H. AYUNTAMIENTO MUNICIPAL CONSTITUCIONAL YAJALÓN, CHIAPAS 2024-2027

DOCUMENTO DE SEGURIDAD

DOC. DE SEGURIDAD

Versión Pública

INDICE

P R E S E N T A C I O N 3
OBJETIVOS DEL DOCUMENTO DE SEGURIDAD 5
RESPONSABILIDADES 5
ALCANCE DEL DOCUMENTO DE SEGURIDAD 7
SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES 8
INVENTARIO DE TRATAMIENTOS Y DATOS PERSONALES 10
FUNCIONES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES 20
ANÁLISIS DE RIESGO 28
ANÁLISIS DE BRECHA 32
Brechas Identificadas 33
Plan de Acción para Mitigar las Brechas 33
BITÁCORAS DE REPORTE DE VULNERACIONES 34
CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS 35
PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES 35
PLAN DE CONTINGENCIA 38
TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES 39
GESTIÓN DE VULNERACIONES DE SEGURIDAD DE LA INFORMACIÓN 40
Procedimientos de Identificación y Notificación de Vulneraciones 40
Medidas de Contención y Remediación 41
Comunicación a los Titulares de los Datos 41
Registro y Evaluación de Vulneraciones 41
MEDIDAS DE SEGURIDAD 43
PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES 44

H. AYUNTAMIENTO 2024 - 2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

PRESENTACION

El H. Ayuntamiento de Yajalón, Chiapas; la información es un activo que debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos. De esta manera, la gestión de la seguridad de la información, como parte de un sistema administrativo más amplio, busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información, aplicando un enfoque basado en los riesgos que la organización afronta.

En este sentido la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), establece un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentra en posesión de sujetos obligados, entre los que figura el H. Ayuntamiento Municipal de Yajalón, Chiapas.

El presente Documento de Seguridad para Sistemas de Datos Personales en medios físicos (Documento), se dicta en cumplimiento de las disposiciones jurídicas vigentes, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

En observancia de esta ley y de conformidad con el artículo 45, se ha diseñado el presente documento de seguridad que tiene como propósito establecer los parámetros que guían el tratamiento de los datos personales al interior del H. Ayuntamiento Municipal de Yajalón, Chiapas, por las diferentes unidades administrativas que lo conforman.

En ese sentido, el H. Ayuntamiento Municipal de Yajalón, Chiapas, ha identificado los procesos que en el ámbito de su competencia involucran el tratamiento de datos personales, a efecto de mantener la seguridad de los mismos durante el ciclo de vida de la información, indicando la forma en la que se trata, las medidas de seguridad adoptadas y las áreas responsables de su protección, así como las finalidades del tratamiento de acuerdo con sus respectivos ámbitos de funciones.

El Documento brinda al H. Ayuntamiento de Yajalón, Chiapas, homogeneidad en la organización, procesos y sistemas, en el que el Comité de Información, juntamente con el área de Tecnologías de la Información y los responsables de los sistemas de datos personales, definen las medidas de seguridad administrativa y física implementadas para la protección de los sistemas de datos personales custodiados.

Esto implica el planteamiento de acciones pertinentes para evitar la alteración, pérdida, transmisión y acceso no autorizado de los datos mediante la implementación de medidas físicas, administrativas y técnicas, tendientes a garantizar la seguridad e integridad de

Dichos datos con el seguimiento y observancia continúan. Incluye además acciones que permitan controlar y verificar que el tratamiento de los datos personales se realice de acuerdo con los principios establecidos para la protección de los datos personales, implicando un compromiso con las disposiciones previstas en la ley y en los lineamientos generales, por parte de los funcionarios involucrados.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, es necesario señalar que todos y cada uno de los elementos que lo integran, constituyen un sistema interno para la gestión y tratamiento de los datos personales en posesión del H. Ayuntamiento Municipal de Yajalón, Chiapas, tal como lo indica el artículo 5, 34 y 45 de la Ley de Protección de Datos Personales en posesión de sujetos obligados del estado de Chiapas, se entiende por sistema de gestión, al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

Finalmente, ante la necesidad de mantener actualizado el documento de seguridad se ha de procurar su mejora continua. Además, se ha procedido a la actualización de los elementos que integran el documento de seguridad; las medidas de seguridad adoptadas en su tratamiento, el análisis de riesgo y brecha, que permiten dar seguimiento a las medidas adoptadas, identificar las posibles vulneraciones y aminorar los riesgos. Todo lo anterior, acompañado del desarrollo del programa de capacitación que permita comprender la importancia de adoptar medidas para la prevención de las vulneraciones a los datos personales.

Así mismo, este documento tiene como propósito controlar internamente los sistemas de datos personales que posee el H. Ayuntamiento de Yajalón, Chiapas; el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

OBJETIVOS DEL DOCUMENTO DE SEGURIDAD

El presente documento tiene como objetivo:

Ofrecer el marco de trabajo necesario para la protección de los datos personales en posesión del H. Ayuntamiento de Yajalón, Chiapas, como un medio para cumplir con las obligaciones que establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas (LPDPPSOCHIS) y los Lineamientos Generales, así como la normatividad que derive de los mismos; estableciendo los elementos y actividades de gestión para la operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, además de promover la adopción de mejores prácticas en relación con la protección de datos personales, con la finalidad de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, emite el presente documento.

