TERCERA SESIÓN EXTRAORDINARIA DEL COMITÉ DE TRANSPARENCIA DE LA ALCALDÍA TLALPAN 2023
20-julio-2023

Punto VII, VIII

Propuesta y aprobación de la Guía para la Elaboración del Documento de Seguridad de la Alcaldía Tlalpan.

ACUERDO: A03/CTSE/03/AT/20-07-2023

2023 AÑO DE Francisco VILLA

NÚMERO DE SESIÓN: Tercera Sesión Extraordinaria 2023, del Comité De Transparencia de la Alcaldía Tlalpan de fecha 20 de julio de 2023
NUMERO DE ACUERDO: *A03/CTSE03/AT/20-07-2023*
JUSTIFICACIÓN;
Con fundamento en los artículos 88, 89 Párrafo 5, 90 fracción II IX y XII, 91 y 217 fracción II de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, así como los artículos 51, segundo párrafo de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y 104 de los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, se sometió a votación del Pleno de esta Comité de Transparencia, con la finalidad de dar cumplimiento a las observaciones derivadas del procedimiento de verificación **01/2023**, por parte del Instituto de Transparencia y de la orden de intervención número **V-1/2023**; con clave 14, Obligaciones de Transparencia", por parte del Órgano Interno de Control en la Alcaldía Tlalpan, el Pleno de este Comité de Transparencia confirma el siguiente:
ACUERDO
Acuerdo Guía para la Elaboración del Documento de Seguridad de la Alcaldía Tlalpan **De conformidad con lo previsto en los artículos 3, fracción XIV, 27, 28 y 29 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, se aprueba la Guía para la Elaboración del Documento de Seguridad de la Alcaldía Tlalpan, la cual entrará en vigencia a partir del 21 de julio de 2023, siendo de observancia obligatoria para las unidades administrativas que tutelan Sistemas de Datos Personales la elaboración de sus documentos de seguridad, con la Guía de mérito.----------** **----------**

Mtra. Sandra Zamudio Arciga Secretaria Particular de la Alcaldesa y Presidenta del Comité de Transparencia	**C. Jorge Romero Marinero** Presidente Suplente Secretario Técnico del Comité de Transparencia
VOCALES TITULARES	**VOCALES SUPLENTES**

Mtro. Aurelio Alfredo Reyes García Director General de Asuntos Jurídicos y de Gobierno	**Lic. José Antonio Domínguez Hernández** Director de Ordenamiento Territorial.
C.P. Guillermo, Nájera Gómez Director General de Administración	**Lic. Ángel Arturo Lugo Flores** Subdirector de Cumplimiento de Auditorias
Dirección General de Obras y Desarrollo Urbano	**Lic. Roberto Carlos Jiménez Almeira** Director de Desarrollo Urbano
Lic. Natalia Guadalupe Márquez Codina Directora General de Desarrollo Social	**Lic. Anarely López Mayo** Líder Coordinador de Proyectos de Sistematización B.
Mtra. Claudia Isela Ramírez Barreda Directora General de Derechos Culturales y Educativos	**Brisna Viridiana Pérez Hernández** Jud. de Educación y Capacitación
C. Jesús Jiménez Martínez Director General de Planeación del Desarrollo	**Lic. Wendolin Marlene Sánchez Montes de Oca** Jud. de Análisis y Seguimiento de Información de Programas y Proyectos

C. Rosalba Hernández Martínez Directora General de Medio Ambiente Desarrollo Sustentable y Fomento Económico	**C. Edgardo Sánchez Cortes** Director de Economía Solidaria, Desarrollo y Fomento Económico
C.P. Oscar Pérez Peña Titular del Órgano Interno de Control en Tlalpan	**Lic. Christofer Alan García Martínez** Jud. de investigaciones del Órgano Interno de Control en Tlalpan
Lic. Irad Platas Chávez Asesor "A" y Secretario Técnico del Concejo de la Alcaldía	**C. Bruno Guzmán Martínez** Asesor de la Secretaría Técnica del Concejo
INVITADOS PEERMANENTES	
Ing. Julio Ignacio Castellanos Torres Director de Modernización y TIC´s	**Lic. Lucero Zamudio Albañil** Jud. de Archivos
Lic. Adolfo León Vergara Jud. de Información Pública y Datos Personales	

GUÍA PARA LA ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD DE LA ALCALDÍA TLALPAN

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES DENOMINADO [DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES].

ALCALDÍA TLALPAN 2021-2024	DOCUMENTO DE SEGURIDAD	
	Fecha de elaboración:	Fecha de última actualización:
	Elaboró el documento:	Aprobó el documento:
	Nombre y firma	Nombre y firma

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

ÍNDICE

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

I. INTRODUCCIÓN

El presente Documento de Seguridad, será de aplicación al Sistema de Datos Personales denominado **[DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES], cuya finalidad es: [INDICAR FINALIDAD ACTUALIZADA]",** que contiene datos de carácter personal, mismos que están bajo responsabilidad de la **[DENOMINACIÓN DE LA UNIDAD ADMINISTRATIVA RESPONSABLE],** Incluyendo los soportes y equipos empleados para el tratamiento de datos personales, que deben ser protegidos conforme a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, con los siguientes datos:

Fecha de registro en RESDP: (Anexo I).
Folio de inscripción:
Fecha de creación: (Gaceta Oficial de la Ciudad de México) (Anexo II).
Fecha de última modificación en el RESDP:

Las personas que intervienen en el tratamiento de datos personales, se ubican en **[INDICAR DOMICILIO ACTUAL, MAPA DE UBICACIÓN Y CROQUIS DEL ÁREA EN QUE SE DA TRATAMIENTO A DATOS PERSONALES]**

En este sentido, solo las siguientes personas servidoras públicas podrán tener acceso y dar tratamiento a los datos personales contenidos en el citado Sistema de Datos Personales:

Personal autorizado para el tratamiento de datos personales	
Nombre de la persona servidora pública Responsable del Sistema de Datos Personales	
Cargo en la estructura orgánica	

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

Datos personales a los que dará tratamiento	
Funciones y obligaciones en materia de datos personales	
Tipo de tratamiento de datos personales	

Nombre de la persona servidora pública Responsable de Seguridad	
Cargo en la estructura orgánica	
Datos personales a los que dará tratamiento	
Funciones y obligaciones dentro de la estructura orgánica	
Funciones y obligaciones en materia de datos personales	
Tipo de tratamiento de datos personales	

[ANEXO III, OFICIO DE DESIGNACIÓN DE RESPONSABLE DE SEGURIDAD]

Nombre de la persona servidora pública usuaria	
Cargo en la estructura orgánica	
Datos personales a los que dará tratamiento	
Funciones y obligaciones dentro de la estructura orgánica	
Funciones y obligaciones en materia de datos personales	
Tipo de tratamiento de datos personales	

El nivel de seguridad que aplica al Sistema de Datos Personales denominado **Usuarios de la Oficina de Información Pública, tiene nivel de seguridad [INDICAR EL NIVEL DE SEGURIDAD] pues se recolecta y da tratamiento, a los siguientes datos personales [INDICAR LAS CATEGORÍAS Y TIPOS DE DATOS PERSONALES]**

El tipo de tratamiento que se da es **mixto, pues se recaban en formatos impresos y electrónicos [INDICAR EL NOMBRE DE CADA FORMATO DE RECOLECCIÓN]**

1. **Físicos (ANEXO IV)**

2. **Automatizados: (ANEXO V)**

La recolección en formatos impresos, **se realiza directamente de las personas solicitantes,** para dar cumplimiento a lo establecido en **[INDICAR EL FUNDAMENTO NORMATIVO]**

Para efecto de coordinar e implementar las medidas de seguridad, se designa a las y los siguientes usuarios: **[INDICAR EL NOMBRE DE LAS PERSONAS USUARIAS] (ANEXO V, OFICIO DE DESIGNACIÓN DE USUARIOS)**

Asimismo, para contar con el control y seguimiento, este Documento de Seguridad correspondiente al Sistema de Datos Personales denominado **[DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES, será** actualizado de forma semestral, o:

1. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
2. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

3. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad

Toda actualización se registrará en el formato denominado “Control de actualizaciones del Documento de Seguridad” **(Anexo VI)**

Sistema de Datos Personales denominado **[DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES, tiene la siguiente:**

Estructura del Sistema de Datos Personales	Descripción
Nombre del Sistema de Datos Personales:	
Finalidad del Sistema de Datos Personales:	
Normatividad aplicable:	
Unidad Administrativa Responsable:	
Fecha de última modificación del Sistema de Datos Personales:	

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

Responsable del Sistema de Datos Personales:	
Encargados:	
Usuarias (os):	
Responsable de Seguridad	

II. INVENTARIO DE DATOS PERSONALES EN EL SISTEMA DE DATOS PERSONALES USUARIOS DE LA OFICINA DE INFORMACIÓN PÚBLICA

INVENTARIO DE DATOS PERSONALES DEL SISTESMA DE DATOS PERSONALES						
CATEGORÍA	**TIPO DE DATOS PERSONALES**	**ORIGEN**	**GRUPO DE PERSONAS DE ORIGEN**	**FORMA DE RECOLECCIÓN**	**MEDIO DE ACTUALIZACIÓN**	**TRATAMIENTO**

CICLO DE VIDA DE LOS DATOS PERSONALES

Tiempo de conservación en medio automatizado:
Tiempo de conservación en el archivo de trámite:
Tiempo de conservación en el archivo de concentración:

En su caso, señale si se contempla la transferencia de la información contenida en el sistema al archivo histórico: sí

TRANSFERENCIAS

Tipo Destinatario	**Destinatario**	**Tipos de datos transferidos**	**Finalidad genérica de la transmisión**	**Fundamento legal**

Elaboró **María Elena Hernández Mora**	**Órgano Colegiado**	**Aprobado**			**Vigente a partir de**		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

REMISIÓN DE DATOS PERSONALES

No se prevén remisiones toda vez que este Sistema de Datos Personales, no cuenta con encargados.

Interrelación [INDICAR LA POSIBLE INTERRELACIÓN

EL CATÁLOGO DE LOS TIPOS DE DATOS PERSONALES

CATEGORÍA	TIPO DE DATOS PERSONALES

III. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE DAN TRATAMIENTO A DATOS PERSONALES

Bajo la consideración de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, todas las personas servidoras públicas que den tratamiento a datos personales están obligadas a conocer y observar las medidas de seguridad, normas, procedimientos y reglas que afecten el tratamiento de los datos personales.

