Consejo de la Judicatura Federal

Guía para la integración del documento de seguridad

Comité de Transparencia

Consejo de la Judicatura Federal

Contenido

Introducción

El objetivo de la *Guía para la integración del documento de seguridad*, es en principio, que las instancias del Consejo de la Judicatura Federal conozcan y tengan presente la importancia y alcances de la protección de datos personales que ejercen día a día.

Tal conocimiento resulta fundamental, no solo para el cumplimiento de las obligaciones previstas en la Constitución Política de los Estados Unidos Mexicanos, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los Lineamientos Generales de Protección de Datos Personales para el Sector Público y la normativa del propio Consejo, sino por el activo papel que guardan en la protección de la identidad de las personas en la sociedad actual, misma que otorga un valor superior a la protección de la intimidad.

Lo anterior es relevante, si se toma en consideración que cada servidor público, independientemente de su nivel jerárquico o de las funciones que le son otorgadas, conserva bajo su custodia el resguardo de la información personal y sensible que las personas confían a las áreas administrativas y órganos jurisdiccionales del Poder Judicial de la Federación para el ejercicio de sus derechos.

Es importante recordar, que el Artículo 12, de la Declaración Universal de Derechos Humanos, dispone lo siguiente:

> *"Artículo 12*
>
> *Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su*

reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."

Disposición que en el servicio público, conlleva la obligación de garantizar la intimidad de las personas a través de la concepción de un papel activo y continuo en la protección de los datos personales.

Por tanto, este papel activo de los servidores públicos, resulta una tarea por demás noble y congruente con la misión y atribuciones del Consejo de la Judicatura Federal y, además, legitima al Poder Judicial de la Federación no sólo como el órgano encargado de velar por el cumplimiento de la ley y la impartición de justicia, sino como defensor de los derechos humanos.

De modo que, garantizar la protección de los datos personales se traduce en uno de los bastiones de lucha que, como ciudadano y servidor público, se ponen a nuestro alcance para combatir la injusticia y la trasgresión de derechos, siempre en defensa de los principios constitucionales mexicanos.

Metodología

El *Acuerdo General del Pleno del Consejo de la Judicatura Federal que establece las disposiciones en materia de protección de datos personales*, establece en su artículo 15, que la Unidad de Transparencia elaborará el **documento de seguridad** a que se refiere el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), el cual se integrará con la información que las instancias le remitan.

En ese sentido, las instancias del Consejo de la Judicatura Federal que cuenten con sistemas de datos personales, deberán comunicar a la Unidad de Transparencia, los siguiente:

I. Las funciones y obligaciones del personal involucrado en su tratamiento.
II. El inventario de datos personales respectivo.
III. Análisis de riesgo.
IV. Análisis de brecha.
V. Un plan de trabajo.

Al respecto, con la finalidad de apoyar a las instancias en la elaboración de los aspectos enlistados, se presenta esta guía, con la intención de clarificar aspectos que puedan auxiliarlas en el conocimiento del derecho a la protección de datos personales, los deberes relativos del Consejo de la Judicatura Federal y la forma en que deberán analizar y realizar los puntos enlistados.

Para lo cual, el presente documento se divide en dos capítulos:

- **Capítulo primero**: nociones del derecho a la protección de datos personales y los deberes de las instancias del Consejo de la Judicatura Federal.
- **Capítulo segundo**: pasos a seguir para la realización del listado de funciones y obligaciones de los servidores públicos involucrados, inventario de datos, análisis de riesgo, análisis de brecha y plan de trabajo.

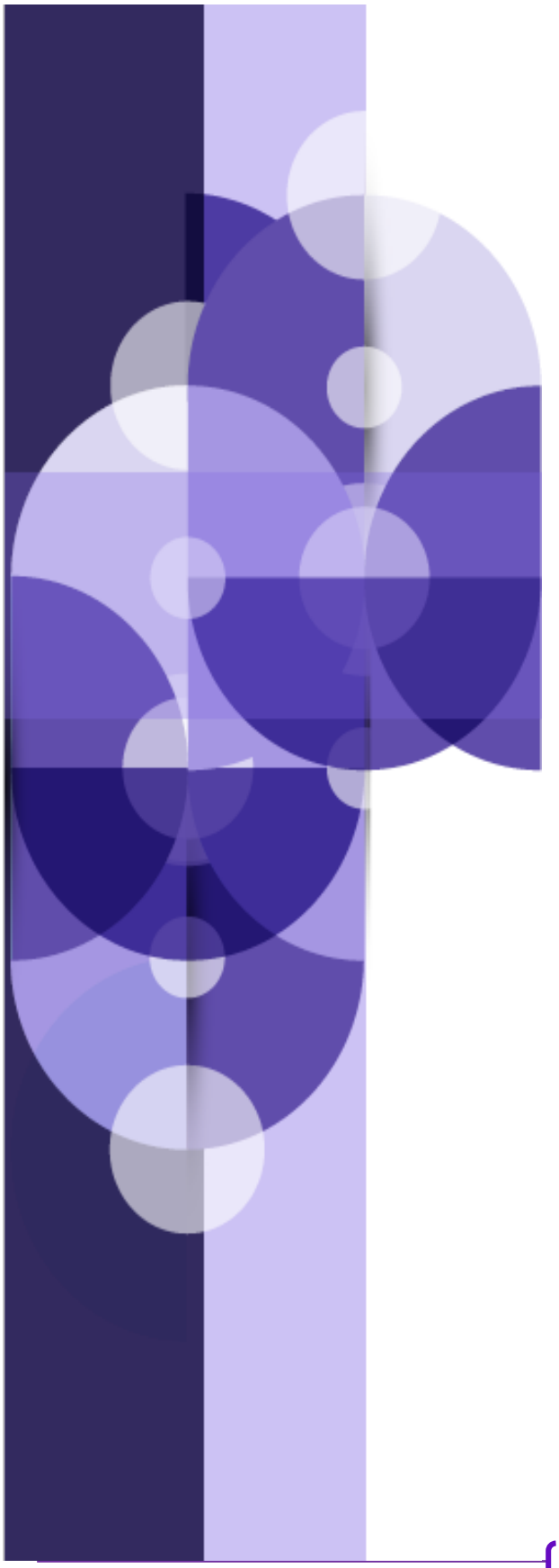
A través del **Capítulo primero**, se expone la calidad con que cuenta el Consejo de la Judicatura Federal y sus instancias, en relación con los deberes estipulados en la LGPDPPSO.

Posteriormente, para contextualizar la totalidad de los deberes estipulados en dicha legislación, se realiza una breve explicación de cada uno de ellos, a efecto de que se encuentren completamente identificados.

En el **Capítulo segundo**, se describen las acciones específicas que cada área debe realizar para la elaboración de los documentos mencionados.

Hecho lo anterior, la instancia estará en aptitud de remitir tales documentos a la Unidad de Transparencia.

Es importante referir, que una vez analizada la información remitida, **la Unidad de Transparencia establecerá mecanismos de monitoreo y revisión de las medidas de seguridad** con que cuenta cada área, así como de las que se haya concluido que deben establecerse.



Capítulo Primero

Nociones del derecho a la protección de datos personales y los deberes de las áreas del Consejo de la Judicatura Federal.

La protección de datos personales

El 1 de junio de 2009, se publicó en el Diario Oficial de la Federación el *Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos*, a través del cual, se agregó al citado numeral la disposición siguiente:

> *"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, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".*

Lo anterior, implicó el establecimiento del derecho fundamental relativo a la protección de los datos personales y los correlativos derechos al acceso, rectificación, cancelación u oposición en torno al manejo de los mismos por parte de cualquier entidad o persona, pública o privada, que tenga acceso o disponga de los datos personales de los individuos.

Cabe precisar, que la iniciativa que originó dicha adición, tuvo por objeto desarrollar en el máximo nivel de nuestra normatividad el derecho a la protección de datos personales, extendiendo su aplicación a todos los niveles y sectores en dos ámbitos fundamentales:

- Los datos personales en posesión de los entes públicos.
- Los datos personales en poder del sector privado.

