



DOCUMENTO DE SEGURIDAD EN MATERIA DE DATOS PERSONALES

**H. Ayuntamiento de Aquismón, S.L.P.
2024-2027**

Agosto 2026.

INDICE

1. INTRODUCCIÓN	1
2. GLOSARIO.....	2
3. MARCO NORMATIVO	4
4. INVENTARIO DE DATOS PERSONALES Y SISTEMAS.....	8
4.1 Catálogo de tratamiento de datos personales:	10
5. FUNCIONES Y OBLIGACIONES.....	12
6. ANÁLISIS DE RIESGOS.....	13
6.1 Matriz de Riesgos:	14
7. ANÁLISIS DE BRECHA	15
8. MEDIDAS DE SEGURIDAD.....	16
8.1 Medidas de seguridad para transferencias.....	17
8.2 Transferencias a terceros.....	17
8.3 Medidas de seguridad en caso de vulneración de datos personales.	18
8.4 Medidas de seguridad físicas y administrativas	19
8.5 Medidas de seguridad en el entorno	20
8.6 Medidas de seguridad técnicas	20
8.7 Métodos de eliminación y borrado seguro de información física y digitalmente cuyo contenido se encuentran datos personales	22
8.7.1 Eliminación física	22
8.7.2 Eliminación digital	22
9. PLAN DE TRABAJO	23
10. MECANISMOS DE MONITOREO	24
11. PROGRAMA GENERAL DE CAPACITACIÓN.....	25
12. ACTUALIZACIÓN DEL DOCUMENTO	26

1. INTRODUCCIÓN.-

El presente documento tiene la finalidad de establecer el marco integral de medidas administrativas, técnicas y físicas ejercidas por el H. Ayuntamiento de Aquismón del Estado de San Luis Potosí, Administración 2024-2027, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que se encuentran en posesión del mismo, así mismo prevenir su daño, pérdida, alteración, destrucción o el uso y/o acceso no autorizado.

Durante el ejercicio de esta Administración, el H. Ayuntamiento de Aquismón, desde sus actividades y funciones, recaba y trata datos personales a través de múltiples sistemas, lo cual es una responsabilidad directa en la implementación de controles de seguridad efectivos que aseguren el cumplimiento de los principios y obligaciones establecidos en la legislación aplicable en materia de protección de datos personales.

Este documento recaba los instrumentos de gestión y control interno que permite identificar los activos de información, evaluar los riesgos del tratamiento de datos personales, determinar las posibles brechas existentes sobre el marco normativo y establece un plan de acción. De la misma forma define funciones y responsabilidades de las áreas involucradas, también define mecanismos de monitoreo y mejora constante.

Finalmente, este documento se considera como un instrumento dinámico, sujeto a revisión y actualización periódica, en función de los cambios en los procesos institucionales, la incorporación de nuevas tecnologías, la evolución de los riesgos y las disposiciones normativas aplicables, con el propósito de mantener un nivel óptimo de protección de los datos personales en todo momento, por lo que su adecuación y perfeccionamiento es una tarea constante desde el Gobierno Municipal.

2. GLOSARIO. -

Para efectos del presente documento de seguridad, se entenderá por los siguientes conceptos:

- I. **Anonimizaciòn:** Es el reducir al mínimo los riesgos de reidentificaciòn de los datos, manteniendo la veracidad de los resultados del tratamiento de los mismos, además de evitar la identificación de las personales;
- II. **Base de datos:** Conjunto ordenado de datos personales referentes a una persona física identificada condicionada a criterios determinados con independencia de la forma o modalidad de su creación;
- III. **CEGAIP:** Comisión Estatal de Garantía de Acceso a la Información Pública del Estado de San Luis Potosí;
- IV. **Confidencialidad:** Propiedad de la información para no estar a disposición o ser revelada a personas, entidades o procesos no automatizados;
- V. **Derechos ARCO:** Derechos de Acceso, Rectificación, Cancelación y Oposición;
- VI. **Disociación:** Es el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, debido a su estructura, el contenido o grado de desagregación;
- VII. **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;
- VIII. **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable;
- IX. **Datos personales sensibles:** Aquellos que afectan la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave;
- X. **Encargado:** Persona física o moral que trata datos personales por cuenta del responsable;
- XI. **Hardware:** Conjunto de componentes físicos de una computadora;
- XII. **Incidente de seguridad:** Evento que compromete la confidencialidad, integridad o disponibilidad de los datos personales;
- XIII. **Inventario de Datos Personales:** Conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de la Administración Pública Municipal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso;
- XIV. **Ley:** Ley de Protección de Datos Personales para los Sujetos Obligados del Estado de San Luis Potosí;
- XV. **Medidas de seguridad:** Conjunto de acciones, controles o mecanismos administrativos, técnicos y físicos para proteger los datos personales;

