, quienes también tienen la encomienda de validar que tal perfil de usuario se apegue a los requerimientos funcionales, teniéndose actualmente implementadas las siguientes medidas de carácter técnico estipuladas por la DIDT para impulsar la operación eficiente y la modernización en la automatización de los procesos necesarios:

Prevención contra acceso no autorizado, detección de amenaza y antidenegación de servicios.

- Cifrado de información de tránsito.
- Almacenamiento y respaldos de información.
- Supervisión contra actividad sospechosa o anómala.
- Redundancia de componentes de comunicaciones y seguridad.
- Monitoreo de sistemas de información.
- Pruebas de seguridad para prevenir vulneración por defectos de software
- Cuidado y uso de los recursos y servicios informáticos.
- Los usuarios no tienen permitido:

• Transmitir, redistribuir, usar, descargar, reproducir y divulgar material con contenido discriminatorio, difamatorio, pornográfico, obsceno, malicioso; información confidencial o reservada propiedad del IMSS sin consentimiento de quien legalmente pueda otorgarlo; material protegido por el derecho de propiedad intelectual; archivos de música, videos, juegos y/o software que pueda distraer a los servidores públicos de sus funciones o que comprometa los bienes informáticos y los servicios de red.

• Exponer las redes del Instituto a cualquier tipo de amenaza interna y/o externa.

La DIDT lleva a cabo acciones de supervisión sólo de aquellos equipos que son propiedad del IMSS, asegurándose de su mantenimiento preventivo, correctivo e instalación de software institucional. Además de auxiliar a las instancias competentes para la realización de inspecciones o supervisión del uso de los bienes informáticos, así como de la información contenida en éstos.

Asignación de bienes informáticos.

El usuario asume la responsabilidad total del resguardo y uso que se le dé a los bienes informáticos y utiliza el software institucional bajo su resguardo, únicamente para la realización de sus funciones y conforme a la licencia de uso, por lo que no deberá distribuirlo o reutilizarlo en un equipo distinto al asignado para el desempeño de sus funciones.

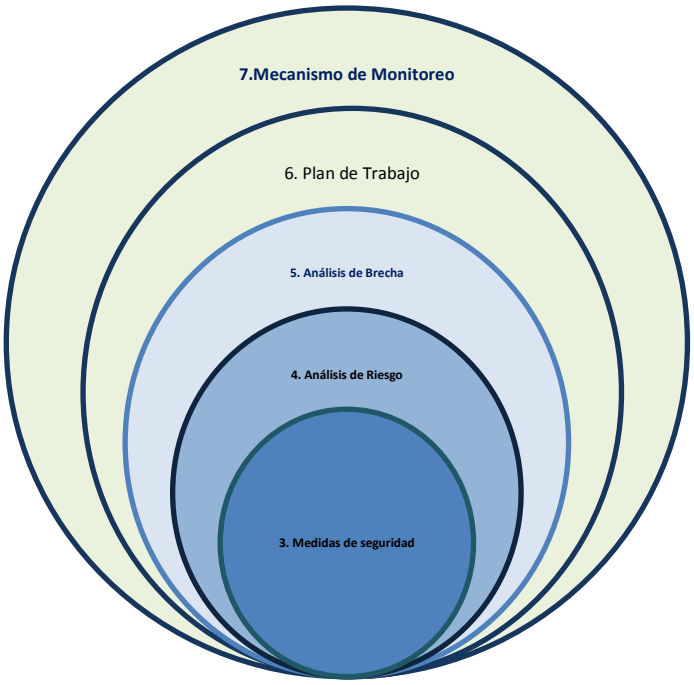
A su vez se abstiene de instalar cualquier software adicional (comercial, shareware, freeware, etcétera) al originalmente preinstalado en los equipos de cómputo, sin previa autorización de la Dirección General de Tecnologías de la Información.

Se eliminan los correos electrónicos no deseados o de personas desconocidas, cadenas de correos y evitar su reenvío, previendo la propagación de virus, páginas de suplantación de identidad (phishing) u otro tipo de software malicioso.

Previo a su ejecución analiza con el software antivirus todos aquellos medios como, discos compactos, DVD, memorias USB u otros tipos de almacenamiento externos al equipo de cómputo, que sean conectados a éste.

Genera el reporte correspondiente ante el la mesa de ayuda, si se sospecha de alguna infección por virus en algún equipo de cómputo.

El usuario se abstiene de introducir software malicioso en el equipo de cómputo, así como herramientas que realicen conexiones desconocidas o túneles, las cuales pueden provocar un daño a la red o información del Instituto Mexicano del Seguro Social, con amenazas como virus, (worms, spyware, ráfagas de correo electrónico no solicitado, o cualquier otro tipo de malware).