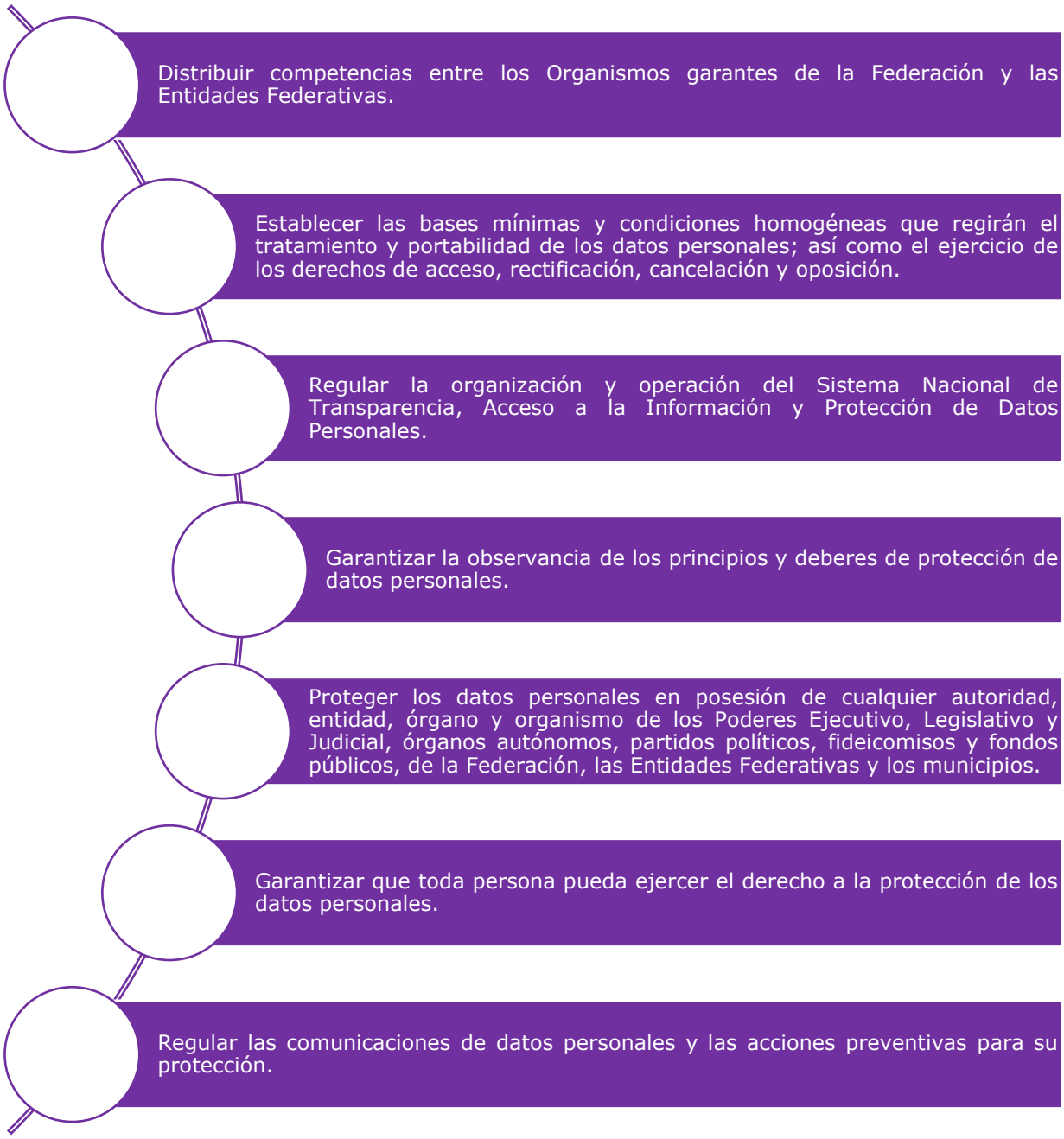
Posteriormente, el 7 de febrero de 2014 se publicó en el Diario Oficial de la Federación el *Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia.*

Dicho decreto, instruyó la instauración de un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados.

Para concretar lo anterior, se previó que tal organismo autónomo debía regirse por las leyes en materia de transparencia y acceso a la información pública, y protección de datos personales en posesión de sujetos obligados.

Por lo que, en su artículo transitorio SEGUNDO, estableció que el Congreso de la Unión debía expedir la Ley General del Artículo 6o. de esta Constitución, así como las reformas que correspondan a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, a la Ley Federal de Datos Personales en Posesión de los Particulares, entre otros.

Así, el 26 de enero de 2017, se promulgó la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, la cual, tiene como **objetivos**, los siguientes:



A efecto de dar cumplimiento a tales objetivos, a través de su contenido, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, desarrolla los principios, deberes y obligaciones para los responsables de datos personales, en beneficio de sus titulares.

Es importante destacar, que el 26 de enero de 2018 se publicó en el Diario Oficial de la Federación, el *Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público, emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* (Lineamientos Generales).

Ordenamiento que tiene por objeto, facilitar y hacer más comprensible y simple el conocimiento y la exigibilidad del derecho a la protección de datos personales en el sector público federal, así como evitar la fragmentación o atomización en innumerables ordenamientos que pudiera repercutir en el cumplimiento efectivo de la LGPDPPSO por parte de los responsables del ámbito federal, o bien, hacer inaccesible el derecho para cualquier persona.

Tal documento, se integra por los apartados siguientes:

Título primero • Objeto del documento y ámbitos de validez subjetivo y objetivo.	**Título segundo** • Principios y deberes de protección de datos personales.	**Título tercero** • Derechos de acceso, rectificación, cancelación y oposición; así como las reglas generales para su efectivo ejercicio.
Título cuarto • Reglas aplicables a la figura del encargado.	**Título quinto** • Disposiciones específicas en materia de transferencias nacionales e internacionales de los datos personales.	**Título sexto** • Acciones preventivas en materia de protección de datos personales.
Título séptimo • Procedimiento de sustanciación de los recursos de revisión e inconformidad.	**Título octavo** • Reglas que deberán regir los procedimientos de investigaciones previas y verificación del cumplimiento de las disposiciones previstas en la Ley, así como las auditorías voluntarias.	**Título noveno** • Medidas de apremio y el régimen de responsabilidades administrativas.

Finalmente, por lo que concierne al Consejo de la Judicatura Federal, debe referirse que el 10 de octubre de 2018, se difundió en el Diario Oficial de la Federación el *Acuerdo General del Pleno del Consejo de la Judicatura Federal que establece las disposiciones en materia de protección de datos personales* (Acuerdo General), el cual, tiene por objeto establecer el procedimiento administrativo interno ante la presentación de solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales; así como las acciones que deberán llevar a cabo las áreas administrativas y órganos jurisdiccionales en la protección, tratamiento y conservación de los datos personales.

Datos personales, transferencia, tratamiento y bases de datos

Para una mejor comprensión de este documento, es preciso tener presente ciertas definiciones que abonarán al claro entendimiento de los deberes en materia de protección de datos personales, y con ello, a la integración de un documento de seguridad.

En ese sentido, resultan claves los conceptos de datos personales, transferencia y tratamiento, pues la protección que ejercen los sujetos obligados, se lleva a cabo en la transferencia y tratamiento de los datos personales en su poder.

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.

Transferencia de Datos Personales

- 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.

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

Deberes en Materia de Protección de Datos Personales

Como se indicó con antelación, el **objeto** de la LGPDPPSO, es establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados.

En el cumplimiento de tales bases, principios y procedimientos, la citada legislación considera como **responsables** a los sujetos obligados que deciden sobre el tratamiento de datos personales; en ese sentido, dada la estructura orgánica del Poder Judicial de la Federación, el **Consejo de la Judicatura Federal** cuenta con el carácter de *sujeto obligado*, y en el ámbito de su competencia, es responsable del cumplimiento de las disposiciones, principios y deberes previstos para la protección de los datos personales, lo cuales son de aplicación y observancia directa.

Es importante destacar, que la legislación en cita reconoce que los sujetos obligados, son integrados por áreas, definidas como las instancias previstas en sus respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales, **por lo que a través de sus diversas instancias, el Consejo de la Judicatura Federal debe acatar los deberes que son impuestos por la LGPDPPSO**.