FUNCIONES Y OBLIGACIONES DE LA PERSONA RESPONSABLE DEL SISTEMAS DE DATOS PERSONALES

La persona responsable del Sistema de Datos Personales denominado **[DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES], tendrá las siguientes funciones y obligaciones**

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

"…

1. Deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.
2. Deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiere.
3. Deberá justificar todo tratamiento de datos personales con finalidades concretas, lícitas, explícitas, legítimas y relacionadas con las atribuciones que la normatividad aplicable les confiera.
4. Podrá tratar datos personales para finalidades distintas a las establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la Ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia.
5. No deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

6. Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca.
7. Deberá adoptar, las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.
8. Deberá suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables.
9. Observará que los plazos de conservación de los datos personales no excedan aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento.
10. Deberá establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos, de conformidad con lo dispuesto en el artículo anterior de la presente Ley
11. Deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

12. Deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.
13. Cuando resulte imposible dar a conocer al titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, el responsable podrá instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emita el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.
14. Deberá adoptar al menos los siguientes mecanismos para cumplir con el principio de responsabilidad:

a) Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales;
b) Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;
c) Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
d) Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
e) Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;
f) Establecer procedimientos para recibir y responder dudas y quejas de los titulares;
g) Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y
h) Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.

15. Deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

16. Las medidas de seguridad adoptadas deberán considerar:

a) El riesgo inherente a los datos personales tratados;
b) La sensibilidad de los datos personales tratados;
c) El desarrollo tecnológico;
d) Las posibles consecuencias de una vulneración para los titulares;
e) Las transferencias de datos personales que se realicen;
f) El número de titulares;
g) Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
h) 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.

17. 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:

a) Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
b) Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
c) Elaborar un inventario de datos personales y de los sistemas de tratamiento;
d) 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;
e) Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
f) 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;
g) Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y

h) Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

18. Deberá documentar las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.
19. Deberá elaborar el documento de seguridad que contenga al menos, lo siguiente:

a) El inventario de datos personales y de los sistemas de tratamiento;
b) Las funciones y obligaciones de las personas que traten datos personales;
c) El análisis de riesgos;
d) El análisis de brecha;
e) El plan de trabajo;
f) Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
g) El programa general de capacitación.

20. Deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:

a) Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
b) Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
c) Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
d) Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

21. En caso de que ocurra una vulneración a la seguridad, deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita. Se considerarán, como vulneraciones a la seguridad, al menos las siguientes:

a) La pérdida o destrucción no autorizada;
b) El robo, extravío o copia no autorizada;
c) El uso, acceso o tratamiento no autorizado, o

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

d) El daño, la alteración o modificación no autorizada.

22. Deberá 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.
23. Deberá informar sin dilación alguna al titular, y según corresponda, al Instituto y a los Organismos garantes de las Entidades Federativas, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.
24. Deberá informar al titular al menos lo siguiente:

a) La naturaleza del incidente;
b) Los datos personales comprometidos;
c) Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
d) Las acciones correctivas realizadas de forma inmediata, y
e) Los medios donde puede obtener más información al respecto.

25. 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 subsistirá aún después de finalizar sus relaciones con el mismo.

Las personas servidoras públicas que dan tratamiento a datos personales tendrán las siguientes funciones y obligaciones:

a) POLÍTICAS GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES DE LA ALCALDÍA TLALPAN

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, es de orden público y de observancia general en la Ciudad de México, en materia de protección de datos personales en posesión de sujetos obligados. En este sentido, las disposiciones que prevé son de aplicación y observancia directa para los sujetos obligados de la Ciudad de México.

Por ello, la Alcaldía Tlalpan como Responsable y para efecto de cumplir con las obligaciones, deberes y principios de calidad, confidencialidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad, transparencia y temporalidad, para la protección de datos personales, en observancia a lo anterior, presenta en el documento de mérito, las **Políticas Generales para la Protección de Datos Personales de la Alcaldía Tlalpan, aprobadas por acuerdo número A02/CTSE03/AT/20-07-23; del Comité de Transparencia en la Tercera Sesión Extraordinaria, celebrada el 20 de julio de 2023.**

Los mecanismos de protección de datos personales contenidos en estas políticas, además de ser de observancia obligatoria para las personas servidoras públicas adscritas a la Alcaldía Tlalpan, tienen como referencia el tratamiento de datos personales, entendido de acuerdo con en el artículo 3, fracción XXXIV de la Ley de Datos Local, como:

> *"…**cualquier operación o conjunto de operaciones efectuadas sobre datos personales o conjunto de datos personales, mediante procedimientos manuales o automatizados relacionadas con la obtención, uso, registro, organización, estructuración, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión o cualquier otra forma de habilitación de acceso, cotejo, interconexión, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales**…"(Sic)*

En este sentido, es deber de toda aquella persona servidora pública que, de tratamiento a datos personales, considerar que éste abarca todas las posibles **acciones de procesamiento físico y/o automatizado,** y la **aplicación**, es decir: recolección, registro, organización, conservación, extracción, utilización, elaboración

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

o modificación de archivos, sistematización, consulta, comunicación, bloqueo de datos personales, baja documental y supresión de sistemas de datos personales.

En tal virtud, para cumplir con un ciclo virtuoso en la protección de datos personales, estas Políticas Generales, establecen de forma enunciativa, más no limitativa, los deberes y obligaciones que han de cumplir: las personas servidoras públicas Responsables de Sistemas de Datos Personales, responsables de seguridad, usuarias, el Comité de Transparencia, el Comité Técnico Interno de Administración de Documentos y de forma específica, la Dirección de Tecnologías de la información, esta última en la materia específica relacionada con la supresión de Sistemas de Datos Personales automatizados.

2. OBJETIVO Y AMBITO DE APLICACIÓN

2.1 Las políticas de protección de datos personales son de aplicación general y obligatoria para:

I. Todas las áreas que tutelan Sistemas de Datos Personales
II. Las personas servidoras públicas Responsables de Sistemas de Datos Personales, Responsables de Seguridad, Usuarias.
III. Todas las personas servidoras públicas adscritas a la Alcaldía Tlalpan y que, en el ejercicio de sus funciones obtengan, usen, registren, organicen, conserven, elaboren, utilicen, comuniquen, difundan, almacenen, posean, accedan, manejen, aprovechen, divulguen, transfieran o dispongan datos personales.

3. NORMATIVIDAD APLICABLE

- Constitución Política de los Estados Unidos Mexicanos
- Constitución Política de la Ciudad de México
- Ley Orgánica de las Alcaldías de la Ciudad de México
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

- Ley General de Archivos.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México
- Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México
- Ley de Archivos de la Ciudad de México
- Reglamento de la Ley de Transparencia y Acceso a la Información Pública de la Administración Pública del Distrito Federal
- Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México
- Manual Administrativo de la Alcaldía Tlalpan.

4. POLÍTICAS GENERALES DE PROTECCIÓN DE DATOS PERSONALES DE LA ALCALDÍA TLALPAN

4.1 Para las actividades de protección de datos personales, la persona servidora pública Responsable del Sistema de Datos Personales, designará por oficio a la persona responsable de seguridad y a las personas servidoras públicas usuarias. En el mismo acto, hará de su conocimiento las medidas de seguridad.

4.2 Las personas Responsables de Sistemas de Datos Personales, deberán cumplir con los siguientes principios:

I. **Calidad:** Los datos personales deben ser ciertos, adecuados, pertinentes y proporcionales, no excesivos, en relación con el ámbito y la finalidad para la que fueron recabados.

II. **Confidencialidad:** El Responsable garantizará que exclusivamente el titular pueda acceder a sus datos, o en su caso, el mismo Responsable y el usuario a fin de cumplir con las finalidades del tratamiento. En cualquier caso, se deberá garantizar la secrecía y la no difusión de los mismos. Sólo el titular podrá autorizar la difusión de sus datos personales.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

III. **Consentimiento**: Toda manifestación previa, de voluntad libre, específica, informada e inequívoca por la que el titular acepta, mediante declaración o acción afirmativa, el tratamiento de sus datos personales.

IV. **Finalidad**: Los datos personales recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados. Los datos personales con fines de archivo de interés público, investigación científica e histórica, o estadísticos no se considerarán incompatibles con la finalidad inicial.

V. La Finalidad incluirá el ciclo de vida del dato personal, de tal manera, que concluida ésta, los datos puedan ser suprimidos, cancelados o destruidos.

VI. **Información:** El Responsable deberá informar al titular de los datos sobre las características principales del tratamiento, la finalidad y cualquier cambio del estado relacionados con sus datos personales.

VII. **Lealtad:** El tratamiento de datos personales se realizará sin que medie dolo, engaño o medios fraudulentos, tengan un origen lícito, y no vulneren la confianza del titular.

VIII. **Licitud.** El tratamiento de datos personales será lícito cuando el titular los entregue, previo consentimiento, o sea en cumplimiento de una atribución u obligación legal aplicable al sujeto obligado; en este caso, los datos personales recabados u obtenidos se tratarán por los medios previstos en el presente ordenamiento, y no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

IX. **Proporcionalidad:** El Responsable tratara sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con la finalidad o finalidades, para lo cual se obtuvieron.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

X. **Transparencia:** La información relacionada con el tratamiento de datos será accesible y fácil de entender, y siempre a disposición del titular.

XI. **Temporalidad:** Los datos personales tendrán un ciclo de vida o una temporalidad vinculada a la finalidad para la cual fueron recabados y tratados. Una vez concluida su finalidad o hayan dejado de ser necesarios, pertinentes o lícitos, pueden ser destruidos, cancelados o suprimidos.

5. Responsable de Sistemas de Datos Personales:

5.1 La persona servidora pública Responsable de Sistemas de Datos Personales, está obligada garantizar la protección de los datos personales contenidos en el Sistema de Datos Personales, para tal efecto:

I. Coordinará las acciones con la persona servidora pública Responsable de Seguridad, con el objetivo de elaborar y actualizar los avisos de privacidad integral y simplificado
II. Vigilará en conjunto con el Responsable de Seguridad, que el aviso de privacidad simplificado, se haga de conocimiento de las personas titulares de los datos personales, previo a la recolección de datos personales
III. Establecerá el mecanismo para verificar que los avisos de privacidad simplificado e integral, sean hechos públicos en la página de la Alcaldía Tlalpan.
IV. Coordinará las acciones pertinentes y adecuadas en conjunto con el Responsable de Seguridad, con el objeto de que el aviso de privacidad integral, sea colocado en un lugar físico visible a todo público y que sea integrado en los formatos de recolección de datos personales.
V. Verificará que el listado de personas servidoras públicas autorizadas para el tratamiento de datos personales, esté instalado en los distintos espacios donde se realiza recolección y tratamiento de datos personales.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

VI. Coordinará las acciones específicas con el Responsable de seguridad a efecto de diagnosticar las necesidades de capacitación en materia de protección de datos personales

VII. Coordinará en conjunto con el Responsable de Seguridad, la elaboración e implementación del Programa de Capacitación en materia de protección de Datos Personales.

VIII. Verificará que las personas servidoras públicas usuarias asistan a las capacitaciones especializadas y apliquen los conocimientos y herramientas adquiridos.