RESPONSABILIDADES

De conformidad con lo dispuesto por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales al interior de cada sujeto obligado, teniendo entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, en esa tesitura dicho órgano tiene las siguientes funciones con relación a este programa:

I. Aprobar, supervisar y evaluar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la presente Ley y demás disposiciones que resulten aplicables en la materia.
II. Coordinar, realizar y supervisar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en las que resulten aplicables en la materia, en coordinación con el oficial de protección de datos personales, en su caso.
III. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.
IV. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se declare improcedente, por cualquier causa, el ejercicio de alguno de los derechos ARCO.
V. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y demás ordenamientos que resulten aplicables en la materia.

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

VII. Coordinar el seguimiento y cumplimiento de las resoluciones emitidas por Transparencia para el Pueblo de Chiapas y las demás Autoridades Garantes competentes.

VIII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales.

Las unidades administrativas, el área coordinadora de archivos y la unidad de transparencia tendrán las funciones y responsabilidades que se describen más adelante en este documento.

Para que los objetivos planteados se logren con éxito, el Programa requiere del apoyo e impulso directo del más alto nivel de la institución. En ese sentido, el Programa se deberá hacer del conocimiento presidente Municipal, a fin de que tomen las medidas necesarias para que el mismo se observe en el H. Ayuntamiento Municipal de Yajalón, Chiapas.

La intervención del presidente Municipal tendrá la finalidad de impulsar la debida implementación del Programa al interior del sujeto obligado, pero no podrá suplir ni afectar las funciones del Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la organización.

Asimismo, para que la implementación del Programa tenga como resultado el cumplimiento integral de las obligaciones que establece la LPDPPSOCHIS y los Lineamientos Generales, el Programa será de observancia obligatoria para todas las personas servidoras públicas del sujeto obligado que en el ejercicio de sus funciones traten datos personales.

El presente Documento de Seguridad es aplicable y de observancia obligatoria para que todas las unidades administrativas de este H. Ayuntamiento de Yajalón, deban realizar las acciones necesarias para cumplir con las obligaciones que establece este Programa, para lo cual deberán asignar los recursos materiales y humanos necesarios, y prever lo que se requiera en sus programas de trabajo.

Para ello, resulta fundamental que el Programa se conozca al interior del sujeto obligado, por lo que el Comité de Transparencia se encargará de difundirlo y socializarlo entre el personal.

ALCANCE DEL DOCUMENTO DE SEGURIDAD

El documento de seguridad aplica a todas las unidades administrativas que realicen tratamientos de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que efectúen, mismos que se encuentran bajo su estricta responsabilidad, tanto en los espacios físicos como los medios electrónicos en los que se resguardan, operan y administran, con observancia de los principios, deberes y obligaciones que establece la ley.

Las unidades administrativas que forman parte del H. Ayuntamiento de Yajalón; y que deberán observar el Programa de Protección de Datos Personales son las siguientes:

- Presidencia Municipal
- Sindicatura Municipal
- Secretaria Municipal
- Consejero Jurídico
- Unidad de Transparencia
- Tesorería Municipal
- Dirección de Obras Públicas
- Dirección de Planeación
- Dirección de Seguridad Pública
- Dirección de Archivo Municipal
- Defensora Municipal de Derechos Humanos
- IMM Instituto Municipal De La Mujer

H. AYUNTAMIENTO 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

La Unidad de Transparencia integra este Documento de Seguridad con base en la información generada por las unidades administrativas del H Ayuntamiento de Yajalón, Chiapas.

SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES

El Sistema de Gestión de Datos Personales es el vínculo mediante el cual el H. Ayuntamiento de Yajalón, Chiapas, garantiza el tratamiento de los datos personales que lleva a cabo como parte de sus funciones, desde su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación correspondiente; para lo cual, se establecen políticas y métodos orientados a salvaguardar la confidencialidad, integridad y disponibilidad de estos datos, de acuerdo con 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.

Por lo cual esta institución inicio proceso de organización y planeación de los medios para la protección de datos, tomando como punto de partida la identificación de los procesos y tareas en los que, conforme a sus atribuciones, las distintas áreas del instituto desarrollan tratamientos de datos personales. Para tal fin, se elaboró un formulario que facilitó a cada unidad administrativa, la identificación de los tratamientos que llevan a cabo como parte de su responsabilidad, considerando lo establecido en el artículo 47 de la Ley de Protección de Datos Personales del Estado de Chiapas; logrando con ello el levantamiento del inventario de datos, tratando de identificar, la categoría y tipo datos usados en cada tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/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 los servidores públicos que tienen acceso al tratamiento, además de si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

El inventario ha contribuido para la determinación del ciclo de vida de los datos personales, entendiendo que, una vez concluida la finalidad de los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o instrucción, vinculado con el proceso de gestión documental que se desarrolla al interior de esta institución.

Una vez integrados los inventarios de tratamientos y de datos, se estableció la metodología para el análisis de riesgo, con la intención de que se identificaran el valor de los datos y su ciclo de vida, así como el valor de exposición, las posibles consecuencias para los titulares por el uso indebido y/o posible vulneración y las condiciones de riesgo a los que podrían encontrarse expuestos por medidas de seguridad poco confiables. Lo anterior, permitió identificar la brecha entre las medidas de seguridad existentes y las medidas de seguridad faltantes para que garanticen la seguridad de los datos, tanto administrativas, como físicas y técnicas.

A partir de esta identificación de posibles vulneraciones es factible prevenir posibles debilidades en la seguridad de los datos y las áreas de oportunidad, aun cuando no haya existido un daño real, mediante la identificación de la ineficiencia de los controles de acceso físico, electrónico y el inadecuado establecimiento de los esquemas de privilegios, sumado al poco conocimiento de procesos y responsabilidades en materia de protección de datos personales, además de la falta de definición de perfiles y roles, falta de seguimiento y monitoreo a las medidas de seguridad, así como la inexistencia de mecanismos para garantizar la confidencialidad por parte del personal.

