DESCRIPCIÓN DE LA METODOLOGÍA Y DESARROLLO DEL ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA DEL DOCUMENTO DE SEGURIDAD COMO BASE PARA EL SISTEMA DE GESTIÓN DE PROTECCIÓN DE PROTECCIÓN DE DATOS PERSONALES (SGPDP) DEL INSTITUTO MEXICANO DE TECNOLOGÍA DEL AGUA

CONTENIDO

1. Introducción

Para garantizar la seguridad de los datos personales, es importante implementar y fortalecer acciones que promuevan y garanticen la confidencialidad, integridad y disponibilidad de estos. En ese sentido se debe tomar en cuenta que en la gestión de la seguridad de la información un paso importante es el proceso de gestión de riesgos. El presente documento describe y establecelos criterios de evaluación y tratamiento de riesgos a realizarse sobre los tratamientos de datos personales del Instituto Mexicano de Tecnología del Agua (IMTA).

Lo anterior permitirá una adecuada toma de decisiones en las acciones que deban implementarse con un nivel aceptable de riesgo sobre los activos de información y apoyo del Sistema de Gestión de seguridad de Datos Personales (SGSDP).

2. Objetivo

Definir la metodología y el procedimiento para evaluar y tratar los riesgos de los datos personalesen el IMTA, así como determinar el nivel de riesgo aceptable. En el contexto de protección de los datos personales, se identificarán como el análisis de riesgo y análisis de brecha que atienden a lo establecido en las fracciones III y IV, del artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

3. Alcance

La evaluación y tratamiento de riesgos aplicará a todo el alcance del Sistema de Gestión de Seguridad de Datos Personales (SGSDP); es decir, a los activos de información y apoyo que pueden tener un impacto sobre la seguridad de los datos personales en el ámbito del SGSDP.

Los usuarios de este documento serán todos los servidores públicos del IMTA incluidos dentro del alcance del SGSDP y que participarán en la evaluación y tratamiento de riesgos.

4. Referencias

4.1 Marco normativo aplicable a la seguridad y protección de datos personales.
4.2 Declaración de aplicabilidad.
4.3 Guía de Implementación de un Sistema de Gestión de Seguridad de Datos Personales(IMTA)

5. Metodología de evaluación y tratamiento de riesgos

5.1 Establecimiento del contexto

El propósito de la gestión de riesgos de seguridad de datos personales es:

- Dar cumplimiento a la Política y los objetivos de seguridad de datos personales.
- Apoyar la implementación del Sistema de Gestión de Seguridad de Datos Personales(SGSDP).
- Preparar el plan para la implementación o mejora continua del Sistema de Gestión de Seguridad de Datos Personales (SGSDP) y el cual se documentará entre otros, a través del Documento de Seguridad.

Con el fin de contar con un enfoque adecuado para la gestión de riesgos de seguridad dela información y de los datos personales se han seleccionado los siguientes criterios básicos:

5.1.1 Criterios de aceptación de riesgos

a) Para determinar los criterios de aceptación de riesgos, además del contexto establecido, han sido considerados los siguientes aspectos:

- Elementos de la estrategia institucional (misión visión y objetivos estratégicos).
- La normatividad aplicable a la seguridad de los datos personales y su tratamiento.
- La operación de los procesos de tratamiento de datos personales.
- Las tecnologías de la información (servicios e infraestructura).
- Los recursos financieros y humanos disponibles que intervienen en el tratamientode datos personales.

b) Los criterios de aceptación se han clasificado de la siguiente manera:

- Si el nivel de riesgo es bajo, es un riesgo aceptable, el cual deberá ser monitoreado como parte de la gestión de riesgos.
- Si el nivel de riesgo es medio o alto, el riesgo **no se puede aceptar en ninguna circunstancia**, por lo que debe ser tratado.

5.1.2 Criterios de impacto

a) Valor de los activos de información y de apoyo impactados.
b) Pérdida de los principios de seguridad de la información. (confidencialidad, integridady disponibilidad).
c) Daño a la integridad de los titulares de datos personales.
d) Degradación en la operación (interna o tercerizada).
e) Vulneraciones de seguridad.

f) Daño en la reputación institucional.
g) Incumplimiento de requisitos legales y contractuales.

5.1.3 Criterios para la evaluación de riesgos

a) El valor estratégico de los tratamientos de datos personales.
b) La criticidad de los activos de información y de apoyo involucrados.
c) Los requisitos legales y las obligaciones contractuales.
d) La importancia operativa y de negocio de la disponibilidad, confidencialidad e integridad.
e) Las expectativas y percepciones de las partes interesadas, así como las consecuencias negativas que puede enfrentar la reputación institucional.