IX. En casos de posibles creaciones, modificaciones o supresiones de Sistemas de Datos Personales, se coordinará con el Responsable de Seguridad, con el objeto de elaborar y dar seguimiento a los Acuerdos respectivos, hasta su publicación en Gaceta.

X. Verificará que una vez publicados los Acuerdos de creación, modificación o supresión de Sistemas de Datos Personales, en la Gaceta Oficial de la Ciudad de México, se realicen las inscripciones, modificaciones o supresiones correspondientes en el Registro Electrónico de Sistemas de Datos Personales.

XI. Coordinará en conjunto con el Responsable del Sistema de Datos Personales, la elaboración, actualización e implementación del Documento de Seguridad.

XII. Coordinará en conjunto con el Responsable de Seguridad, la elaboración e implementación de mecanismos de monitoreo, actualizarán el análisis de brecha y de riesgo conforme a las necesidades de protección de datos personales.

XIII. Instruir al Responsable de Seguridad a efecto de que realice las actualizaciones pertinentes y adecuadas al documento de seguridad y lleve el control de las mismas.

XIV. Aplicará, cuando así resulte necesario, los Lineamientos Internos para el Bloqueo de Datos Personales y para la Supresión de Sistemas de Datos Personales de la Alcaldía Tlalpan.

XV. Establecerá, de ser el caso, las cláusulas en los contratos para que los sujetos obligados en el ámbito público o privado a los cuales sean

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

transferidos datos personales se obliguen a la confidencialidad de éstos durante y posterior a la vigencia del instrumento jurídico.

XVI. Proponer la implementación de buenas prácticas para la protección de datos personales.

XVII. Coordinará en conjunto con el Responsable de Seguridad, la generación de evidencias de los controles implementados para garantizar la confidencialidad de los datos, así como de los talleres, cursos, seminarios y actividades de capacitación en que haya participado el personal involucrado en el tratamiento de datos personales.

XVIII. Coordinará en conjunto con el Responsable de Seguridad, las acciones indispensables a efecto de que el documento de seguridad y el Sistema de Datos Personales, sea contemplado en las actas de entrega recepciones correspondientes.

XIX. Coordinará en conjunto con el Responsable de Seguridad, las acciones indispensables a efecto de que en los casos de supresión de sistemas de datos personales se cumpla con la norma en materia de archivos y de protección de datos personales.

XX. Deberán tomar las medidas para mitigar riesgos de brecha de integridad en los sistemas de datos personales, implementando controles de acceso, alertas y registros ante modificaciones, así como el sistema de monitoreo para la verificación continua del tratamiento de datos personales.

XXI. Establecerá para la mitigación de riesgos, cuando menos las siguientes medidas de seguridad:

a) Evaluar si las medidas de seguridad disponibles antes de la brecha de datos personales eran adecuadas al nivel de riesgo.

b) Introducir, en caso de ser necesario, medidas de seguridad adicionales o corregir fallos o deficiencias en las medidas de seguridad adoptadas.

c) Considerará, cuando menos las siguientes opciones:

- Políticas y formación en protección de datos y seguridad de la información. ▪ Sistemas actualizados.
- Registro de incidentes.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

- Monitoreo periódico.
- Control de acceso físico y lógico.
- Diferentes niveles de acceso a los datos.
- Copias de seguridad / Plan de recuperación.
- Anonimización.

XXII. Establecerá estrategias y procedimientos de recuperación de datos personales ante situaciones en que se presenten brechas de datos personales, incluyendo procedimientos de copia de seguridad y recuperación ante incidentes.

XXIII. Determinará el nivel de seguridad de los Sistemas de Datos Personales, previo análisis realizado con su responsable de seguridad, sus usuarios. Para tal efecto, considerará lo siguiente:

a) Los categorías y tipos de datos personales recolectados en los formatos establecidos para dicho objetivo

b) Las categorías y tipos de datos personales, que obren en la documentación que acompañe al formato de recolección de datos personales, ejemplo: identificación oficial, comprobantes de estudio, acta de nacimiento, etc. Para lo cual realizará una evaluación minuciosa de los datos personales recolectados de forma directa (formatos institucionales), documentación con que se acompañe el formato.

c) Para determinar el nivel de seguridad, considerará los siguientes criterios:

Nivel básico: datos personales de identificación; datos Personales electrónicos; datos Personales laborales; datos personales de naturaleza pública.
Nivel medio: datos personales patrimoniales; datos Personales sobre procedimientos administrativos y/o jurisdiccionales; datos personales académicos.

Nivel alto: datos personales de movimientos migratorios; datos sobre la salud; datos personales biométricos, datos personales especialmente protegidos y/o sensibles

6. Usuarias (os)

6.1 Las personas servidoras públicas usuarias:

I. Contarán con una ejemplar del oficio de designación, así como de las medidas de seguridad a implementar.
II. Tendrán dominio de las medidas de seguridad y aplicarlas en el diario tratamiento de datos personales.
III. Cumplirán con el deber de informar a las personas titulares de los datos personales, cuando menos: el nombre del Sistema de Datos Personales, la finalidad, los datos personales que recolectarán y el área en donde podrán ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO)
IV. Verificarán que los formatos que les sean asignados para la recolección de datos personales, cuenten con el aviso de privacidad actualizado. De no estar actualizado, dejar evidencia de que se le ha informado tal situación al Responsable de Seguridad.
V. Resguardarán con total confidencialidad los formatos mediante los cuales recolectan datos personales.
VI. Registrarán los accesos realizados al sistema físico, como automatizado, en su respectiva bitácora de accesos
VII. Informarán al Responsable se Seguridad, acerca de los recursos materiales indispensables para la protección de datos personales, dejando evidencia que haga constar que ha sido informado.
VIII. Informarán al Responsable de Seguridad, cualquier vulneración a los datos personales, dejando evidencia que haga constar que ha sido informado.
IX. Informarán al Responsable de Seguridad, de los posibles riesgos en el proceso de recolección, como en el tratamiento de datos personales, dejando evidencia que haga constar que ha sido informado.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

X. Cumplirá, previa instrucción de la persona Responsable, con las presentes políticas, las medidas de seguridad y políticas establecidas en el Documento de Seguridad y demás disposiciones que, para efecto de la protección de datos personales, disponga la persona Responsable.

7. Responsable de Seguridad

7.1 Las personas Responsables de Seguridad

I. Se encargará de actualizar el listado de personas usuarias, autorizadas para la recolección y tratamiento de datos personales.
II. Verificará que los formatos para la recolección de datos personales:
   a) Cuenten con el aviso de privacidad simplificado
   b) Precisen los datos personales a recolectar y que éstos estén ajustados a la finalidad del Sistema de Datos Personales.
III. Previa elaboración, aprobación y publicación en la Gaceta Oficial de la Ciudad de México del correspondiente acuerdo de, creación, modificación o supresión:
   a) Actualizará la información del Registro Electrónico de Sistemas de Datos Personales
   b) Conservará de forma impresa y digital los acuses de inscripción y modificación, así como las evidencias suficientes en caso de supresión de sistemas de datos personales.
IV. Para los acuerdos de creación, considerará los siguientes rubros susceptibles de publicarse en la Gaceta Oficial de la Ciudad de México:
   a) Denominación del sistema
   b) Finalidad o finalidades y sus usos previstos
   c) Normatividad aplicable
   d) Transferencias
   e) Personas físicas o grupos de personas sobre las que se recaben o traten datos personales.
   f) Estructura Básica del Sistema de Datos Personales y la Descripción de los Tipos de Datos

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

g) Instancias Responsables del Tratamiento del Sistema de Datos Personales: nombre del Sujeto Obligado, nombre de la Unidad Administrativa Responsable, usuarios, encargados
h) Áreas ante las que podrán ejercerse los derechos de acceso, rectificación, cancelación y oposición (ARCO) y procedimiento a través del cual se podrán ejercer los derechos ARCO
i) Nivel de seguridad y mecanismos de protección aplicables: nivel de Seguridad y medidas de Seguridad:

V. Para los acuerdos de modificación, considerará los siguientes rubros susceptibles de publicarse en la Gaceta Oficial de la Ciudad de México:
a) Denominación del Sistema
b) Finalidad o finalidades y usos previstos
c) Normatividad aplicable
d) Transferencias
e) Personas Físicas o Grupos de Personas sobre las que se Recaben o Traten Datos Personales
f) Estructura Básica del Sistema de Datos Personales y la Descripción de los Tipos de Datos
g) Instancias Responsables del Tratamiento del Sistema de Datos Personales: nombre del Sujeto Obligado, nombre de la Unidad Administrativa Responsable, usuarios, encargados
h) Áreas ante las que podrán ejercerse los derechos de acceso, rectificación, cancelación y oposición (ARCO) y procedimiento a través del cual se podrán ejercer los derechos ARCO
i) Nivel de seguridad y mecanismos de protección aplicables: nivel de Seguridad y medidas de Seguridad:

VI. Actualizará el documento de seguridad, con la guía elaborada por la Coordinación de la Oficina de Transparencia

VII. Integrará en el documento de seguridad, de manera enunciativa más ni los siguientes anexos:
a) Acuses de inscripción y modificación
b) Acuerdos de creación y modificación
c) Oficios de designación de responsable de seguridad y usuarios.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

d) Formatos para la recolección de datos personales actualizados y con su respectivo aviso de privacidad
e) Avisos de privacidad integral y simplificado
f) Bitácoras de acceso
g) Bitácoras de incidencias
h) Control de modificaciones del documento de seguridad
i) Oficios mediante los cuales se hacen las gestiones para reducir las brechas identificadas.

VIII. Actualizará los avisos de privacidad y con el visto bueno del Responsable del Sistema de Datos Personales, informará a la Coordinación de la Oficina de Transparencia, dichas modificaciones, a efecto de llevar a cabo su publicación en el micro sitio de transparencia de la Alcaldía Tlalpan.

IX. Verificará la implementación de las medidas de seguridad de forma permanente y previa instrucción del Responsable del Sistema de Datos Personales, realizará la gestión correspondiente ante la Coordinación de la Oficina de Transparencia, a efecto de llevar a cabo los ejercicios de monitoreo correspondientes

X. Verificará, que con respecto a la recolección de datos personales:
a) Únicamente se recolecten datos personales por los medios establecidos en el inventario de datos personales, elaborado por el Responsable del Sistema de Datos Personales.
b) Se recaben datos personales, exclusivamente para procesos institucionales.
c) Los datos personales recolectados, guarden congruencia con los tipos y categorías de datos personales publicados en acuerdos de creación y/o modificación.
d) Previo a la recolección de datos personales, se ponga a disposición de las personas titulares de los datos personales, el aviso de privacidad.