Las amenazas que se buscan prevenir pueden ser de diferentes tipos:

- Robo, extravío o copia no autorizada
- Uso, acceso o tratamiento no autorizado
- Daño, alteración o modificación no autorizado
- Pérdida o destrucción no autorizada

El riesgo que puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada comprometiendo su confidencialidad, disponibilidad e integridad; y en este sentido, las medidas de seguridad por parte de cada dirección están orientadas justamente a proteger los datos personales. En el marco del sistema de gestión y política de seguridad institucional, se procurará:

- Tratar a los datos personales conforme a la Ley;
- Identificar a los servidores públicos de este Ayuntamiento responsables del tratamiento de los datos personales;
- Que los tratamientos de datos personales estén sujetos al principio de consentimiento siempre que la Ley lo permita;
- Responder al principio de información a los titulares sobre el uso que dará y sus finalidades;
- Mantener la actualización y pertinencia de los datos personales;
- Priorizar la supresión de los datos personales cuando haya concluido el proceso para el que fueron obtenidos;
- Ajustar el tratamiento de los datos personales a las finalidades para la que fueron obtenidos y estrictamente los necesarios para las finalidades;
- Obtener datos personales a través de medios legales, con respeto a la expectativa de privacidad del titular;
- Velar por el cumplimiento de los principios, estableciendo y manteniendo medidas de seguridad y de confidencialidad durante el ciclo de vida de los datos personales, en estricto respeto de los derechos de los titulares;
- Mantener actualizado el inventario de datos personales que maneja el Ayuntamiento;

Buscando el logro de lo anterior, y tomando como punto de partida la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que, de acuerdo con otras experiencias y mejores prácticas tomadas como referencia, se encaminan a la mejora continua por parte de las personas involucradas en el tratamiento, en la búsqueda de lograr la salvaguarda del derecho a la privacidad y protección de datos personales, se han determinado las líneas de acción para el personal encargado de tratamiento de datos, con el propósito de generar mecanismos para el resguardo adecuado, actuando en apego a la LPDPPSO de Chiapas y los lineamientos correspondientes.

INVENTARIO DE TRATAMIENTOS Y DATOS PERSONALES

Para llevar a cabo el debido cumplimiento de las obligaciones en nuestra institución es necesario que cada una de las unidades administrativas realice un diagnóstico de los tratamientos de datos personales que llevan a cabo.

El diagnóstico en mención se basa en la elaboración de un inventario con la Información básica de cada tratamiento de datos personales que se realizan en este H. Ayuntamiento Municipal de Yajalón, Chiapas.

Por "inventario de tratamientos de datos personales" se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas del H. Ayuntamiento Municipal de Yajalón, Chiapas, realizado con orden y precisión.

Así, en coordinación con las áreas, como resultado del proceso de análisis y actualización de la información, se logró identificar a las unidades administrativas que realizan tratamientos con datos personales, las cuales son:

- Presidencia Municipal
- Sindicatura Municipal
- Secretaria Municipal
- Consejero Jurídico
- Unidad de Transparencia
- Tesorería Municipal
- Dirección de Obras Públicas
- Dirección de Planeación
- Dirección de Seguridad Pública

- Dirección de Archivo Municipal
- Defensora Municipal de Derechos Humanos
- IMM Instituto Municipal De La Mujer

Todos los tratamientos se realizan en apego a sus facultades y obligaciones que la normatividad les confiere, a través de las diversas áreas que lo integran y permiten el desarrollo de los procesos que realizan para el cumplimiento de dichas funciones.
En base a lo anterior, fue posible identificar 55 procesos que se desarrollan, que implican tratamiento de datos personales. a continuación, se describen:

UNIDAD ADMINISTRATIVA	AREA O DEPARTAMENTO	PROCESO O TRATAMIENTO
Presidencia Municipal	Presidencia Municipal	Atención a la ciudadanía
Sindicatura Municipal	Sindicatura Municipal	Juicios Civiles
		Juicios Laborales
		Juicios Administrativos
		Procedimientos y Juicios Penales
Secretaria Municipal	Secretaria Municipal	Elaboración de nombramientos
		Elaboración de Constancias
		Expedición de constancias
		Redacción de actas de cabildo
		Permiso de funcionamiento de bebidas alcohólicas
		Fierro marcador
		Traslados de ganado
		Llenado de certificados de defunción

		Certificación de documentos
		Junta de reclutamiento del servicio militar nacional
Consejero Jurídico	Consejero Jurídico	Asesorías jurídicas
		Acuerdos
		Canalizaciones
		Revisión de contratos
		Revisión de convenio
		Certificaciones
Unidad de Transparencia	Unidad de Transparencia	Atención a las Solicitudes de Acceso a la Información y de Datos Personales
		Actualización de las Obligaciones de Transparencia
Tesorería Municipal	Tesorería Municipal	Cobro de ingresos
		Nómina de Personal
		Comprobación para diferentes tipos de gastos
		Padrón de Proveedores
		Expediente Único de Personal
Dirección de Obras Públicas	Dirección de Obras Públicas	Elaboración de Contratos
		Padrón de contratistas

		Expediente de obras
		Padrón de Beneficiarios
Dirección de Planeación	Dirección de Planeación	Movimiento de Personal (Altas y Baja)
		Incapacidades Médicas
		Permisos
		Servicio Social
		Control De Entradas Y Salidas Del Personal
		Control de expedientes curriculares
Dirección de Seguridad Pública	Dirección de Seguridad Pública	Expediente Único de Personal
		Certificado del centro estatal de control y confianza.
Dirección de Archivo Municipal	Dirección de Archivo Municipal	Recepción de cajas de archivo
		Organización de documentos por departamento
		Recepcionar los archivos de trámite
		Vigilar la estructura y ciclo vital de los documentos
		Llevar el control de los archivos solicitados o prestados.

