

DOCUMENTO DE SEGURIDAD

H. AYUNTAMIENTO DE ACAPETAHUA, CHIAPAS.
UNIDAD DE TRANSPARENCIA

PROTECCIÓN DE
DATOS PERSONALES



ÍNDICE

1. INTRODUCCIÓN.....	2
2. -OBJETIVOS Y ALCANCES DEL DOCUMENTO.	3
2.1.- Objetivos generales.....	3
2.2.- Objetivos específicos.....	3
2.3.- Alcance del documento.	3
3. - SISTEMA DE GESTIÓN DE SEGURIDAD DE LOS DATOS PERSONALES EN POSESIÓN DEL H. AYUNTAMIENTO DE ACAPETAHUA CHIAPAS.....	5
4. - INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.	9
CATEGORÍAS DE DATOS PERSONALES	13
5. - FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES.	16
6. - ANALÍSIS DE RIESGO Y BRECHA	19
7. - GESTIÓN DE VULNERACIONES Y PLAN DE CONTINGENCIA.....	27
8. - MEDIDAS DE SEGURIDAD GENERALES	29
A. Medidas administrativas.....	29
B. Medidas físicas	30
C. Medidas técnicas.....	30
- MONITOREO DE LAS MEDIDAS DE SEGURIDAD	32
9. - PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD.....	34
10. - PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES.....	36
11. - ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD.....	39
12. - VIGENCIA, APROBACIÓN Y OBSERVANCIA DEL DOCUMENTO DE SEGURIDAD ...	40



1. INTRODUCCIÓN

Este Documento de Seguridad para los Sistemas de Datos Personales en medios físicos tiene por objeto establecer las disposiciones y medidas necesarias para garantizar la adecuada protección de los datos personales que se encuentran bajo resguardo y tratamiento del H. Ayuntamiento Municipal de Acapetahua, Chiapas, de conformidad con la legislación aplicable en materia de protección de datos personales. La elaboración y aprobación del presente instrumento se realiza en cumplimiento de lo establecido en el artículo 55 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, disposición que establece la responsabilidad de los sujetos obligados de contar con un Documento de Seguridad que contemple las medidas de carácter administrativo, físico y técnico necesarias

para salvaguardar la información personal. En este sentido, el Documento establece los criterios, procedimientos y medidas de protección que deberán observarse en el tratamiento de los datos personales contenidos en los sistemas físicos del Ayuntamiento, con la finalidad de prevenir su pérdida, alteración, destrucción, acceso, uso o tratamiento no autorizado.

Se busca fortalecer los mecanismos internos de seguridad y control, promoviendo que el tratamiento de los datos personales se realice de manera responsable y conforme a los principios establecidos en la normativa aplicable, particularmente los principios de licitud, consentimiento, calidad, confidencialidad, seguridad, disponibilidad y temporalidad. El presente instrumento también contempla la estructura organizacional y funcional relacionada con el tratamiento de datos personales, identificando las áreas, puestos y niveles jerárquicos que, de acuerdo con sus atribuciones y responsabilidades, tienen acceso o intervienen en el manejo de información personal. Esto permitirá establecer con mayor claridad las obligaciones y responsabilidades del personal autorizado, así como las medidas de seguridad que deberán observarse dentro de cada área.

El Documento de Seguridad deberá considerarse como un instrumento de carácter dinámico, sujeto a revisión y actualización cuando existan modificaciones en la estructura administrativa del Ayuntamiento, en los sistemas de tratamiento, en los procedimientos internos o en las disposiciones legales aplicables. Lo anterior permitirá mantener vigentes las medidas de seguridad implementadas y garantizar una protección adecuada de los datos personales durante todo su ciclo de tratamiento. Con estas acciones, el H. Ayuntamiento Municipal de Acapetahua, Chiapas, reafirma su compromiso con la protección de los datos personales que se encuentran bajo su responsabilidad, procurando que su tratamiento se realice de manera segura, responsable y apegada a la normativa vigente.



2. -OBJETIVOS Y ALCANCES DEL DOCUMENTO.

2.1.- Objetivos generales.

Tiene como objetivo establecer las bases, criterios y mecanismos necesarios para garantizar la adecuada protección de los datos personales que se encuentran bajo posesión y responsabilidad del H. Ayuntamiento Municipal de Acapetahua, Chiapas, en cumplimiento de las obligaciones previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), los Lineamientos Generales y demás disposiciones normativas aplicables.

2.2.- Objetivos específicos.

- **Identificar áreas responsables:** Localizar las unidades administrativas que manejan datos personales.
- **Asignar roles:** Definir quiénes son los responsables y usuarios autorizados de la información.
- **Establecer controles:** Fijar las medidas de seguridad y los mecanismos de monitoreo para su aplicación correcta.
- **Gestionar riesgos:** Detectar riesgos y brechas de seguridad para tomar decisiones de mejora continua.
- **Capacitar al personal:** Fomentar una cultura de buenas prácticas y conciencia sobre el manejo de la información.

2.3.- Alcance del documento.

El Documento de Seguridad será aplicable a todas las unidades administrativas del H. Ayuntamiento Municipal de Acapetahua, Chiapas, que, en el ejercicio de sus atribuciones, realicen actividades relacionadas con la obtención, uso, almacenamiento, consulta, conservación, transmisión o cualquier otra forma de tratamiento de datos personales.

Su alcance comprende los sistemas y procesos que involucren datos personales, tanto en medios físicos como electrónicos, así como los espacios en los que dicha información sea recibida, utilizada, resguardada o administrada. Todas las áreas



deberán observar los principios, deberes y obligaciones establecidos en la legislación vigente en materia de protección de datos personales. Quedan fuera del alcance de este instrumento aquellos datos personales que se encuentren sujetos

a las obligaciones específicas en materia de transparencia y acceso a la información pública, de conformidad con la legislación aplicable.

Las unidades administrativas del H. Ayuntamiento de Acapetahua, Chiapas, que deberán observar las disposiciones de este Documento son:

No.	UNIDAD ADMINISTRATIVA
1	PRESIDENCIA MUNICIPAL
2	SINDICATURA MUNICIPAL
3	CONTRALORIA MUNICIPAL
4	SECRETARIA MUNICIPAL
5	TESORERIA MUNICIPAL
6	DIRECCIÓN DE OBRAS PÚBLICAS
7	FOMENTO AGROPECUARIO
8	UNIDAD DE TRANSPARENCIA
9	CONSEJO MUNICIPAL DE SEGURIDAD PÚBLICA
10	SEGURIDAD PÚBLICA MUNICIPAL
11	JUZGADO MUNICIPAL
12	SISTEMA PARA EL DESARROLLO INTEGRAL DE LA FAMILIA (DIF)
13	COPLADEM

Asimismo, cualquier otra unidad administrativa que forme parte de la estructura del Ayuntamiento y que realice actividades de tratamiento de datos personales deberá cumplir con las disposiciones establecidas en este instrumento de seguridad.



