Suprema Corte
de Justicia de la Nación

Análisis de Riesgo y Análisis de Brecha. Metodología de Cálculo

ABRIL 2026

1. Justificación

La actualización de la metodología para el análisis de riesgo toma como referencia la "Metodología de Análisis de Riesgo BAA (beneficio, accesibilidad y anonimidad del atacante)"[1] que sustentó el primer ejercicio de encuesta de análisis de riesgo. A la luz de los hallazgos y la implementación del *Plan de trabajo en materia de protección de datos personales* (Plan de Trabajo), resultó necesario reformular la encuesta para implementarla de manera electrónica, actualizar los niveles de riesgo a través de herramientas que permitan automatizar su cálculo y elegir una escala cuyos niveles sean más claros para definir el riesgo final en cada tratamiento de datos personales. Esto no modifica la esencia de la metodología y tampoco altera los niveles que deben responder cada uno de los tratamientos.

Asimismo, el análisis de brecha es la herramienta para identificar la distancia que existe entre las medidas recomendadas en el Plan de Trabajo y las medidas implementadas para cada uno de los tratamientos reportados, cuya encuesta también se pone a disposición de manera electrónica con la finalidad de automatizar los resultados.

Estas actualizaciones resultan importantes y necesarias para actualizar el Documento de Seguridad 2019, en la medida que durante los últimos meses se han agregado, fusionado o eliminado tratamientos de datos personales, además de que se han implementado la mayoría de las medidas de seguridad recomendadas inicialmente.

2. Metodología de cálculo, nivel riesgo

Este apartado tiene la finalidad de ilustrar la metodología para calcular el riesgo en los tratamientos de datos personales. Los niveles de riesgo tienen una escala tríadica: bajo (0 a 59), medio (60 a 89) y alto (en adelante).

El nivel de riesgo del tratamiento se obtiene de sumar los valores obtenidos en cuatro categorías de riesgo que a continuación se detallan:

a) **Riesgo por tipo de dato (inherente):** contempla el riesgo inherente a la naturaleza de los datos personales; es decir, el riesgo que representa cada categoría de datos personales. Por ejemplo, un dato de salud tiene, en sí mismo, un nivel de riesgo superior a uno de identificación, como el nombre. A continuación, de manera

[1] INAI, Metodología de Análisis de Riesgo BAA, 2015.

ejemplificativa, se presenta una escala en donde se asignan los valores según el tipo de dato:

CATEGORÍA DE DATOS	RIESGO
Datos identificativos o de contacto (nombre, edad, sexo, domicilio, teléfono, correo, firma, etc.)	10
Datos laborales o patrimoniales (nombramiento, remuneración, bienes, información fiscal o bancaria, procedimientos, etc.)	20
Datos biométricos o de salud (expediente clínico, peso, resultados clínicos, huellas dactilares, imagen, voz, etc.)	30
Datos sensibles (menores de edad, identidad de género, preferencia sexual, enfermedades, migratorios, origen étnico, etc.)	40

b) **Riesgo por número de titulares:** el riesgo inherente aumenta según el número de registros de personas titulares en la base de datos. Es decir, el riesgo se altera si la base de datos cuenta con muchos registros. Para tener una mayor claridad, se propone la siguiente escala:

NÚMERO DE TITULARES	RIESGO
Menos de 100 titulares	0
De 100 a 1,000 titulares	5
De 1,000 a 10,000 titulares	10
Mas de 10,000 titulares	15

c) **Riesgo por número de acceso:** se mide determinando la cantidad de accesos potenciales a los datos personales que se pretenden proteger en un intervalo de tiempo determinado, por ejemplo, durante 24 horas. Para este parámetro entre más accesos, mayor riesgo, según la siguiente escala:

ACCESOS	RIESGO
Menos de 10 accesos	10
De 10 a 20 accesos	20
De 20 a 30 accesos	30
Más de 30 accesos	40

d) **Riesgo por tipo de entorno:** este factor representa el nivel de anonimidad para acceder o hacer uso de los datos personales que se tratan. Entre mayor anonimidad ofrezca el entorno, mayor riesgo existe de que se vulnere la seguridad, de acuerdo con la siguiente escala:

ENTORNO	RIESGO
Físico (archivero de la unidad)	10
Equipo de cómputo	20
Nube (intranet, one dirve, Google drive, etc.)	30
Internet	40

La suma de los factores anteriores resulta en el nivel de riesgo. La escala tríadica para calificar a los resultados es la siguiente:

NIVEL DE RIESGO	Bajo	Medio	Alto
	30 - 59	60 - 89	90 - 100+

3. Metodología de cálculo, nivel de brecha

El nivel de riesgo que se desarrolló anteriormente permite identificar lo riesgoso que resulta cada uno de los tratamientos de datos personales y a saber qué medidas de seguridad le corresponden de acuerdo con el Catálogo de Medidas de Seguridad.

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 ejemplo, si se recomienda implementar al tratamiento “A” un conjunto

de medidas "C", y el área responsable de dicho tratamiento informa que de ese conjunto de medidas hacen falta implementar algunas, la identificación de lo que falta implementar se conoce como "brecha".

Es importante mencionar que la premisa para la recomendación de medidas de seguridad se reforzó de tal manera que los márgenes de diferencia entre una categoría de tratamientos y otra, según su nivel de riesgo, es mínima, pues se buscó que la mayoría de las medidas fueran implementadas en todos los tratamientos de datos personales, independientemente de su nivel de riesgo. Con base en esto, todas las medidas de seguridad aplican para todos los tratamientos, excepto las marcadas con "+" que aplican sólo para los tratamientos de riesgo medio y las marcadas con "*" que aplican sólo para tratamientos de riesgo alto.

MEDIDAS DE SEGURIDAD			
	Administrativas	**Físicas**	**Técnicas**
A	Declaratoria de confidencialidad	Cuidado de los bienes informáticos	Cuidado de la contraseña personal
B	Listado de Personal	Prevenir accesos no autorizados	Actualización de contraseñas
C	Clasificación de archivos físicos	No instalar equipos ajenos	Reportar fallas
D	Clasificación de archivos electrónicos	Traslado de equipos de cómputo	No instalar softwares
E	Capacitación	Archivero con candado+	Contraseñas robustas
F	Bitácora de vulneraciones	Candados de seguridad para equipos de cómputo*	Respaldo de información
G	Depuración y borrado seguro del archivo físico	Zona de confidencialidad*	
H	Depuración y borrado seguro del archivo electrónico		
I	Bitácora de consulta*		
J	Responsable de seguridad		
K	Transferencias		

Dudas o comentarios dirigirse a:

Unidad de Transparencia de la Suprema Corte de Justicia de la Nación

Correo electrónico:

datospersonales@mail.scjn.gob.mx

Suprema Corte
de Justicia de la Nación