

DOCUMENTO DE SEGURIDAD

PARA LA PROTECCIÓN DE DATOS PERSONALES

AYUNTAMIENTO DE BENEMÉRITO DE LAS AMÉRICAS, CHIAPAS



1.- Introducción.....	1
2.- Objetivos y alcances del documento.	4
2.1 Objetivos generales.....	4
2.2 Objetivos específicos.	4
2.3 Alcances del documento.....	5
3.- Sistema de Gestión de Seguridad de los datos personales en posesión del Ayuntamiento de Benemérito de las Américas.	7
ESQUEMA.....	9
4.- Inventario de Datos Personales y de los sistemas de tratamiento del Ayuntamiento de Benemérito de las Américas.....	12
5.- Funciones y Obligaciones de las personas que tratan Datos Personales.	18
6.- Análisis de Riesgos y de Brecha.....	21
7.- Gestión de vulneraciones y plan de contingencia.....	22
8.- Medidas de Seguridad generales.....	23
8.1 Medidas administrativas.....	23
8.2 Medidas físicas.	24
8.3 Medidas técnicas.....	26
9.- Plan de trabajo.	29
10.- Programa de Capacitación en materia de Protección de Datos Personales.	30
I. Introducción al derecho a la protección de datos personales.....	30
II. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.....	31
III. Programa Institucional de Protección de Datos Personales.....	31



1.- INTRODUCCIÓN.

El derecho a la protección de los datos personales es un derecho humano reconocido en la Constitución Política de los Estados Unidos Mexicanos, en sus artículos 6, apartado A, fracción II, y 16, párrafo segundo, que reconoce a toda persona la protección de sus datos personales, así como el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, en los términos que establezca la ley. Su regulación específica para el sector público es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 20 de marzo de 2025, cuya última reforma fue publicada el 14 de noviembre de 2025.

La protección de datos personales es el derecho que tiene toda persona a controlar la forma en que se recopila, utiliza, almacena, comparte y resguarda la información que permite identificarla, ya sea de manera directa o indirecta. En ese sentido, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas establece un conjunto de bases, principios y procedimientos que garantizan el derecho a la protección de los datos personales en posesión de los sujetos obligados.

El Ayuntamiento de Benemérito de las Américas, en lo sucesivo el Ayuntamiento, constituye, en términos de la citada Ley local, un sujeto obligado en materia de protección de datos personales y responsable de su tratamiento en el ejercicio de las atribuciones que tiene conferidas. En consecuencia, tiene el deber de garantizar a los titulares que sus datos personales sean tratados de manera legal, segura y confidencial, evitando su uso indebido, divulgación no autorizada, alteración o pérdida, y deberá cumplir con las obligaciones previstas en dicha Ley y demás normativa aplicable.

De ahí que el presente Documento de Seguridad tiene por objeto establecer el marco de referencia para el tratamiento de los datos personales que se realiza al interior del Ayuntamiento, a través de los distintos órganos administrativos que integran su estructura orgánica, con la finalidad de mantener vigentes y fortalecer, mediante la mejora continua, las medidas de protección de dichos datos, en términos de lo dispuesto



por los artículos 25, 26, 27, 29, 30 y demás relativos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

En ese sentido, el Ayuntamiento ha identificado los procesos que, en el ámbito de sus atribuciones, implican el tratamiento de datos personales, con el propósito de garantizar el cumplimiento de los deberes de confidencialidad y seguridad durante todo el ciclo de vida de la información. Para ello, se especifica la forma en que dichos datos son tratados, las medidas de seguridad implementadas, los órganos administrativos responsables de su protección y las finalidades del tratamiento, de conformidad con las funciones y competencias de cada área.

De conformidad con el artículo 28 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, las acciones relacionadas con las medidas de seguridad deben estar debidamente documentadas e integradas en un sistema de gestión, entendido como el conjunto de elementos y actividades interrelacionados que permiten establecer, operar, monitorear, mantener y mejorar de manera continua el tratamiento y la seguridad de los datos personales. Asimismo, el artículo 29 del mismo ordenamiento establece la obligación de los responsables de elaborar su Documento de Seguridad como parte de un proceso de mejora continua.

En cumplimiento de dichas disposiciones, el Ayuntamiento ha desarrollado acciones coordinadas entre los órganos administrativos que intervienen en el tratamiento de datos personales, entre las que destacan la elaboración de los inventarios de datos personales, la revisión y el fortalecimiento de las medidas de seguridad implementadas, así como la realización de análisis de riesgos y de brecha, con el propósito de monitorear la eficacia de las medidas adoptadas, identificar posibles vulnerabilidades y mitigar los riesgos asociados al tratamiento, a fin de prevenir la alteración, pérdida, transmisión, acceso, uso o tratamiento no autorizados de los datos personales y garantizar su confidencialidad, integridad y disponibilidad durante todo su ciclo de vida.

Asimismo, se impulsa un proceso permanente de sensibilización institucional sobre la importancia de adoptar medidas preventivas y correctivas, tomando como referencia los



resultados de la revisión de los sistemas de tratamiento, así como los esquemas de autorregulación y capacitación del personal.