XI. Notificará las incidencias, previa aprobación de la Persona Responsable de Sistema de Datos Personales.

XII. Coordinará las acciones para la detección de necesidades de capacitación, alimentando el formato diseñado para tal efecto.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

XIII. Una vez aprobado el Programa anual de Capacitación en materia de Protección de Datos Personales de la Alcaldía Tlalpan, la persona responsable de seguridad, deberá estar atenta al cronograma de actividades de capacitación y mediante oficio solicitar la inscripción de las personas servidoras públicas que acudirán a las actividades capacitadoras.

XIV. Verificará que el oficio se notifique a la Coordinación de la Oficina de Transparencia, cinco días hábiles previos a la fecha programada para impartir la capacitación y que las personas a inscribir, cuenten con el perfil establecido en el formato de detección de necesidades de capacitación.

XV. Deberá cumplir las obligaciones establecidas en la presente política y demás disposiciones que, para efecto de la protección de Datos Personales, le instruya la persona Responsable.

8 Comité de Transparencia

8.1 El Comité de Transparencia

I. Establecerá y supervisará la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y en aquellas disposiciones que resulten aplicables en la materia;

II. Supervisará, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.

III. Aprobará las herramientas y/o mecanismos de monitoreo en materia de protección de datos personales, así como su metodología de implementación.

a) El mecanismo de monitoreo se conformará por un conjunto de indicadores cualitativos y cuantitativos.
b) Se implementará en los meses de enero-junio de cada ejercicio fiscal
c) Los resultados del monitoreo se presentarán en la Segunda Sesión Ordinaria del Comité de Transparencia.
d) Las mejoras implementadas por los Responsables de sistemas de datos personales, se informarán en la Primera Sesión Ordinaria del Comité de

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

Transparencia, del ejercicio siguiente a la implementación del mecanismo.

IV. Hará de conocimiento los avances en materia de capacitación, análisis de brecha y análisis de riesgo.

V. Analizará y en su caso aprobará las políticas y lineamientos que para efecto de la protección de datos personales le sean propuestas.

9 COMITÉ TÉCNICO INTERNO DE ADMINISTRACIÓN DE DOCUMENTOS

9.1 Valorará la baja documental de aquellos documentos que hayan prescrito en su vigencia administrativa, en conformidad con los plazos de conservación establecidos en el catálogo de disposición documental y que no posean los valores secundarios o históricos considerados para ser conservados de manera permanente, de acuerdo con la Ley y las disposiciones jurídicas aplicables.

9.2 Coordinará las acciones en conjunto con los Responsables de Sistemas de Datos Personales y con la Coordinación de Oficina de Transparencia, a efecto de verificar que la baja documental, concuerde no solo con la conclusión de los valores documentales y ciclo de vida sino también con la finalidad de los Sistemas de Datos Personales.

9.3 Instruirá y asesorará a las personas responsables de Sistemas de Datos Personales, a efecto de que, en los Acuerdos aprobados, se fundamente con la normatividad en materia archivística y en materia de protección de datos personales

9.4 Verificará en conjunto con las personas Responsables de Sistemas de Datos Personales, y con la Coordinación de Oficina de Transparencia, con la finalidad de que se garantice la protección de los datos personales en todo el proceso de baja documental.

9.5 Deberá garantizar lo siguiente:

a) En el caso del Sistema de Datos Personales físico (en papel), que el método de destrucción de los expedientes, de certeza de su inutilización.

b) Para los Datos Personales almacenados en medios ópticos, deberá dañar la superficie hasta que sea ilegible y posteriormente partir el disco. Aun

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

tratándose de medios ópticos regrabables, éstos no podrán ser utilizados nuevamente, ya que deben destruirse por completo.

9.6 En el caso de los Sistemas de Datos Personales electrónicos almacenados en equipos de cómputo o dispositivos móviles, deberán destruirse en presencia de las figuras establecidas en el numeral 9.5, así como del titular de la Dirección de Tecnologías de la Información. Asimismo, deberán eliminarse, cumpliendo las siguientes normas:

a) Verificar que en caso de tratarse de sistema operativo o software diferentes, no realicen respaldos automáticos o de seguridad de la información a eliminar, si estos existieran, también serán considerados para su eliminación, bajo el mismo procedimiento aquí descrito.

b) Eliminar la información con herramientas propias del sistema operativo, utilizando el eliminado seguro.

c) Utilizar herramientas de software para verificar la posibilidad de recuperación de la información eliminada.

d) Utilizar herramientas de software para sobrescribir la información eliminada varias veces con datos aleatorios.

GLOSARIO

a. **Áreas:** Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;

b. **Aviso de privacidad:** Documento a disposición del titular de los datos personales, generado por el responsable, de forma física, electrónica o en cualquier formato, previo a la recolección y tratamiento de sus datos, con el objeto de informarle sobre la finalidad del tratamiento, los datos recabados, así como la posibilidad de acceder, rectificar, oponerse o cancelar el tratamiento de los mismos;

c. **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

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

creación, tipo de soporte, procesamiento, almacenamiento y organización;

d. **Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación o supresión en la base de datos o sistema de datos personales que corresponda;
e. **Comité de Transparencia:** Instancia a la que hace referencia la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México;
f. **Consentimiento:** Manifestación de la voluntad libre, específica, informada e inequívoca del titular de los datos a través de la cual autoriza mediante declaración o acción afirmativa, que sus datos personales puedan ser tratados por el responsable;
g. **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información como puede ser nombre, número de identificación, datos de localización, identificador en línea o uno o varios elementos de la identidad física, fisiológica, genética, psíquica, patrimonial, económica, cultural o social de la persona;
h. **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, información biométrica, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

i. **Derechos ARCO:** Los derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de datos personales;
j. **Disociación:** El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;
k. **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;
l. **Encargado:** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable;
m. **Evaluación de impacto en la protección de datos personales:** Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos que comprometan el cumplimiento de los principios, deberes y derechos de las personas titulares de los datos personales, así como los deberes de los responsables y encargados, previstos en la normativa aplicable;
n. **Fuentes de acceso público:** Aquellas bases de datos, sistemas o archivos en poder de los sujetos obligados, que por disposición de ley puedan ser consultadas públicamente;
o. **Medidas compensatorias:** Mecanismos alternos para dar a conocer a las personas titulares de los datos personales el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance, cuando no se haya podido recabar el consentimiento previo al tratamiento de los datos personales de una persona física, sea por emergencias de salud pública, seguridad o desastres naturales;

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

p. **Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales y los sistemas de datos personales;
q. **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;
r. **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 consideran 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;

1.19 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 consideran 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;

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

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;

s. **Responsable:** Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos, que decida y determine finalidad, fines, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de datos personales;
t. **Sistema de Datos Personales**: Conjunto de organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de los sujetos obligados, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso;
u. **Supresión:** La eliminación, borrado o destrucción de los Sistemas de Datos Personales o de datos personales de una persona física bajo las medidas de seguridad previamente establecidas por el responsable, una vez que se ha cumplido la finalidad y el dato personal ha cumplido su ciclo de vida;
v. **Titular:** La persona física a quien corresponden los datos personales;
w. **Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;
x. **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas sobre datos personales o conjunto de datos personales, mediante procedimientos manuales o automatizados relacionadas con la obtención, uso, registro, organización, estructuración, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión o cualquier otra forma de habilitación de acceso, cotejo,

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

interconexión, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales;

y. **Coordinación de la Oficina de Transparencia:** Instancia a la que hace referencia la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México; como Unidad de Transparencia.
z. **Usuario:** Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales.

b) LINEAMIENTOS INTERNOS PARA EL BLOQUEO DE DATOS PERSONALES Y PARA LA SUPRESIÓN DE SISTEMAS DE DATOS PERSNALES.

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, es de orden público y de observancia general en la Ciudad de México, en materia de protección de datos personales en posesión de sujetos obligados. En este sentido, las disposiciones que prevé son de aplicación y observancia directa para los sujetos obligados de la Ciudad de México.

Por ello, la Alcaldía Tlalpan como Responsable y para efecto de cumplir con las obligaciones, deberes y principios de calidad, confidencialidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad, transparencia y temporalidad, para la protección de datos personales, en observancia a lo anterior, presenta en el documento de mérito, **Lineamientos internos para el bloqueo de datos persnales y la supresión de sistemas de datos personales de la Alcaldía Tlalpan. aprobadas por acuerdo número A01/CTSE03/AT/20-07-23; del Comité de Transparencia en la Tercera Sesión Extraordinaria, celebrada el 20 de julio de 2023.**

Los mecanismos de bloqueo de datos personales contenidos en estos Lineamientos, además de ser de observancia obligatoria para las personas servidoras públicas adscritas a la Alcaldía Tlalpan, tienen como referencia el deber de bloquear los datos personales, una vez que se determine la conclusión de la finalidad y el ciclo de vida

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

de los datos personales, entendiendo el bloqueo de acuerdo con en el artículo 2, fracción IV de la Ley de Datos Local, como:

> "…La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación o supresión en la base de datos o sistema de datos personales que corresponda;"(Sic)

En este sentido, *El responsable estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.* el bloqueo de datos personales consiste en la **identificación y reserva de los mismos, adoptando las medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización.**

En tal virtud, para cumplir con un ciclo virtuoso en la protección de datos personales, estos Lineamientos, establecen de forma enunciativa, más no limitativa, los deberes y obligaciones que han de cumplir: las personas servidoras públicas Responsables de Sistemas de Datos Personales, responsables de seguridad, usuarias, el Comité de Transparencia, el Comité Técnico Interno de Administración de Documentos y de forma específica, la Dirección de Tecnologías de la información, esta última en la materia específica relacionada con la supresión de Sistemas de Datos Personales automatizados.

OBJETIVO Y ÁMBITO DE APLICACIÓN

Los presentes Lineamientos Internos para el Bloqueo de Datos Personales y para la supresión de Sistemas de Datos Personales, están diseñados para el cumplimiento de lo previsto en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y sus Lineamientos Generales, tienen por **objetivo:** establecer las directrices de operación, seguridad y control para el bloqueo y supresión de sistemas de datos personales y son de observancia para las unidades administrativas que en ejercicio de sus funciones y atribuciones tutelan sistemas de datos personales.

Ámbito de aplicación

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

Los presentes Lineamientos Internos para la Protección de Datos Personales de la Alcaldía Tlalpan, son de aplicación general y obligatoria para los responsables de Sistemas de Datos Personales, Responsables de Seguridad y Usuarios que recolecten y den tratamiento a datos personales.