3. - SISTEMA DE GESTIÓN DE SEGURIDAD DE LOS DATOS PERSONALES EN POSESIÓN DEL H. AYUNTAMIENTO DE ACAPETAHUA CHIAPAS.

De conformidad con los artículos 77 y 78 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, el Comité de Transparencia del H. Ayuntamiento Municipal de Acapetahua, Chiapas, es la máxima autoridad interna en materia de protección de datos personales y tendrá a su cargo coordinar y supervisar las acciones necesarias para garantizar su adecuada protección.

Entre sus principales responsabilidades se encuentran:

- Coordinar y supervisar las acciones relacionadas con la protección de datos personales.
- Vigilar el cumplimiento de las medidas de seguridad establecidas en el presente Documento.
- Promover programas de capacitación para el personal que intervenga en el tratamiento de datos personales.
- Dar seguimiento a las obligaciones y resoluciones relacionadas con la protección de datos personales.
- Informar al órgano interno de control cuando tenga conocimiento de posibles irregularidades en el tratamiento de datos personales, conforme a la legislación aplicable.

Las unidades administrativas serán responsables de aplicar las medidas de seguridad correspondientes y de garantizar que los datos personales sean tratados únicamente para las finalidades y dentro de las atribuciones que correspondan.

La Unidad de Transparencia tendrá las atribuciones previstas en el artículo 79 de la Ley, brindando orientación y apoyo en el ejercicio de los Derechos ARCO y en las demás obligaciones relacionadas con la protección de datos personales.

Las personas servidoras públicas que tengan acceso o intervengan en el tratamiento de datos personales deberán cumplir con las medidas de seguridad establecidas en este Documento y mantener la debida confidencialidad de la información.

De acuerdo con el artículo 29 de la Ley, deberán identificarse las funciones y obligaciones del personal que participe en el tratamiento de datos personales, por lo que cada área deberá establecer las responsabilidades que correspondan a sus servidores públicos.



El H. Ayuntamiento Municipal de Acapetahua, Chiapas, establecerá y mantendrá mecanismos para garantizar la adecuada protección de los datos personales que se encuentren bajo su responsabilidad, desde su obtención hasta su eliminación, conservación o cualquier otra forma de tratamiento, procurando en todo momento preservar su confidencialidad, integridad y disponibilidad. Para ello, las unidades administrativas identificarán los procesos y actividades en los que se realice tratamiento de datos personales, considerando las funciones que les corresponden y las finalidades para las cuales la información es obtenida.

Como parte del sistema de gestión, se realizarán análisis de riesgos y de brecha, con la finalidad de identificar las amenazas y vulnerabilidades que puedan afectar los datos personales, así como determinar las medidas de seguridad necesarias para disminuir los riesgos identificados.

Las medidas de seguridad podrán ser de carácter administrativo, físico y técnico, y estarán orientadas a prevenir situaciones como el robo, extravío, pérdida, alteración, destrucción, acceso, uso o tratamiento no autorizado de los datos personales.

Las unidades administrativas deberán mantener controles adecuados para proteger la información y procurar la mejora continua de las medidas implementadas. Asimismo, deberán promover entre el personal una cultura de protección de datos personales y establecer claramente las funciones y responsabilidades de quienes intervengan en su tratamiento.

En el marco de este sistema de gestión, el Ayuntamiento procurará:

- Tratar los datos personales de manera lícita y conforme a las disposiciones aplicables.
- Utilizar los datos únicamente para las finalidades que justificaron su obtención.
- Procurar que los datos personales sean adecuados, correctos y, cuando corresponda, actualizados.
- Mantener la confidencialidad y seguridad de la información durante su ciclo de vida.
- Respetar los derechos de las personas titulares de los datos personales.
- Identificar al personal autorizado para intervenir en el tratamiento de los datos.
- Implementar medidas administrativas, físicas y técnicas para prevenir vulneraciones.
- Capacitar y sensibilizar al personal respecto de sus obligaciones en materia de protección de datos personales.



Con estas acciones, el H. Ayuntamiento Municipal de Acapetahua, Chiapas, fortalecerá la gestión y protección de los datos personales bajo su responsabilidad, mediante la identificación de riesgos, la implementación de medidas de seguridad y la revisión periódica de los controles establecidos.

ESQUEMA



la identificación de vulnerabilidades tiene por objeto prevenir posibles dificultades en la seguridad de los datos bajo un enfoque proactivo; es decir, identificar áreas de oportunidad en materia de seguridad de datos personales sin que éstas constituyan un daño efectivo, es que 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.



La determinación del nivel de riesgo deberá considerar tanto la probabilidad de que ocurra una vulneración como el impacto que esta pudiera generar en las personas titulares.

Se muestra el ciclo de vida de los datos personales:



Entre las principales amenazas que deberán considerarse dentro del análisis se encuentran:

- Robo, extravío o copia no autorizada de los datos personales.
- Acceso, uso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizada de la información.
- Pérdida o destrucción de los datos personales.

A partir de los resultados obtenidos, el H. Ayuntamiento Municipal de Acapetahua, Chiapas, podrá determinar las medidas de seguridad que deberán implementarse o fortalecerse en cada unidad administrativa, así como las acciones necesarias para atender las deficiencias identificadas mediante el análisis de brecha.



Los resultados de ambos análisis deberán servir como base para la elaboración y seguimiento del plan de trabajo correspondiente, procurando que las medidas de seguridad sean revisadas y mejoradas de manera periódica. De esta forma, el Ayuntamiento podrá fortalecer progresivamente la protección de los datos personales y mantener condiciones adecuadas de confidencialidad, integridad y disponibilidad de la información bajo su responsabilidad.

4. - INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

Para cumplir adecuadamente con las obligaciones en materia de protección de datos personales, cada unidad administrativa del H. Ayuntamiento Municipal de Acapetahua, Chiapas, deberá identificar y documentar los tratamientos de datos personales que realiza en el ejercicio de sus atribuciones.

Las unidades administrativas que realicen tratamientos de datos personales deberán proporcionar y mantener actualizada la información correspondiente a los sistemas y procesos que se encuentren bajo su responsabilidad.