- XVI. **Nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible;
- XVII. **Respaldo:** Es una copia de seguridad de la información digital que se actualiza con el paso del tiempo;
- XVIII. **Responsable:** El Ayuntamiento Municipal que decide sobre el tratamiento de los datos personales;
- XIX. **Riesgo:** Combinación de la probabilidad de un evento y su consecuencia desfavorable;
- XX. **Riesgo de Seguridad:** Es la probabilidad de que cierta amenaza pueda explotar vulnerabilidades de un activo o grupo;
- XXI. **SABG:** Secretaría Anticorrupción y Buen Gobierno;
- XXII. **Sistema de tratamiento:** Conjunto organizado de recursos para el tratamiento de datos personales;
- XXIII. **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normativa aplicable;
- XXIV. **Tratamiento:** La obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, transferencia o disposición de datos personales;
- XXV. **Titular:** La persona física a quien corresponden los datos personales; y
- XXVI. **Transferencia:** Es toda comunicación de datos personales fuera del Sujeto Obligado realizada a persona distinta del titular, responsable o encargado.

3. MARCO NORMATIVO. -

I. Constitución Política del Estado Libre y Soberano de San Luis Potosí

Artículo 17 Fracción III.

El sistema para garantizar el acceso a la información pública. En el Estado de San Luis Potosí es derecho humano de todas las personas, conocer y acceder a la información pública, con las excepciones previstas en esta Constitución, y en la ley de la materia.

Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes, asentada en archivos, bases de datos y registros públicos o privados de quienes tengan el carácter de entes obligados conforme a la ley; así como a actualizar, rectificar, suprimir o mantener en reserva dicha información, en los términos de la ley. En cualquier caso, la ley protegerá a las personas contra cualquier lesión en sus derechos, resultante del tratamiento de sus datos personales.

La información relativa a la vida privada y a los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Para tal efecto, los sujetos obligados ejercerán sus atribuciones conforme a las disposiciones aplicables.

Se establecerán mecanismos de acceso a la información pública y procedimientos de revisión expeditos que se sustanciarán ante las instancias competentes en los términos que fija esta Constitución y las leyes. El ejercicio de este derecho se regirá por los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

Los sujetos obligados deberán promover, respetar, proteger y garantizar los derechos de acceso a la información pública y a la protección de datos personales. Las leyes en la materia determinarán las bases y procedimientos del ejercicio de estos derechos, así como la competencia de las autoridades para conocer de los procedimientos de revisión contra los actos que emitan los sujetos obligados.

La tutela del derecho al acceso a la información pública a la fecha sigue correspondiendo Comisión Estatal de Garantía de Acceso a la Información Pública del Estado de San Luis Potosí.

Respecto al Poder Judicial y al Poder Legislativo del Estado, así como a los organismos constitucionales autónomos, esta tutela será atribución de sus órganos de control interno o áreas homólogas, en sus respectivos ámbitos de competencia, en los términos establecidos en la Ley General y la Ley local de la materia.

II. Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí.

ARTÍCULO 2°. Son objetivos de esta Ley:

I. Establecer la competencia que tiene el Estado de San Luis Potosí en materia de transparencia y acceso a la información y las bases para la coordinación con el Instituto Nacional de Transparencia, Acceso a la Información y **Protección de Datos Personales**;

ARTÍCULO 82. Los sujetos obligados serán **responsables de los datos personales en su posesión** y, en relación con éstos, deberán:

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso, rectificación, corrección y oposición al tratamiento de datos, en los casos que sea procedente, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con la normatividad aplicable;

II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido, o dicho tratamiento se haga en ejercicio de las atribuciones conferidas por ley;

III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de la normatividad aplicable, excepto en casos en que el tratamiento de los datos se haga en ejercicio de las atribuciones conferidas por ley;

IV. Procurar que los datos personales sean exactos y actualizados;

V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y

VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información de acuerdo a la normatividad aplicable. Lo anterior, sin perjuicio a lo establecido por el artículo 73 fracción XXIX-S de la Constitución Política de los Estados Unidos Mexicanos y lo que establece el artículo 142 de esta Ley.