Por lo anterior, y con fundamento en las disposiciones señaladas, el Ayuntamiento emite el presente Documento de Seguridad para la Protección de Datos Personales, en observancia de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como de las demás obligaciones previstas en la normativa aplicable. Para el Ayuntamiento, la política de seguridad de los datos personales constituye un compromiso permanente con el cumplimiento de las disposiciones de la legislación general y de la normativa local aplicable.



2.- OBJETIVOS Y ALCANCES DEL DOCUMENTO.

2.1 Objetivos generales.

Establecer el marco de referencia, las directrices y las acciones necesarias para garantizar la protección de los datos personales en posesión del Ayuntamiento de Benemérito de las Américas, mediante la implementación, operación, seguimiento y mejora continua de las medidas de seguridad administrativas, físicas y técnicas, para garantizar su confidencialidad, integridad y disponibilidad, en cumplimiento de los principios, deberes y obligaciones previstos en la normativa aplicable.

2.2 Objetivos específicos.

- **Identificar** las posibles vulnerabilidades, amenazas y riesgos de los que pueden ser objeto, en un plano general, los diversos sistemas de tratamiento de datos personales.
- **Mitigar** las vulnerabilidades, amenazas y riesgos identificados en los sistemas de tratamiento de datos personales.
- **Establecer e implementar** las medidas de seguridad administrativas, físicas y técnicas aplicables a los tratamientos de datos personales que realiza el Ayuntamiento, a fin de preservar su confidencialidad, integridad y disponibilidad, así como prevenir y reducir los riesgos asociados a dichos tratamientos.
- **Establecer planes de contingencia** adecuados para el caso de que se materialice alguna vulnerabilidad, amenaza o riesgo dentro de los sistemas de tratamiento de datos personales.
- **Dar cumplimiento y promover la mejora continua** de las obligaciones, controles y procesos en materia de protección de datos personales, mediante su seguimiento, evaluación y actualización, de conformidad con la normativa aplicable y las condiciones operativas del H. Ayuntamiento.



2.3 Alcances del documento.

El presente Documento de Seguridad se elabora conforme a lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas y demás normativa aplicable.

El alcance de este documento se refiere al conjunto de medidas, procedimientos y controles que el Ayuntamiento establece para garantizar la protección de los datos personales que trata en los sistemas de información, procesos administrativos o servicios a cargo de los órganos administrativos que conforman su estructura orgánica. Para determinar su ámbito de aplicación se considera el siguiente **Cuerpo Técnico Administrativo**:

1. **Presidencia.**
2. **Secretaría.**
3. **Obras Públicas.**
4. **Contraloría.**
5. **Tesorería.**
6. **Agua potable.**
7. **Panteones.**
8. **Calles, parques y jardines.**
9. **Asistencia a la salud.**
10. **Asistencia a la educación.**
11. **Asistencia agropecuaria.**

Dichos órganos administrativos, de acuerdo con el ámbito de su competencia y en el ejercicio de sus funciones, llevan a cabo el uso y tratamiento de datos personales, mismos que se encuentran bajo su estricta responsabilidad tanto en los medios electrónicos como



en los espacios físicos en que se administran, operan y resguardan. En consecuencia, el presente Documento comprende las áreas que integran dicho Cuerpo Técnico Administrativo, en la medida en que, de acuerdo con sus atribuciones, intervengan en la obtención, uso, conservación, organización, consulta, comunicación, resguardo o cualquier otra forma de tratamiento de datos personales.

Cada una de las áreas señaladas deberá observar, dentro del ámbito de sus atribuciones, las medidas de seguridad aplicables a los tratamientos que realice, atendiendo a la naturaleza de la información, los medios utilizados y los riesgos asociados. En este sentido, la Unidad de Transparencia integra el presente Documento con base en la información generada por las áreas, acorde al ámbito de sus funciones y de conformidad con las disposiciones aplicables, por lo que su alcance comprende los procesos, actividades, expedientes, documentos, archivos, sistemas, bases de datos y demás medios físicos o electrónicos en los que se realicen tratamientos de datos personales, con independencia del área que los genere, administre, utilice o resguarde.



3.- SISTEMA DE GESTIÓN DE SEGURIDAD DE LOS DATOS PERSONALES EN POSESIÓN DEL AYUNTAMIENTO DE BENEMÉRITO DE LAS AMÉRICAS.

Para el tratamiento de los datos personales que lleva a cabo el Ayuntamiento, mediante su obtención, uso, registro, organización, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable, se establecen políticas, procedimientos y mecanismos de seguridad orientados a garantizar su confidencialidad, integridad y disponibilidad. El presente apartado establece los elementos que integran el Sistema de Gestión de Seguridad, mediante el cual se articulan las acciones necesarias para identificar, evaluar, implementar, mantener, monitorear y mejorar dichas medidas.

Lo anterior se realiza en apego a los principios, deberes y obligaciones previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley General de Transparencia y Acceso a la Información Pública, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, así como demás disposiciones normativas aplicables en la materia.

En tal virtud, el Ayuntamiento inició su proceso de planificación de los esquemas de protección de datos mediante la identificación de los procesos y tareas en los que, de acuerdo con el ámbito de funciones de sus áreas, se involucra el tratamiento de datos personales. Para ello se dispuso de un instrumento homogéneo y estandarizado que permitió a los órganos administrativos realizar el levantamiento del inventario de los datos personales bajo su responsabilidad, considerando los elementos mínimos que establecen el artículo 27 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y el artículo 53 de los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas.