H. AYUNTAMIENTO 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

Defensora Municipal de Derechos Humanos	Defensora Municipal de Derechos Humanos	Solicitudes para actas de nacimiento extemporáneas etapa 1 menores de edad
		Solicitudes para actas de nacimiento extemporáneas etapa 2 mayores de edad
		Atención a la primera infancia
		Adultos y adultos mayores en caso de violación de derechos humanos
		Vinculación de base de datos con el registro civil del Estado
		Recepción de datos para solitud de actas extemporáneas
		Administración de correspondencia de Derechos Humanos Estatal
Instituto Municipal De La Mujer	Instituto Municipal De La Mujer	Asesorías jurídicas a las mujeres y niñas violentadas
		Terapia psicológica
		Programas de microcrédito "semillas autonomía".

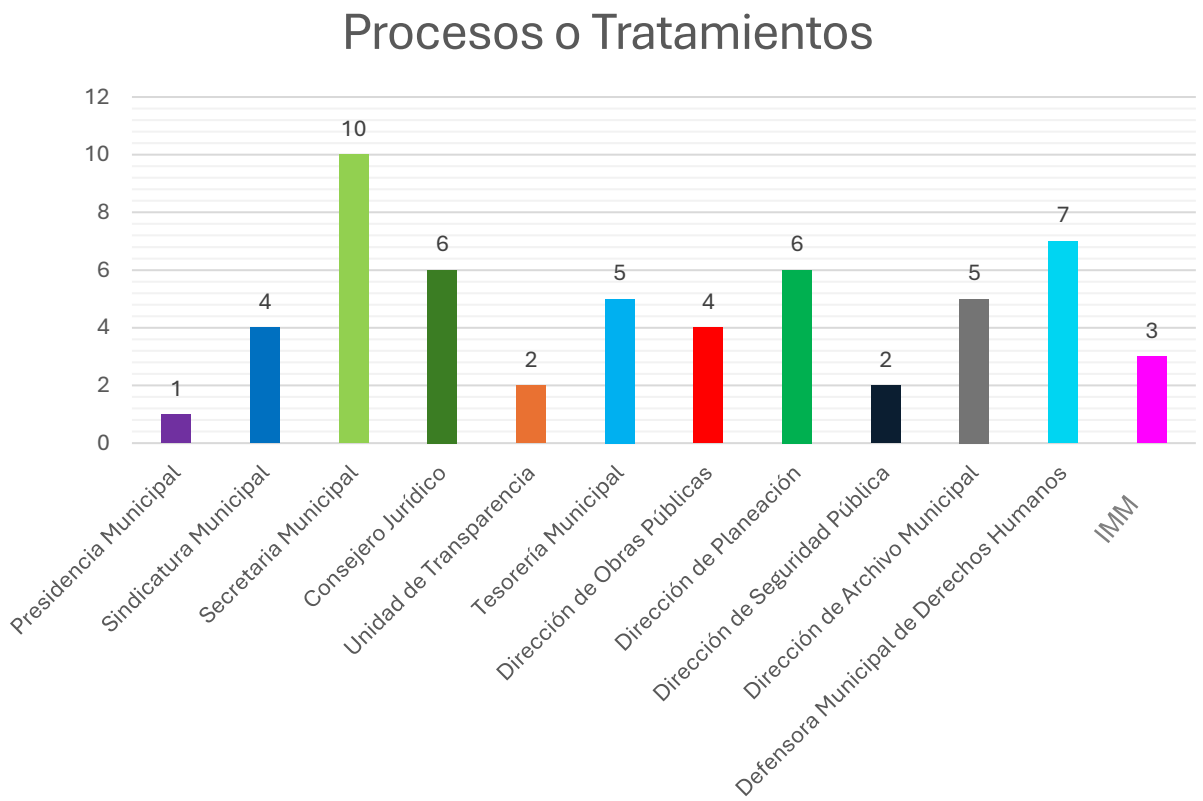
Como resultado del proceso de análisis, se identificaron también los datos personales utilizados en los tratamientos, mismos que corresponden a las tres categorías, tal como se señala a continuación:

De Identificación
Nombre, firma, domicilio, CURP, RFC, número de seguridad social, cédula profesional, año de nacimiento o edad, antecedentes laborales, características físicas, correo electrónico, Curriculum vitae, datos académicos, datos de identificación, datos laborales, datos familiares, datos personales contenido en documento para acreditar personalidad del representante, datos personales contenidos en la identificación oficial presentada por la persona física, datos sindicales, descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil, entre otros),imagen en fotografía y/o video, huella dactilar, huella digital, menor de edad, clave de elector, estado civil, teléfono, sexo, nacionalidad, nivel educativo, ocupación, sexo, títulos profesionales.

Patrimoniales
Número de cuentas bancarias, estados de cuenta, CLABE interbancaria, institución bancaria, facturas, beneficiarios, datos contenidos en declaraciones patrimoniales, descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil, entre otros).

Sensibles
Circunstancias socioeconómicas, creencias religiosas, filosóficas o morales, datos de salud, datos sobre procedimientos judiciales o seguidos en forma de juicio, discapacidad, estado de interdicción o incapacidad legal. información genética, información migratoria, lengua indígena, origen étnico o racial, otros datos biométricos, pertenencia a pueblo indígena.