Toda solicitud de acceso a la información de datos personales que sea presentada por una tercera persona que no tenga derecho a disponer de éstos, deberá ser notificada con su contenido a la persona titular de la información desde el momento de su recepción, con el objeto de garantizar su derecho a la protección de datos personales, conforme a lo establecido por los artículos, 19, 24, 25 y 27 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de San Luis Potosí, los cuales en el tenor señalan:

III. Ley de protección de datos personales en posesión de los sujetos obligados del estado de San Luis Potosí.

ARTÍCULO 1º. La presente Ley es de orden público y observancia obligatoria en el Estado de San Luis Potosí; y tiene por objeto garantizar el derecho que tiene toda persona a la protección de sus datos personales.

ARTÍCULO 16. El responsable podrá tratar los datos personales en su posesión para finalidades distintas a aquéllas que motivaron el tratamiento original de los mismos, siempre y cuando cuente con atribuciones expresas conferidas en ley y medie el consentimiento del titular, en los términos previstos en la presente Ley y demás normatividad que resulte aplicable. Principio de lealtad

ARTÍCULO 17. El responsable deberá abstenerse de tratar los datos personales a través de medios engañosos o fraudulentos, privilegiando, en todo momento, la protección de los intereses del titular y su expectativa razonable de privacidad.

ARTÍCULO 30. Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades concretas, explícitas lícitas y legítimas que justificaron su tratamiento.

En el establecimiento de los plazos de conservación de los datos personales, el responsable deberá considerar los valores administrativos, contables, fiscales, jurídicos e históricos de los datos personales, así como atender las disposiciones aplicables en la materia de que se trate.

Principio de proporcionalidad

ARTÍCULO 32. El responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para las finalidades concretas, explícitas lícitas y legítimas que justifiquen su tratamiento.

Criterio de minimización

ARTÍCULO 33. El responsable procurará realizar esfuerzos razonables para tratar los datos personales al mínimo necesario, con relación a las finalidades que motivan su tratamiento.

Principio de información

ARTÍCULO 34. El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales.

Objeto del aviso de privacidad

ARTÍCULO 35. El aviso de privacidad tendrá por objeto informar al titular sobre los alcances y condiciones generales del tratamiento, a fin de que esté en posibilidad de tomar decisiones informadas sobre el uso de sus datos personales y, en consecuencia, mantener el control y disposición sobre ellos.

Características del aviso de privacidad

ARTÍCULO 36. El aviso de privacidad deberá caracterizarse por ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento. En el aviso de privacidad queda prohibido:

- I. Usar frases inexactas, ambiguas o vagas;
- II. Incluir textos o formatos que induzcan al titular a elegir una opción en específico;
- III. Marcar previamente casillas, en caso de que éstas se incluyan para que el titular otorgue su consentimiento, y
- IV. Remitir a textos o documentos que no estén disponibles para el titular.

Sistema de gestión y documento de seguridad

ARTÍCULO 50. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión. Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley.

Documento de seguridad

ARTÍCULO 51. El responsable deberá elaborar y aprobar un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo conforme a lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables en la materia. El documento de seguridad será de observancia obligatoria para los encargados y demás personas que realizan algún tipo de tratamiento de datos personales.

4. INVENTARIO DE DATOS PERSONALES Y SISTEMAS. -

El control de documentos y tiramiento de datos personales que realizan las unidades administrativas de la administración pública del Municipio de Aquismón pueden resguardarse de forma física y/o digitalmente.

Dichos datos personales que manejan las unidades administrativas previstas con base a la estructura orgánica y las leyes de protección de datos personales deberán contar con su respectivo tratamiento y tener responsables de las mismas.