4. Análisis de Riesgos

De conformidad con el artículo 33, fracción IV, de la LGPDPSO, el análisis de riesgo debe ser elaborado considerando las amenazas y vulnerabilidades existentes para los datos personales que son recabados y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, el tipo de hardware, software, o las características del responsable, entre otros.

Para lograr identificar los riesgos existentes, es necesario tomar en consideración las medidas de seguridad que están adoptando las áreas responsables, tomando como referencia el nivel de riesgo que presenta cada tratamiento de datos personales.

De conformidad con lo estipulado en el artículo 60 de los Lineamientos Generales, en la realización del análisis de riesgo se deberá considerar lo siguiente:

• La existencia de requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico para proteger los datos personales.

• El valor de los datos personales de acuerdo con su clasificación previamente definida, y su ciclo de vida, de conformidad con la normatividad aplicable.

• El valor y exposición de los activos involucrados en su tratamiento.

Un activo es la información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de datos personales que tenga valor para el Instituto Mexicano del Seguro Social.

Existen dos tipos de activos, los primarios y de soporte. Los activos primarios corresponden a los procesos de gestión y actividades, así como a la información crítica, por ejemplo, toda la información vital para la operación institucional, la información personal especificada dentro del marco regulatorio de privacidad e información estratégica.

Los activos de soporte son aquellos que apoyan a los activos primarios para su operación y consisten en: equipo de cómputo (hardware), aplicaciones (software), equipos de comunicaciones, personal, instalaciones y estructura organizacional.

La aplicación de la Metodología de Análisis de Riesgo BAA fue la clave para calcular los factores antes referidos. Esta metodología se conoce así por las tres variables en las que se enfoca para determinar el nivel de riesgo de los datos personales:

Beneficio para el atacante;
Accesibilidad para el atacante; y

Anonimidad del atacante.

En suma, la combinación de los tres factores analizados permitió definir el nivel de riesgo latente por tratamiento, lo cual contribuirá a identificar la efectividad de las medidas de seguridad que deban implementarse en cada caso aplicando los siguientes principios:

Licitud. El tratamiento de los datos personales tenga que hacerse, siempre, de forma lícita y legítima o leal, con apego a la normativa aplicable.

Finalidad. Es el propósito, motivo o razón por el cual se tratan los datos personales.

Lealtad. Tratamiento de los datos de manera lícita y en apego a la legalidad.

Consentimiento. Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

Calidad. Significa que los datos deben ser correctos, exactos y completos y estar actualizados según sea necesario con respecto a los fines para los cuales se hayan recopilado.

Proporcionalidad. Quienes tratan datos personales deben usarlos solamente para los finales para los cuales fueron recabados, siendo éstos los estrictamente necesarios.

Información. El medio a través del cual el responsable del tratamiento informa al titular de los datos personales, entre otros aspectos, sobre qué datos personales obtiene y para qué los va a tratar.

Responsabilidad. Los responsables de los datos deben adoptar e implementarán las medidas correspondientes para el cumplimiento de los principios.

Hecho lo anterior, es menester puntualizar que las medidas de seguridad que deberán adoptarse por el responsable deben tomar como referencia el nivel de riesgo que presenta cada tratamiento de datos personales.

Para ello, es necesario calcular los factores de riesgo por tipo de dato, por tipo de acceso y por entorno desde el cual se realizan los tratamientos de los datos personales.
A partir del tipo de dato es posible reconocer el factor de riesgo inherente, como se muestra a continuación:

Tipo de dato	Riesgo Inherente	Nivel de Riesgo
Datos identificativos	Bajo	1
volumen de titulares (personas) que conforman la base de datos	Muy Alto	4
Número de Accesos	Muy Alto	4
Entorno Internet	Muy Alto	4

Realizar un análisis de riesgos por cada tratamiento ayudará a identificar el nivel de medidas de seguridad que deben ser implementadas para la protección de los datos personales.

Una vez identificado el ideal de medidas de seguridad que deberían implementarse, se realiza un comparativo con aquellas que son implementadas por las áreas, obteniendo con ello un análisis de brecha, con el cual resulta posible construir planes de trabajo,

mecanismos de monitoreo y revisión de medidas de seguridad y programas de capacitación, elementos que conforman el Documento de Seguridad de este Alto Tribunal.