De manera inicial, se consideran sujetas a la identificación y registro de tratamientos de datos personales las siguientes áreas del Ayuntamiento:

No.	UNIDAD ADMINISTRATIVA
1	PRESIDENCIA MUNICIPAL
2	SINDICATURA MUNICIPAL
3	CONTRALORIA MUNICIPAL
4	SECRETARIA MUNICIPAL
5	TESORERIA MUNICIPAL
6	DIRECCIÓN DE OBRAS PÚBLICAS
7	FOMENTO AGROPECUARIO
8	UNIDAD DE TRANSPARENCIA
9	CONSEJO MUNICIPAL DE SEGURIDAD PÚBLICA
10	SEGURIDAD PÚBLICA MUNICIPAL
11	JUZGADO MUNICIPAL
12	SISTEMA PARA EL DESARROLLO INTEGRAL DE LA FAMILIA (DIF)
13	COPLADEM



Los tratamientos de datos personales deberán realizarse únicamente dentro del ámbito de las atribuciones y funciones conferidas a cada unidad administrativa, observando los principios, deberes y obligaciones establecidos en la legislación aplicable.

Mediante la información recabada fue posible identificar **53** procesos que desarrollan y utilizan el tratamiento de datos personales, se describen los siguientes;

ÁREA	PROCESO O TRATAMIENTO
PRESIDENCIA MUNICIPAL	EN ESTA UNIDAD ADMINISTRATIVA SE REALIZA LO SIGUIENTE: 1. ATENCION A LA CIUDADANIA
SINDICATURA MUNICIPAL	LOS TRATAMIENTOS IDENTIFICADOS CORRESPONDEN A: 2. JUICIOS LABORALES 3. JUICIOS ADMINISTRATIVOS 4. PROCEDIMIENTOS ADMINISTRATIVOS
CONTRALORIA MUNICIPAL	ESTA AREA REALIZA ACTIVIDADES RELACIONADAS CON: 5. PROCESO DE ENTREGA-RECEPCION 6. DECLARACION DE SITUACION PATRIMONIAL 7. CONTROL DE INVENTARIO
SECRETARIA MUNICIPAL	LOS PROCESOS IDENTIFICADOS SON: 8. CONVENIOS 9. ELABORACION DE CONSTANCIAS 10. REGISTRO DE FIERRO MARCADOR 11. ELABORACION DE NOMBRAMIENTOS 12. ACTAS DE CABILDO 13. TRAMITE DE CARTILLA DE SERVICIO MILITAR 14. PERMISOS DE EVENTOS 15. LICENCIAS DE NEGOCIOS



TESORERIA MUNICIPAL	EN ESTA AREA SE IDENTIFICAN LOS SIGUIENTES PROCESOS: 16. NOMINA DE PERSONAL 17. EXPEDIENTE UNICO DE PERSONAL 18. COMPROBACION PARA DIFERENTES TIPOS DE GASTOS 19. PADRON DE PROVEEDORES 20. COBRO DE INGRESOS
DIRECCIÓN DE OBRAS PÚBLICAS	LOS TRATAMIENTOS RELACIONADOS CON ESTA AREA COMPRENDEN: 21. PADRON DE CONTRATISTAS 22. ELABORACION DE CONTRATOS 23. EXPEDIENTE DE OBRAS 24. REGISTRO DE CONTRATISTAS 25. PADRON DE BENEFICIARIOS 26. COMPROBACIONES 27. SUPERVISIONES DE OBRAS
FOMENTO AGROPECUARIO	ESTA UNIDAD REALIZA TRATAMIENTOS RELACIONADOS CON EL: 28. PADRON DE BENEFICIARIOS 29. COMPROBACIONES
UNIDAD DE TRANSPARENCIA	ESTA UNIDAD REALIZA ACTIVIDADES RELACIONADAS CON LA: 30. ATENCION A LAS SOLICITUDES DE ACCESO A LA INFORMACION Y DE DATOS PERSONALES 31. SEGUIMIENTO AL DIRECTORIO DE SUJETOS OBLIGADOS 32. ACTUALIZACION DE LAS OBLIGACIONES DE TRANSPARENCIA 33. SEGUIMIENTO DE DENUNCIAS POR INCUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA



CONSEJO MUNICIPAL DE SEGURIDAD PÚBLICA	LOS TRATAMIENTOS IDENTIFICADOS CORRESPONDEN AL: 34. EXPEDIENTE UNICO DE PERSONAL 35. CONVENIOS Y CONTRATOS 36. TRAMITE DE CARTA LABORAL 37. CERTIFICADO DEL CENTRO ESTATAL DE CONTROL Y CONFIANZA
SEGURIDAD PÚBLICA MUNICIPAL	LOS PROCESOS IDENTIFICADOS COPRENDEN EL: 38. REGISTRO DE DETENIDOS 39. NOTIFICACIONES 40. REQUISITOS PARA CUMPLIR CON LOS LINEAMIENTOS (NACIONALIDAD) 41. ALTA DE ELEMENTOS EN EL SISTEMA
JUZGADO MUNICIPAL	ESTA UNIDAD REALIZA TRATAMIENTOS RELACIONADOS CON: 42. ACTOS CONCILIATORIOS 43. ASUNTOS FAMILIARES (SEPARACIÓN, REGIMEN DE VISITAS, GUARDA Y CUSTODIA)
SISTEMA PARA EL DESARROLLO INTEGRAL DE LA FAMILIA (DIF)	ESTA AREA REALIZA LO SIGUIENTE: 44. ASISTENCIA ALIMENTARIA 45. APOYOS FUNCIONALES 46. SALUD Y BIENESTAR INTEGRAL 47. ATENCION PSICOLOGICA 48. PADRON DE BENEFICIARIOS 49. COMPROBACION DE IDENTIDAD 50. ESTUDIOS SOCIOECONOMICOS 51. PROTECCION LEGAL
COPLADEM	ESTA UNIDAD REALIZA ACTIVIDADES RELACIONADAS CON: 52. FORMACION DE COMITÉ DEL FAIS 53. MANEJO Y CONTROL DE LA PLATAFORMA SIFAIS DEL PROGRAMA BIENESTAR



CATEGORÍAS DE DATOS PERSONALES

Como resultado de la identificación de los tratamientos realizados por las unidades administrativas del H. Ayuntamiento Municipal de Acapetahua, Chiapas, se reconocen diversas categorías de datos personales que pueden ser objeto de tratamiento, de acuerdo con las funciones y atribuciones de cada área.

DATOS DE IDENTIFICACIÓN Y CONTACTO:

Nombre, firma, CURP, RFC, domicilio, teléfono, correo electrónico, fecha de nacimiento o edad, nacionalidad, sexo, estado civil, ocupación, nivel educativo, datos académicos, cédula y títulos profesionales, antecedentes laborales, así como información contenida en expedientes y documentos de identificación.

DATOS PATRIMONIALES:

Cuentas y números bancarios, CLABE interbancaria, estados de cuenta, institución bancaria, facturas, información contenida en declaraciones patrimoniales y descuentos o deducciones personales.