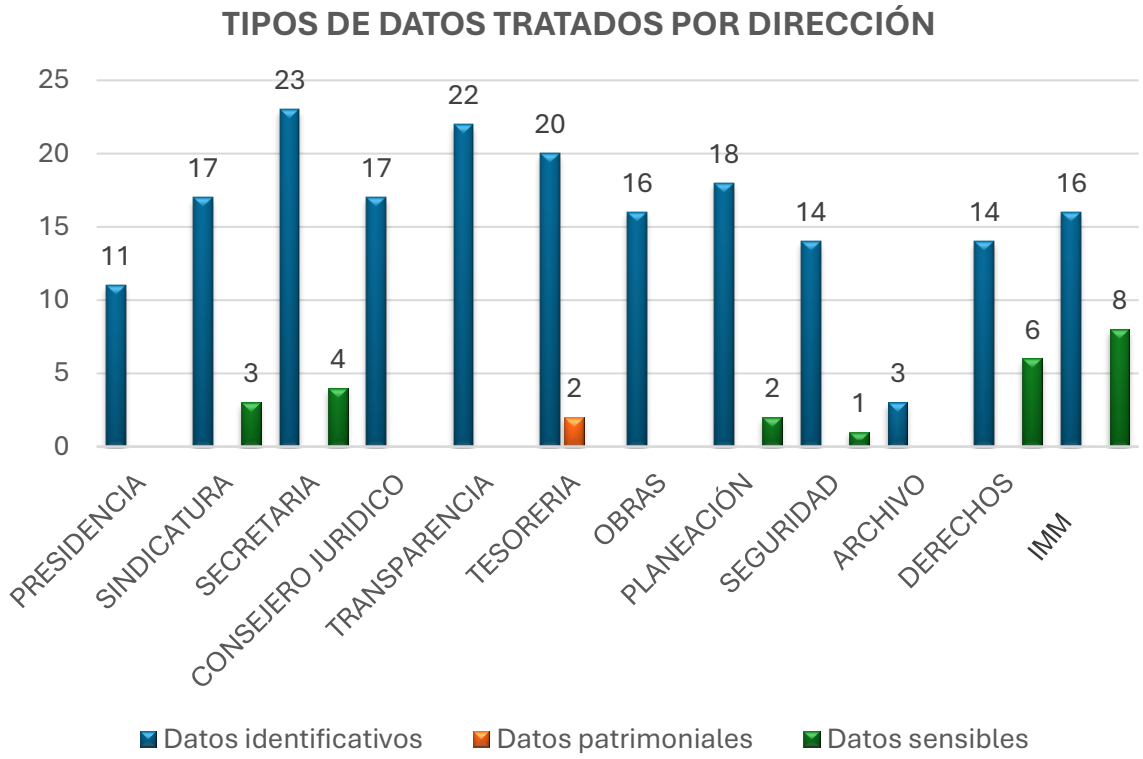
Estos datos son utilizados en 55 procesos, de los cuales una le corresponde a la Presidencia Municipal, cuatro a Sindicatura Mpal. diez a Secretaria Municipal, seis a Consejero Jurídico, dos a Unidad de Transparencia, cinco a Tesorería Mpal. Cuatro a la Dirección de Obras Públicas, seis de planeación, dos Dirección seguridad pública, cinco de Dirección de Archivos Mpal. siete a la defensora de los derechos humanos y tres a la Dirección de IMM Instituto Municipal de la Mujer Asimismo, en 55 procesos se utilizan datos personales de identificación, mientras que en 3 se recabaron datos personales patrimoniales y en lo que se refiere a datos sensibles, se manejan en 17 tratamientos.



Como se puede observar en la gráfica, el área que desarrolla mayor número de procesos es la Secretaría Municipal, con un total de diez procesos o tratamientos, tales como la elaboración de nombramientos, expedición de constancias y certificación de documentos. Por otro lado, la Presidencia Municipal es la que menos procesos realiza, con solamente uno, enfocado en la atención a la ciudadanía.

De todos los datos solicitados, todas las áreas solicitan datos de identificación, tales como nombres, direcciones y números de identificación. Solamente las áreas de Tesorería Municipal, Sindicatura Municipal y Defensora Municipal de Derechos Humanos solicitan datos patrimoniales, que incluyen información sobre ingresos, propiedades y bienes inmuebles. Además, las áreas de Sindicatura Municipal, Consejero Jurídico, Defensora Municipal de Derechos Humanos, IMM y Dirección de Seguridad Pública solicitan datos sensibles