Descripción y estructura del inventario de datos personales.

En el documento base del inventario de datos personales se indican cuales son los datos que se recaban, con que finalidad se obtienen y su método de obtención, el fundamento legal que faculta al área administrativa para el tratamiento de datos personales, los medios de almacenamiento, sitios de resguardo y a la persona servidora pública encargada de organizar y resguardar la base o inventario de datos personales, así como los colaboradores que tienen acceso a las mismas.

Dentro de los inventarios de datos personales se define una categoría de los datos, estableciendo cuales son los tipos de datos personales que pueden estar sujetos a tratamiento de acuerdo a las disposiciones de cada unidad administrativa:

- a. **Datos de identificación y contacto:** nombre, género, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, firma autógrafa, edad, fotografía y referencias personales, identificación personal, imagen.
- b. **Datos sobre características físicas:** Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, cicatrices, tatuajes.
- c. **Datos laborales:** puesto o cargo que desempeña, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información generada durante los procedimientos de reclutamiento, selección y contratación y experiencia/capacitación laboral.
- d. **Datos académicos:** trayectoria educativa, escolaridad, título, cédula profesional, certificados y reconocimientos.
- e. **Datos patrimoniales y/o financieros:** bienes muebles, bienes inmuebles, ingresos, egresos y cuentas bancarias, información fiscal, historial crediticio, número de tarjeta, seguros, afores.
- f. **Datos biométricos:** Huella dactilar.
- g. **Datos migratorios:** País de origen, VISA, Pasaporte, Tiempo residiendo en el país.

- h. Datos sobre pasatiempos, entretenimiento y diversión:** pasatiempos, aficiones, deportes, juegos de interés.
- i. Datos sobre la ideología, creencias religiosas, filosóficas o morales:** Creencias religiosas.
- j. Datos de salud:** Estado de salud físico presente pasado o futuro, diagnóstico, estado de salud mental, información genérica.
- k. Datos sobre vida sexual:** Si es sexualmente activo.
- l. Datos de origen étnico o racial:** Etnia a la que pertenece.
- m. Otros:** Datos que por mandato legal son de acceso público.

En el apartado de “Forma de obtención” de la tabla de inventario de datos personales a continuación se describe el tipo de personas de quienes se obtienen y cómo recaban los datos personales que pueden estar sujetos a tratamiento:

- a. Personas que laboran en las diversas direcciones de cada dependencia del H. Ayuntamiento Municipal 2024-2027.
- b. Personas externas que prestan algún servicio para las diferentes direcciones del H. Ayuntamiento Municipal 2024-2027.
- c. Personas externas que participan en actividades que llevan a cabo las direcciones del H. Ayuntamiento Municipal 2024-2027.

4.1 Catálogo de tratamiento de datos personales:

Administración Pública del Municipio de Aquismón 2024-2027

<i>DIRECCIÓN</i>	<i>DOCUMENTO</i>
1. Dirección de Turismo	Registro de Hoteles y Restaurantes
2. CODESOL	Registro de Programas
3. CODESOL	Programas de apoyo a la ciudadanía
4. Dirección de Alcoholes	Padrón de establecimientos
5. Secretaría General	Constancias de identidad
6. Secretaría General	Constancias de residencia
7. Secretaría General	Comité de ética
8. Secretaría General	Comité de participación ciudadana
9. Secretaría General	Consejo de seguridad
10. Secretaría General	Comité de planeación
11. Secretaría General	Consejo de protección civil
12. Secretaría General	Comité de transparencia
13. Secretaría General	Comité de consulta ciudadana
14. Secretaría General	Consejo de turismo
15. Secretaría General	Refrendos
16. Dirección de obras públicas	Licencias de uso de suelo
17. Dirección de obras públicas	Licencias de subdivisión y notificación
18. Dirección de obras públicas	Licencias de construcción
19. Dirección de obras públicas	Licencia de certificación panteón
20. Dirección de agua potable	Permiso de conexión agua
21. Contraloría interna	Declaración patrimonial

22. Dirección de obras publicas

Permiso de obras

23. Dirección de obras publicas

Permiso de uso de suelo

24. CODESOL

Información de obras públicas



5. FUNCIONES Y OBLIGACIONES. -

Para el correcto uso de este documento, es necesario establecer los deberes de los servidores públicos a cargo de las diversas direcciones que participan en el tratamiento de los datos personales