El inventario permitió identificar, entre otros aspectos, la categoría y tipo de datos sometidos a tratamiento, incluidos los de carácter sensible; los medios a través de los



cuales se obtienen; el sistema físico o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento; el nombre, cargo y adscripción de las personas servidoras públicas con acceso a los datos; y si son objeto de transferencia, así como los destinatarios y las causas que la justifican. Asimismo, contribuyó a considerar el ciclo de vida de los datos personales, de modo que quienes intervienen en el tratamiento conocen que, concluida la finalidad, los datos deben someterse a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, conforme a las disposiciones que regulan la gestión documental.



Confidencialidad · Integridad · Disponibilidad

Ciclo de vida de los datos personales

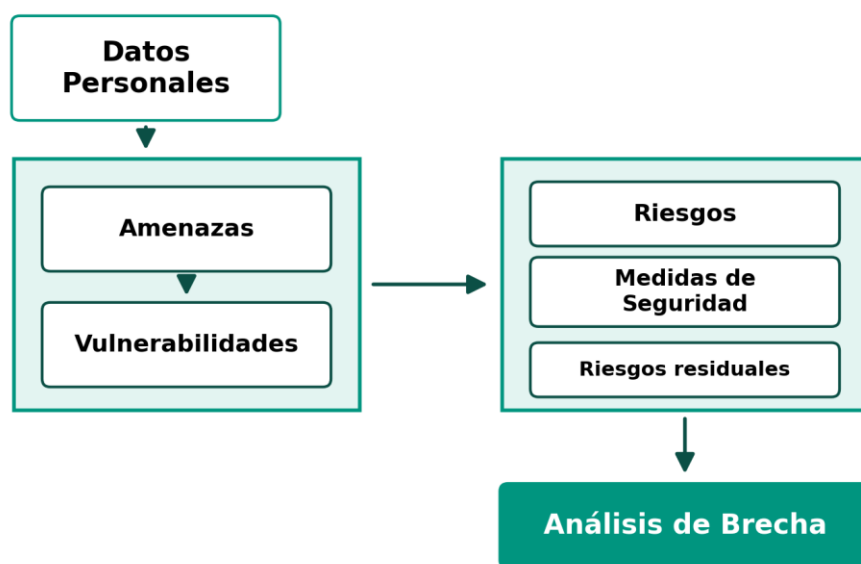
Una vez integrados los inventarios y en observancia del artículo 27, fracción IV, de la Ley local, las áreas responsables llevaron a cabo el análisis de riesgos, en el cual se evaluaron el valor de los datos personales en función de su categoría y ciclo de vida; el valor de exposición de los activos involucrados en el tratamiento; las posibles consecuencias para los titulares en caso de una vulneración de seguridad; y los factores de riesgo a los que se encuentra expuesta la información.

A partir de los resultados se realizó el análisis de brecha, mediante el cual se identifican las diferencias entre las medidas de seguridad implementadas y aquellas necesarias para atender los riesgos identificados. Con base en ello, además de promover el reconocimiento de las medidas de seguridad administrativas (conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información), físicas (acciones o mecanismos para proteger el entorno físico de los datos y de los recursos involucrados en su tratamiento) y técnicas (las que se valen de la tecnología para proteger



el entorno digital de la información), se identifican nuevas medidas que deberán desarrollarse para fortalecer los controles actualmente implementados, conforme al siguiente esquema:

ESQUEMA



El Sistema de Gestión de Seguridad de los Datos Personales deberá mantenerse actualizado y sujeto a seguimiento y evaluación periódica, considerando los cambios en los tratamientos, los medios utilizados, las condiciones de operación y los riesgos identificados.

En cumplimiento del deber de confidencialidad, el Ayuntamiento ha implementado mecanismos orientados a preservar la confidencialidad de los datos personales durante las diferentes fases de su tratamiento, entre los que se encuentran:

- **Cláusulas de confidencialidad.** Incorporación, cuando resulte aplicable, de cláusulas de confidencialidad en los contratos celebrados con encargados y con el personal del Ayuntamiento, mediante las cuales se establecen obligaciones relacionadas con la protección y confidencialidad de los datos personales a los que tengan acceso con motivo de sus funciones.



- **Capacitación y sensibilización.** Diseño de una propuesta de capacitación dirigida al personal del Ayuntamiento, orientada a generar conciencia sobre la importancia de preservar la confidencialidad de los datos personales, la cual se desarrolla en el apartado 10 de este Documento.

Con el propósito de adoptar un enfoque proactivo, es decir, identificar áreas de oportunidad en materia de seguridad de datos personales sin que éstas constituyan un daño efectivo, se listan como posibles **vulnerabilidades** las siguientes:

1. Falta de controles para acceder a los sistemas de tratamiento de datos personales.
2. Negligencia en el tratamiento de datos.
3. Reproducción no autorizada de los datos.
4. Destrucción total o parcial no autorizada.
5. Divulgación no autorizada de los datos.