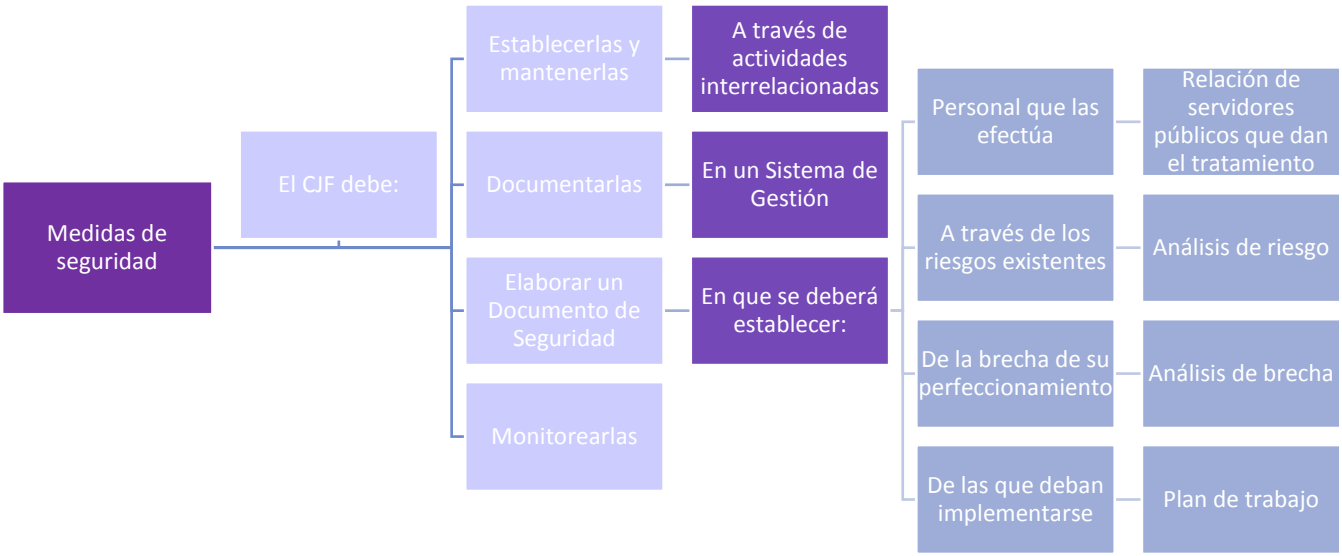
Sentado lo anterior, es pertinente referir que la LGPDPPSO establece dos deberes, el de confidencialidad y el de **seguridad de los datos personales**.

Respecto del deber de seguridad, el capítulo II, del Título Segundo de la legislación de la materia, señala que la forma en que deberá ser acreditado es a través del establecimiento y mantenimiento de **medidas de seguridad**, que permitan proteger los datos personales, garantizando su confidencialidad, integridad y disponibilidad.

Para establecer y mantener las medidas de seguridad, se instruye la implementación de actividades interrelacionadas mínimas, las cuales deberán documentarse en un sistema de gestión.

Asimismo, se deberá elaborar un documento de seguridad, que integre el inventario de datos personales y de los sistemas de su tratamiento, las funciones y obligaciones de las personas que efectúen dicho tratamiento, el análisis de riesgo, el análisis de brecha, el plan de trabajo, los mecanismos de monitoreo y revisión de las medidas de seguridad y el programa general de capacitación.

Lo anterior, se muestra en el diagrama siguiente:

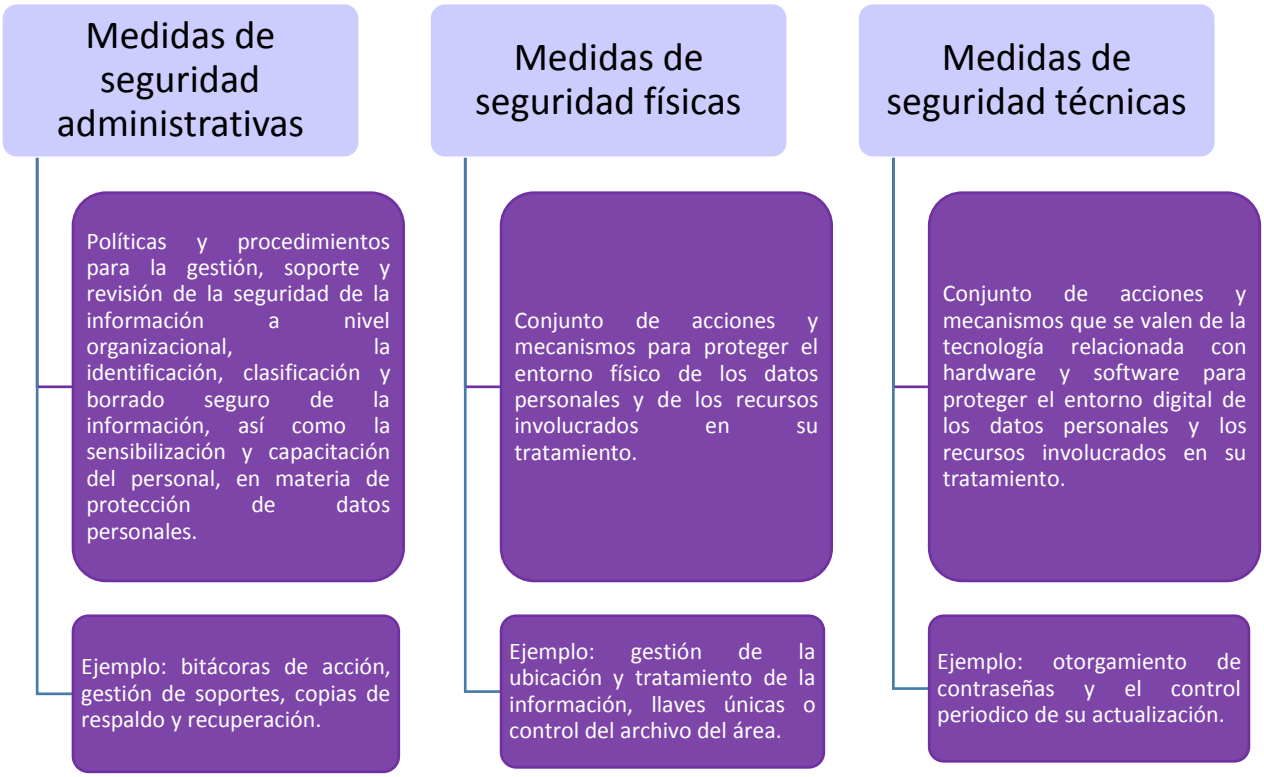


A través del cumplimiento de las acciones descritas, las instancias del Consejo de la Judicatura Federal, sistematizarán la protección de los datos personales, a través de medidas de prevención, monitoreo y de actuación en caso de una vulneración, garantizando el respeto irrestricto al derecho de la protección de datos personales.

Es importante destacar que, el cumplimiento del deber de seguridad de los datos personales, logrará que las instancias del Consejo de la Judicatura Federal sean conscientes de la necesidad de identificar y tratar los riesgos **en todos los niveles de probabilidad**, comprometiendo a sus servidores públicos a la identificación de acciones encaminadas a su prevención; además establecerá una base confiable para la planificación de sus funciones, mejorando con ello la eficacia y eficiencia operativa, creando una cultura de autocontrol y autoevaluación.

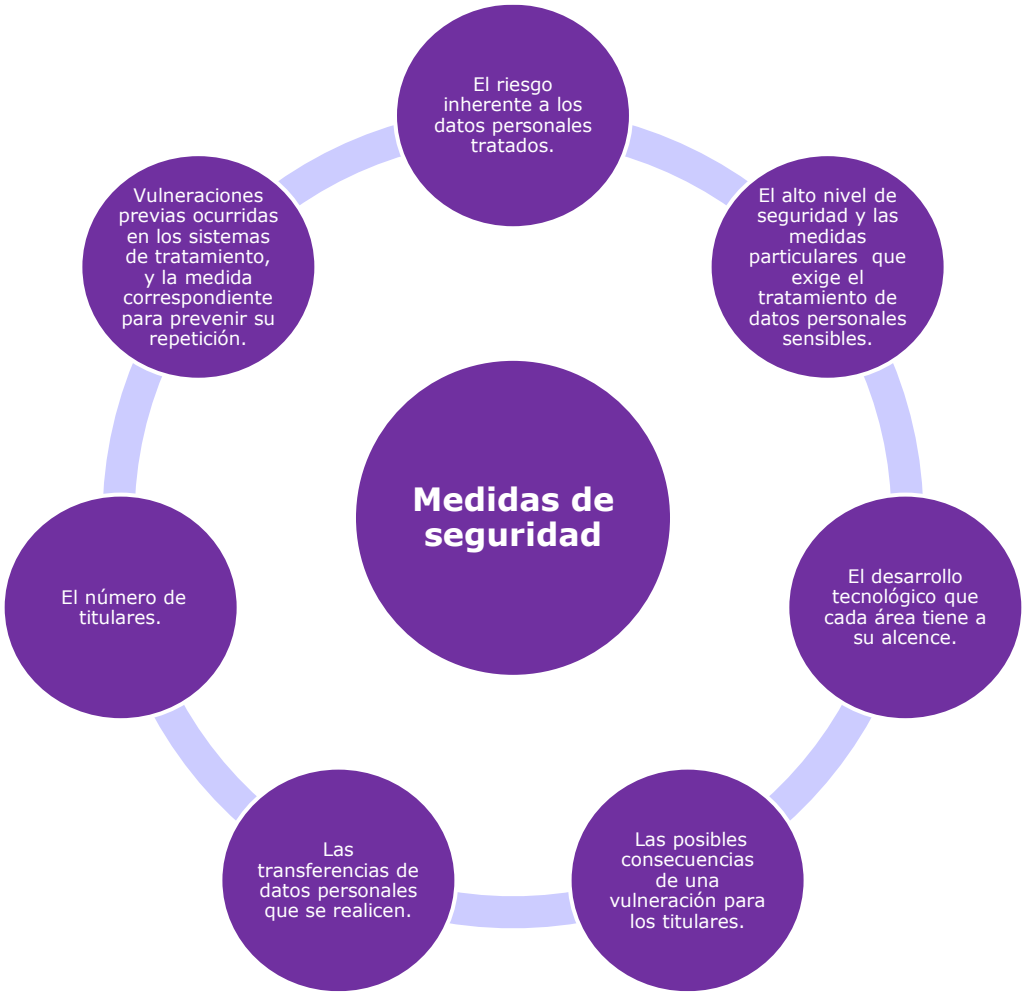
Medidas de seguridad

Las medidas de seguridad, son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que **permitan proteger los datos personales**.