El servidor público deberá:

1. Tener a la vista el aviso de privacidad;
2. Dar a conocer el aviso de privacidad a la ciudadanía previo a la obtención de la información;
3. En caso de dudas o quejas de los titulares de los datos personales orientarlos a que acuda a la Unidad de Transparencia Municipal;
4. Rectificar que la información recolectada esté completa;
5. Conocer y seguir las medidas de seguridad para el cuidado de los datos personales;
6. Recabar los datos personales para la finalidad para la cual estos fueron solicitados;
7. Conocer, aplicar y sujetarse al Aviso de Privacidad y los lineamientos de Protección de Datos Personales del Estado de San Luis Potosí;
8. Guardar confidencialidad de los datos recabados;
9. Tomar por lo menos una vez una capacitación sobre el uso y tratamiento de Datos Personales, de forma anual;
10. No realizar transferencias de datos personales que no vayan a cumplir con la finalidad de la cual fueron recabados;
11. Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales;
12. Informar a la Unidad de Transparencia, sobre los cambios que sufran sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales; y
13. Los demás que sean determinados por el marco normativo aplicable.

Son obligaciones del Responsable de la Unidad de Transparencia:

1. Auxiliar y orientar al titular que lo requiera con relación al manejo de datos personales;
2. Gestionar las solicitudes para los ejercicios de derechos ARCO;
3. Establecer mecanismos para asegurar la protección de datos personales; y
4. Las demás que le sean aplicadas en la materia.

6. ANÁLISIS DE RIESGOS. -

Es un proceso de varios pasos destinado a mitigar el impacto de los riesgos en las operaciones de todo tipo, por lo que para que esto suceda, se debe utilizar el análisis de riesgos para asegurarse de que todos los aspectos, estén protegidos de posibles amenazas. La realización de análisis de riesgos periódicos también minimiza la vulnerabilidad ante acontecimientos inesperados.

Por lo anterior, el H. Ayuntamiento de Aquismón realiza un análisis sistemático de los riesgos asociados al tratamiento de datos personales, con el objetivo de identificar, evaluar y mitigar posibles vulnerabilidades que puedan afectar la seguridad de la información.

Para ello, se consideran los siguientes elementos:

- a. **Identificación de activos:** Sistemas, bases de datos, archivos físicos y plataformas digitales que contienen datos personales;
- b. **Identificación de amenazas:** Accesos no autorizados, pérdida de información, ataques cibernéticos, errores humanos, desastres naturales, entre otros;
- c. **Identificación de vulnerabilidades:** Deficiencias en controles de acceso, falta de actualización de sistemas, ausencia de capacitación, entre otros; y
- d. **Evaluación del riesgo:** Se determina con base en la probabilidad de ocurrencia y el impacto potencial (bajo, medio, alto).

Los riesgos identificados deberán documentarse en una matriz de riesgos, la cual servirá como base para la implementación de medidas de seguridad y su mejora continua.

6.1 MATRIZ DE RIESGOS:

Activo	Amenaza	Vulnerabilidad	Riesgo	Medidas mitigación	de
Bases de datos de funcionarios	Accesos no autorizados a los sistemas tecnológicos.	Contraseñas débiles, servidores sin SSL.	Alto	Política de contraseñas, Capacitaciones sobre servidores.	de
Documentos con información ciudadana	Acceso no autorizado a personas a oficinas administrativas	Pérdida de información	Alto	Control de acceso más estricto.	
Números telefónicos de autoridades comunales	Acceso no autorizado a personas ajenas al Ayuntamiento	Robo de información	Medio	Control de acceso más estricto	
Daño físico de documentos	Posibles desastres causados por múltiples situaciones	Pérdida de información	Alto	Mantenimiento constante a la infraestructura del Ayuntamiento y mejora en la cultura de convivencia	

7. ANÁLISIS DE BRECHA. -

El análisis de brecha tiene como finalidad identificar las diferencias existentes entre las medidas de seguridad actualmente implementadas por el Ayuntamiento y aquellas requeridas por la normativa aplicable en materia de protección de datos personales.