5. Análisis de Brecha

Una vez identificado el ideal de medidas de seguridad que deberían implementarse, se realiza un comparativo con aquellas que ya están siendo operadas por las áreas, obteniendo con ello un análisis de brecha, que hará viable la construcción de planes de trabajo, mecanismos de monitoreo y revisión de medidas de seguridad y programas de capacitación, tal y como lo establece el artículo 61 de la Ley General que a la letra dice:

“. Artículo 61. Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:

Las medidas de seguridad es existentes y efectivas; Las medidas de seguridad faltantes, y La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.”.

Así las cosas, tenemos que el análisis de brecha consiste en identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados por las Unidades Administrativas que cuentan con sistemas o realizan el tratamiento de datos personales.

El análisis de brecha es de naturaleza diagnóstica y contribuirá a conocer las áreas de oportunidad por cada tratamiento. A su vez, esta información dará sustento a las políticas y mecanismos institucionales en materia de protección de datos personales que se deban aprobar en su momento, por el Comité de Transparencia para atenderlas de manera paulatina y en coordinación con cada una de las áreas.

Como se puede observar, las unidades administrativas que operan sistemas en los que se tratan datos personales ya cuentan con las siguientes medidas de seguridad implementadas:

Declaración de confidencialidad: La declaratoria es puesta a disposición de todo el personal que utiliza un equipo de cómputo y más aún si tienen intervención en el tratamiento de datos personales para que estén informados de los deberes y medidas de seguridad que deben tomar en consideración en sus actividades relacionadas con dichos tratamientos.

Listado de personal: Se cuenta con el documento que contiene la relación del personal que interviene en el tratamiento de datos personales, en donde se incluye nombre, cargo, funciones en el tratamiento y obligaciones en materia de datos personales por cada tratamiento como una más de las medidas de seguridad.

Capacitación: El personal involucrado en el tratamiento de los datos personales regularmente se capacita de manera periódica en materia de datos personales autorizados por el Comité de Transparencia en el Programa Anual de Capacitación.

Bitácora de vulneraciones: La Dirección de Innovación y Desarrollo Tecnológico cuenta con un control informativo en donde se reporten los tipos de vulneraciones con los siguientes datos, plasmándose datos clave, tales como: fecha y lugar en donde se produjo, nombre y cargo de quien notifica la incidencia, nombre y cargo de la persona a la que se le comunica, y las medidas que se implementaron para subsanar la misma.

Toda vulneración se debe notificarse, además de al área responsable, a la Dirección de Innovación y Desarrollo Tecnológico para que tome las acciones pertinentes, reduciendo al máximo los riesgos de vulnerabilidad.

Depuración y borrado seguro del archivo físico: Institucionalmente se cuenta con estricto apego a lo dispuesto por la disposición legal en materia de conservación de derechos, realizando la Transferencia, depuración de los archivos de manera periódica, conforme a los plazos de conservación y parámetros dispuestos la normativa en materia.

Depuración y borrado seguro del archivo electrónico: Para dar cumplimiento a todas las disposiciones normativas se lleva a cabo de manera segura la eliminación de manera segura y permanente, las bases de datos o parte de ellas que se encuentren en archivo electrónico, en desuso o que hayan cumplido su finalidad o el tiempo de conservación dispuesto para el archivo administrativo.

Bitácora de consulta: La Dirección de Innovación y Desarrollo Tecnológico se tiene establecida una bitácora como control para registrar el nombre, cargo, fecha y hora de consulta de la base de datos.

6. Plan de Trabajo

El Artículo 62 de la LGPDPPSO establece que: "… De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.".

Partiendo de esta disposición podemos precisar que el presente documento ofrece una radiografía institucional en materia de protección de los datos personales, reflejando las fortalezas, acciones realizadas así como las pendientes por realizar, situación que se abordará en el programa de trabajo respectivo, puntualizando las áreas de oportunidad, lo que será fundamental para la toma de decisiones.

A partir de las acciones relatadas es que se está trabajando en el diseño de un plan de trabajo, implementación, factibilidad, mecanismos de monitoreo y revisión de medidas de seguridad, elementos que también se integrarán en su momento al documento de seguridad y son imprescindibles para que el Comité de Transparencia disponga lo conducente.

Es importante precisar que el documento de seguridad representa, además de una obligación legal, un instrumento vital para la coordinación de los trabajos de todas las áreas del Instituto Mexicano del Seguro Social encaminados al fortalecimiento y mejora en el tratamiento e implementación de medidas de seguridad de los datos personales bajo su resguardo.

7. Mecanismos de Monitoreo.

En términos de lo dispuesto por la LGPDPPSO, para la garantizar la óptima protección de datos personales, el responsable deberá establecer entre otras actividades, la de monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que puedan estar sujetos los datos personales.