Así, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el Consejo de la Judicatura Federal debe establecer y mantener medidas de seguridad que permitan proteger los datos personales contra su **daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad**.

Para lograr lo anterior, deben de establecerse medidas de seguridad de carácter administrativo, físico y técnico, considerando los elementos siguientes:



Cabe precisar, que el segundo párrafo del artículo 55, de los *Lineamientos Generales de Protección de Datos Personales para el Sector Público* (Lineamientos Generales), establece que las medidas de seguridad referidas, constituyen **mínimos exigibles**, por los que las instancias pueden adoptar las medidas adicionales que estimen necesarias para brindar mayores garantías en la protección de los datos personales en su posesión.

Actividades Interrelacionadas

Para proteger los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, el Consejo de la Judicatura Federal, a través de sus instancias, se encuentra obligado a implementar las actividades interrelacionadas siguientes:

- Crear políticas internas para la gestión y tratamiento de los datos personales.
- Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.
- Elaborar un inventario de datos personales y de los sistemas de tratamiento.
- Realizar un análisis de riesgo de los datos personales.
- Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes.
- Elaborar un plan de trabajo para la implementación de medidas de seguridad faltantes.
- Monitorear y revisar las medidas de seguridad.
- Diseñar y aplicar diferentes niveles de capacitación del personal.

Es importante referir, que las acciones relacionadas con las medidas de seguridad para el **tratamiento** de los datos personales, deberán estar documentadas y contenidas en un sistema de gestión.

Respecto de las políticas internas para la gestión y **tratamiento** de los datos personales, los Lineamientos Generales establecen que para su diseño e implementación se deberá realizar, al menos, lo siguiente:

- ✓ El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la LGPDPPSO y los propios Lineamientos generales.
- ✓ Los roles y responsabilidades específicas de los involucrados internos y externos dentro de la instancia, relacionados con el **tratamiento** de datos que se efectúe.
- ✓ Las sanciones en caso de incumplimiento.
- ✓ La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados.
- ✓ El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales.
- ✓ El proceso general de atención de los derechos acceso, rectificación, cancelación y oposición.

Por lo que toca a las demás actividades, serán abordadas en apartados siguientes.

Sistema de Gestión

Es el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en el artículo 34 de la LGPDPPSO.

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales se documentan en el sistema de gestión, al respecto, el artículo 65 de los Lineamientos Generales, establecen que tal sistema, deberá implementarse de forma que permita planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.

Documento de seguridad

Es el instrumento que concentra y describe de forma general las medidas de seguridad técnicas, físicas y administrativas implementadas por las áreas, mismo que se integra por los elementos siguientes:

La formulación del documento de seguridad es de suma relevancia, pues su actualización será necesaria en los eventos siguientes:

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.

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

Cabe recordar, que la presente guía tiene como finalidad que las instancias integren y analicen la información necesaria para que la Unidad de Transparencia construya el documento de seguridad del Consejo de la Judicatura Federal.

Bitácora de vulneraciones

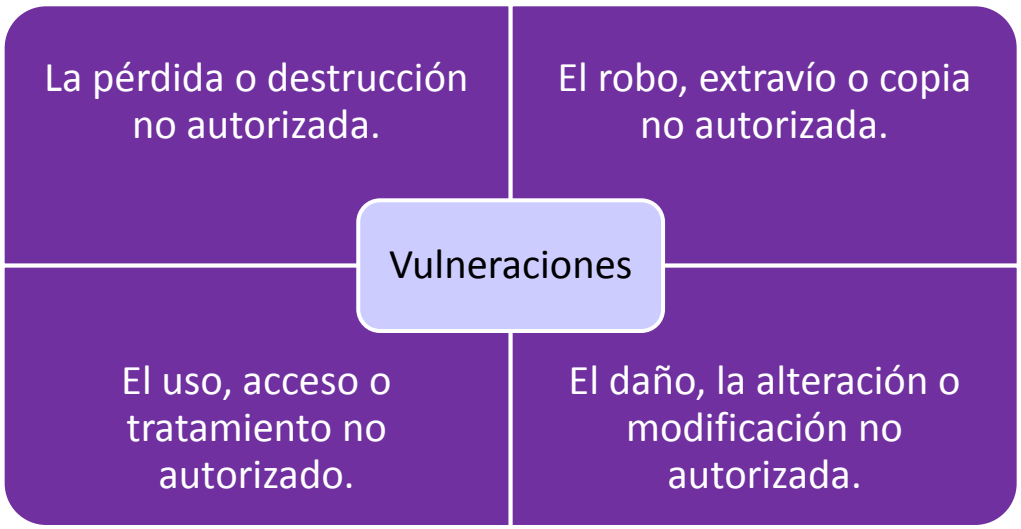
Es importante precisar que una *vulneración*, implica necesariamente que un dato personal sufrió un daño, pérdida, alteración, destrucción o un uso, acceso o tratamiento no autorizado.

Lo anterior, se traduce en que los casos en que alguna de las afectaciones en cita **no haya sido concretada**, no constituirán una vulneración, sino un incidente.

En efecto, en el tratamiento de los datos personales pueden acontecer diversos incidentes, sin embargo, constituirán una vulneración en el momento en que una amenaza haya trascendido al grado de generar un perjuicio verificable.

Lo anterior, no implica que las instancias no registren los incidentes que hayan acaecido en el tratamiento y resguardo de los datos personales, si no que deberán separar su control y análisis respecto de las vulneraciones demostradas.

Sentado lo anterior, debe referirse que la vulneración de los datos personales, puede suceder de las formas siguientes:



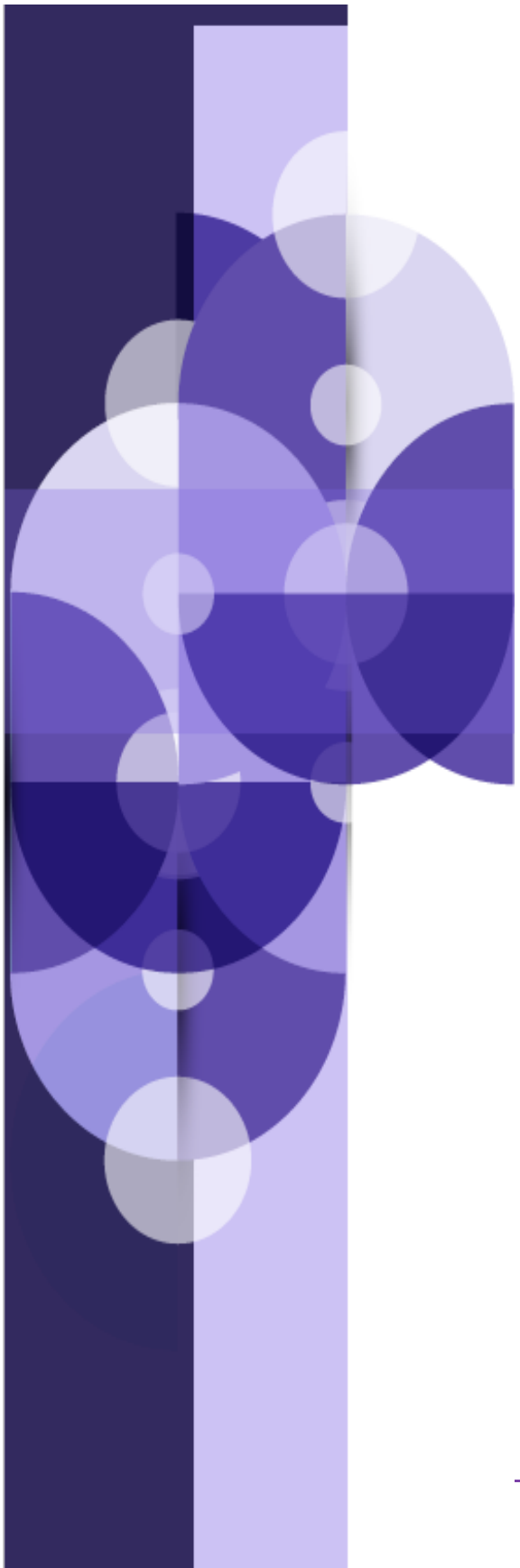
El Consejo de la Judicatura Federal, a través de sus instancias, debe llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

Asimismo, establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que debe subsistir aún después de finalizar sus relaciones con el mismo.