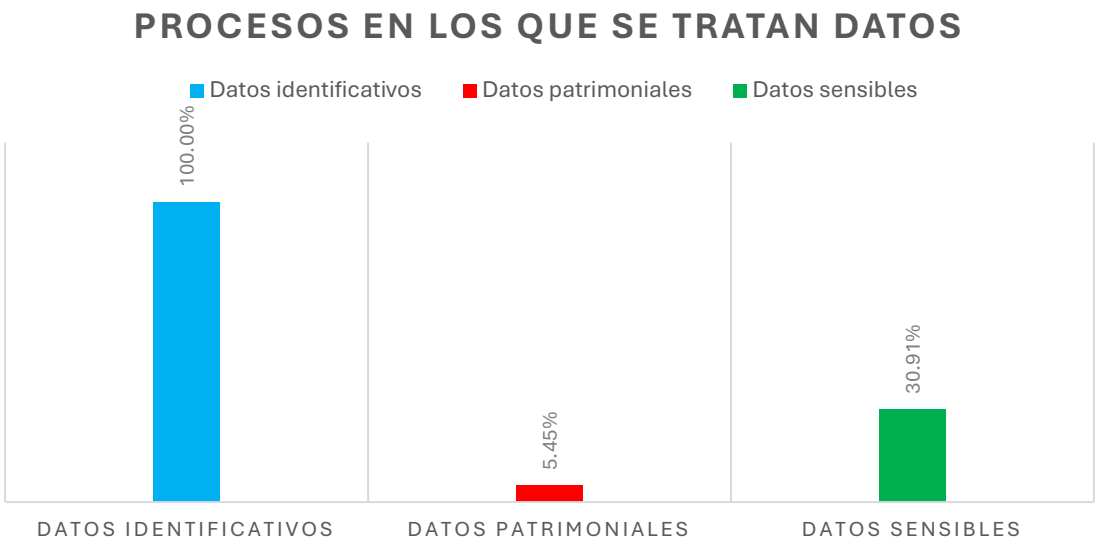
Numero de datos usados por unidad



Es posible observar que la Secretaría, la Tesorería y la Sindicatura son las áreas que desarrollan el mayor número de procesos en los que se tratan datos personales, de acuerdo con sus atribuciones y obligaciones. Lo anterior, debido a que las áreas que las integran cuentan con atribuciones para administrar los recursos humanos, materiales y financieros del ayuntamiento; lo cual implica que los procesos correspondientes a la protección de datos personales sean aplicados con mayor cuidado y puntualidad. Por lo tanto, esas áreas que cuentan con mayor número de procesos, en materia de protección de datos, deben contar con un enfoque de importancia en el desarrollo de las actividades.

Es evidente que todas las áreas analizadas manejan una variedad de datos personales, con un énfasis particular en los datos identificativos debido a la naturaleza de sus funciones. Sin embargo, también es crucial destacar la importancia del manejo de datos patrimoniales y sensibles

En relación con los procesos en los que se tratan datos personales, el 100 por ciento de los procesos usa datos identificativos, el 5.45 por ciento usa datos patrimoniales, y el 30.91 por ciento usa datos sensibles, como se muestra a continuación:

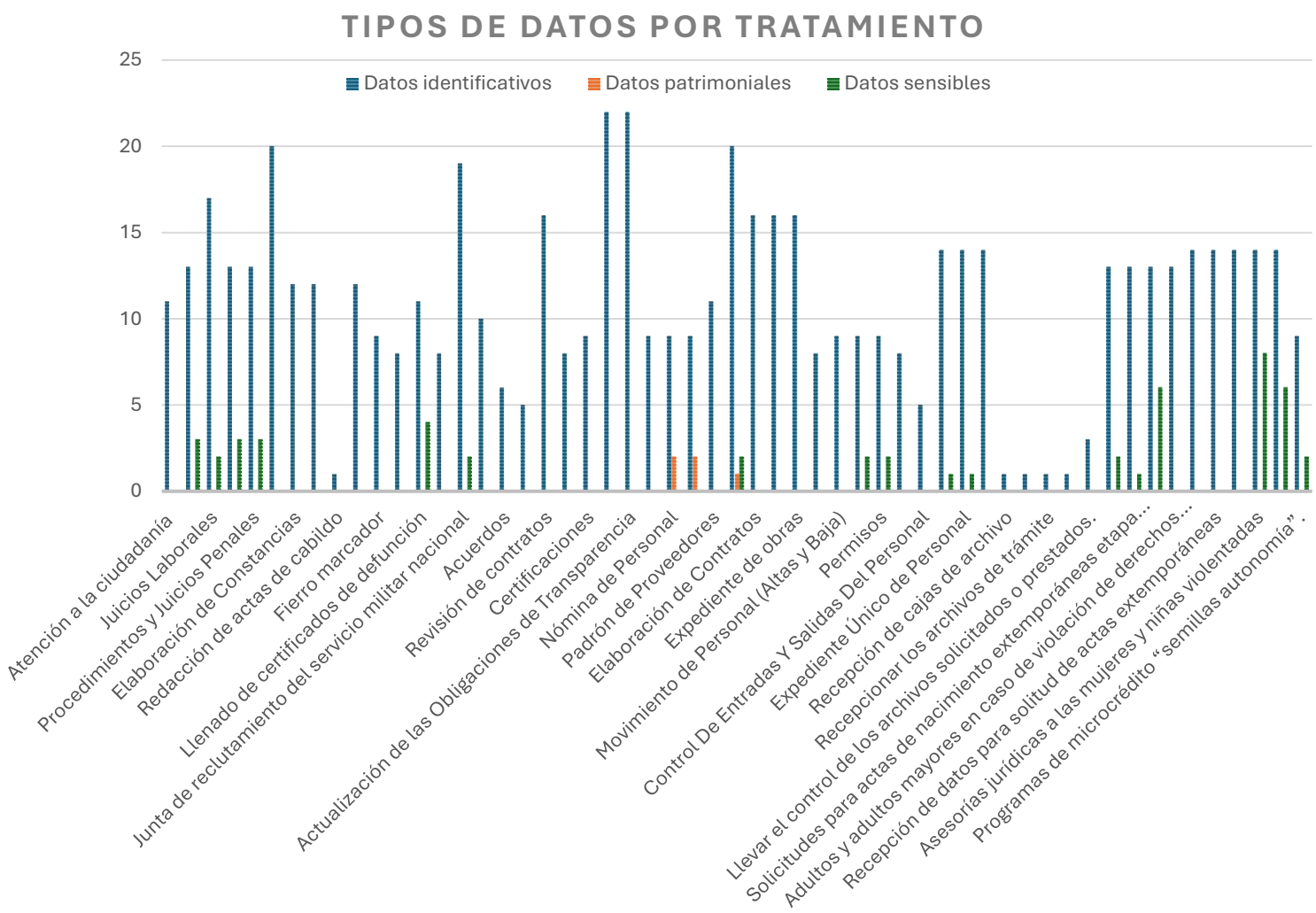


Datos Identificativos (100%): Este tipo de datos es indispensable para todos los procesos administrativos y legales. Incluye información como nombre completo, domicilio, teléfono, correo electrónico, CURP, y otros datos necesarios para identificar a las personas involucradas en los diversos procedimientos. La totalidad de los procesos, sin excepción, requiere la utilización de datos identificativos para llevar a cabo sus funciones de manera eficaz y eficiente.