DATOS SENSIBLES:

Información relacionada con el estado de salud, discapacidad, circunstancias socioeconómicas, creencias religiosas, filosóficas o morales, información sobre procedimientos judiciales, estado de interdicción o incapacidad legal, información migratoria y lengua indígena, cuando resulte aplicable.

DATOS LABORALES:

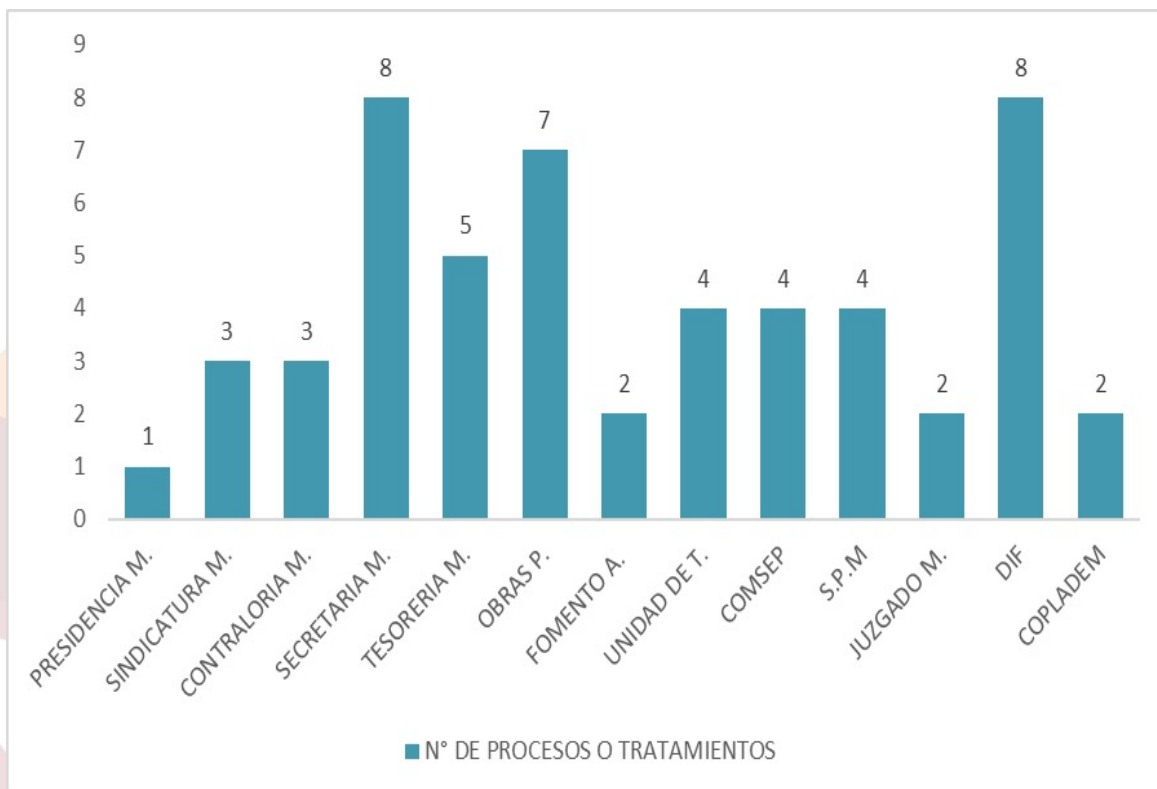
Área de Adscripción, Cargo, Correo electrónico institucional, Teléfono Institucional, Domicilio laboral, Nombre del Representante Legal y categoría.

Las categorías señaladas podrán variar de acuerdo con la naturaleza y finalidad de cada tratamiento, por lo que las unidades administrativas deberán identificar únicamente los datos personales que efectivamente recaben y utilicen en el ejercicio de sus funciones.



Como resultado de la implementación de los inventarios de datos personales, se identificaron los órganos administrativos que, en el ejercicio de sus atribuciones, llevan a cabo tratamientos que implican la recopilación y el manejo de un mayor volumen de datos personales, por lo que requieren la aplicación de medidas de seguridad acordes con el nivel de riesgo asociado a dichos tratamientos.

A continuación, se muestra la gráfica que representa el No de procesos o tratamientos que realiza cada área.



Se observa que las áreas que más datos manejan son SECRETARIA MUNICIPAL Y DIF MUNICIPAL.

La identificación de los datos personales tratados por el H. Ayuntamiento Municipal de Acapetahua, Chiapas, constituye una actividad necesaria para conocer la información que las distintas unidades administrativas recaban y utilizan en el desarrollo de sus funciones. Para ello, se consideran los procesos y actividades que implican la obtención, registro, organización, almacenamiento, consulta, utilización, conservación, transmisión o cualquier otra forma de tratamiento de datos personales.



A partir de la revisión de las actividades realizadas por las unidades administrativas, se identifican los tipos de datos personales que pueden encontrarse en expedientes, documentos, formatos, registros, archivos físicos y medios electrónicos, así como las finalidades para las cuales son utilizados. Esta identificación permite reconocer las características de la información que se encuentra bajo responsabilidad del Ayuntamiento y determinar las medidas necesarias para su adecuado manejo y protección.

Asimismo, conocer los tratamientos realizados permite identificar las áreas y personas servidoras públicas que intervienen en el manejo de los datos personales, así como los medios y sistemas empleados para su resguardo. Lo anterior facilita la determinación de responsabilidades y contribuye a que el acceso a la información se encuentre limitado al personal que, por razón de sus funciones, se encuentre autorizado para ello.

La identificación de los datos y tratamientos también constituye un elemento de apoyo para realizar el análisis de los riesgos a los que puede estar expuesta la información personal. A partir de ello, podrán determinarse las medidas administrativas, físicas y técnicas que resulten necesarias para prevenir situaciones que puedan afectar la confidencialidad, integridad o disponibilidad de los datos personales.

De igual manera, esta información permitirá detectar las necesidades de capacitación del personal que participa en el tratamiento de datos personales, con la finalidad de fortalecer sus conocimientos y sensibilizarlo sobre la importancia de cumplir con los principios, deberes y obligaciones establecidos en la legislación vigente. Las actividades de capacitación deberán considerar las funciones y responsabilidades específicas de cada unidad administrativa.

La identificación y revisión de los tratamientos deberá mantenerse como una actividad permanente, de manera que cualquier modificación en los procesos, incorporación de nuevos servicios, utilización de nuevos medios o sistemas, o cambio en las finalidades del tratamiento pueda ser considerado oportunamente para actualizar las medidas de seguridad correspondientes.