Al respecto, el artículo 18 del Acuerdo General, establece que en las actividades relacionadas con la operación de los sistemas de datos personales tales como el acceso, actualización, respaldo y recuperación de información, los titulares de las instancias deberán llevar a cabo, en forma adicional, las medidas siguientes:

- ✓ Llevar el control y registro del sistema de datos personales que contengan la operación cotidiana, respaldos, usuarios, y accesos, así como la transmisión de datos y sus destinatarios; y en su caso, una bitácora de incidentes y vulneraciones a la seguridad de los datos.
- ✓ Garantizar que, durante la transmisión de datos personales y el transporte de los soportes de almacenamiento, los datos no sean accedidos, reproducidos, alterados o suprimidos sin autorización;
- ✓ Llevar el control de inventarios y la clasificación de los medios magnéticos u ópticos de respaldo de los datos personales.
- ✓ Aplicar procedimientos para la destrucción de medios de almacenamiento y de respaldo obsoletos que contengan datos personales, con apoyo de la Dirección General de Tecnologías de la

Información o de la Dirección General de Archivo y Documentación en términos de sus respectivas competencias.



Capítulo Segundo

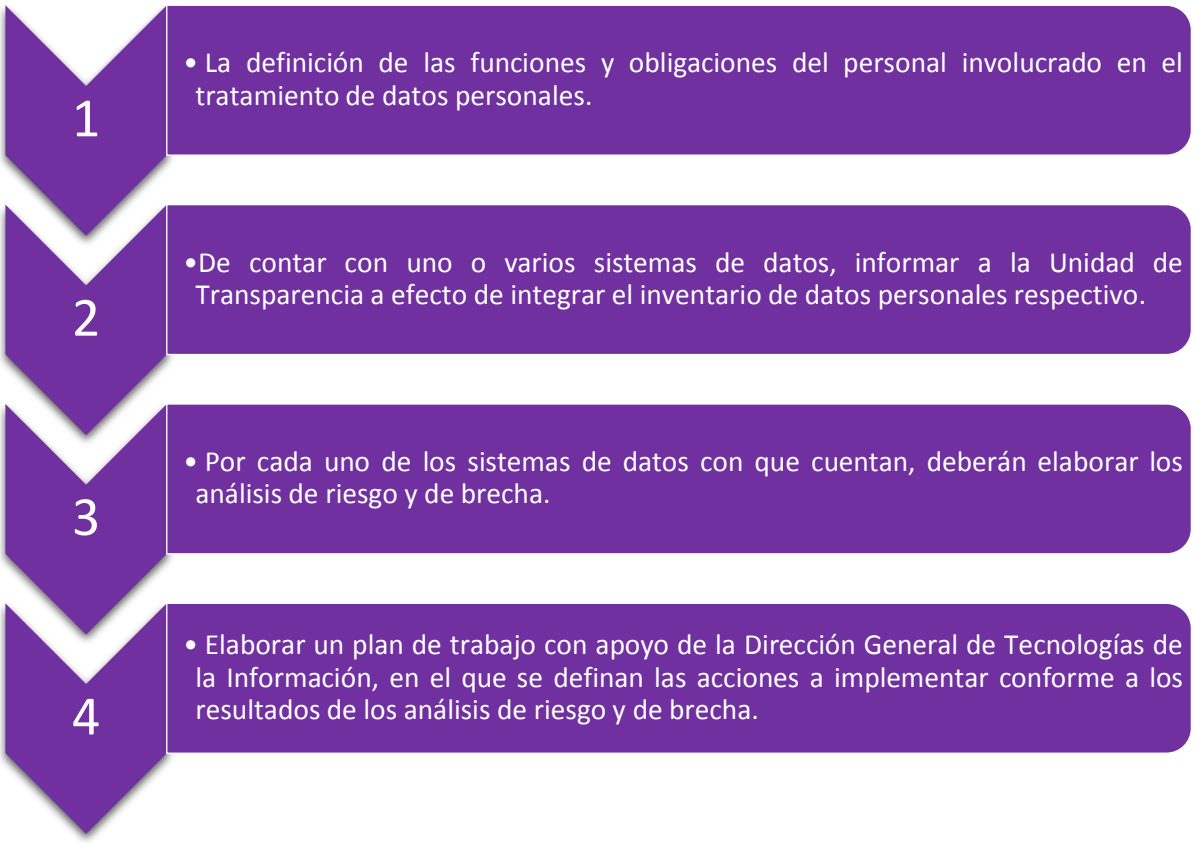
Pasos a seguir para la realización del listado de funciones y obligaciones de los servidores públicos involucrados, inventario de datos, análisis de riesgo, análisis de brecha y plan de trabajo.

Integración del documento de seguridad

La presente guía, permitirá a las **instancias** del Consejo de la Judicatura Federal concentrar los elementos necesarios para la elaboración del documento de seguridad.

El artículo 35 de la LGPDPPSO, establece que dicho documento, deberá contener al menos, lo siguiente:

En ese sentido, el artículo 15 del *Acuerdo General del Pleno del Consejo de la Judicatura Federal que establece las disposiciones en materia de protección de datos personales* (Acuerdo General), establece que **la Unidad de Transparencia elaborará el documento de seguridad**, el cual se integrará, entre otros elementos, por las acciones siguientes, mismas que **deberán realizar cada una de las instancias del Consejo**:



Por tanto, **cada instancia deberá remitir a la Unidad de Transparencia los elementos antes referidos**, de conformidad con las características que se desarrollarán en los apartados siguientes.

Es importante destacar, que con base a las medidas de seguridad, hábitos y prácticas expuestas por cada instancia, se elaborarán mecanismos de monitoreo y revisión, que permitan verificar la protección de los datos personales e implementar mejoras de manera continua.

Por tanto, los documentos en cuestión, deberán ser construidos de forma en que su monitoreo y revisión constante, resulten tareas sencillas, siempre encaminadas a la eficiencia y eficacia de las medidas de seguridad existentes.

Definición de funciones y obligaciones

Para identificar las funciones y obligaciones de los servidores públicos que traten datos personales, en principio debe identificarse que el *tratamiento de datos personales*, consiste en:

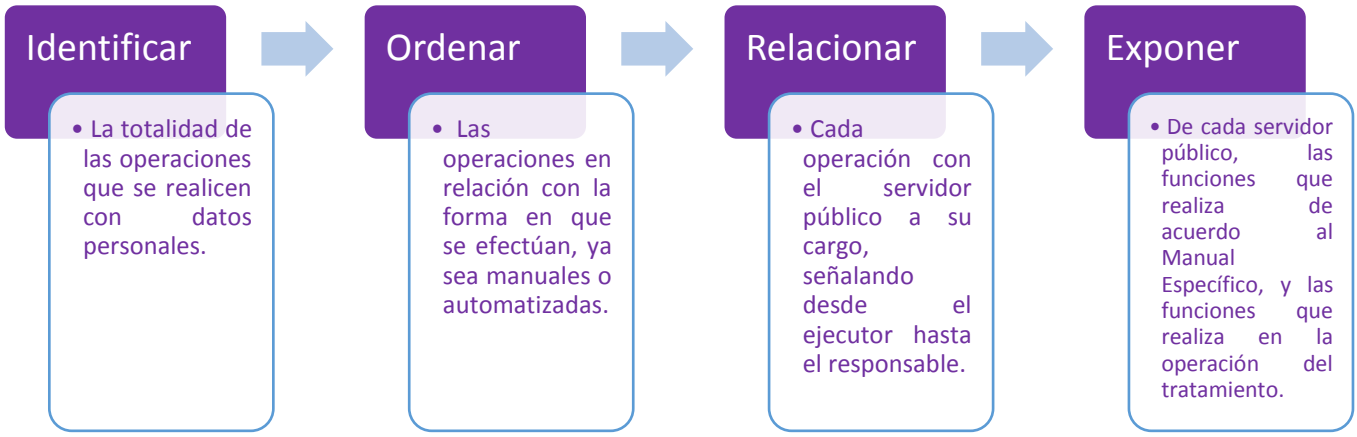
Cualquier **operación o conjunto de operaciones** efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, en virtud del desarrollo de sus facultades.

