Acuerdo No. T-SE-CT-05/2025

ACUERDO POR EL CUAL SE ESTABLECE LA ELABORACIÓN DE ANÁLISIS DE RIESGO Y BRECHA DE LOS DATOS PERSONALES -------------------------------------

------------------------------ ACUERDO --------------------------------

Primero. El Comité de Transparencia del H. Ayuntamiento de Taretan, es competente para emitir el presente Acuerdo. --

Segundo. Se aprueba la Elaboración del Análisis de Riesgo y Brecha de los Datos Personales del H. Ayuntamiento de Taretan, siendo el siguiente: ------------------------------------

Justificación

El análisis de riesgo toma como referencia la "Metodología de Análisis de Riesgo BAA (beneficio, accesibilidad y anonimidad del atacante)". A través de la implementación del Plan de Trabajo en materia de protección de datos personales (Plan de Trabajo), se determinaron los niveles de riesgos 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.

Metodología de Cálculo, Nivel de Riesgo

En este apartado se pretende ilustrar la metodología para calcular el riesgo en los tratamientos de datos personales. Los niveles de riesgo tienen una escala: 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, se presenta una escala en donde se asignan los valores según el tipo de dato:

Categoría	Riesgo
Datos identificativos (nombre, edad, sexo, domicilio, teléfono, correo, firma, etc.)	**10**
Datos laborales y 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 registro 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
Más de 10,000 titulares	15

c) **Riego 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 computo	20
Nube (intranet, one drive, Google drive, etc.)	30
Internet	40

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

Nivel de Riesgo	Bajo	Medio	Alto
	30-59	60-89	90-100+

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.

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 recomienda implementar el 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 hace 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 su categoría de tratamiento y otra, según su nivel de riesgo, es mínima, pues se busca 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 los marcados con "+" que aplican solo para los tratamientos de riesgo medio y las marcadas con "*" que aplican solo 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 contraseña
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		

---------- TRANSITORIOS ----------

Primero. El presente Acuerdo entrará en vigor en la fecha de su aprobación. ----------

Segundo. Se instruye al Secretario Técnico del Comité de Transparencia que realice lo conducente a efecto de que la Elaboración del Análisis de Riesgo y Brecha de los Datos Personales del H. Ayuntamiento de Taretan, aprobado por medio del presente Acuerdo sea publicado en la página web oficial del H. Ayuntamiento de Taretan https://taretan.gob.mx/ y, en la página web de la Plataforma Nacional de Transparencia https://consultapublicamx.plataformadetransparencia.org.mx/vutweb/faces/view/consultaPublica.xhtml?idEntidad=MTY=&idSujetoObligado=MzUwMg==#inicio a efecto de dar cumplimiento a las obligaciones de transparencia aplicables al H. Ayuntamiento de Taretan en cuanto a sujeto obligado.-

Tercero. Hágase del conocimiento del presente al Secretario Técnico del H. Ayuntamiento, para los efectos conducentes. ----------

Aprobado en la Cuarta Sesión Ordinaria del Comité de Transparencia del H. Ayuntamiento de Taretan celebrada el 12 doce de diciembre de 2025 dos mil veinticinco en Taretan, Michoacán, por los integrantes del mismo Comité. ----------

Comité de Transparencia

Lic. Héctor Hugo Medina Sandoval
Presidente

Ing. Rodrigo Gamiño García
Secretario del Comité

Lic. Alicia Ruiz Pureco
Vocal del Comité

Lic. Atzimba Cabrera Martínez
Vocal del Comité

C. Karen Liliana Meza Gurrero
Vocal del Comité

La presente hoja de firmas corresponde al acuerdo número T-SE-CT-05/2025 aprobado en la Cuarta Sesión Ordinaria celebrada por el Comité de Transparencia del H. Ayuntamiento de Taretan el 12 doce de diciembre de 2025 dos mil veinticinco. --