Con estas acciones, el H. Ayuntamiento Municipal de Acapetahua, Chiapas, podrá fortalecer progresivamente la gestión de los datos personales bajo su responsabilidad y establecer las bases necesarias para su adecuada protección, procurando que la información sea utilizada únicamente para las finalidades que correspondan y que durante todo su ciclo de vida se mantengan las condiciones necesarias de seguridad y confidencialidad.



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

Como resultado de la identificación de los procesos y actividades en los que las unidades administrativas del H. Ayuntamiento Municipal de Acapetahua, Chiapas, realizan algún tratamiento de datos personales, resulta necesario establecer con claridad las funciones y responsabilidades de las personas servidoras públicas que intervienen en el manejo de dicha información.

El tratamiento de datos personales deberá realizarse en el ámbito de las atribuciones y facultades que correspondan a cada unidad administrativa, observando en todo momento los principios, deberes y obligaciones establecidos en la legislación vigente en materia de protección de datos personales. En este sentido, las personas servidoras públicas que, con motivo de sus funciones, tengan acceso o intervengan en el tratamiento de información personal serán responsables de utilizarla únicamente para las finalidades que correspondan y de aplicar las medidas de seguridad establecidas para su protección.

La responsabilidad en el tratamiento comprende las distintas etapas por las que pueden pasar los datos personales, desde su obtención y registro hasta su almacenamiento, consulta, utilización, conservación, transmisión o eliminación, según corresponda. Por ello, cada área deberá procurar que las actividades relacionadas con datos personales se desarrollen dentro del marco de sus atribuciones y de conformidad con las disposiciones aplicables.

Lo anterior permite fortalecer el principio de legalidad que rige la actuación de las personas servidoras públicas, evitando que los datos personales sean recabados, utilizados o compartidos sin una justificación jurídica o fuera de las funciones que corresponden a cada unidad administrativa. En consecuencia, las funciones de las áreas que intervienen en el tratamiento de datos personales deberán relacionarse con las atribuciones que les confiere la normativa aplicable, particularmente la legislación en materia de protección de datos personales y las disposiciones que regulan la organización y funcionamiento de los municipios del Estado de Chiapas.

A continuación, se establecen las principales funciones y responsabilidades de las unidades administrativas del H. Ayuntamiento Municipal de Acapetahua, Chiapas, que, de acuerdo con sus atribuciones, realizan actividades que involucran el tratamiento de datos personales.



NOMBRE DE LA (S) PERSONA (S) FUNCIONARIA (S) QUE TRATAN DATOS PERSONALES	ÁREA	PROCESO O TRATAMIENTO
LIC. CARLOS FERNANDO MARTINEZ REYES (SECRETARIO)	PRESIDENCIA MUNICIPAL	EN ESTA UNIDAD ADMINISTRATIVA SE REALIZA LO SIGUIENTE: • ATENCION A LA CIUDADANIA
LIC. OLGA MARIA OCHOA PERERA (SINDICA MUNICIPAL)	SINDICATURA MUNICIPAL	LOS TRATAMIENTOS IDENTIFICADOS CORRESPONDEN A: • JUICIOS LABORALES • JUICIOS ADMINISTRATIVOS • PROCEDIMIENTOS ADMINISTRATIVOS
C.P. ROMEO LOPEZ ESPINOZA (CONTRALOR MUNICIPAL)	CONTRALORIA MUNICIPAL	ESTA AREA REALIZA ACTIVIDADES RELACIONADAS CON: • PROCESO DE ENTREGA-RECEPCION • DECLARACION DE SITUACION PATRIMONIAL • CONTROL DE INVENTARIO
LIC. HEBERTO REYES LOPEZ (SECRETARIO MUNICIPAL)	SECRETARIA MUNICIPAL	LOS PROCESOS IDENTIFICADOS SON: • CONVENIOS • ELABORACION DE CONSTANCIAS • REGISTRO DE FIERRO MARCADOR • ELABORACION DE NOMBRAMIENTOS • ACTAS DE CABILDO • TRAMITE DE CARTILLA DE SERVICIO MILITAR PERMISOS DE EVENTOS • LICENCIAS DE NEGOCIOS
C.P. GERARDO OCTAVIO PINTO ZEPEDA (TESORERO MUNICIPAL)	TESORERIA MUNICIPAL	EN ESTA AREA SE IDENTIFICAN LOS SIGUIENTES PROCESOS: • NOMINA DE PERSONAL • EXPEDIENTE UNICO DE PERSONAL • COMPROBACION PARA DIFERENTES TIPOS DE GASTOS • PADRON DE PROVEEDORES • COBRO DE INGRESOS
ING. MARTIN LOPEZ SOLIS (INGENIERO MUNICIPAL)	DIRECCIÓN DE OBRAS PÚBLICAS	LOS TRATAMIENTOS RELACIONADOS CON ESTA AREA COMPRENDEN: • PADRON DE CONTRATISTAS • ELABORACION DE CONTRATOS • EXPEDIENTE DE OBRAS • REGISTRO DE CONTRATISTAS • PADRON DE BENEFICIARIOS • COMPROBACIONES • SUPERVISIONES DE OBRAS
M.V.Z VICTOR ADRIAN CANDELARIA ZEBADUA (DIRECTOR DE F.A)	FOMENTO AGROPECUARIO	ESTA UNIDAD REALIZA TRATAMIENTOS RELACIONADOS CON EL: • PADRON DE BENEFICIARIOS • COMPROBACIONES