Datos Patrimoniales (5.45%): Una menor proporción de los procesos administrativos y legales requiere la utilización de datos patrimoniales. Estos datos pueden incluir información sobre propiedades y bienes inmuebles, cuentas bancarias, saldos de cuentas bancarias, descuentos personales (como ahorros voluntarios, hipotecas, seguros médicos, seguros de automóviles, entre otros), y beneficiarios. Aunque su uso es limitado a menos del 6 por ciento de los procesos, su importancia es crítica en aquellos casos específicos donde se necesita evaluar la situación económica o patrimonial de las personas involucradas.

Datos Sensibles (30.91%): Una proporción considerable de los procesos (aproximadamente el 31 por ciento) maneja datos sensibles. Estos datos pueden incluir información sobre la salud, circunstancias socioeconómicas, creencias religiosas, filosóficas o morales, discapacidad, estado de interdicción o incapacidad legal, información genética, información migratoria, lengua indígena, opiniones políticas, origen étnico o racial, otros datos biométricos, pertenencia a pueblo indígena y vida sexual. La gestión de estos datos requiere un alto nivel de protección y confidencialidad debido a su naturaleza delicada y su potencial impacto en los derechos y libertades de las personas.

Este análisis pone de manifiesto la diversidad de datos personales utilizados en los distintos procesos administrativos y legales, subrayando la necesidad de implementar políticas robustas de protección de datos que garanticen la seguridad y privacidad de la información manejada.



Se destaca que no existe un sistema de base de datos del Ayuntamiento de Yajalón donde se puedan guardar los datos personales; cada área se encarga de buscar y desarrollar estrategias para brindar mayor protección a los datos personales, mediante archiveros o software para poder almacenar de manera electrónica en los equipos de cómputo.

El inventario de datos personales del Ayuntamiento de Yajalón se integra como un elemento del sistema de gestión de datos personales, en base a los hallazgos identificados en su actualización que junto con las medidas de seguridad representa un instrumento útil para la implementación de las medidas necesarias en materia de protección de datos personales.

Así mismo, se busca ayudar a planear capacitaciones enfocadas en materia de protección de datos hacia los funcionarios del H. Ayuntamiento de Yajalón, teniendo como objetivo preparar y sensibilizar a los funcionarios para los tratamientos que ellos realizan de conformidad con los estándares nacionales e internacionales en la materia. En tal virtud se consolida el inventario de datos personales del H. Ayuntamiento de Yajalón, Chiapas, como

un elemento de la política implementada para la observancia de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), aportando con ello certeza a la ciudadanía sobre cuál es y cuál es el destino de los datos que se recaban por este Sujeto Obligado.

FUNCIONES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES

En consideración e identificación de los procesos en los que se tratan datos personales, relacionado en el Inventario de Datos Personales, por las áreas que integran el H. Ayuntamiento de Yajalón, Chiapas, es muy importante plantear y definir actividades de acuerdo a las facultades y obligaciones establecidas en la Ley de Protección de Datos Personales en posesión de Sujetos Obligados del Estado de Chiapas, que otorga a los servidores públicos la aplicación correcta de este sistema en el tratamiento de los datos personales derivado de sus atribuciones.

Al momento de recibir o recabar los datos personales, el servidor público que se encargue de su recepción deberá:

1. Tener a la vista el Aviso de Privacidad.
2. Dar a conocer el aviso de privacidad al titular de los datos personales previo a la obtención de sus datos.
3. En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la DTB.
4. Al obtener los datos personales cerciorarse de que la información esté completa, actualizada, sea veraz, y comprensible.
5. Comunicar discrepancias de los datos personales recabados a su jefe inmediato o al administrador de los datos personales, ello cuando se dé cuenta.
6. Conocer y seguir las medidas de seguridad que le sean aplicables para el cuidado de los datos personales, durante el periodo en el que posea los datos personales.
7. Recabar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.
8. Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del estado de Chiapas.
9. Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del H. Ayuntamiento Municipal de Yajalón, Chiapas. En el tratamiento de datos personales.
10. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
11. Tomar, una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.

12. Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

UNIDAD ADMINISTRATIVA	**NOMBRE Y CARGO DE LA(S) PERSONA(S) FUNCIONARIA(S)QUE TRATA(N) DATOS PERSONALES**	PROCESO O TRATAMIENTO
Presidencia Municipal	Secretaria Ejecutiva Auxiliar Presidencia Municipal	Atención a la ciudadanía
Sindicatura Municipal	Auxiliar Presidencia Municipal	Juicios Civiles
		Juicios Laborales
		Juicios Administrativos
		Procedimientos y Juicios Penales
Secretaria Municipal	Auxiliar Secretaria Municipal Auxiliar Secretaria Municipal Auxiliar Secretaria Municipal	Elaboración de nombramientos
		Elaboración de Constancias
		Expedición de constancias
		Redacción de actas de cabildo
		Permiso de funcionamiento de bebidas alcohólicas
		Fierro marcador
		Traslados de ganado
		Llenado de certificados de defunción