Relacionadas con:

- Obtención.
- Uso.
- Registro.
- Organización.
- Conservación.
- Elaboración.
- Utilización.
- Comunicación.
- Difusión.
- Almacenamiento.
- Posesión.
- Acceso.
- Manejo.
- Aprovechamiento.
- Divulgación.
- Transferencia o disposición **de datos personales.**

El artículo 57 de los Lineamientos Generales, dispone que se deberán establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de **todas las personas que traten datos personales**.

De modo que, para identificar las funciones y obligaciones de los servidores públicos que traten datos personales, las instancias deberán realizar lo siguiente:



Lo anterior, deberá realizarse de acuerdo a la tabla que se adjunta como **anexo I**.

Una vez realizadas dichas acciones, deberá remitir a la Unidad de Transparencia el documento con la firma del titular de la instancia, en formato impreso y digital, anexando las observaciones que se estimen pertinentes para el entendimiento de lo reportado.

Inventario de Datos Personales y de los Sistemas de su Tratamiento

La LGPDPPSO, establece en su artículo 33, fracción III, como una de las actividades interrelacionadas con el establecimiento y mantenimiento de las medidas de seguridad de los datos personales, la realización de un inventario de datos personales y de los sistemas de tratamiento.

El artículo 2, fracción IX, del Acuerdo General, dispone que el *inventario de datos personales*, se refiere al catálogo de sistemas de datos con independencia de su forma de almacenamiento.

El artículo 58 de los Lineamientos Generales, estipula que dicho inventario deberá elaborarse con la información básica de cada tratamiento de datos personales, considerando, al menos, los elementos siguientes:

- ✓ El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales.
- ✓ Las finalidades de cada tratamiento de datos personales.
- ✓ El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no.
- ✓ El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales.
- ✓ La lista de servidores públicos que tienen acceso a los sistemas de tratamiento.
- ✓ En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable.

- ✓ En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

Es importante destacar, que la información relativa a este apartado, fue concentrada por la Unidad de Transparencia de acuerdo a los informes enviados por cada instancia, por lo que se deberá realizar un análisis con la información de esta guía, para que solo en caso de actualización o modificación, sea remitido un nuevo Inventario de Datos Personales y de los Sistemas de su Tratamiento.

Para realizar lo anterior, como **anexo II**, se incluye el inventario de datos personales y sistemas con que cuenta la Unidad de Transparencia.

Análisis de riesgo

Los titulares de las instancias, **por cada uno de los sistemas de datos** con que cuentan deberán elaborar el correspondiente *análisis de riesgo*, mismo que habrán de remitir a la Unidad de Transparencia.

De conformidad con el artículo 33, fracción IV, de la LGPDPPSO, 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 comprender lo anterior, es preciso indicar que el **riesgo**, es la combinación de la posibilidad de que se materialice una amenaza y sus posibles consecuencias negativas. Por tanto, puede ser catalogado según su probabilidad de materialización y el impacto que tiene en caso de concretarse.

Para evaluar el riesgo, es preciso determinar el **impacto** de la exposición a la amenaza, en el contexto de la probabilidad de su materialización. Así, el impacto se fija con base a los probables daños que pueden producirse si la amenaza se concreta.

Un impacto, sería aceptable si no tuviera consecuencias sobre el titular de los datos personales, por otro lado, sería significativo si hubiera un daño grave sobre sus derechos.

En ese orden de ideas, el análisis de los riesgos será el resultado de una reflexión sobre las implicaciones que los tratamientos de datos de carácter

personal tienen sobre los titulares. Es decir, determinará el alcance de un posible daño.

Este ejercicio, identificará las amenazas a las que están sujetos los datos personales, dando oportunidad a las instancias de hacer un verdadero estudio sobre la efectividad de las medidas de seguridad implementadas, o bien, la necesidad de actualizarlas. Ello con la finalidad de elegir la medida de seguridad que mejor se adapte a la protección de tal información, minimizando con ello el peligro e impacto de su vulneración.

El artículo 60 de los Lineamientos Generales, estipula que en la realización del análisis de riesgo se deberá considerar lo siguiente:

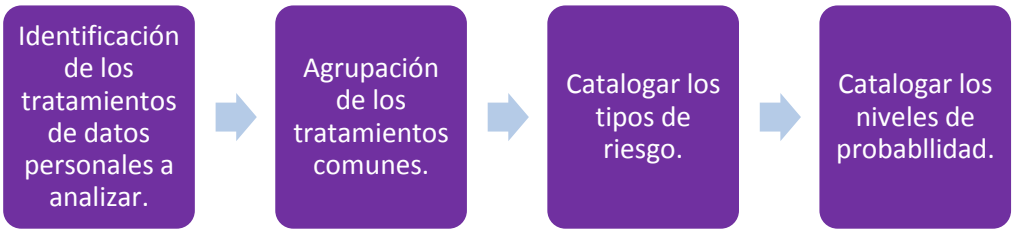
- ✓ La existencia de requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico para proteger los datos personales.
- ✓ El valor de los datos personales de acuerdo a su clasificación previamente definida, y su ciclo de vida, de conformidad con la normatividad aplicable.
- ✓ Que sea ponderable el valor de los datos personales con la exposición de los activos involucrados su tratamiento.
- ✓ Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.
- ✓ El riesgo inherente a los datos personales tratados, su sensibilidad (datos personales sensibles), el desarrollo tecnológico, las posibles consecuencias de una vulneración para los titulares, las transferencias de datos personales que se realicen, el número de titulares, las vulneraciones previas ocurridas en los sistemas de tratamiento, y el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener

los datos personales tratados para una tercera persona no autorizada para su posesión; siempre en función y estricto apego a la normatividad aplicable.

Ahora bien, para comenzar a realizar el análisis de riesgo, deben ubicarse claramente las **fuentes de información sobre las que versará su estudio**, entre las cuales pueden considerarse:

Fuentes de información para el análisis de riesgo			
Infraestructura tecnológica.	Inventario de Datos Personales y de los Sistemas de Tratamiento.	Cumplimiento de obligaciones normativas.	Hábitos de seguridad del personal del CJF.

Ubicada la fuente o fuentes de las que derivará el análisis de riesgo, deberán realizarse las siguientes **acciones preparativas**:



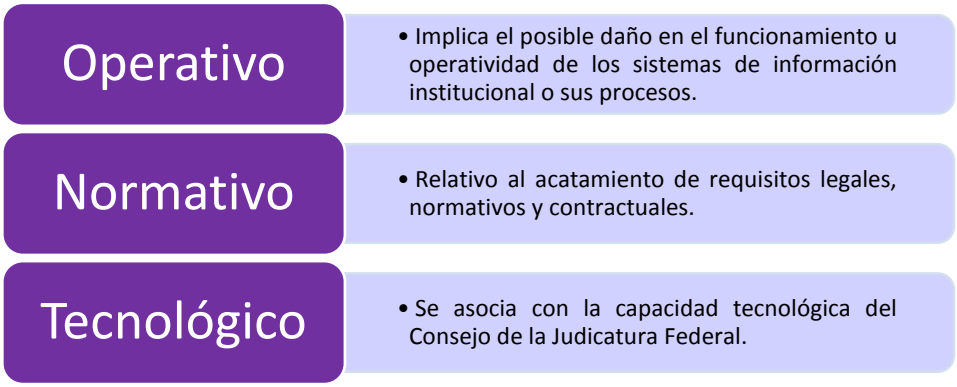
Al partir de la **identificación de los tratamientos** de datos personales a examinar, la instancia vislumbrará un panorama general del tipo de datos a

analizar, su ciclo de vida, los servidores públicos a cargo de su uso y protección y cualquier elemento que contribuya al estudio de sus posibles amenazas.

Posteriormente, se recomienda **agrupar los tratamientos comunes**, es decir, aquellos que guarden mayor similitud, lo que facilitará su análisis conjunto, pues es probable que los tratamientos similares estén expuestos a los mismos riesgos.

Una vez realizado lo anterior, procederá la formulación de un **catálogo de riesgos**, el cual debe considerar el tipo de dato personal que se recaba y/o utiliza, el grado de importancia del tratamiento, el número de personas que intervienen y la tecnología que se utiliza.