LIC. TANIA GISELT ANTONIO CRUZ (DIRECTORA DE LA UNIDAD DE TRANSPARENCIA)	UNIDAD DE TRANSPARENCIA	ESTA UNIDAD REALIZA ACTIVIDADES RELACIONADAS CON LA: • ATENCION A LAS SOLICITUDES DE ACCESO A LA INFORMACION Y DE DATOS PERSONALES • SEGUIMIENTO AL DIRECTORIO DE SUJETOS OBLIGADOS • ACTUALIZACION DE LAS OBLIGACIONES DE TRANSPARENCIA • SEGUIMIENTO DE DENUNCIAS POR INCUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA
LIC. FRANCISCO GABRIEL MINA ESCOBAR (DIRECTOR DE COMSEP)	CONSEJO MUNICIPAL DE SEGURIDAD PÚBLICA	LOS TRATAMIENTOS IDENTIFICADOS CORRESPONDEN AL: • EXPEDIENTE UNICO DE PERSONAL • CONVENIOS Y CONTRATOS • TRAMITE DE CARTA LABORAL • CERTIFICADO DEL CENTRO ESTATAL DE CONTROL Y CONFIANZA
LIC. CLAUDIA ARELI RAMIREZ GARCIA (DIRECTORA DE S.P.M)	SEGURIDAD PÚBLICA MUNICIPAL	LOS PROCESOS IDENTIFICADOS COPRENEN EL: • REGISTRO DE DETENIDOS • NOTIFICACIONES • REQUISITOS PARA CUMPLIR CON LOS LINEAMIENTOS (NACIONALIDAD) • ALTA DE ELEMENTOS EN EL SISTEMA
LIC. VENANCIO SANTO RINCON (JUEZ MUNICIPAL)	JUZGADO MUNICIPAL	ESTA UNIDAD REALIZA TRATAMIENTOS RELCIONADOS CON: • ACTOS CONCILATORIOS • ASUNTOS FAMILIARES (SEPARACIÓN, REGIMEN DE VISITAS, GUARDA Y CUSTODIA)
C. MATILDE VALDIVIESO ORDOÑEZ (DIRECTORA DEL DIF)	SISTEMA PARA EL DESARROLLO INTEGRAL DE LA FAMILIA (DIF)	ESTA AREA REALIZA LO SIGUIENTE: • ASISTENCIA ALIMENTARIA • APOYOS FUNCIONALES • SALUD Y BIENESTAR INTEGRAL • ATENCION PSICOLOGICA • PADRON DE BENEFICIARIOS • COMPROBACION DE IDENTIDAD • ESTUDIOS SOCIOECONOMICOS • PROTECCION LEGAL
ING. BRENDA JUNCO OVALLE (DIRECTORA DE COPLADEM)	COPLADEM	ESTA UNIDAD REALIZA ACTIVIDADES RELACIONADAS CON: • FORMACION DEL COMITÉ FAIS • MANEJO Y CONTROL DE LA PLATAFORMA SIFAIS DEL PROGRAMA BIENESTAR



6. - ANÁLISIS DE RIESGO Y 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.



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.



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.



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.



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.



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.



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.



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.



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 administrativas, físicas y técnicas tienen como finalidad proteger los datos personales que son tratados por el H. Ayuntamiento Municipal de Acapetahua, Chiapas, y reducir los riesgos que puedan afectar su confidencialidad, integridad y disponibilidad. Estas medidas deberán aplicarse de acuerdo con las características de cada tratamiento, los medios utilizados para el manejo de la información y el nivel de riesgo identificado. Su implementación estará orientada a prevenir situaciones como pérdida, extravío, daño, destrucción, alteración, acceso, uso, tratamiento o divulgación no autorizada de los datos personales.

Para fortalecer la protección de la información, se consideran las siguientes medidas:

A. Medidas administrativas

I. Capacitación y sensibilización.

Promover actividades de capacitación dirigidas a las personas servidoras públicas que intervienen en el tratamiento de datos personales, con el propósito de fortalecer sus conocimientos sobre los principios, deberes, obligaciones y medidas de seguridad establecidos en la legislación vigente.

II. Control de documentos y expedientes.

Establecer mecanismos para controlar la recepción, préstamo, consulta y devolución de documentos y expedientes que contengan datos personales, procurando mantener un registro que permita identificar su ubicación y las personas que hayan tenido acceso a ellos.

III. Resguardo de la información.

Implementar procedimientos para el adecuado manejo y resguardo de expedientes y documentos que contengan datos personales, considerando las disposiciones aplicables en materia de gestión documental y archivos.

IV. Compromiso de confidencialidad.

Establecer mecanismos mediante los cuales las personas servidoras públicas que tengan acceso a datos personales conozcan y asuman el deber de confidencialidad respecto de la información que manejen con motivo de sus funciones.

V. Registro y atención de incidencias.

Establecer mecanismos para reportar, registrar y dar seguimiento a incidentes relacionados con la seguridad de los datos personales, con la finalidad de identificar sus causas y adoptar las acciones preventivas o correctivas correspondientes.



B. Medidas físicas

I. Protección de documentos físicos.

Resguardar los expedientes, documentos y demás soportes físicos que contengan datos personales en espacios destinados para su conservación, procurando que permanezcan protegidos contra pérdida, daño, deterioro, sustracción o acceso de personas no autorizadas.

II. Control de acceso a las instalaciones.

Establecer mecanismos de control para limitar el acceso a las áreas en las que se encuentren documentos, archivos, equipos o cualquier otro medio que contenga datos personales, permitiendo el ingreso únicamente a las personas autorizadas.

III. Protección de equipos y espacios de trabajo.

Procurar que los equipos de cómputo, escritorios, archiveros, cajones y demás espacios utilizados para el tratamiento de datos personales permanezcan bajo condiciones que reduzcan el riesgo de acceso o consulta por personas no autorizadas.

IV. Protección frente a factores ambientales.

Adoptar medidas razonables para prevenir daños ocasionados por factores como humedad, polvo, incendios, filtraciones de agua u otras circunstancias que puedan afectar los documentos y soportes que contengan datos personales.

C. Medidas técnicas

I. Control de usuarios y contraseñas.

Utilizar cuentas de usuario y contraseñas individuales para el acceso a los equipos y sistemas que contengan datos personales, evitando compartirlas, prestarlas o dejarlas expuestas. Las contraseñas deberán contar con características que dificulten su identificación o descifrado por personas no autorizadas.

II. Protección de credenciales de acceso.

Cuando se detecte que una cuenta, usuario o contraseña pudo haber sido utilizada por una persona no autorizada, deberá informarse oportunamente al responsable correspondiente para adoptar las medidas necesarias, incluyendo el cambio o bloqueo de las credenciales comprometidas.

III. Uso de medios institucionales.

Procurar que las actividades laborales que involucren datos personales se realicen mediante cuentas de correo electrónico, sistemas y herramientas institucionales



autorizadas, evitando utilizar medios personales o no autorizados para almacenar o transmitir información.

IV. Protección de archivos electrónicos.

Mantener los documentos y archivos electrónicos que contengan datos personales bajo mecanismos de protección adecuados, tales como contraseñas, permisos de acceso u otros controles disponibles, de acuerdo con las características de los equipos y sistemas utilizados.

V. Control de impresión y reproducción.

Evitar que documentos impresos que contengan datos personales permanezcan expuestos o sean abandonados en impresoras, copiadoras, escritorios u otros espacios de uso común. Las copias y reproducciones deberán realizarse únicamente cuando sean necesarias para el cumplimiento de las funciones correspondientes.

VI. Respaldo de información.

Cuando la naturaleza del tratamiento lo requiera, establecer mecanismos de respaldo de la información electrónica para reducir el riesgo de pérdida o destrucción de los datos personales y facilitar su recuperación ante incidentes.

VII. Actualización y protección de equipos.

Mantener los equipos y sistemas utilizados para el tratamiento de datos personales en condiciones adecuadas de funcionamiento y, cuando corresponda, aplicar actualizaciones y mecanismos de protección que contribuyan a reducir vulnerabilidades de seguridad.