Aunado a las anteriores vulnerabilidades, de manera enunciativa mas no limitativa, se examinan algunos tipos de **amenazas**, intencionales o no, a las que podría enfrentarse la institución y sus activos de información:

TIPO DE AMENAZAS
• Robo, extravío o copia no autorizada. • Uso, acceso o tratamiento no autorizado. • Daño, alteración o modificación no autorizada. • Pérdida o destrucción no autorizada. • Otras.

El riesgo que, de manera general, puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades es el de facilitar el acceso no autorizado a los datos personales con el fin de comprometer su confidencialidad, disponibilidad e integridad, por lo que las medidas de seguridad de las áreas están orientadas a protegerlos.



A partir de la identificación de vulnerabilidades y amenazas se han establecido medidas de seguridad generales que, de acuerdo con la experiencia y las mejores prácticas, son monitoreadas para lograr la mejora continua por parte de todos los involucrados en el tratamiento. Como parte del sistema de gestión y de la política de seguridad institucional, se enmarcan las políticas y procedimientos generales que se desarrollan en el presente Documento. Con base en lo anterior, el Ayuntamiento determina las pautas de acción del personal encargado del tratamiento, buscando en todo momento actuar conforme a la legislación vigente y a los Lineamientos de la materia, en consideración de la salvaguarda del derecho a la privacidad y a la protección de datos de las personas.



4.- INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO DEL AYUNTAMIENTO DE BENEMÉRITO DE LAS AMÉRICAS.

Por inventario de tratamiento de datos se entiende el control documentado del conjunto de operaciones que realizan los órganos administrativos del Ayuntamiento con motivo de los datos que se recaban de las personas, a través de procedimientos automatizados o físicos, que van desde su obtención, registro, organización, conservación, utilización, cesión, difusión e interconexión, hasta la rectificación, cancelación y oposición, con motivo de la atención del ejercicio de estos derechos en el ámbito de sus atribuciones.

Para el debido cumplimiento de las obligaciones del presente Documento fue necesario que cada una de las áreas que intervienen en el tratamiento de datos personales realizara un diagnóstico de los tratamientos que lleva a cabo en el ejercicio de sus atribuciones, mediante la integración de un inventario de datos personales y de los sistemas de tratamiento. La información contenida en dicho inventario constituye un elemento de referencia para la identificación de los riesgos, la determinación de las medidas de seguridad aplicables y la actualización de este Documento, por lo que deberá mantenerse actualizada conforme a las modificaciones que se presenten en los tratamientos y en los sistemas o medios utilizados.

En coordinación con los órganos administrativos y derivado del proceso de actualización de información, se advirtió que **tres (03) áreas** del Ayuntamiento llevan a cabo tratamiento de datos personales:

- 1. Secretaría Municipal.**
- 2. Tesorería Municipal.**
- 3. Contraloría Municipal.**

En el ejercicio de sus atribuciones se identificaron **10 procesos** en cuyo cauce se actualiza algún tratamiento de datos personales. Cada área realiza el tratamiento con una finalidad definida por sus funciones, tal como se señala en el siguiente cuadro:



Órgano administrativo	Proceso o tratamiento	Finalidad
Secretaría Municipal	1. Registro de Fierro Marcador de Ganado.	Otorgar una constancia con la que se comprueba que el fierro marcador de ganado fue registrado en los libros de actas.
	2. Expedición de Constancias (incluye constancias de domicilio).	• Expedición de Cartilla Militar. • Constancia de origen (para la elaboración de acta de nacimiento y su aclaración). • Constancias de bajos recursos (beca y pediátrico). • Constancia de dependencia económica. • Constancia de extranjero. • Constancia de no reclutamiento. • Constancia de residencia. • Constancia de vecindad. • Constancia de inscripción a la Junta Municipal de Reclutamiento.
Tesorería Municipal	3. Procedimiento de viáticos y pasajes.	Llevar el control de las comisiones, verificar que sean oficiales y que los viáticos se otorguen con base en los días comisionados.
	4. Registro en el Sistema Integral de Administración Hacendaria Municipal (SIAHM).	Conformar la Cuenta Pública Municipal de Benemérito de las Américas, Chiapas, con base en la normatividad vigente.



Órgano administrativo	Proceso o tratamiento	Finalidad
	5. Integración de la cuenta pública municipal.	Integrar la Cuenta Pública Municipal de Benemérito de las Américas, Chiapas, con base en la normatividad vigente.
	6. Integración de soporte de pago de los gastos ejecutados con aportaciones federales FAISMUN.	Integrar el soporte de pago de los gastos ejecutados con aportaciones federales FAISMUN.
	7. Integración de soporte de pago de los gastos ejecutados con aportaciones federales FORTAMUN.	Integrar el soporte de pago de los gastos ejecutados con aportaciones federales FORTAMUN.
	8. Elaboración de orden de pago por bienes o servicios prestados por diferentes proveedores.	Elaborar la orden de pago de bienes o servicios prestados por diferentes proveedores.
Contraloría Municipal	9. Atención de procedimientos administrativos.	Integrar los procedimientos administrativos originados a partir de las investigaciones realizadas, para iniciar e investigar los procedimientos de responsabilidad administrativa cuando se trate de actos u omisiones que puedan constituir faltas administrativas no graves, faltas administrativas graves o faltas de particulares, derivadas de actos u omisiones de las personas servidoras públicas de la Administración Pública Municipal.