1. LINEAMIENTOS INTERNOS PARA EL BLOQUEO DE DATOS PERSONALES Y LA SUPRESIÓN DE SISTEMAS DE DATOS PERSONALES DE LA ALCALDIA TLALPAN

I. PRINCIPIOS PARA LA PROTECCIÓN DE DATOS PERSONALES

Artículo 1. El responsable del tratamiento de Datos Personales deberá observar los principios de:

I. **Calidad:** Los datos personales deben ser ciertos, adecuados, pertinentes y proporcionales, no excesivos, en relación con el ámbito y la finalidad para la que fueron recabados.
II. **Confidencialidad:** El Responsable garantizará que exclusivamente el titular pueda acceder a sus datos, o en su caso, el mismo Responsable y el usuario a fin de cumplir con las finalidades del tratamiento. En cualquier caso, se deberá garantizar la secrecía y la no difusión de los mismos. Sólo el titular podrá autorizar la difusión de sus datos personales.
III. **Consentimiento**: Toda manifestación previa, de voluntad libre, específica, informada e inequívoca por la que el titular acepta, mediante declaración o acción afirmativa, el tratamiento de sus datos personales.
IV. **Finalidad**: Los datos personales recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados. Los datos personales con fines de archivo de interés público, investigación científica e histórica, o estadísticos no se considerarán incompatibles con la finalidad inicial.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

La Finalidad incluirá el ciclo de vida del dato personal, de tal manera, que concluida ésta, los datos puedan ser suprimidos, cancelados o destruidos.

V. **Información:** El Responsable deberá informar al titular de los datos sobre las características principales del tratamiento, la finalidad y cualquier cambio del estado relacionados con sus datos personales.

VI. **Lealtad:** El tratamiento de datos personales se realizará sin que medie dolo, engaño o medios fraudulentos, tengan un origen lícito, y no vulneren la confianza del titular.

VII. **Licitud.** El tratamiento de datos personales será lícito cuando el titular los entregue, previo consentimiento, o sea en cumplimiento de una atribución u obligación legal aplicable al sujeto obligado; en este caso, los datos personales recabados u obtenidos se tratarán por los medios previstos en el presente ordenamiento, y no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

VIII. **Proporcionalidad:** El Responsable tratara sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con la finalidad o finalidades, para lo cual se obtuvieron.

IX. **Transparencia:** La información relacionada con el tratamiento de datos será accesible y fácil de entender, y siempre a disposición del titular.

X. **Temporalidad:** Los datos personales tendrán un ciclo de vida o una temporalidad vinculada a la finalidad para la cual fueron recabados y tratados. Una vez concluida su finalidad o hayan dejado de ser necesarios, pertinentes o lícitos, pueden ser destruidos, cancelados o suprimidos.

II. LINEAMIENTOS GENERALES DE OPERACIÓN

Artículo 2. Las personas servidoras públicas adscritas a la Alcaldía Tlalpan, deberán conocer la normatividad para el tratamiento de datos personales.

Artículo 3. Todas las actividades que consideren tratamiento de datos personales, deberán ser materializadas en la publicación de creación de sistemas de datos personales, su inscripción en el Registro Electrónico de Sistemas de Datos Personales (RESDP), Documento de Seguridad y de ser el caso, sus respectivos acuerdos de

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

modificación, así como las posteriores actualizaciones en el RESDP y su respectivo documento de seguridad.

Artículo 4. Los datos personales recolectados, podrán ser tratados únicamente para cumplir con la finalidad con la cual se haya publicado la creación, o en su caso la modificación del sistema de datos personales. Por lo que deberán ser consideradas en el inventario de datos personales de la unidad administrativa responsable del o los sistemas de datos personales.

Artículo 5. Los datos personales, se conservarán de conformidad con lo establecido en la finalidad y en el ciclo de vida, tomando en cuenta los aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo

Artículo 6. Cuando la finalidad de un Sistema de Datos Personales y el ciclo de vida de los datos personales que obre en los archivos de la Alcaldía Tlalpan, hayan dejado de ser necesarios para el cumplimiento de la finalidad o finalidades para la que fueron recolectados, deberá ser suprimido

La supresión de Sistemas de Datos Personales, se llevará a cabo previa publicación de Acuerdo de Supresión en la Gaceta Oficial de la Ciudad de México, una vez realizada la publicación, los Responsables contarán internamente con 5 días hábiles para coordinar las acciones necesarias para la correcta supresión en el Registro Electrónico de Sistemas de Datos Personales (RESDP), y cuatro días más para efecto de llevar a cabo la supresión en el RESDP

III. LINEAMIENTOS PARA EL BLOQUEO DE DATOS PERSONALES

Artículo 7.- El bloqueo tiene por objeto impedir el tratamiento del Sistema de Datos Personales y su acceso por cualquier persona, con excepción de que alguna disposición legal prevea lo contrario, así como evitar su pérdida, destrucción o extravío. Previo al bloqueo de datos personales las áreas deberán:

I. Identificar los plazos de conservación de los datos personales, o bien de los documentos y o expedientes que obren en los mismos
II. Asegurarse de que los plazos de conservación atiendan y consideren:
   a) Las disposiciones aplicables en materia de archivos y,
   b) Los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

c) Observar los plazos de prescripción previstos en la normativa en materia de archivos, o en su caso, en las cláusulas contractuales, para efectos de las posibles responsabilidades.

III. El bloqueo de los datos personales, se realizará tomando en cuenta los plazos de conservación previstos en el Catalogo de Disposición Documental, así como en el Cuadro General de Clasificación Archivística de la Alcaldía Tlalpan, así como el momento en que se inició el tratamiento de los datos personales y el último de los mismos.

IV. Durante el bloqueo, los datos personales no serán objeto de tratamiento, salvo disposición expresa de una Ley o que exista una resolución judicial, orden o mandato fundado y motivado, de autoridad competente.

V. El bloqueo de datos personales deberá realizarse tomando en cuenta los medios de almacenamientos físicos y/o electrónicos en que se encuentra la información.

VI. En el bloqueo de datos personales en medios digitales, las áreas deberán considerar:

a) Trasladar temporalmente los datos personales seleccionados a otra base de datos.

b) Utilizar técnicas de enmascaramiento de datos del registro (s) o de la base de datos seleccionado (s) o de la base de datos.

c) Cifrar la información del registro (s) seleccionado (s) de la base de datos.

d) Impedir el acceso de las personas servidoras públicas que dan tratamiento a las bases de datos que contienen datos personales.

e) Si los datos personales están publicados en internet, retirarlos temporalmente.

f) Indicar claramente, en los sistemas informáticos y sus bases de datos que los datos que se pretenden tratar se encuentran limitados en su tratamiento

g) Establecer herramientas, procedimientos y protocolos que garanticen la autenticación, autorización y registro del acceso a las bases de datos que contengan datos bloqueados.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

Artículo 8. El responsable del sistema de datos personales, elaborará los inventarios de datos personales, en conjunto con el responsable de seguridad y con los usuarios, mismo que contendrá de forma enunciativa, más no limitativa:

I. El nombre del Sistema de Datos Personales a cancelar.
II. La justificación de que no existe la obligación legal de mantener por más tiempo el Sistema de Datos Personales,
III. La justificación de que el Sistema de Datos Personales ha dejado de ser útil de conformidad con el Aviso de Privacidad aplicable.
IV. La instrucción al Responsable del Sistema de Datos Personales de recuperar, cuando sea posible, las copias o reproducciones de ese Sistema de Datos Personales, entregados a otras Unidades Administrativas de la Alcaldía Tlalpan, con el fin de evitar su tratamiento o notificar el bloqueo.
V. Señalar las medidas de seguridad a emplear, con el objetivo de impedir el tratamiento del Sistema de Datos Personales durante el periodo de bloqueo.

Artículo 9. El plazo de tres meses de bloqueo de los datos personales comienza a computarse a partir del día hábil siguiente de la notificación de la publicación del acuerdo de supresión en la Gaceta Oficial de la Ciudad de México, ya que, a partir de ese día, deberá impedirse cualquier tratamiento del Sistema de Datos Personales a suprimir. Las notificaciones derivadas de este procedimiento, deberán realizarse por oficio.

Artículo 10. El Responsable se cerciorará que los tres meses del periodo de bloqueo, todas las copias y/o reproducciones que se tengan del Sistema de Datos Personales se protejan con mismas medidas de seguridad que el original, para evitar su tratamiento, alteración, destrucción o acceso no autorizado.

IV. LINEAMIENTOS PARA LA SUPRESIÓN DE SISTEMAS DE DATOS PERSONALES

Artículo 11. El Sistema de Datos Personales físico, deberá destruirse en presencia de las personas: Responsable del Sistema de Datos Personales, del Responsable de Seguridad, titular de la Unidad Departamental de Acceso a Ia Información y Datos Personales, titular de la Coordinación de Transparencia y titular del área responsable

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

de archivos se deberá emitir un Acta de Baja documental en donde se incluyan los siguientes datos:

I. Fecha de notificación a la persona titular de la Alcaldía Tlalpan
II. El número de reproducciones que se tengan del Sistema de Datos Personales
III. Especificación del tipo de bases de datos (físicas o electrónicas)
IV. Declaración de decir verdad que durante tres meses el Sistema de Datos Personales no fue tratado y se evitó su alteración, destrucción o acceso no autorizado.
V. Acuerdo de supresión del o los sistemas de datos personales

Artículo 12. Los Sistemas de Datos Personales físicos, se destruirán en trituradora, de tal forma que se garantice su inutilización.

Artículo 13. Los Sistemas de Datos Personales en medios ópticos, primero se deberá dañar la superficie hasta que sea ilegible y posteriormente partir el disco.

Artículo 14. Para la supresión de los Sistemas de Datos Personales electrónicos almacenados en equipos de cómputo o dispositivos móviles:

I. Deberá destruirse en presencia de las personas: Responsable del Sistema de Datos Personales, del Responsable de Seguridad, titular de la Unidad Departamental de Acceso a la Información y Datos Personales, titular de la Coordinación de Transparencia, titular del área responsable de archivos y del titular de la Dirección de Tecnologías
II. Se verificará que en caso de tratarse de sistema operativo o software diferentes, no realicen respaldos automáticos o de seguridad de la información a eliminar, si estos existieran, también serán considerados para su eliminación, bajo el mismo procedimiento.
III. Se eliminará la información con herramientas propias del sistema operativo, utilizando el eliminado seguro
IV. Se utilizarán herramientas de software para verificar la posibilidad de recuperación de la información eliminada.
V. Se utilizarán herramientas de software para sobrescribir la información eliminada varias veces con datos aleatorios.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

VI. Se verificará nuevamente si es posible recuperar la información eliminada, si es así, aplicar nuevamente el paso 5.
VII. El procedimiento puede variar de acuerdo al equipo y el sistema operativo.