Las medidas señaladas deberán ser observadas por las unidades administrativas y por las personas servidoras públicas que intervengan en el tratamiento de datos personales. Su aplicación deberá revisarse periódicamente y fortalecerse de acuerdo con los resultados del análisis de riesgos y de brecha, así como con las modificaciones que se presenten en los procesos, sistemas o medios utilizados por el Ayuntamiento. La implementación progresiva de estas medidas permitirá al H. Ayuntamiento Municipal de Acapetahua, Chiapas, fortalecer las condiciones de seguridad de los datos personales bajo su responsabilidad y reducir la posibilidad de que se presenten vulneraciones que puedan afectar los derechos y libertades de las personas titulares.



- MONITOREO DE LAS MEDIDAS DE SEGURIDAD

El monitoreo de las medidas de seguridad constituye una actividad necesaria para verificar que los controles administrativos, físicos y técnicos implementados para la protección de los datos personales sean adecuados y se mantengan en condiciones de funcionamiento. Esta supervisión permitirá detectar oportunamente posibles deficiencias, vulnerabilidades o situaciones que puedan poner en riesgo la información bajo responsabilidad del H. Ayuntamiento Municipal de Acapetahua, Chiapas.

La revisión de las medidas de seguridad deberá realizarse de manera periódica y considerar las características de los procesos, los medios utilizados para el tratamiento de los datos personales y los riesgos identificados. Los resultados obtenidos podrán utilizarse para establecer acciones preventivas, correctivas y de mejora continua.

Entre las acciones de monitoreo que podrán realizarse se consideran las siguientes:

1. Revisión de contraseñas y mecanismos de acceso.

Verificar periódicamente que las contraseñas y demás mecanismos utilizados para acceder a equipos o sistemas que contengan datos personales sean individuales, seguras y se encuentren bajo control de las personas autorizadas, evitando su divulgación o uso compartido.

2. Supervisión de las medidas de seguridad.

Revisar periódicamente el cumplimiento de las medidas administrativas, físicas y técnicas establecidas para la protección de los datos personales, identificando aquellas que requieran actualización, fortalecimiento o corrección.

3. Control de acceso a las áreas de resguardo.

Verificar que el ingreso a los espacios donde se encuentren documentos, expedientes, equipos o sistemas que contengan datos personales se encuentre limitado al personal autorizado y que, cuando corresponda, existan mecanismos para identificar y controlar el acceso de personas externas.

4. Revisión de equipos y espacios de trabajo.

Supervisar que los equipos de cómputo, archivos, escritorios, impresoras y demás espacios utilizados para el tratamiento de datos personales mantengan condiciones adecuadas de seguridad y que la información no permanezca expuesta innecesariamente.



5. Seguimiento de incidencias.

Dar seguimiento a los reportes relacionados con posibles vulneraciones o incidentes de seguridad, procurando identificar sus causas, consecuencias y medidas necesarias para evitar que vuelvan a presentarse.

6. Evaluación y mejora continua.

Utilizar los resultados obtenidos mediante el monitoreo para fortalecer las medidas de seguridad y, cuando sea necesario, establecer nuevas acciones de protección de acuerdo con los cambios en los procesos, sistemas, tecnologías o niveles de riesgo.

El monitoreo deberá realizarse de manera coordinada entre las unidades administrativas responsables de los tratamientos y las áreas que, de acuerdo con sus atribuciones, participen en la protección de la información. Las observaciones y resultados derivados de estas actividades deberán considerarse para mantener actualizadas las medidas de seguridad y contribuir a la mejora continua del sistema de gestión de datos personales del H. Ayuntamiento Municipal de Acapetahua, Chiapas.



9. - PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

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



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. - PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

La adecuada protección de los datos personales dentro del H. Ayuntamiento Municipal de Acapetahua, Chiapas, requiere que las personas servidoras públicas que intervienen en su tratamiento cuenten con conocimientos suficientes sobre las obligaciones que deben observar y las medidas de seguridad que deben aplicar en el desarrollo de sus funciones.

La capacitación y sensibilización del personal constituye una herramienta necesaria para fortalecer la cultura institucional de protección de datos personales, promover el cumplimiento de la legislación vigente y reducir los riesgos derivados del manejo inadecuado de la información. Por ello, se propone desarrollar actividades de capacitación de manera periódica, considerando las funciones que desempeña cada unidad administrativa y el tipo de información que se encuentra bajo su responsabilidad.

El programa deberá dirigirse principalmente a las personas servidoras públicas que, por razón de sus funciones, recaben, utilicen, consulten, almacenen, conserven, transmitan o realicen cualquier otro tratamiento de datos personales. Los contenidos podrán ajustarse de acuerdo con las necesidades detectadas mediante la revisión de los procesos y el análisis de riesgos y de brecha.

Como propuesta, se consideran los siguientes temas:

I. MARCO JURÍDICO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

- Antecedentes y finalidad de la protección de datos personales.
- Principios y deberes aplicables al tratamiento de datos personales.
- Obligaciones de los sujetos obligados.
- Derechos de las personas titulares.
- Alcances y aplicación de la legislación vigente en el Estado de Chiapas.
- Responsabilidades derivadas del tratamiento de datos personales.

II. OBLIGACIONES Y RESPONSABILIDADES EN EL TRATAMIENTO DE DATOS PERSONALES

- Principios que deben observarse durante el tratamiento.
- Deber de confidencialidad.
- Medidas administrativas, físicas y técnicas de seguridad.
- Responsabilidades de las personas servidoras públicas.
- Control y autorización de acceso a los datos personales.
- Prevención y atención de vulneraciones de seguridad.



- Procedimientos y consecuencias derivadas del incumplimiento de las obligaciones.
- Derechos de acceso, rectificación, cancelación y oposición.

III. GESTIÓN Y PROTECCIÓN DE LOS DATOS PERSONALES

- Identificación de los procesos que involucran datos personales.
- Identificación de las categorías de datos personales.
- Sistemas y medios físicos o electrónicos utilizados para el tratamiento.
- Ciclo de vida de los datos personales.
- Medidas de seguridad administrativas, físicas y técnicas.
- Análisis de riesgos y análisis de brecha.
- Funciones y responsabilidades de las áreas y personas que intervienen en el tratamiento.
- Control, resguardo y conservación de documentos y expedientes.

IV. AVISOS DE PRIVACIDAD Y PRINCIPIO DE INFORMACIÓN

- Importancia del aviso de privacidad.
- Aviso de privacidad integral y simplificado.
- Elementos que debe contener el aviso de privacidad.
- Finalidades del tratamiento.
- Obtención y manejo del consentimiento, cuando corresponda.
- Deber de informar a las personas titulares sobre el tratamiento de sus datos.
- *Identificación del responsable y medios para ejercer los derechos correspondientes.