Órgano administrativo	Proceso o tratamiento	Finalidad
	10. Declaraciones patrimoniales.	Llevar el registro de las declaraciones patrimoniales de cada persona servidora pública de la Administración Pública Municipal, conforme a la evolución patrimonial (inicial, modificación y conclusión) y de intereses, verificando los datos manifestados relacionados con el patrimonio y sus dependientes económicos.

Los datos personales se obtienen **directamente de la persona titular**, por los siguientes medios:

- De manera personal, con la presencia física de la persona titular de los datos personales o de su representante, en su caso.
- Por correo electrónico.
- Por escrito presentado directamente en las oficinas del sujeto obligado.

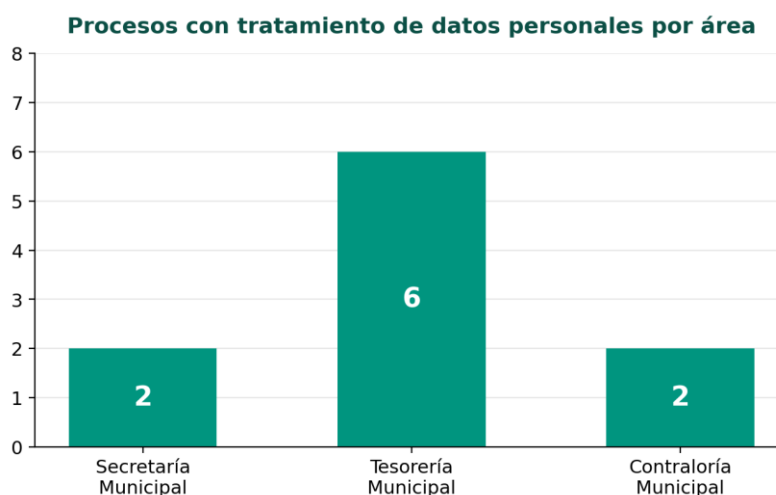
El tratamiento se realiza conforme a la normativa aplicable y a las atribuciones de cada área. Durante el proceso de sistematización se observó que los datos personales tratados en los 10 procesos identificados corresponden a las siguientes tres categorías:

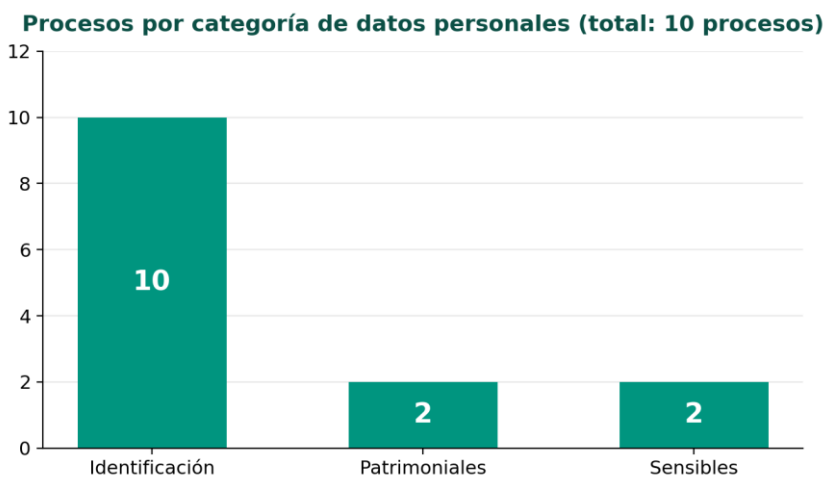
1. De identificación	Nombre, domicilio, CURP, fotografía, huella digital, edad, clave de elector, estado civil, RFC, correo electrónico personal, teléfono, sexo, información académica, fecha y lugar de nacimiento, número de seguridad social, antecedentes laborales, beneficiarios, curriculum vitae, nacionalidad, ocupación, cédula y títulos profesionales.
-----------------------------	--



2. Patrimoniales	Cuentas bancarias, estados de cuenta, CLABE interbancaria, institución bancaria, facturas y descuentos personales (ahorro voluntario, hipoteca, seguro médico, entre otros).
3. Sensibles	Pertenencia a un pueblo o comunidad indígena, condición de discapacidad y situación de vulnerabilidad.

De los 10 procesos identificados, 02 corresponden a la Secretaría Municipal, 06 a la Tesorería Municipal y 02 a la Contraloría Municipal. Se identificó el tratamiento de datos personales de identificación en los 10 procesos (100%), de datos patrimoniales en 02 (20%) y de datos personales sensibles en 02 (20%), conforme a la información registrada para cada tratamiento. Esta distribución constituye un elemento del diagnóstico institucional y sirve de base para determinar las medidas de seguridad aplicables, atendiendo a la naturaleza de los datos, las características de cada tratamiento y los riesgos asociados.





A partir de lo anterior, el Inventario de Datos Personales del Ayuntamiento posibilitó la identificación de hallazgos en relación con el tratamiento de datos personales, aportando los elementos que permiten focalizar las áreas con mayor incidencia en el tratamiento, en particular la Tesorería Municipal, y con ello enfocar los trabajos de atención para el cumplimiento de las disposiciones jurídicas en materia de protección de datos, aplicando medidas de seguridad acordes con el nivel de riesgo asociado a cada tratamiento.