ENCARGADO DEBERÁ:

1. **[INDICAR LOS DEBERES QUE CUMPLIRÁRÁ LA PERSONA ENCARGADA, PARA CUMPLIR LAS MEDIDAS DE SEGURIDAD]**

Responsable del Sistema de Datos Personales	
Responsable de seguridad	
Usuarios	

IV. MEDIDAS DE SEGURIDAD

Para garantizar los niveles de seguridad exigidos, las y los usuarios de tratamiento de datos personales, implementarán los siguientes controles:

a) Medidas de seguridad

El Sistema de Datos Personales denominado **[DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES],** implementará las siguientes medidas de seguridad:

Medidas de seguridad técnicas son las aplicables a sistemas de datos personales en soportes electrónicos, servicios e infraestructura de acciones y tecnologías de la información, entre otras, se prevén las siguientes acciones:

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

- **[INIDICAR LAS MEDIDAS TÉCNICAS GENERALES]**
- **[INDICAR LAS MÉDIDAS TÉCNICAS A SEGUIR DURANTE EL TRASLADO SOBRE REDES ELECTRÓNICAS SE CUMPLIRÁN LAS SIGUIENTES MEDIDAS DE SEGURIDAD]**
- **Resguardo de sistemas de datos personales con soportes físicos** se **cumplirán las siguientes medidas de seguridad [INDICAR LAS MEDIDAS DE SEGURIDAD]**

Medidas de seguridad administrativas: son aquellas que deben implementarse para la consecución de los objetivos contemplados en los siguientes apartados: **Medidas de seguridad administrativas**: son aquellas que deben implementarse para la consecución de los objetivos contemplados en los siguientes apartados: **[INDICAR LAS MEDIDAS DE SEGURIDAD ADMINISTRATIVA]**

PROCEDIMIENTO DE CUSTODIA [INDICAR LAS MEDIDAS DE SEGURIDAD A SEGUIR]

- **La <u>salida</u> de documentos o información que contenga datos personales, sólo será autorizada por la persona Responsable del Sistema de Datos Personales**
  INDICAR:

<u>PROCEDIMIENTO DE AUTORIZACIÓN</u>

a) EN EL **TRASLADO [INDICAR LAS MEDIDAS DE SEGUIRIDAD]**
b) **Procedimiento para el traslado físico**: **[INDICAR LAS MEDIDAS DE SEGUIRIDAD]**
c) **Traslado físico de soportes electrónicos se cumplirán las siguientes medidas de seguridad: [INDICAR LAS MEDIDAS DE SEGUIRIDAD]**

➢ Las **entradas y salidas** de soportes correspondientes al Sistema de Datos Personales denominado **[DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES] deberán** ser registradas de acuerdo al siguiente procedimiento:

Procedimiento para el registro de entradas y salidas de soportes

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

El registro de entradas y salidas deberá contener por lo menos la siguiente información:

a) **Registro de entradas:** tipo de soporte, fecha y hora, emisor, número de soportes, tipo de información que contienen, forma de envío y la persona responsable de la recepción
b) **Registro de salidas:** tipo de soporte, fecha y hora, destinatario, número de soportes, tipo de información que contienen, forma de envío y la persona responsable de la entrega. **En el caso de gestiones automatizadas, indicar el sistema informático utilizado.**
c) En caso de proceder alguna acción cuyo objeto sea la disposición documental autorizada, en cualquier medio, por destrucción o baja de la misma, cualquier soporte que contenga datos de carácter personal deberá destruirse o borrarse, adoptando las medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
d) Para el tratamiento de datos personales en entornos desprotegidos, se implementarán medidas de seguridad alternativas

Borrado seguro de datos

a) Borrado seguro de los archivos delicados en equipos
b) Borrado seguro de los directorios delicados en equipos
c) Formateo de los discos duros

- **PARA LA IMPLEMENTACIÓN DE UN BORRADO SEGURO EN CUALQUIER EQUIPO DE CÓMPUTO, DISPOSITIVO O MEDIO DE ALMACENAMIENTO SE DEBE CUMPLIR UNO DE SOLO SIGUIENTES SUPUESTOS: •**
  a) Baja de equipo por obsolescencia
  b) Baja de equipo por descompostura
  c) Reasignación de equipo interna de la Coordinación
  d) Reasignación a una dependencia diferente de la Coordinación
  e) Solicitante exigiendo la cancelación de sus datos personales
  f) Diseño de lineamientos para garantizar el proceso de borrado tanto en el sistema físico como automatizado
  g) Adquisición de trituradoras para la destrucción de los documentos
  h) Implementación de herramientas digitales para o la destrucción de medios de almacenamiento electrónicos, o la desmagnetización y sobre escritura de los equipos de cómputo: [**INDICAR LAS MEDIDAS DE SEGURIDAD A SEGUIR]**

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

- **Procedimiento de custodia**

❖ **La salida de documentos o información que contenga datos personales, sólo será autorizada por la persona Responsable del Sistema de Datos Personales**

Procedimiento de autorización [INDICAR LAS MEDIDAS DE SEGURIDAD]

PROCEDIMIENTO PARA EL TRASLADO FÍSICO: **[INDICAR LAS MEDIDAS DE SEGURIDAD]**

Traslado físico de soportes electrónicos se cumplirán las siguientes medidas de seguridad: [INDICAR LAS MEDIDAS DE SEGURIDAD]

a) Deberá precisar si los archivos electrónicos que contienen datos personales son cifrados antes de su envío y proporcionar detalles técnicos del cifrado tales como el tipo de algoritmo utilizado y la longitud de la llave (o clave).

➢ Las **entradas y salidas** de soportes correspondientes al Sistema de Datos Personales denominado **[DENOMINACIÓN DE LA UNIDAD ADMINISTRATIVA]** deberán ser registradas de acuerdo al siguiente procedimiento:

Procedimiento para el registro de entradas y salidas de soportes
El registro de entradas y salidas deberá contener por lo menos la siguiente información:

e) **Registro de entradas:** tipo de soporte, fecha y hora, emisor, número de soportes, tipo de información que contienen, forma de envío y la persona responsable de la recepción
f) **Registro de salidas:** tipo de soporte, fecha y hora, destinatario, número de soportes, tipo de información que contienen, forma de envío y la persona responsable de la entrega. **En el caso de gestiones automatizadas, indicar el sistema informático utilizado.**
g) En caso de proceder alguna acción cuyo objeto sea la disposición documental autorizada, en cualquier medio, por destrucción o baja de la misma, cualquier soporte que contenga datos de carácter personal deberá destruirse o borrarse,

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

adoptando las medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

h) Para el tratamiento de datos personales en entornos desprotegidos, se implementarán medidas de seguridad alternativas**:**

Medidas de seguridad físicas: atañen a las acciones que deben implementarse para contar con:

a) [INDICAR LAS MEDIDAS DE SEGURIDAD A SEGUIR]

V. REGISTO DE INCIDENCIAS

Es el registro de vulneraciones a la seguridad del sistema, consistente en la pérdida o destrucción no autorizada, robo, extravío o copia no autorizada, uso, acceso, o tratamiento no autorizado, daño, alteración o modificación de la información.

La persona servidora pública responsable del Sistema de Datos Personales denominado [DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES], deberá analizar las causas por la cuales se presentó la incidencia, con acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales, con el fin de que la vulneración no se repita, e informar al titular de los datos y al órgano garante para tomar las medidas de mitigación correspondientes.

Para dar cumplimiento a este apartado del Documento de Seguridad, en caso de incidencias o vulneraciones, el Responsable llevará a cabo el registro de incidencias o vulneraciones en la siguiente una **bitácora de incidencias y/o vulneraciones (ANEXO VII)**:

BITÁCORA DE INCIDENCIAS Y/O VULNERACIONES DEL SISTEMA DE DATOS PERSONALES DENOMINADO USUARIOS DE LA OFICINA DE INFORMACIÓN PÚBLICA						
Nombre y cargo de quien reporta el incidente	Número de incidencias	Descripción de la incidencia	Fecha en que ocurrió	Motivo de la incidencia	Acciones implementadas de forma inmediata	Nombre y cargo de quien recibe la notificación

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

Soportes físicos oficios, expedientes, archiveros, ficheros, computadoras, discos duros robados o dañados						
Soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados.						
¿Quién autorizó la recuperación de datos personales?						
Elaborado por					Fecha de elaboración:	
Aprobado por:					Fecha de aprobación:	

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

En caso de vulneración, el Responsable del Sistema de Datos Personales denominado Usuarios de la Oficina de Información Pública:

1. **Deberá informar sin dilación alguna al titular y al INFOCDMX**

En cuanto confirme la vulneración deberá informar al titular de los datos personales al menos:

1. La naturaleza del incidente
2. Los datos personales comprometidos,
3. Los derechos que puede adoptar del titular de los datos personales para proteger sus datos personales,
4. Las acciones correctivas que realizó en forma inmediata,
5. Los medios donde puede obtener más información.

Por lo que hace al deber de informar al INFOCDMX, considerará al menos:

1. Las medidas de mitigación llevadas a cabo,
2. Los niveles de seguridad que tiene adoptados,
3. El documento de gestión en donde el Instituto realizará las recomendaciones y medidas pertinentes para la protección de datos personales

VI. IDENTIFICACIÓN Y AUTENTICACIÓN

Las y los usuarios autorizados para dar tratamiento a datos personales, implementarán las medidas y normas relativas a la identificación y autenticación[1] para

[1] Identificar consiste en tomar conocimiento de que una persona es quien dice ser. Lo anterior se logra, por ejemplo, con una identificación que tenga validez oficial y en un ambiente electrónico con el nombre de usuario que se introduce al momento de ingresar al sistema (login). b) Autentificar (o autenticar) a una persona se refiere a comprobar que esa persona es quien dice ser. Ello se logra cuando se cotejan uno o más datos en dicha identificación oficial contra (i) los datos en alguna otra identificación, documento, certificado digital (como el de la firma electrónica) o dispositivo que tenga la persona, (ii) los datos que sepa o tenga memorizados (su firma autógrafa o su contraseña, por ejemplo) o (iii) una o más características que coincidan con lo que es dicha persona (fotografía o huella dactilar, por ejemplo). c) Autorizar se refiere al acceso que se le permite a la persona que se ha identificado y autenticado apropiadamente. Esto depende del o de los permisos que le conceda el responsable de autorizar los accesos.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

acceder a los datos personales**: [INDICAR LOS MECANISMOS DE AUTENTICACIÓN E IDENTIFICACIÓN]**

VII. CONTROL DE ACCESO, GESTIÓN DE SOPORTES, Y COPIAS DE RESPALDO Y RECUPERACIÓN

b) Control de acceso

Las y los usuarios autorizados para dar tratamiento a datos personales, solo accederán a aquellos datos y recursos que se precisen para el desarrollo de sus funciones, para tales efectos se llevará la "**Bitácora de registro de acceso y actividades de tratamiento de datos personales" (Anexo VIII),** tanto físicos como electrónicos, cuyo objetivo es tener perfectamente detectadas las actividades de tratamiento de datos personales, quién la lleva a cabo, el objetivo del tratamiento correspondiente a cada actividad, las categorías de datos personales a las que se da tratamiento cotidiano y las medidas seguridad implementadas.