Entre los tipos de riesgos que existen, se encuentran los siguientes:



Finalmente, es conveniente jerarquizar **niveles de probabilidad** de los riesgos que fueron catalogados, para lo cual, podrían tomarse en consideración las descripciones siguientes:

Nivel	Descripción
Muy poco probable	La amenaza puede ocurrir sólo en circunstancias excepcionales.
Poco probable	La amenaza puede ocurrir en una cantidad considerable de circunstancias.
Probable	La amenaza puede ocurrir en cualquier momento.
Seguro	Se espera que la amenaza se materialice.

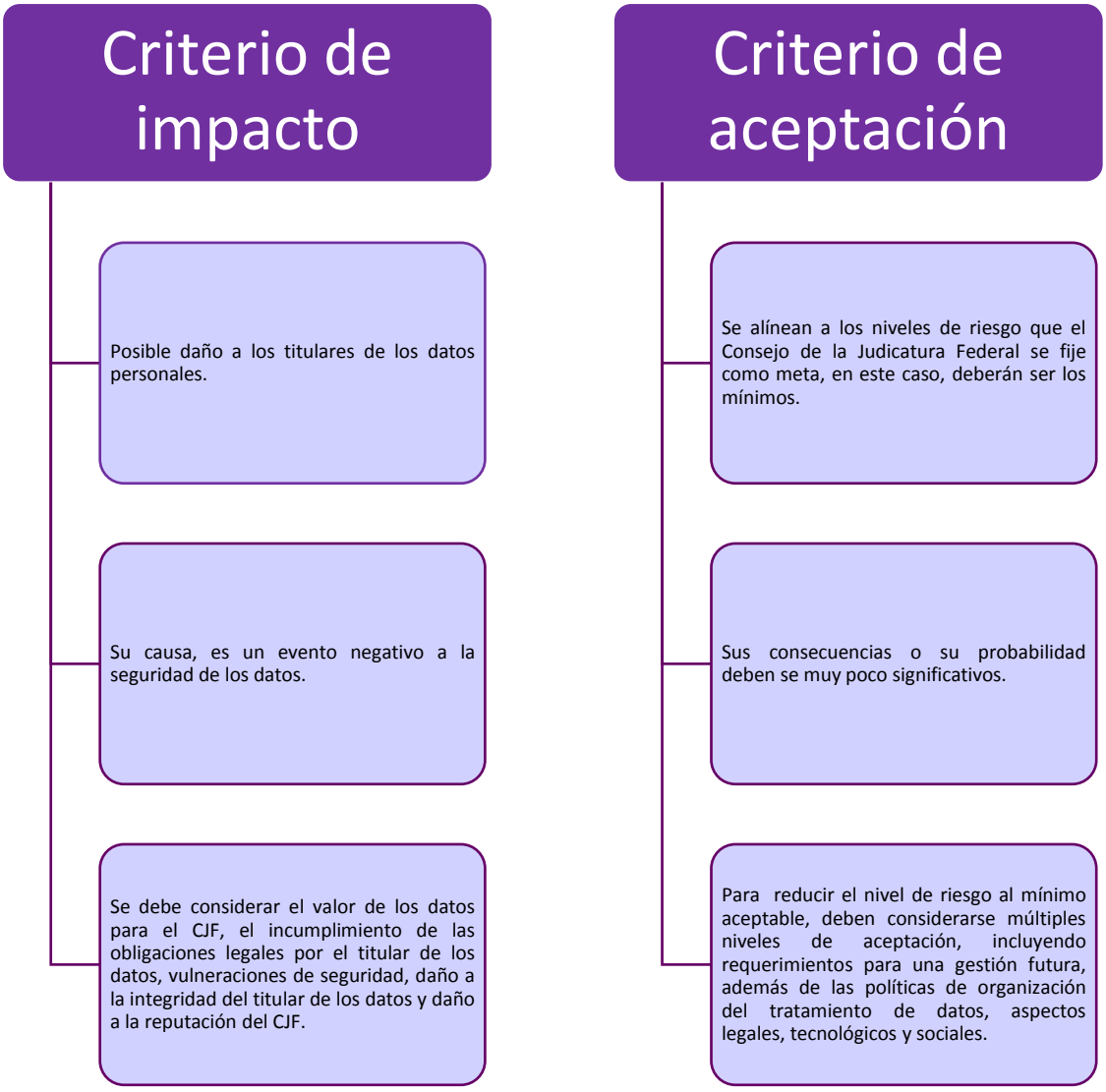
Concretadas las acciones preparativas anteriormente mencionadas, se tendrán claros los datos personales a analizar y el tratamiento que la instancia realice, además de la definición de los tipos de riesgo existentes y los niveles de su probabilidad.

Ahora bien, habiendo verificado la fuente de información y realizado las acciones preparativas, la instancia deberá proceder al llenado de la ***"Examinación de Riesgo"***, que resulta ser un cuestionario que se agrega como **anexo III**, y que tiene como finalidad ejecutar el estudio de las amenazas identificadas, para así concluir el tipo de riesgo y la probabilidad de cada una.

Es importante referir que, para el vaciado de datos en la *Examinación de Riesgo*, deben tenerse claros los factores que inciden en el nivel de riesgo de cada sistema de datos, algunos de los cuales, son los siguientes:

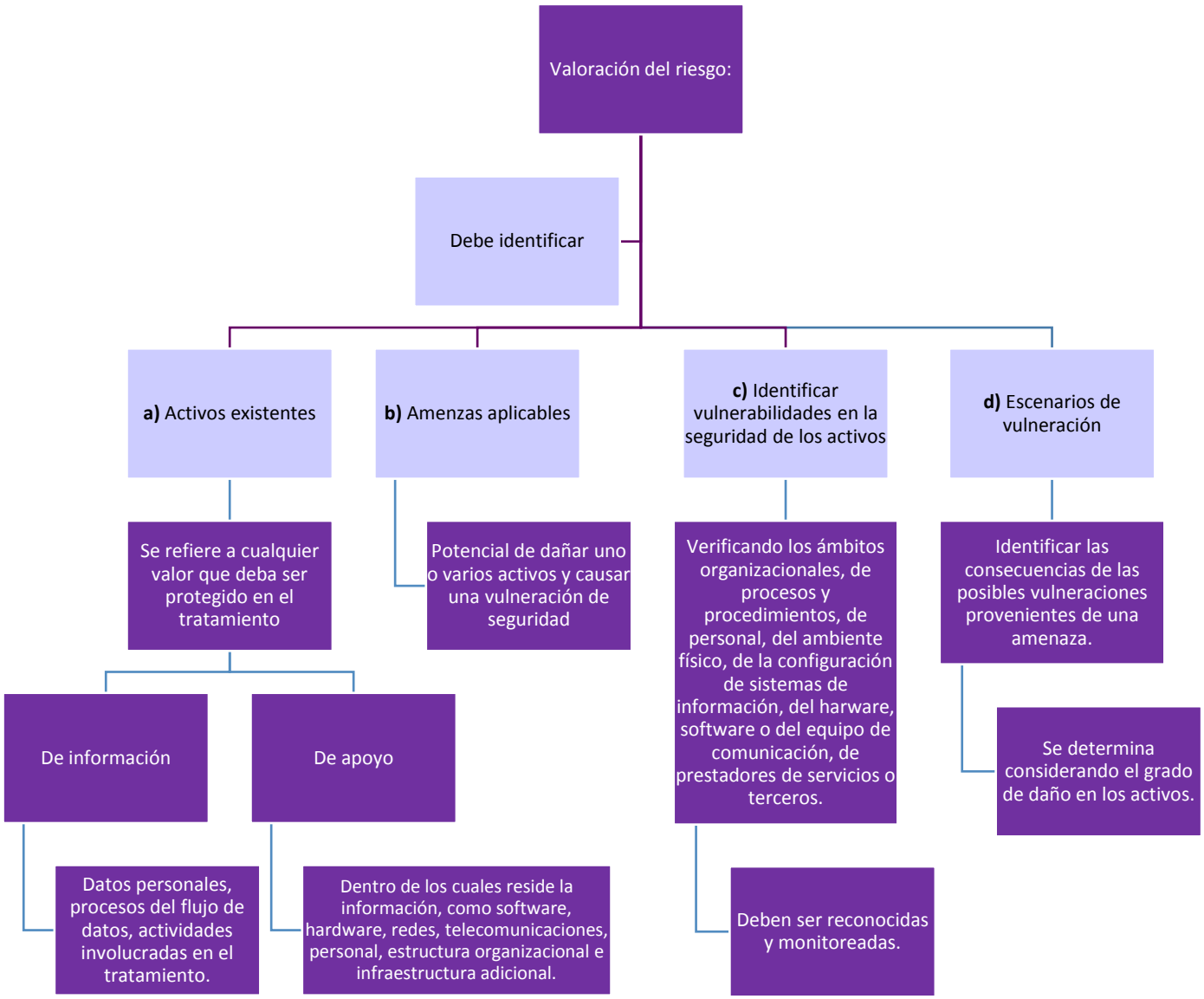
Factores que pueden incidir en el nivel de riesgo	El riesgo inherente a cada dato personal
	La sensibilidad del dato personal
	El desarrollo tecnológico
	Posibles consecuencias de la vulneración del dato personal
	Número de titulares
	Vulnerabilidades previas courridad en el sistema de datos
	El riesgo por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión
	Requerimientos regulatorios y obligaciones contractuales utilizadas para definir los objetivos y alcances
	Valor del dato personal, de acuerdo a su clasificación por tipo y su flujo
	Valor y exposición de los activos involucrados con el dato personal
	Expectativas de las partes interesadas, así como consecuencias negativas a la reputación del Consejo de la Judicatura Federal, que pudieran derivar de una vulneración.