5.2 Identificación de riesgos

5.2.1 Activos de información

a) Un **activo** es todo elemento de valor involucrado en el tratamiento de datos personales, entre ellos, las bases de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documentos en papel.
b) Los **activos críticos** son aquellos que el responsable considera como los más valiosos que, si ocurre su pérdida, destrucción, robo, extravío, copia, uso, acceso, tratamiento, daño, alteración o modificación no autorizada, **podría provocar una crisis**, y comprometer las operaciones, la prestación de servicios o incluso la existencia del Instituto.
c) Se deberán identificar todos los activos de información y de apoyo dentro del alcance del SGSDP que pueden afectar la confidencialidad, integridad y disponibilidad de los datos personales en resguardo del INAI.
d) Los activos podrán ser información documentada en papel o en formato electrónico, aplicaciones, bases de datos, personal, hardware, software, infraestructura tecnológica, instalaciones y servicios o procesos externos.
e) Se deberá determinar el valor del activo en función de los tres principios fundamentales de seguridad de la información: confidencialidad, integridad y disponibilidad, aplicándose una escala del 1 al 3, dónde 1 es el valor más bajo y 3 el más alto.
f) El valor del activo se calculará sumando los valores asignados a la confidencialidad, integridad y disponibilidad, empleándose los siguientes rangos para obtener el valor (cualitativo y cuantitativo) final.

Rango	Valor Cualitativo	Valor Cuantitativo
1 – 3	Bajo	1
4 – 6	Medio	2

7 – 9	Alto	3

Para determinar adecuadamente la valoración de los activos y su asociación con cada principio de seguridad de la información, se establecen las siguientes preguntas:

Principio	Pregunta
Confidencialidad	¿Qué importancia tendría el activo si estuviera disponible o fuera conocido o revelado a personas, entidades o procesos no autorizados?
Integridad	¿Qué importancia tendría el activo si fuera alterado o modificado sin autorización o control?
Disponibilidad	¿Qué importancia tendría el activo si no estuviera accesible o utilizable a petición de una entidad autorizada?

g) Por cada activo se deberá identificar un propietario: persona o entidad (área que trata los datos personales) con la responsabilidad y la autoridad para gestionar un activo. El propietario del activo deberá determinar el valor de este. En su caso, también se deberá identificar el custodio de este.

5.2.2 Amenazas y vulnerabilidades

a) Se deberán identificar todas las amenazas y vulnerabilidades relacionadas con cada activo. Las amenazas y vulnerabilidades se identificarán utilizando los catálogos definidos para tal fin.
b) Cada activo puede estar relacionado con varias amenazas, y cada amenaza puede estar vinculada con varias vulnerabilidades.
c) La identificación de amenazas y vulnerabilidades será realizada por los propietarios de los activos.

5.3 Estimación del riesgo

Se utilizará una escala cuantitativa y su equivalencia cualitativa con atributos calificativos para describir la magnitud de los impactos o consecuencias potenciales y la posibilidad de que ocurran. La estimación del impacto y probabilidad será realizada por los propietarios de los riesgos.

Los elementos para estimar el riesgo son:

5.3.1 Impacto / consecuencias

Se refiere al grado del daño o costo que pudiera ser causado a partir de que un evento no deseado ocurriera.

La estimación del grado de impacto o consecuencias debe ser determinado mediante la aplicación de criterios en función de los tres principios de seguridad de la información:

- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de la información de completitud y exactitud.
- **Disponibilidad:** propiedad de la información de ser y estar accesible y utilizable a petición de una entidad autorizada.

Grado de Impacto		Criterio
Bajo	1	El daño o pérdida de confidencialidad, integridad y disponibilidad de activos de información, no afecta la operación (interna o tercerizada) de los procesos y servicios institucionales, sin embargo, podría provocar pérdidas financieras menores y tolerables para el Instituto.
Medio	2	El daño o pérdida de confidencialidad, integridad y disponibilidad de activos de información podría interrumpir parcialmente la operación (interna o tercerizada) de los procesos y servicios institucionales, provocar pérdidas exponenciales y consecuencias moderadas en la imagen y reputación institucional o en el cumplimento de los requisitos legales o contractuales.
Alto	3	El daño o pérdida de confidencialidad, integridad y disponibilidad de activos de información podría interrumpir totalmente la operación (interna o tercerizada) de los procesos y servicios institucionales, provocar pérdidas financieras y/o patrimoniales mayores, daños en la imagen y reputación institucional, incumplimiento de requisitos legales ocontractuales.