La persona servidora pública Responsable del Sistema de Datos Personales denominado **[DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES],** llevará a cabo el siguiente procedimiento para solicitar altas, modificaciones, bajas e inactivación de cuentas: **[INDICAR EL PROCEDIMIENTO]**

Procedimiento para la cancelación y actualización de contraseñas [INDICAR EL PROCEDIMIENTO]

Exclusivamente el personal que se indica a continuación, podrá tener acceso a los datos personales contenidos en el Sistema de Datos Personales denominado **[DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES].**

Nombre de la persona servidora pública que da tratamiento a datos personales	Cargo	Tratamientos específicos
	Responsable del Sistema	

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

	Responsable del Sistema de Datos Personales	
	Usuaria	
	Usuario	

c) Gestión de soportes

Los soportes que contengan datos de carácter personal deben ser etiquetados para permitir su identificación, inventariados y almacenados en de forma física en los expedientes con número de serie [**INDICAR EL NÚMERO DE SERIE DOCUMENTAL]**. La **organización** de los soportes o documentos garantizará la correcta conservación de los documentos, la localización y consulta de la información y posibilitará el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), para tales fines se realizará en los siguientes dispositivos **[INDICAR LOS DISPOSITIVOS Y SU NÚMERO DE INVENTARIO]** con carga de inventario a las personas servidoras públicas:[**INDICAR EL NOMBRE DE LAS PERSONAS SERVIDORAS PÚBLICAS QUE DAN USO A LOS DISPOSITIVOS EN LOS CUALES SE DA TATAMIENTO A DATOS PERSONALES]**

Procedimiento establecido para habilitar o retirar el permiso de acceso y los controles de acceso existentes.

1. **La custodia de los documentos y/o dispositivos que contengan datos personales que aún no se archiven por encontrarse en trámite, deberán protegerse por las y los usuarios con la finalidad de impedir el acceso a personas no autorizadas.**

Procedimiento de custodia

1. **[INDICAR LOS PROCEDIMIENTOS]**

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

2. **La <u>salida</u> de documentos o información que contenga datos personales, sólo será autorizada por la persona Responsable del Sistema de Datos Personales**

<u>Procedimiento de autorización</u> [INDICAR LOS PROCEDIMIENTOS]

Procedimiento de protección para los casos en que sea necesario el traslado de datos personales [INDICAR LOS PROCEDIMIENTOS]

Procedimiento para el traslado físico: **[INDICAR LOS PROCEDIMIENTOS]**

Traslado físico de soportes electrónicos: **[INDICAR LOS PROCEDIMIENTOS]**
Traslado sobre redes electrónicas: [**INDICAR LOS PROCEDIMIENTOS]**

Resguardo de sistemas de datos personales con soportes físicos:

a) **SEÑALAR LAS MEDIDAS DE SEGURIDAD QUE HA IMPLEMENTADO EL SUJETO OBLIGADO PARA EL RESGUARDO DE LOS SOPORTES FÍSICOS DEL SISTEMA DE MANERA QUE EVITE LA ALTERACIÓN, PÉRDIDA O ACCESO NO AUTORIZADO A LOS MISMOS.**
b) **SEÑALAR EN UN LISTADO LAS PERSONAS QUE TIENEN ACCESO A LOS SOPORTES FÍSICOS DEL SISTEMA**.

Las **entradas y salidas** de soportes correspondientes al Sistema de Datos Personales denominado **[DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES]** deberán ser registradas de acuerdo al siguiente procedimiento:

Procedimiento para el registro de entradas y salidas de soportes

El registro de entradas y salidas deberá contener por lo menos la siguiente información:

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

Registro de entradas: tipo de soporte, fecha y hora, emisor, número de soportes, tipo de información que contienen, forma de envío y la persona responsable de la recepción

Registro de salidas: tipo de soporte, fecha y hora, destinatario, número de soportes, tipo de información que contienen, forma de envío y la persona responsable de la entrega. **En el caso de gestiones automatizadas, indicar el sistema informático utilizado.**

En caso de proceder alguna acción cuyo objeto sea la disposición documental autorizada, en cualquier medio, por destrucción o baja de la misma, cualquier soporte que contenga datos de carácter personal deberá destruirse o borrarse, adoptando las medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

Para el tratamiento de datos personales en entornos desprotegidos, se implementarán medidas de seguridad alternativas**:**

Entorno desprotegido	Medidas alternativas a tomar

d) Copias de respaldo y recuperación

Es obligatorio realizar copias de respaldo del Sistema de Datos Personales denominado **[DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES]**, los procedimientos establecidos para copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Procedimiento de respaldo [INDICAR LOS PROCEDIMIENTOS DE RESPALDO]

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

Almacenar copias de respaldo [INDICAR LOS PROCEDIMIENTOS PARA LAS COPIAS DE RESPALDO]

Las recuperaciones de datos personales del Sistema de Datos Personales denominado **[DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES]**, deberán ser autorizados por la persona servidora pública responsable. Asimismo, se conservará una copia de respaldo y de los procedimientos de recuperación de los datos personales.

Este procedimiento contempla la recuperación de información que contenga datos de carácter personal desde copias de respaldo ante una incidencia cuya resolución requiere dicha recuperación.

Comunicar la necesidad de recuperación de datos

1. Ante una necesidad de recuperación de datos, el usuario comunicará la necesidad de recuperación de datos al Responsable de Seguridad.

2. La recuperación de datos se reportará como incidencia según lo establecido en el procedimiento de notificación y gestión de incidencias.

Analizar necesidad de recuperación de datos [SEÑALAR LOS PASOS A SEGUIR]

Autorizar recuperación de datos [SEÑALAR LOS PASOS A SEGUIR]

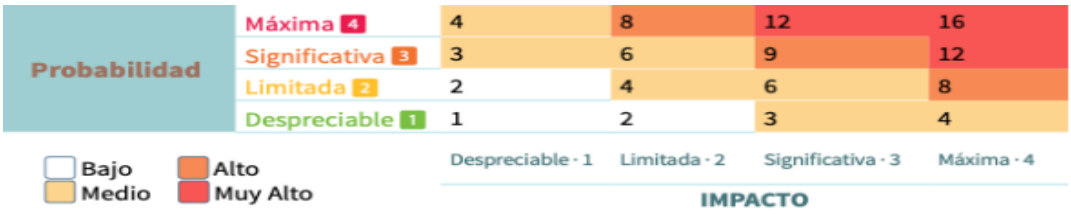
Recuperar datos [SEÑALAR LOS PASOS A SEGUIR]

Cerrar incidencia de recuperación de datos [SEÑALAR LOS PASOS A SEGUIR]

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

VIII. ANÁLISIS DE RIESGO.

Son los proyectos e iniciativas de mejoras de la seguridad de información, en la que se debe de considerar las amenazas, vulneraciones y los recursos involucrados en su tratamiento, partiendo del cálculo de la probabilidad de que ocurran las posibles amenazas.



1. Riesgo bajo: valores entre 1 y 2
2. Riesgo medio: valores entre 3 y 6
3. Riesgo alto: valores entre 7 y 9
4. Riesgo muy alto: valores entre 10 y 16

Ejemplo de valoración del riesgo inherente:

Tipo de amenaza	Amenaza	Riesgo	Probabilidad	Impacto	Riesgo inherente
Acceso ilegítimo a los datos	Fuga de información	Terceras personas acceden a los datos vulnerado su confidencialidad	Significativa Valoración: 3	Significativo Valoración: 3	Alto Valoración: 9
	Operaciones de tratamiento no autorizadas	Uso ilegítimo de los datos que vulneran los derechos de los interesados	Máxima Valoración: 4	Limitado Valoración: 2	Alto Valoración: 8
Modificación no autorizada de los datos	Ataque de software malicioso (Ciberataque)	Se modifican los datos perdiendo su integridad	Significativa Valoración: 3	Limitado Valoración: 2	Medio Valoración: 6
	Operaciones de tratamiento que modifican los datos de forma ilegítima	Uso ilegítimo de los datos que vulneran los derechos de los interesados	Máxima Valoración: 4	Significativo Valoración: 3	Muy Alto Valoración: 12
Indisponibilidad de los datos	Corte del suministro eléctrico que impide el acceso a los datos	Imposibilidad de acceso a los datos porque no están disponibles	Limitada Valoración: 2	Limitado Valoración: 2	Medio Valoración: 4
	Ciberataque que impide acceder a los datos	Imposibilidad de acceso a los datos porque no están disponibles	Significativa Valoración: 3	Significativo Valoración: 3	Alto Valoración: 9

Tipo de amenaza	Amenaza	Riesgo	Probabilidad	Impacto	Riesgo inherente
Indisponibilidad de los datos personales	Ciberataque a la PNT	Imposibilidad de acceso a los datos personales por hackeo a la PNT	Significativo Valoración: 3	Significativo Valoración: 3	Alto Valoración 4

ANÁLISIS DE BRECHA

a) Análisis de brecha en materia de gestión de insumos para la protección de datos personales

La persona servidora pública responsable del Sistema de Datos Personales denominado [**DENOMINACIÓN DEL SISTEMA DE DATOS PERSONALES],** deberá realizar un análisis de brecha con el objetivo de detectar las medidas de seguridad existentes, las medidas de seguridad faltantes, las acciones a emprender para

solventar las medidas faltantes y el plazo de tiempo para la atención. El análisis de brecha permite:

a) Evaluar la situación actual en materia de tratamiento de datos personales
b) Identificar los riesgos asociados a los procesos realizados por las personas responsables de sistemas de gestión de datos personales y de tratamiento.
c) Determinar las necesidades, para subsanar sus deficiencias y adaptarse a los deberes que marca la Ley
d) Crear una base sólida para iniciar la planificación eficiente de las medidas de seguridad.

ANALISIS DE BRECHA EN MATERIA DE GESTIÓN DE INSUMOS PARA LA PROTECCIÓN DE DATOS PERSONALES

OBJETIVO	MEDIDAS DE SEGURIDAD EXISTENTES	MEDIDAS DE SEGURIDAD FALTANTES	ACCIONES PARA ATENDER LAS MEDIDAS FALTANTES	PLAZO DE TIEMPO PARA LA ATENCIÓN

b) Análisis de brechas de datos personales, frente a diversos sucesos y su notificación

El análisis de brechas de datos personales, frente a sucesos diversos, se basará en detectar la afectación a los principios de confidencialidad, disponibilidad e integridad, dependiente del suceso que haya acontecido. En este sentido se entenderá lo siguiente:

Brecha en la Confidencialidad: Una brecha afecta a la confidencialidad cuando los datos personales de un tratamiento han podido ser accedidos por terceros sin permiso, incluyendo cuando los datos son filtrados.