Además, en el llenado de la información de dicha examinación, deben tenerse claros los criterios de impacto y aceptación.



Los criterios anteriores, serán la directriz para el análisis del riesgo de cada sistema de datos, mismo que quedará plasmado en la *Examinación de Riesgo.*

Finalizado el llenado de la *Examinación de Riesgo,* para estar en posibilidad de implementar las conclusiones que deriven del análisis de riesgo, deberá **valorarse el riesgo identificado** de forma cuantitativa, cualitativa o ambas; se propone la forma siguiente:



Además, deberán determinarse las consecuencias potenciales de conformidad con los criterios siguientes:

Para finalizar el análisis de riesgo, deberá emitirse un ***Documento de Conclusiones del Análisis de Riesgo***, el cual deberá contener el desahogo de los puntos siguientes:

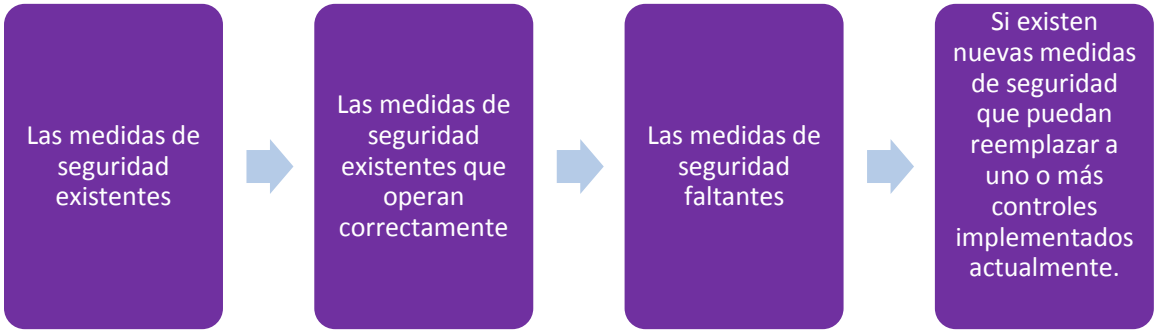
1. Identificación clara de las fuentes de información utilizadas.
2. Catálogo de riesgos.
3. Niveles de probabilidad contemplados.
4. Formato de *Examinación del Riesgo* debidamente requisitado (anexo III).
5. El activo o activos objeto del riesgo (el dato personal, proceso del flujo de datos, actividades involucradas en el tratamiento, sistema dentro del cual reside la información, personal, estructura organizacional o infraestructura adicional).
6. Valor de riesgo para cada uno de los activos identificados, con respecto de cada una de las vulneraciones vislumbradas o documentadas.
7. Identificación de los escenarios de vulneración que podrían llevar a cada uno de los activos a posibles vulneraciones.
8. Medidas de seguridad y controles que permitan prevenir dichos riesgos.

Es pertinente indicar, que las medidas de seguridad y controles propuestos, deberán ser jurídica, técnica y financieramente posibles para el Consejo de la Judicatura Federal.

Análisis de brecha

Una vez identificados los riesgos y medidas de seguridad necesarias, resulta procedente el análisis de brecha, el cual consiste en identificar los controles que hacen falta implementar a partir de aquellos definidos como necesarios.

En tal virtud, el análisis de brecha deberá considerar los elementos siguientes:



Para realizar lo anterior, es importante tener claras las medidas de seguridad y controles existentes, por lo que se sugiere identificarlas previamente, reconociendo el grado de desarrollo que mantienen, para lo cual, pueden examinarse las características siguientes:

- Que se encuentren documentadas
- Que se encuentran implementadas
- Que generen registros de su operación
- Que existan métricas que permitan dar seguimiento a su eficacia
- Que existan reportes dirigidos a sus titulares para la toma de decisiones
- Que existan acciones que permitan incrementar su eficacia
- El grado de automatización que tiene la medida, es decir, si tiene poca o nula interacción de una persona en su operación

Plan de trabajo

El Plan de Trabajo, concentrará los retos que en materia de seguridad de datos personales afronten las instancias, sustentado en el análisis de los riesgos y las medidas de seguridad que se estiman deben implementarse, en el contexto de su propia organización interna y la evolución tecnológica de sus sistemas.

Así, de conformidad con el artículo 62 de los Lineamientos Generales, el Plan de Trabajo debe contener 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 de su instancia y externo del Consejo de la Judicatura Federal y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

El artículo 14, fracción V, del Acuerdo General, establece que para la elaboración del documento de seguridad, los titulares de las instancias deben elaborar un plan de trabajo con apoyo de la Dirección General de Tecnologías de la Información, para que la Unidad de Transparencia los integre al Plan de Trabajo del Consejo de la Judicatura Federal.

Como se indicó anteriormente, el análisis de riesgo permitirá obtener el valor de riesgo para cada uno de los activos identificados, los escenarios que podrían llevar a posibles vulneraciones y los controles y medidas de seguridad que permitan tratar dichos riesgos.

Asimismo, en análisis de brecha permitirá, entre otros aspectos, confirmar las medidas de seguridad existentes que operan correctamente, las medidas de seguridad faltantes, y si existen nuevas medidas de seguridad que puedan reemplazar los controles implementados.

De modo que en el plan de trabajo, deberán concentrarse las conclusiones relativas a los riesgos detectados y que pueden tener más impacto sobre los datos personales tratados, los controles de seguridad más relevantes, las medidas de seguridad faltantes, y las nuevas medidas de seguridad que puedan reemplazar los controles existentes.

Además, deberán incluirse los mecanismos de seguridad pertinentes para supervisar continuamente la eficacia de las medidas de seguridad.

En conclusión, de conformidad con artículo 33 fracción VII y 63 de los Lineamientos Generales, dicho documento deberá contener de manera detallada, lo siguiente:

- ✓ Los riesgos localizados, amenazas y vulneraciones a las que están sujetos los datos personales.
- ✓ Los riesgos y amenazas que se estimen de atención preferente.
- ✓ Los hábitos de seguridad del personal encargado del tratamiento de datos personales.
- ✓ Las medidas de seguridad que se estimen deben efectuarse para su protección.
- ✓ Los mecanismos de control y monitoreo que deben efectuarse para verificar su eficacia, contemplando los elementos siguientes:

  - Los nuevos activos que se incluyan en la gestión de riesgos, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar.
  - Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica.
  - Las nuevas amenazas que podrían estar activas dentro y fuera del Consejo y que no han sido valoradas.
  - La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
  - Las vulnerabilidades identificadas, para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
  - El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
  - Incidentes y vulneraciones de seguridad ocurridas.

- ✓ Los responsables de las acciones, mecanismos y controles.
- ✓ Los periodos de monitoreo que se establecerán para la supervisión de las medidas de seguridad.
- ✓ Las fechas de compromiso para su efectuación.

Para facilitar el análisis de las conclusiones realizadas, podrá utilizarse el gráfico que se presenta como **anexo IV.**

Sanciones aplicables

Respecto a la seguridad de los datos personales, resulta necesario destacar que el artículo 163 de la LGPDPPSO estipula que **serán causas de sanción** por incumplimiento de las obligaciones establecidas, las siguientes:

- 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.
- Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGPDPPSO.
- No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO.
- 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.
- Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO.
- Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO.

Por tanto, a efecto de que la Unidad de Transparencia actualice el documento de seguridad, las instancias deberán **notificar de manera inmediata**, las modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo, las acciones que se pretendan establecer para mitigar el impacto de una vulneración a la seguridad ocurrida y las acciones correctivas y preventivas ante una vulneración de seguridad.