5.- FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES.

Como resultado de la identificación de los procesos en los que intervienen datos personales, relacionados en el Inventario de Datos Personales, resulta importante vincular estas actividades con las funciones y facultades que la normatividad municipal aplicable otorga a las personas servidoras públicas responsables de dicho tratamiento, a fin de dar cumplimiento al principio de legalidad que debe atender todo servidor público y delimitar el tratamiento al ejercicio de las funciones institucionales conferidas a cada área.

A continuación, se presentan las personas servidoras públicas que, en los órganos administrativos del Cuerpo Técnico Administrativo del Ayuntamiento, llevan a cabo tratamientos de datos personales:

Órgano administrativo	Nombre y cargo de la persona servidora pública que trata los datos personales	Proceso o tratamiento
Secretaría Municipal	C. José Dagoberto Martínez Antonio Secretario Municipal	• Registro de Fierro Marcador de Ganado. • Expedición de Constancias (incluye constancias de domicilio).



Órgano administrativo	Nombre y cargo de la persona servidora pública que trata los datos personales	Proceso o tratamiento
Tesorería Municipal	C. Eliana Jeronimó Mejía Tesorera Municipal	• Procedimiento de viáticos y pasajes. • Registro en el Sistema Integral de Administración Hacendaria Municipal (SIAHM). • Integración de la cuenta pública municipal. • Integración de soporte de pago de los gastos ejecutados con aportaciones federales FAISMUN. • Integración de soporte de pago de los gastos ejecutados con aportaciones federales FORTAMUN. • Elaboración de orden de pago por bienes o servicios prestados por diferentes proveedores.
Contraloría Municipal	Lic. Amer Díaz Zea Contralor Municipal	• Atención de procedimientos administrativos. • Declaraciones patrimoniales.

Las personas servidoras públicas que traten datos personales tendrán, de manera general, las siguientes obligaciones:

- Tratar los datos personales únicamente para las finalidades registradas en el inventario y dentro del ámbito de sus atribuciones.
- Guardar confidencialidad respecto de los datos personales a los que tengan acceso y abstenerse de difundirlos, transferirlos o ponerlos a disposición de personas no autorizadas.



- Aplicar las medidas de seguridad administrativas, físicas y técnicas establecidas en este Documento.
- Reportar de manera inmediata al superior jerárquico cualquier extravío, robo, alteración o acceso no autorizado a documentos, equipos o sistemas que contengan datos personales.
- Participar en las acciones de capacitación y sensibilización en materia de protección de datos personales.
- Mantener actualizada la información del inventario respecto de los tratamientos a su cargo y atender las acciones de mejora derivadas de los análisis de riesgos y de brecha.



6.- ANÁLISIS DE RIESGOS Y DE BRECHA.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.



7.- GESTIÓN DE VULNERACIONES Y PLAN DE CONTINGENCIA.

Sección Clasificada del Documento de Seguridad, apartado de Gestión y Plan de Contingencia.

Se testa el apartado número 7, que contiene la Gestión de Vulneraciones y Plan de contingencia, toda vez que contiene información sensible sobre la forma en que el sujeto obligado previene, detecta, contiene, responde y recupera la operación ante incidentes de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.



8.- MEDIDAS DE SEGURIDAD GENERALES.

Las medidas de seguridad son definidas por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas como el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales.

Las medidas generales de seguridad administrativas, físicas y técnicas que el Ayuntamiento de Benemérito de las Américas aplica y procura fortalecer para mantener la confidencialidad e integridad de la información, proteger los datos personales contra daño, pérdida, destrucción o alteración, evitar el uso, acceso o tratamiento no autorizado e impedir la divulgación no autorizada, son las siguientes:

8.1 Medidas administrativas.

Son el conjunto de políticas, procedimientos, mecanismos y acciones organizacionales destinadas a garantizar que el tratamiento de los datos personales se realice conforme a la normativa aplicable y a prevenir vulneraciones de seguridad, así como la identificación, clasificación y borrado seguro de la información y la sensibilización y capacitación del personal.

1. Resguardo de los expedientes en archiveros del área, bajo los criterios, directrices y lineamientos establecidos en la legislación archivística vigente.
2. Identificación y puesta a resguardo de los datos personales por parte del personal encargado de su tratamiento.
3. Implementación de formatos de entrada y salida para el préstamo de documentos que contengan datos personales.
4. Cursos de inducción al personal encargado del tratamiento sobre los procedimientos de las actividades que realizan y sobre protección de datos personales, así como capacitación y sensibilización periódica en la materia.