5.3.2 Probabilidad

Se refiere a la posibilidad de que un evento ocurra, considerando la cantidad de veces que podría presentarse en determinado periodo de tiempo, basándose en las eventualidadesconocidas y el conocimiento del entorno, o bien a través de juicio de experto.

Grado de Probabilidad	Criterio

Baja	1	Si no ha habido ningún tipo de antecedente registrado y/o que por el entorno la posibilidad de que suceda sea mínima.
Media	2	Si solo se ha tenido un antecedente registrado en un periodo anual y/o esporádicamente en intervalos de 3 a 5 años o que por el tipo de entorno y condiciones sea posible que ocurra.
Alta	3	Si ha habido más de dos eventos al término de un año o bien que por las condiciones actuales o el tipo de entorno sea sumamente posible que suceda.

5.3.3 Determinación del nivel de riesgo

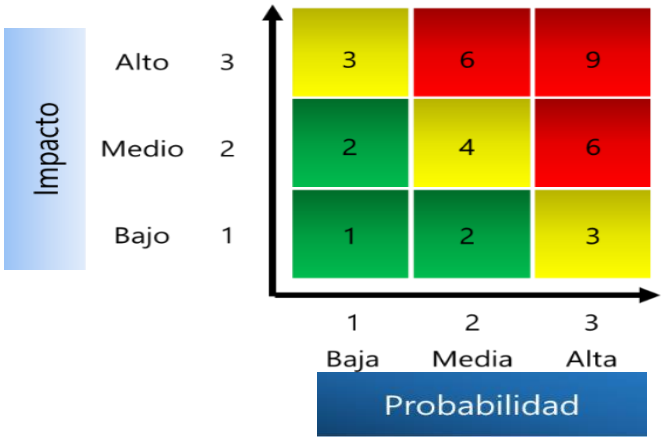
a) El nivel de riesgo debe ser representado en una escala cualitativa de 3 niveles, en ordencreciente (bajo, medio y alto) y su equivalencia cuantitativa (1, 2 y 3) respectivamente.

b) La fórmula que se utilizará para determinar el nivel de riesgo será la siguiente:

c) Los valores del impacto y la probabilidad deberán ingresarse en el Cuadro deevaluación de riesgos para obtener el nivel de riesgo. El nivel de riesgo se calculará multiplicando los dos valores.

5.4 Evaluación del riesgo

a) La siguiente imagen muestra un mapa de color con los resultados de las valoracionesrealizadas en el inciso anterior.



b) La siguiente tabla muestra el nivel de riesgo en escala cuantitativa y cualitativa.

Impacto		Probabilidad		Nivel de riesgo	
Cuantitativo	**Cualitativo**	**Cuantitativo**	**Cualitativo**	**Cuantitativo**	**Cualitativo**
3	Alto	1	Baja	3	Medio
3	Alto	2	Media	6	Alto
3	Alto	3	Alta	9	Alto
2	Medio	1	Baja	2	Bajo
2	Medio	2	Media	4	Medio
2	Medio	3	Alta	6	Alto
1	Bajo	1	Baja	1	Bajo
1	Bajo	2	Media	2	Bajo
1	Bajo	3	Alta	3	Medio

c) Una vez realizadas las valoraciones, se procederá a evaluar el riesgo comparando el nivel de riesgo con los criterios de aceptación del riesgo establecidos en el numeral 5.1.1, en dónde:

1. Los valores 1 y 2 (bajo) serán riesgos aceptables.
2. Los valores 3 y 4 (medio) serán riesgos no aceptables, por lo que deberán ser tratados.
3. Los valores 6 y 9 (alto) serán riesgos no aceptables por lo que deberán ser tratados.
4. Para los riesgos no aceptables, se deberá priorizar el tratamiento del riesgo para aquellos activos de mayor a menor valor; 3 (alto), 2 (medio) y 1 (bajo).

d) Con el fin de evitar retrabajo o costos innecesarios se deben identificar en su caso, controles existentes que permitan reducir el nivel de riesgo; éstos

tendrán que ser ingresados en el Cuadro de evaluación de riesgos, determinando su nivel de madurez.

e) Si el nivel de madurez de los controles existentes es 1, el riesgo no tendrá que ser tratado.

f) Si el nivel de madurez de los controles existentes es 2 el riesgo deberá ser tratado

5.5 Identificación de los propietarios de los riesgos

a) Para cada riesgo se deberá identificar un propietario: persona o unidad administrativa con la responsabilidad y la autoridad para gestionar un riesgo, destacando que podráo no ser el mismo que el propietario del activo.