Para ello y con base en el Plan de Trabajo planteado por cada unidad administrativa, se estará solicitando al Administrador de cada uno de los sistemas de tratamiento de

datos personales envíe a la División de Transparencia y Acceso a la Información copia de la evidencia que sustente las acciones realizadas.

El requerimiento referido, se hará durante el mes de diciembre de 2022, a efecto de informar sobre los avances correspondientes al Comité de Transparencia. Para considerar las acciones respectivas dentro de su programa de trabajo 2023.
Posteriormente, en la actualización anual que corresponda, se estará trabajando con los titulares de las unidades administrativas, respecto de la efectividad de las medidas de seguridad implementadas, con la finalidad de evitar alteración, pérdida o acceso no autorizado a los datos personales objeto de tratamiento en los distintos sistemas.

8. Programa General de Capacitación.

Entre las atribuciones de la Unidad de Integridad y Transparencia, está la de presidir el Comité de Transparencia y coordinar la capacitación continua y especializada del personal que integra el Comité de Transparencia del IMSS, así como del personal adscrito al propio organismo en las materias de su competencia.

A su vez, el Comité de Transparencia tiene entre sus atribuciones en materia de protección de datos personales, establecer programas de capacitación y actualización para los servidores públicos.

Derivado de lo anterior, la Unidad de Integridad y Transparencia someterá a consideración y aprobación el Programa de Capacitación 2022 por parte del Comité de Transparencia, con el propósito de capacitar en materia de transparencia, acceso a la información y protección de datos personales, a los servidores públicos del IMSS cuyas actividades tiene relación directa con éstos temas, sin perjuicio de otras actividades de capacitación interna en relación con temas específicos.

Dicho Programa se sustenta en las acciones de capacitación que propone el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) a impartir a lo largo de este año.

Por lo anterior, se prevé iniciar con la primera etapa de capacitación en el primer semestre de 2022, para los Servidores Públicos de Mando, por ser éstos los responsables de los sistemas de tratamiento, para posteriormente generar un efecto multiplicar a los administradores y los operadores de los sistemas en los que se manejan datos personales de cada una de las unidades administrativas, que incluirá los siguientes temas:

- Teoría y normatividad en materia de Datos Personales.
- Principios, deberes y derechos.
- Responsabilidades de los operadores.
- Medidas de seguridad a observar
- Medidas de apremio y sanciones.

9. Actualizaciones.

De conformidad con lo establecido en el artículo 36 de la LGPDPPSO, el Documento de Seguridad será actualizado cuando ocurra alguno de los siguientes eventos:

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

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

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

Cuando se efectúe la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Como una medida de actualización general, se establece que, cuando se lleve a cabo la creación de un nuevo sistema de tratamiento de datos personales o simplemente la creación de bases de datos personales, independientemente del soporte, el Titular de la Unidad Administrativa deberá designar al Administrador del sistema y dar aviso a la Unidad de Integridad y Transparencia, de la creación del nuevo sistema, debiendo mencionar entre datos, el nombre, objetivo y fundamento legal del Sistema, los nombres, cargos y obligaciones del Administrador del sistema y de los operadores, los datos personales recabados y su finalidad, con el objeto de integrarlos al inventario de Sistemas de Tratamiento de Datos del Instituto Mexicano del Seguro Social.

Otro factor que estará determinando la actualización del presente documento, será la emisión por parte del INAI de las herramientas metodológicas para orientar a los responsables en el cumplimiento de sus obligaciones en materia de protección de datos personales, a saber:

1. Recomendaciones para prevenir vulneraciones.
2. Recomendaciones para el manejo de incidentes de seguridad y
3. Recomendaciones para realizar el análisis de riesgo.

Por lo anterior, la periodicidad para la revisión y en su caso actualización del presente Documento de Seguridad será, por primera vez de manera anual a partir de ahí, cada dos años.

Una vez que sufra alguna actualización, el Documento de Seguridad deberá ser sometido nuevamente para aprobación del pleno del Comité de Transparencia del IMSS.

Aprobación.

Mediante Acuerdo número CTSP-0088/01/2023, el Comité de Transparencia del Instituto Mexicano del Seguro Social, de conformidad con lo establecido en los artículos 35, 83 y 84, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; y en cumplimiento con lo dispuesto los Lineamientos Generales de Protección de Datos Personales para el Sector Público, aprobó el presente **Documento de Seguridad para el Tratamiento de Datos Personales, presentado por la Unidad de Transparencia del Instituto Mexicano del Seguro Social.**

Este documento describe y da cuenta de las medidas de seguridad técnicas, físicas y administrativas adoptadas por este Sujeto Obligado, con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de los datos personales**.**