5. Clasificación de la información en términos de las disposiciones previstas en la normatividad aplicable.
6. Generación de los avisos de privacidad respectivos.
7. Conocimiento y cumplimiento de los principios, deberes, procedimientos y demás obligaciones inherentes a la materia, así como de las sanciones por su incumplimiento.
8. Definición de los roles que desempeñan las personas servidoras públicas que tratan datos personales y de las responsabilidades por su incumplimiento.
9. Procedimientos para el alta, modificación y baja de usuarios con acceso a los sistemas de tratamiento.
10. Reporte al superior jerárquico de los incidentes detectados de pérdida o alteración de documentos que contengan datos personales, y procedimiento para el registro, atención, documentación y seguimiento de incidentes y vulneraciones de seguridad.
11. Análisis de riesgos, evaluaciones y revisiones periódicas de las medidas de seguridad y del cumplimiento de las políticas y controles.
12. Implementación de acciones correctivas y preventivas derivadas de revisiones, incidentes o vulneraciones, y reuniones de seguimiento para evaluar la eficacia de las medidas y promover la mejora continua.
13. Vista a la Contraloría Municipal cuando se detecten hechos u omisiones que puedan constituir responsabilidades administrativas derivadas de una vulneración de datos personales.

8.2 Medidas físicas.

Son los controles implementados para proteger las instalaciones, los equipos, los documentos y demás soportes físicos que contienen datos personales, con el fin de prevenir el acceso, uso, daño, pérdida, alteración o destrucción no autorizados, aplicados



como medida de prevención contra posibles amenazas a los recursos y a cualquier información de carácter confidencial del Ayuntamiento.

1. Resguardo de documentos e información en archivos físicos de trámite y concentración.
2. Mobiliario con chapas con llave, a fin de mantener el control de acceso de personas a los espacios de resguardo de información.
3. Limitación del número de personas con acceso a los archivos físicos y resguardo de llaves en oficinas de acceso restringido.
4. Registro de las personas que consultan los expedientes, con identificación de su área de adscripción.
5. Suscripción, en la medida de lo posible, de responsivas de confidencialidad con el personal que trata datos personales.
6. Cultura de escritorios limpios, retirando al término de las labores los documentos o dispositivos que contengan datos personales para evitar su extravío o mal uso, y mantenimiento de impresoras y escáneres libres de documentos con datos personales.
7. Autorización previa para la salida de equipos o soportes que contengan datos personales, con registro y control de su préstamo, asignación, traslado y devolución, y medidas de protección física durante el traslado, evitando dejarlos sin supervisión o en lugares inseguros.
8. Procedimientos de borrado seguro de los equipos de cómputo, dispositivos móviles y demás medios de almacenamiento que contengan datos personales, que impidan la recuperación de la información antes de su reutilización, reasignación, mantenimiento, baja o disposición final.
9. Mantenimiento y respaldos periódicos de la información institucional.
10. Extintores de incendio cercanos a las áreas donde se resguardan datos personales.



11. Obligación de reportar de manera inmediata el extravío, robo o acceso no autorizado a cualquier recurso o soporte que contenga datos personales.

8.3 Medidas técnicas.

Son el conjunto de acciones, mecanismos y controles que, mediante el uso de tecnologías de hardware y software, tienen como finalidad proteger el entorno digital, los sistemas de información, las redes y los recursos involucrados en el tratamiento de datos personales, preservando su **confidencialidad, integridad y disponibilidad**, así como prevenir accesos, modificaciones, pérdidas o divulgaciones no autorizadas. Para tal efecto se establecen las siguientes medidas:

1. **Control de acceso:** el acceso a sistemas, equipos, archivos y recursos que contengan datos personales deberá realizarse de acuerdo con las funciones y responsabilidades de cada persona servidora pública, bajo los principios de mínimo privilegio y necesidad de conocer.
2. **Administración de privilegios basada en roles:** los privilegios deberán ser autorizados por la persona titular del área correspondiente, documentados, revisados periódicamente y revocados de forma inmediata cuando cambien las funciones de la persona usuaria o concluya su relación con el Ayuntamiento.
3. **Gestión de usuarios y contraseñas:** las cuentas y contraseñas serán personales e intransferibles; se definirán políticas de contraseñas y los permisos de acceso se modificarán, restringirán o cancelarán cuando cambien las funciones de la persona usuaria o concluya su relación laboral o administrativa. Se deshabilitarán las cuentas del personal que cause baja, para lo cual el área deberá notificarlo oportunamente.
4. **Autenticación y registro de actividades:** se implementarán mecanismos que aseguren la identidad de la persona usuaria y bitácoras que permitan identificar quién accedió, fecha y hora, información consultada o modificada e intentos fallidos de acceso.



5. **Protección de credenciales:** las personas usuarias informarán de inmediato cualquier sospecha de pérdida, divulgación, uso indebido o compromiso de sus credenciales de acceso, o que hayan sido utilizadas por un tercero.
6. **Uso del correo electrónico institucional:** deberá utilizarse preferentemente para fines institucionales; el envío de datos personales se limitará a los casos necesarios para el cumplimiento de las funciones y se realizará con las medidas de seguridad correspondientes.
7. **Resguardo de información electrónica:** los documentos y archivos electrónicos con datos personales se conservarán en los sistemas, equipos o medios institucionales destinados para tal efecto, con acceso restringido al personal autorizado.
8. **Resguardo de documentación física:** los documentos físicos con datos personales se mantendrán en espacios que restrinjan su acceso a personas no autorizadas, como archiveros, cajones o espacios bajo llave.
9. **Restricción de divulgación:** la información con datos personales no deberá compartirse, difundirse, transferirse o ponerse a disposición de personas no autorizadas, por medios electrónicos o físicos.
10. **Impresión y reproducción de documentos:** la impresión, digitalización o copia de documentos con datos personales se realizará solo cuando sea necesario para las funciones institucionales, evitando dejar documentos expuestos en impresoras, escáneres o áreas de uso común.
11. **Respallos de información:** se realizarán respaldos de la información electrónica con datos personales, de acuerdo con las necesidades institucionales y los recursos tecnológicos disponibles, para favorecer su disponibilidad y recuperación ante incidentes.
12. **Actualización y protección de sistemas:** los sistemas, equipos y herramientas utilizados para el tratamiento se mantendrán, en la medida de las capacidades institucionales, actualizados y protegidos; la instalación de programas o software será responsabilidad exclusiva del personal designado para el soporte informático.