Por lo consiguiente durante entrevistas realizadas a diversos funcionarios municipales se obtuvo lo siguiente:

- a. Quienes recaban la información a través de diferentes trámites y requisitos, son personas que trabajan en el Ayuntamiento;
- b. La información se almacena de forma física y digital dependiendo del evento y/o proceso realizado, quedando su custodia en expedientes en las mismas áreas recolectoras;
- c. El lugar donde se almacena la información física es dentro de las instalaciones del Ayuntamiento de Aquismón;
- d. El acceso a las áreas está restringido y bajo llave, a cargo del Director responsable;
- e. Una vez que el evento o proceso termina la información recabada se almacena en un espacio para documentos físicos históricos en caso de ser digital se resguarda con un periodo de tiempo de duración de la actual Administración; y
- f. Se procede a la entrega- recepción, en periodo de cambio de Administración.

Estas medidas de seguridad son viables siempre y cuando se apliquen de manera continua y consistente.

El riesgo latente que se provoca por la falta de conocimiento y/o compromiso puede ser minimizado por medio del establecimiento obligatorio de dichas medidas de seguridad mejora continua, así como capacitaciones periódicas sobre el tema.

8. MEDIDAS DE SEGURIDAD. -

Con base a la información recabada se establecen las siguientes medidas de seguridad de carácter físico, técnico y administrativo.

Objetivo	Descripción
Control de servidores públicos	Debe de realizarse una base de datos con la información de los servidores públicos que están capacitados para recabar datos personales.
Control de servidores públicos	Obligatoriedad de asistir al menos a 1 capacitación sobre manejo de datos personales.
Control de servidores públicos	Emitir documento de seguridad para el conocimiento y cumplimiento de las medidas de seguridad
Obtención de datos personales	Para evitar el desvío de información o mala captura que el servidor encargado esté acreditado para la captura de información.
Aviso de privacidad	El servidor encargado de recabar los datos personales deberá de notificar al ciudadano sobre el aviso de privacidad y el uso que se le dará a su información
Aviso de privacidad	El aviso de privacidad siempre deberá de estar visible en las plataformas del Ayuntamiento y en las oficinas públicas.
Almacenamiento físico	Una vez recabada la información deberá de ser guardada en un espacio designado exclusivamente para esta función.
Almacenamiento físico	Cuando el evento y/o proceso concluya se deberá de eliminar la información de forma adecuada.

8.1 Medidas de seguridad para transferencias.

Transferencias al interior del sujeto obligado y a otros sujetos obligados:

- a. Solo podrán ser transferidos los datos personales para dar seguimiento y conclusión al trámite o sistema de tratamiento bajo la finalidad que éstos prevean;
- b. El área que entrega los datos personales deberá cerciorarse de transferir la totalidad de los datos que resulten necesarios para el seguimiento o la conclusión del trámite o sistema de tratamiento correspondiente. Limitándose a la entrega de datos adicionales que no resulten necesarios;
- c. El área que entrega los datos personales deberá cerciorarse de que los datos que transfiere sean completos y veraces;
- d. El área que reciba los datos personales deberá conservar los mismos sujetándose a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y adoptando las medidas de seguridad previstas en este documento;
- e. El área que reciba los datos personales deberá encargarse de la supresión de los datos que reciba cuando esta corresponda; y
- f. El área que entrega y el área que recibe los datos personales deberán dar acceso a los datos personales en tratándose de procedimientos de derecho ARCO.

8.2 Transferencias a terceros.

- a. El tercero que reciba los datos personales deberá sujetarse a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y deberá adoptar las medidas de seguridad previstas en este documento.

- b. En caso de ser necesario conforme a las disposiciones normativas, se deberá firmar un acuerdo de confidencialidad que proteja el tratamiento de los datos personales que recaba este sujeto obligado y transfiere al tercero.