5.6 Tratamiento del riesgo

a) El tratamiento de riesgos se implementará mediante el Cuadro de tratamiento de riesgos, copiando desde el Cuadro de evaluación de riesgos todos los riesgos identificados como no aceptables.
b) El tratamiento de riesgos será realizado por el propietario del riesgo y en aquellos casos en los que se requiera, de manera conjunta y coordinada con el custodio del activo.
c) Para los riesgos valorados en 3 y 4, así como 6 y 9 se deberá seleccionar una opción de tratamiento conforme a:

I. **Reducir el riesgo** - las acciones tomadas para reducir la probabilidad, consecuencias negativas, o ambas, asociados con un riesgo. (Ejemplo: elección deuno o varios controles de estándares internacionales u otros controles de seguridad).
II. **Aceptar el riesgo** – aceptación del agobio de la pérdida o el beneficio de la ganancia de un riesgo en particular. Esta opción estará permitida solamente si la selección de otras opciones de tratamiento del riesgo costara más que el impactopotencial o en el caso de que dicho riesgo se pudiera materializar.
III. **Evitar el riesgo** - decisión de no participar en, o la acción de retirarse de una situación de riesgo.
IV. **Transferir el riesgo** - compartir con un tercero el agobio de la pérdida o el beneficio de la ganancia un riesgo. (Ejemplo: suscribiendo una póliza de

seguros, un contrato con proveedores o socios, un acuerdo de nivel operacional, etc.).

d) La elección de opciones se implementará a través del Cuadro de tratamiento de riesgos.

e) Para el caso de que se eligieran varios controles de seguridad para un riesgo, se insertarán filas adicionales en la tabla, inmediatamente debajo de la fila en que se especifica el riesgo.

f) En el caso de la opción I (elección de controles de seguridad), será necesario evaluar el nuevo valor de impacto y probabilidad en el Cuadro de tratamiento de riesgos, conel fin de evaluar la efectividad de los controles planificados.

5.7 Declaración de aplicabilidad y Plan de tratamiento riesgos (análisis de brecha)

a) La Unidad de transparencia y las Unidades Administrativas deberán documentar en la Declaración de aplicabilidad lo siguiente:

- Controles de la Guía de Implementación de un Sistema de Gestión de Seguridad de Datos Personales que aplicables.
- Controles de la Guía de Implementación de un Sistema de Gestión de Seguridad de Datos Personales queno serán aplicables, describiendo la justificación de esa decisión.
- Controles de la Guía de Implementación de un Sistema de Gestión de Seguridad de Datos Personales implementados o no implementados.

b) La Unidad de transparencia, las Unidades Administrativas y en su caso el encargado deberán integrar el Plan de tratamiento de riesgos en el que se planificarála implementación de los controles.

c) La elección o diseño de controles se podrán identificar desde cualquier fuente segúnsea necesario.

d) Los propietarios de riesgos, el Comité de Transparencia y la Unidad de Transparencia podrán aceptar todos los riesgos residuales a través de la Declaración de aplicabilidad.

e) Los propietarios de riesgos, el Comité de Transparencia y la Unidad de Transparenciapodrán aprobar el Plan de tratamiento de riesgos.

5.8 Revisiones periódicas de la evaluación y el tratamiento de riesgos

a) Los propietarios de riesgos deberán revisar los riesgos vigentes y deberán actualizar los Cuadros de evaluación de riesgos y tratamiento de riesgos respectivamente, de acuerdo con los nuevos riesgos identificados.
b) La revisión se realizará al menos una vez por año, o con mayor frecuencia en caso de cambios organizacionales significativos, cambios importantes en tecnología, en los objetivos estratégicos, en el entorno del marco normativo aplicable relacionado con seguridad de la información y/o de datos personales

5.9 Informes

a) La Unidad de transparencia documentará los resultados de la evaluación y del tratamiento de riesgos y de todas las revisiones subsecuentes.
b) La Unidad de transparencia supervisará el progreso de la implementación del Plan detratamiento de riesgos e informará periódicamente los resultados al Comité deTransparencia.