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

Brecha en la Disponibilidad: Una brecha afecta a la disponibilidad de los datos personales cuando han estado inaccesibles de forma temporal o permanente para quien legítimamente debe poder tratarlos o acceder a ellos.
Brecha en la Integridad: Una brecha afecta a la integridad cuando se han alterado los datos personales de forma ilegítima y el tratamiento de esos datos personales puede causar un daño a los afectados.

A continuación, se muestra el cuadro para la identificación de brechas de datos personales, frente a diversos sucesos.

Identificación de brechas de datos personales, frente a diversos sucesos.

Suceso	Disponibilidad	Integridad	Confidencialidad
Documentación perdida, robada o conservada en lugares inseguros	x		
Datos personales enviados por error de forma electrónica		x	
Datos personales enviados por error de forma impresa			
Datos personales en dispositivos obsoletos			x
Publicación no intencional/autorizada			
Dispositivos perdidos o robados			
Hackeo de dispositivos que contienen datos personales			
Suplantación de identidad (phising)			
Incidencias técnicas			
Datos personales mostrados a titulares incorrectos			

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

Para la notificación de brechas de datos personales, el Responsable del Sistema de Datos Personales, identificará las categorías y tipos de datos personales afectadas, tomando en cuenta lo siguiente:

1. Las categorías y tipos de datos personales recolectados y publicados en Acuerdo de creación o modificación (vigentes),
2. Las categorías y tipos de datos personales recolectados, inscritos en el RESDP
3. Las categorías y tipos de datos recolectados, publicados e inscritos deberán coincidir con los requisitos y los rubros que conforman los formatos para recabar datos personales.

Categoría	Tipos de datos personales

4. Los perfiles de personas físicas afectadas, mismos que deberán coincidir con lo establecido en la finalidad del sistema de datos personales, así como con el rubro: personas físicas o grupos de personas sobre las que se recaben o traten datos personales, que obra en el acuerdo de creación o modificación (vigente)
5. Al menos de forma aproximada, el número de personas cuyos datos personales se han visto afectados por la brecha de datos personales. Es necesario indicar un número mayor que 0. En este sentido, el número de personas afectadas se refiere al número de personas físicas cuyos derechos o libertades podrían verse dañados como consecuencia de una brecha de datos personales, por ejemplo, por el tratamiento ilícito o no autorizado que se pueda producir de sus datos personales, la imposibilidad de acceder a un servicio o en definitiva la pérdida de control sobre sus datos personales.
6. Determinar las consecuencias, a efecto de poder dar paso al análisis de riesgo en el tratamiento de datos personales sobre los que se ha producido una brecha. De forma enunciativa, más no limitativa, se consideran las siguientes posibles consecuencias

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

a) Imposibilidad de ejercer algún derecho o acceso a un servicio
b) Usurpación de identidad
c) Pérdidas financieras
d) Daños a la imagen
e) Pérdida de confidencialidad de datos personales afectados por secreto profesional
f) Daños psicológicos o físicos
g) Pérdida de control sobre sus datos personales
h) Riesgo a la vida y seguridad de las personas

IX. RESPONSABLE DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES

Persona designada por el Sujeto Obligado para establecer y mantener las medidas de seguridad para la protección de datos personales de sus sistemas. Sus deberes son:

1. Crear políticas internas para la gestión y tratamiento de los datos personales, el ciclo de vida de los Datos Personales (obtención, uso y supresión),
2. Definir las funciones y obligaciones del personal involucrado,
3. Elaborar el inventario de Datos Personales,
4. Realizar el análisis de riesgo considerando las amenazas y vulnerabilidades existentes,
5. Solicitar los recursos involucrados en su tratamiento para la compra de hardware, software, contratación de personal del responsable,
6. Realizar el análisis de brecha,
7. Elaborar un plan de trabajo,
8. Implementar las medidas de seguridad faltantes, las políticas de gestión y tratamiento,
9. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, las amenazas y vulneraciones,
10. Diseñar y aplicar capacitaciones del personal bajo su mando, dependiendo de sus roles y responsabilidades

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

X. REGISTRO DE ACCESO Y TELECOMUNICACIONES

POLÍTICAS DE ASIGNACIÓN DE CLAVES DE ACCESO [INDICAR LAS POLÍTICAS]

POLÍTICAS DE CONTROL DE CLAVES DE ACCESO [INDICAR LAS POLÍTICAS]

POLÍTICAS DE RESGUARDO DE CLAVES DE ACCESO [INDICAR LAS POLÍTICAS]

DETECTORES Y DEFENSAS CONTRA ACCESOS NO AUTORIZADOS [INDICAR LAS DIRECTRICES]

LINEAMIENTOS DE SEGURIDAD DE SISTEMAS DIGITALES [INDICAR LOS LINEAMIENTOS]

a) **Autorización para el acceso para sistemas digitales [INDICAR LOS PASOS A SEGUIR]**

b) **Controles de seguridad para la red y los servicios de red [INDICAR LOS CONTROLES]**

c) **Segmentación de redes [INDICAR LOS PASOS A SEGUIR]**

d) **Seguridad en los parámetros de la red [INDICAR LOS PASOS A SEGUIR]**

e) **Regulación para el correo electrónico [INDICAR LOS PASOS A SEGUIR]**

f)

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

XI. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

El monitoreo es el Control del desarrollo cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo y como resultado de un proceso de mejora continua.

Tipo	Objeto	Periodicidad a diciembre 2023	Insumos o medidas intervenidas	Forma de implementación
Revisión	Revisar la actualización de los insumos del Documento de Seguridad y las medidas de seguridad que lo requieran.	Semestral	Documento de seguridad: - Inventario de tratamientos. - Análisis de riesgo. - Análisis de brecha. Medidas de seguridad: - Listado de servidores públicos que intervienen en tratamientos. -	Alerta semestral para revisión y actualización de sus tratamientos registrados, listados de servidores públicos y las declaratorias de confidencialidad, será a través de formularios puestos a disposición para registrar o actualizar dichas medidas.
Seguimiento Asesorías técnico especializadas	Reforzar el conocimiento e implementación de medidas de seguridad	Cuando las áreas lo requieran	Documento de seguridad: - Inventario de tratamientos. - Análisis de riesgo. - Análisis de brecha. Medidas de seguridad: - Listado de servidores públicos que intervienen en tratamientos. -	Asesorías técnico especializadas con temáticas particulares, indicadas por las Unidades Administrativas

XII. PLAN DE TRABAJO

Es la herramienta con la que se organiza y simplifica las actividades necesarias para la implementación de medidas de seguridad faltantes para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales, por lo que se prevén las siguientes acciones

Objeto	Actividad específica	Periodo de tiempo
Revisar la actualización de los insumos	Diseñar un mecanismo de monitoreo	Junio-diciembre 2023
		Enero-mayo 2024

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

del Documento de Seguridad y las medidas de seguridad que lo requieran.	Aplicar el mecanismo de monitoreo en las unidades administrativas	
	Sistematizar los resultados	Junio-julio 2024
	Implementar las mejoras detectadas a través del mecanismo de monitoreo	Agosto-diciembre 2024
	Requisición de insumos para la protección de datos personales (espacio amplio, archiveros con llave	Agosto 2023
Reforzar el conocimiento e implementación de medidas de seguridad	Solicitar a las personas responsables de sistemas de datos personales, su diagnóstico de necesidades de capacitación en materia de datos personales (ANEXO XXII)	Julio 2023
	Incorporar las necesidades de capacitación manifestadas por las personas titulares de sistemas de datos personales, en el proyecto de Programa Anual de Capacitación en materia de Protección de Datos Personales 2024	Agosto-septiembre 2023
	Aprobación del Programa Anual de Capacitación en materia de Protección de Datos Personales 2024	Octubre- noviembre
	Implementación del Programa Anual de Capacitación en materia de Protección de Datos Personales 2024	Enero 2024

XIII. PROGRAMA DE CAPACITACIÓN

Como medida de seguridad administrativa del tipo preventivo, efectiva y eficiente, el Programa Anual de Capacitación, permite que el tratamiento de datos personales se haga de una manera correcta y se evite el mal uso, sustracción, divulgación. En este sentido, para la debida protección de los datos personales, esta unidad administrativa realizará las capacitaciones en materia de protección de datos personales ofertadas por los Institutos de Transparencia Federal y Local. **(Anexo IX)**

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó **Jorge Romero Marinero**		**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
Aprobó **Comité de Transparencia**	**Comité de Transparencia** **ACUERDO. A03/CTSE03/AT/20-07-23**	**20**	**07**	**2023**	**21**	**07**	**2023**

DETECCIÓN DE NECESIDADES DE CAPACITACIÓN (DNC) 2023, RESPONSABLES DE SISTEMAS DE DATOS PERSONALES

Fecha de elaboración	

DATOS GENERALES:

Nombre del Sistema de Datos Personales	
Nombre de la persona Responsable del Sistema de Datos Personales	
Nombre de la persona con la que se coordinaran las acciones de capacitación	

No	Curso	Público objetivo	Cantidad estimada de personal a capacitar		
			Presencial	Virtual	Total
1	Registro Electrónico de Sistemas de Datos Personales	Responsables de Sistemas de Datos Personales, Responsable de Seguridad,			
2	Medidas de Seguridad y Documento de Seguridad	Responsables de Sistemas de Datos Personales, Responsable de Seguridad, Usuarios (as)			
3	Aviso de privacidad y acuerdos de creación, modificación y supresión de Sistemas de Datos Personales	Responsables de Sistemas de Datos Personales, Responsable de Seguridad, Usuarios (as)			
4	Análisis de brecha	Responsables de Sistemas de Datos Personales, Responsable de Seguridad, Usuarios (as)			
5	Análisis de riesgo	Responsables de Sistemas de Datos Personales, Responsable de Seguridad, Usuarios (as)			
6	Mecanismos de monitoreo	Responsables de Sistemas de Datos Personales, Responsable de Seguridad, Usuarios (as)			

OTROS:

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023

Mencione en orden de importancia, **3 temas además de los cursos arriba señalados**, que considera requiere el Responsables de Sistemas de Datos Personales, Responsable de Seguridad, Usuarios (as) de su unidad administrativa, en las materias que nos ocupan.

Id	Tema
1	
2	
3	

FIRMAS:

Autorizó: **Responsable del Sistema de Datos Personales**	**Elaboró:** **Responsable de Seguridad del Sistema de Datos Personales**

Elaboró María Elena Hernández Mora	Órgano Colegiado	Aprobado			Vigente a partir de		
Revisó Jorge Romero Marinero		Día	Mes	Año	Día	Mes	Año
Aprobó Comité de Transparencia	Comité de Transparencia ACUERDO. A03/CTSE03/AT/20-07-23	20	07	2023	21	07	2023