8.3 Medidas de seguridad en caso de vulneración de datos personales.

Si se llega a vulnerar la seguridad deberá de ser registrada en la bitácora de vulnerabilidades para posteriormente y de forma urgente ser notificada al responsable de datos personales del Ayuntamiento y la Unidad de Transparencia, las que afecten o impacten de forma significativa los derechos patrimoniales o morales del titular, en un plazo máximo de veinticuatro horas en cuanto se confirmen y este en proceso las acciones encaminadas para dimensionar la afectación, con la finalidad de que los titulares puedan tomar medidas correspondientes para la defensa de sus derechos, dicha notificación debe contener lo siguiente:

1. La naturaleza del incidente.
2. Los datos personales comprometidos.
3. Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses.
4. Las acciones correctivas realizadas de forma inmediata.
5. Los medios donde puede obtener mayor información al respecto.

Plan de contingencia

En caso de vulneración y pérdida de información sobre datos personales que sean útiles para el manejo, administración y trabajo continuo del Ayuntamiento, y, una vez realizadas las medidas de seguridad que antes se mencionaron anteriormente, se dispondrán de los respaldos electrónicos realizados por cada área administrativa en donde se contienen copias de los documentos y archivos que contienen datos personales.

8.4 Medidas de seguridad físicas y administrativas.

Las direcciones del H. Ayuntamiento de Aquismón deberán de implementar como mínimo las siguientes medidas generales de seguridad física, para evitar daños, sustracciones o intromisiones no autorizadas en las instalaciones y archivos de información del sujeto obligado:

- a. En la medida de lo posible asignar un espacio general el cual deberá de estar dividido por direcciones para el almacenamiento físico de los documentos que contienen datos personales, cuya preferencia no debe de ser un paso o área de uso frecuente por el personal de trabajo;
- b. Tener bajo llave o en archiveros seguros los documentos donde se encuentre la información de datos personales;
- c. Evitar que se dejen descuidados o sin atención los espacios y/o documentos que contengan datos personales;
- d. Verificar que los documentos que usen datos personales nunca se usen como hojas de reciclaje, así mismo rectificar que el documento fue destruido en su totalidad cuando el tiempo de almacenamiento expire; e
- e. Implementar programas de capacitación para el uso y protección de datos personales.

8.5 Medidas de seguridad en el entorno.

Las direcciones del H. Ayuntamiento de Aquismón deberán de ejecutar las siguientes medidas de seguridad de entorno para evitar accesos no autorizados a las instalaciones las cuales deberán de cumplir con lo siguiente:

- a. Registrar a los visitantes que accedan a las instalaciones;
- b. Portar gafete o credencial de identificación del H. Ayuntamiento;
- c. Asegurar el retiro de pases de visita;
- d. Identificar a los servidores públicos adscritos al H. Ayuntamiento los cuales deberán de portar el debido uniforme y credenciales y/o gafete de identificación;

8.6 Medidas de seguridad técnicas.

Consisten en mecanismos que se valen de tecnología, asegurando el acceso a sistemas informáticos y bases de datos, relacionados al software y hardware, es decir protegen el entorno digital de los datos personales, cuyas obligaciones son las siguientes:

- a. Registrar la información que corresponden en los tratamientos de datos personales y mantenerlos actualizados;
- b. Verificar durante mantenimientos y monitoreo que el personal interno o externo del equipo no vulnere la seguridad de la información contenida en los equipos de TI;

- c. Eliminar de forma segura toda la información de datos personales una vez haya concluido el ciclo de guardado del mismo; e
- d. Implementar medidas de seguridad tecnológicas necesarias para el tratamiento de datos personales.

De la misma manera, las Direcciones del H. Ayuntamiento deberán de implementar al menos las siguientes medidas de seguridad en equipos de TI:

- a. Tener contraseñas fuertes en las cuentas locales de los equipos;
- b. No usar correos personales para el envío o recibimiento de información de datos personales;
- c. Limitar y/o restringir el acceso a los equipos que contengan datos personales a funcionarios que no tengan la autorización de manejo de datos personales;
- d. Tener contraseñas fuertes para las redes de internet y cambiarlas de forma continua;
- e. Limitar o restringir el uso de internet a personas o equipos que consideren pertinentes; y
- f. Recibir al menos una vez al año capacitaciones sobre ciber seguridad.

8.7 Métodos de eliminación y borrado seguro de información física y digitalmente cuyo contenido se encuentran datos personales.