V. PREVENCIÓN Y ATENCIÓN DE VULNERACIONES

- Identificación de incidentes de seguridad.
- Robo, pérdida, extravío o destrucción de información.
- Acceso, uso o tratamiento no autorizado.
- Alteración o modificación de datos personales.
- Reporte y seguimiento de incidentes.
- Acciones preventivas y correctivas.
- Medidas para reducir la posibilidad de que una vulneración vuelva a presentarse.



VI. CULTURA DE PROTECCIÓN DE DATOS PERSONALES

- Buenas prácticas en el manejo de información personal.
- Uso responsable de equipos y sistemas.
- Protección de contraseñas y mecanismos de acceso.
- Manejo adecuado de documentos físicos y electrónicos.
- Prevención de divulgaciones no autorizadas.
- Responsabilidad individual en el tratamiento de datos personales.
- Importancia de mantener la confidencialidad de la información.

La capacitación deberá considerar las necesidades particulares de cada unidad administrativa, procurando que los conocimientos adquiridos puedan aplicarse directamente en las actividades que desarrollan las personas servidoras públicas.

El programa podrá llevarse a cabo mediante cursos, talleres, reuniones de sensibilización, materiales informativos u otras actividades que permitan reforzar periódicamente los conocimientos del personal. Se deberá procurar que las acciones de capacitación sean evaluadas y, cuando resulte necesario, actualizadas conforme a las modificaciones de la legislación, los procesos internos y los riesgos identificados.

Con la implementación de estas actividades, el H. Ayuntamiento Municipal de Acapetahua, Chiapas, fortalecerá las capacidades del personal encargado del tratamiento de datos personales y contribuirá a establecer una cultura institucional orientada a la prevención, protección y uso responsable de la información personal.



11. - ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD.

El H. Ayuntamiento Municipal de Acapetahua, Chiapas, deberá mantener actualizado este Documento de Seguridad, de conformidad con lo establecido en el artículo 30 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, con la finalidad de que las medidas de protección correspondan a las condiciones reales en que se lleva a cabo el tratamiento de los datos personales.

La actualización deberá realizarse cuando se produzcan modificaciones sustanciales en los tratamientos de datos personales que impliquen un cambio en el nivel de riesgo, así como cuando, derivado del monitoreo, revisión y mejora continua del sistema de gestión, se identifiquen aspectos que requieran ser modificados o fortalecidos. También deberá actualizarse cuando sea necesario establecer acciones para mitigar los efectos de una vulneración de seguridad o cuando, como consecuencia de ésta, se determinen medidas correctivas y preventivas que deban incorporarse al sistema de protección de datos personales.

Las modificaciones que se realicen deberán considerar, según corresponda, los resultados del análisis de riesgos y de brecha, las medidas de seguridad administrativas, físicas y técnicas, las funciones y responsabilidades de las áreas involucradas y las acciones previstas en el plan de trabajo.

Con independencia de los supuestos anteriores, el Documento de Seguridad será revisado por lo menos una vez al año, con el propósito de verificar que su contenido se encuentre actualizado y sea acorde con los procesos, tratamientos, sistemas, medios y condiciones de seguridad existentes en el H. Ayuntamiento.

De cada revisión o actualización deberá procurarse dejar constancia de los cambios realizados, las causas que los originaron y, cuando corresponda, las acciones que deberán implementarse para fortalecer la protección de los datos personales.

Cuando de la revisión resulte necesario modificar el Documento de Seguridad, éste deberá someterse nuevamente a consideración y, en su caso, aprobación del Comité de Transparencia del H. Ayuntamiento Municipal de Acapetahua, Chiapas, atendiendo a las atribuciones que le corresponden en materia de protección de datos personales.

La actualización permanente de este instrumento permitirá al Ayuntamiento mantener un proceso de mejora continua y fortalecer las condiciones de confidencialidad, integridad y disponibilidad de los datos personales bajo su responsabilidad.



12. - VIGENCIA, APROBACIÓN Y OBSERVANCIA DEL DOCUMENTO DE SEGURIDAD

El presente Documento de Seguridad entrará en vigor a partir de la fecha en que sea aprobado por el Comité de Transparencia del H. Ayuntamiento Municipal de Acapetahua, Chiapas, y será de observancia obligatoria para las unidades administrativas y personas servidoras públicas que, con motivo de sus funciones, intervengan en el tratamiento de datos personales.

Las disposiciones contenidas en este instrumento deberán ser consideradas en las actividades relacionadas con la obtención, uso, almacenamiento, consulta, conservación, transmisión, eliminación y demás formas de tratamiento de datos personales que se realicen dentro del Ayuntamiento.

Las unidades administrativas deberán observar las medidas y responsabilidades establecidas en este Documento, así como informar oportunamente cualquier situación que pueda representar un riesgo para la seguridad de los datos personales o que requiera la modificación de las medidas implementadas.

Este Documento permanecerá vigente mientras no sea sustituido o modificado por una nueva versión aprobada por la autoridad competente. Su contenido deberá revisarse periódicamente y actualizarse cuando las condiciones de los tratamientos, los riesgos identificados, las medidas de seguridad o la legislación aplicable así lo requieran.

La aprobación, modificación y actualización del Documento de Seguridad deberá quedar debidamente documentada, señalando la fecha correspondiente y, cuando resulte aplicable, el número de sesión o acta mediante la cual haya sido aprobada.

Con la observancia de este instrumento, el H. Ayuntamiento Municipal de Acapetahua, Chiapas, reafirma su compromiso de proteger los datos personales bajo su responsabilidad y de fortalecer de manera permanente las medidas destinadas a garantizar su confidencialidad, integridad y disponibilidad.



ACAPETAHUA

H. AYUNTAMIENTO 2024-2027

• Con trabajo y esfuerzo juntos hagamos el Cambio •

“2026, Año de Jaime Sabines Gutiérrez”

DOCUMENTO DE SEGURIDAD

SISTEMA DE DATOS PERSONALES DE TRANSPARENCIA PARA EL PUEBLO DE CHIAPAS

FECHA DE ELABORACION DEL
DOCUMENTO DE SEGURIDAD:

29 DE SEPTIEMBRE DE 2026

FECHA DE ÚLTIMA ACTUAIZACION
DEL DOCUMENTO DE SEGURIDAD:

29 DE SEPTIEMBRE DE 2026

ELABORO:

LIC. TANIA GISELT ANTONIO CRUZ

RESPONSABLE DE LA UNIDAD DE
TRANSPARENCIA

APROBO:

**MTRA. SOFIA TRINIDAD REYES
ACOSTA**

PRESIDENTA DE LA UNIDAD DE
TRANSPARENCIA