13. Auditorías y revisión de controles: se procurará la definición de procedimientos y controles de seguridad de la información y su revisión periódica mediante auditorías.

Las medidas señaladas deberán aplicarse de manera proporcional a los riesgos asociados al tratamiento de los datos personales y mantenerse sujetas a revisión y actualización conforme a las necesidades y condiciones tecnológicas del Ayuntamiento.



9.- PLAN DE TRABAJO.

Sección Clasificada del Documento de Seguridad, apartado del Plan de Trabajo.

Se testa el apartado número 9, que contiene el Plan de Trabajo, en virtud de ser un instrumento de gestión que deriva del análisis de riesgo y del análisis de brecha, en él se establecen las acciones específicas que el sujeto obligado implementará para corregir deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de datos personales, de conformidad con lo dispuesto en los artículos 103, fracción III, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo trigésimo octavo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.



10.- PROGRAMA DE CAPACITACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

La capacitación constituye un elemento estratégico para el fortalecimiento del Sistema de Gestión de Seguridad de Datos Personales, ya que permite que las personas servidoras públicas adquieran, actualicen y fortalezcan los conocimientos, habilidades y competencias necesarias para desempeñar adecuadamente las funciones relacionadas con el tratamiento de datos personales, en estricto apego a la normativa aplicable.

En materia de protección de datos personales, la capacitación permanente es un mecanismo indispensable para asegurar la correcta implementación de las medidas de seguridad administrativas, físicas y técnicas; fortalecer la actualización y mejora continua de los inventarios y sistemas de tratamiento; promover el cumplimiento de los principios, deberes y obligaciones previstos en la legislación aplicable; y fomentar una cultura institucional de protección de datos personales entre el personal que interviene en su tratamiento.

En este sentido, el Ayuntamiento contempla el diseño e implementación de un Programa Institucional de Capacitación especializado, dirigido a las personas servidoras públicas que, de acuerdo con sus funciones, participen en el tratamiento de datos personales, con el propósito de fortalecer sus capacidades técnicas y operativas y de homologar los criterios institucionales para la aplicación de la normativa y de las medidas de seguridad. El programa deberá considerar las necesidades institucionales y actualizarse conforme a los cambios normativos, operativos y de los sistemas de tratamiento. De manera enunciativa mas no limitativa, se propone abordar los siguientes contenidos temáticos:

I. Introducción al derecho a la protección de datos personales

1. Marco conceptual.
2. Principios aplicables al tratamiento de datos personales.
3. Deberes de los sujetos obligados.
4. Sistemas de tratamiento de datos personales.



5. Medidas de seguridad administrativas, físicas y técnicas.
6. Avisos de privacidad y derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).
7. Procedimientos de tutela, medios de impugnación y régimen de responsabilidades.

II. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados

1. Antecedentes y evolución normativa.
2. Ámbito de aplicación.
3. Objeto y finalidad de la Ley.
4. Principales obligaciones de los sujetos obligados.
5. Responsabilidades y consecuencias derivadas del incumplimiento.

III. Programa Institucional de Protección de Datos Personales

1. Sistemas de tratamiento de datos personales.
2. Inventario de datos personales y bases de datos.
3. Documento de Seguridad.
4. Medidas de seguridad administrativas, físicas y técnicas.
5. Análisis de brecha y análisis de riesgos.
6. Funciones y responsabilidades de las personas servidoras públicas que intervienen en el tratamiento de datos personales.
7. Prevención y atención de vulneraciones de seguridad.
8. Acciones de monitoreo, supervisión y mejora continua del Sistema de Gestión de Seguridad de Datos Personales.

La capacitación deberá formar parte de las acciones de seguimiento y mejora continua del Sistema de Gestión de Seguridad de los Datos Personales en Posesión del Ayuntamiento



de Benemérito de las Américas, procurando su actualización y aplicación conforme a las necesidades de las áreas involucradas.

DOCUMENTO DE SEGURIDAD		
SISTEMA DE DATOS PERSONALES DEL AYUNTAMIENTO DE BENEMÉRITO DE LAS AMÉRICAS		
	Fecha de elaboración del Documento de Seguridad: 15 de Septiembre de 2026	Fecha de última actualización del Documento de Seguridad: 15 de septiembre de 2026
	Elaboró: C.P. Suly Fany Díaz Moreno Responsable de la Unidad de Transparencia del Ayuntamiento	Aprobó: C. Juan Gómez Morales Presidente Municipal de Benemérito de las Américas