La eliminación de información de datos personales tiene que cumplir primero un ciclo de vida el cual se tendrá que establecer previo a la recaudación de la información en el documento del inventario de datos personales, así como notificarle a la persona que brindará la información el tiempo del ciclo de vida de sus datos personales y los métodos por los cuales serán eliminados una vez llegue a ese punto.

8.7.1 Eliminación física.

- 1) **Trituración mediante uso de maquina especializada:** Consiste en cortar los documentos de tal forma que las hojas queden reducidas a partículas lo cual hace prácticamente imposible de unir o poder usar; y
- 2) **Destrucción de los medios de almacenamiento digital:** Con el fin de que no se puedan recuperar la información eliminada digitalmente, el método ideal seria perforar las unidades de almacenamiento con una herramienta para que quede completamente sin vida útil.

8.7.2 Eliminación digital:

- 1) **Formateo:** Consiste en realizar un borrado de bajo nivel (nivel computadora) para la limpieza de las unidades de almacenamiento digitales, para su posterior eliminación física, de esta forma garantiza una capa más de eliminación de información.

9. PLAN DE TRABAJO. -

Derivado del análisis de riesgos y del análisis de brecha, se busca enmarcar los deberes de las direcciones municipales para la máxima protección de datos personales. Debido a la importancia y el contexto actual en esta materia, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad del plan de trabajo es plasmar de manera enunciativa, mas no limitativa las actividades que las direcciones municipales realizarán para la aplicación del presente documento de seguridad

Para la ejecución del **PLAN DE TRABAJO** se implementará lo siguiente:

- 1) Se remitirá el presente documento a todos los titulares de las direcciones que recaben datos personales vía circular interna, emitida desde la Contraloría Interna Municipal;
- 2) Establecer un programa de capacitación en materia de protección de datos personales los cuales serán emitidos a todos los titulares de las direcciones que recaben este tipo de datos; y
- 3) Se mantendrán actualizadas las versiones del aviso de privacidad y se colocarán en lugares visibles dentro de las direcciones que recaben datos personales.

10. MECANISMOS DE MONITOREO. -

El Ayuntamiento de Aquismon implementará mecanismos permanentes de monitoreo y evaluación de las medidas de seguridad, esto con el objetivo de que éstas sigan siendo eficaces e idóneas para el H. Ayuntamiento.

Estos mecanismos incluyen:

- a) **Visitas a 2 áreas aleatoriamente:** Se verificará de primera mano la aplicación, actualización e impacto de las medidas de seguridad; y
- b) **Revisión de reportes e inventarios de datos personales a los titulares encargados:** El monitoreo de avances aplicación servirá como pilar para el seguimiento y actualización de las medidas de seguridad.



11. PROGRAMA GENERAL DE CAPACITACIÓN.

-

Se establecerán capacitaciones conforme a las necesidades del H. Ayuntamiento de Aquismon en cuanto a la implementación y aplicación del sistema de manejo de datos personales, así mismo se contempla una capacitación introductoria la cual se llevará a cabo anualmente.

Las fechas de capacitación serán notificadas por el Responsable de datos personales, con al menos una semana de anticipación para su correcta inserción en la agenda de los involucrados.



12. ACTUALIZACIÓN DEL DOCUMENTO. -

El presente Documento de Seguridad deberá ser revisado al menos una vez al año y actualizado de manera periódica, cada vez que sea necesaria o cuando se presenten cambios relevantes, tales como:

- a) Modificaciones en la normativa aplicable;
- b) Implementación de nuevos sistemas o tecnologías;
- c) Cambios en los procesos de tratamiento de datos personales;
- d) Identificación de nuevos riesgos o incidentes de seguridad; o
- e) Cambios de Administración o Responsables.

Toda actualización deberá documentarse y ser aprobada por la Contraloría Interna y autorizada por el Presidente Municipal.

ELABORÓ

C. JUAN DIEGO PEREZ HERNANDEZ
OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

APROBÓ

LIC. MARGARITO MARTINEZ LEDEZMA
CONTRALOR INTERNO MUNICIPAL

AUTORIZÓ

C. CUAHUTEMOC BALDERAS YAÑEZ
PRESIDENTE MUNICIPAL CONSTITUCIONAL
DE AQUISMON, S.L.P