H. AYUNTAMIENTO 2024-2027
YAJALON
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

		Certificación de documentos
		Junta de reclutamiento del servicio militar nacional
Consejero Jurídico	Consejero Jurídico Municipal	Asesorías jurídicas
		Acuerdos
		Canalizaciones
	Auxiliar	Revisión de contratos
		Revisión de convenio
		Certificaciones
Unidad de Transparencia	Director de la Unidad de Transparencia	Atención a las Solicitudes de Acceso a la Información y de Datos Personales
		Actualización de las Obligaciones de Transparencia
Tesorería Municipal	Tesorero Municipal	Cobro de ingresos
		Nómina de Personal
		Comprobación para diferentes tipos de gastos
	Auxiliar	Padrón de Proveedores
		Expediente Único de Personal

H. AYUNTAMIENTO 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

Dirección de Obras Públicas	Director De Obras Públicas	Elaboración de Contratos
		Padrón de contratistas
		Expediente de obras
		Padrón de Beneficiarios
Dirección de Planeación	Auxiliar administrativo	Movimiento de Personal (Altas y Baja)
		Incapacidades Médicas
		Permisos
		Servicio Social
		Control De Entradas Y Salidas Del Personal
		Control de expedientes curriculares
Dirección de Seguridad Pública	Director de Seguridad Publica	Expediente Único de Personal
		Certificado del centro estatal de control y confianza.
Dirección de Archivo Municipal	Responsable De Archivo Municipal	Recepción de cajas de archivo
		Vigilar la estructura y ciclo vital de los documentos
		Recepcionar los archivos de trámite

H. AYUNTAMIENTO 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

	Auxiliar De Archivo Municipal	Organización de documentos por departamento
		Llevar el control de los archivos solicitados o prestados.
Defensora Municipal de Derechos Humanos	Defensor Mpal. Derechos humanos Auxiliar Administrativo	Solicitudes para actas de nacimiento extemporáneas etapa 1 menores de edad
		Solicitudes para actas de nacimiento extemporáneas etapa 2 mayores de edad
		Atención a la primera infancia
		Adultos y adultos mayores en caso de violación de derechos humanos
		Vinculación de base de datos con el registro civil del Estado
		Recepción de datos para solitud de actas extemporáneas
		Administración de correspondencia de Derechos Humanos Estatal
IMM	Directora De Instituto Municipal De La Mujer	Asesorías jurídicas a las mujeres y niñas violentadas

H. AYUNTAMIENTO 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

Instituto Municipal De La Mujer	Auxiliar Administrativo	Terapia psicológica
		Programas de microcrédito "semillas autonomía".

UNIDAD ADMINISTRATIVA	FUNCIONES	ACCIONES
Presidencia Municipal	Ejecutar las decisiones del Ayuntamiento, ser el conducto para presentar las iniciativas de Ley en materia municipal, cumplir y hacer cumplir las leyes y reglamentos aplicables en el Municipio.	Atender las necesidades primordiales que las autoridades solicitan para el bienestar de la localidad y del Municipio.
Sindicatura Municipal	Representar legalmente al Ayuntamiento, vigilar la correcta aplicación de los recursos y el cumplimiento de las obligaciones legales.	Supervisar el uso adecuado de los recursos municipales y asegurar el cumplimiento de las leyes y regulaciones en todas las operaciones municipales.
Secretaria Municipal	Coordinar las actividades administrativas del Ayuntamiento, llevar la correspondencia oficial, y custodiar los documentos municipales.	Administrar la correspondencia oficial y documentos municipales, garantizar su correcta organización y custodia, y coordinar las actividades administrativas del Ayuntamiento.

H. AYUNTAMIENTO 2024 - 2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

Consejero Jurídico	Asesorar legalmente al Ayuntamiento, representar y defender los intereses del municipio en asuntos legales.	Proporcionar asesoramiento legal al Ayuntamiento y representar al municipio en juicios y procedimientos legales.
Unidad de Transparencia	Garantizar el acceso a la información pública y proteger los datos personales de los ciudadanos.	Responder a las solicitudes de acceso a la información pública y garantizar la protección de los datos personales en cumplimiento de la normativa de transparencia y protección de datos.
Tesorería Municipal	Administrar los recursos financieros del municipio, llevar la contabilidad y realizar los pagos correspondientes.	Gestionar los ingresos y egresos del municipio, llevar los registros contables y asegurar el cumplimiento de las obligaciones financieras.
Dirección de Obras Públicas	Planificar, ejecutar y supervisar las obras públicas en el municipio.	Desarrollar proyectos de infraestructura, supervisar su ejecución y asegurar la calidad de las obras realizadas en el municipio.
Dirección de Planeación	Elaborar planes y programas de desarrollo municipal, coordinar la ejecución de proyectos estratégicos.	Diseñar planes de desarrollo municipal, coordinar la implementación de proyectos y monitorear su avance y cumplimiento de objetivos.

H. AYUNTAMIENTO 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

Dirección de Seguridad Pública	Mantener el orden y la seguridad en el municipio, prevenir y combatir la delincuencia.	Realizar patrullajes, responder a emergencias, y coordinar acciones de prevención y combate a la delincuencia en el municipio.
Dirección de Archivo Municipal	Organizar y custodiar los archivos y documentos municipales, asegurar su preservación y acceso.	Gestionar el archivo municipal, asegurar la correcta organización y preservación de documentos, y facilitar su acceso según las normativas aplicables.
Defensora Municipal de Derechos Humanos	Proteger y promover los derechos humanos de los ciudadanos, atender denuncias y quejas sobre violaciones a los derechos humanos.	Recibir y atender denuncias y quejas, promover campañas de concienciación y educación sobre derechos humanos, y coordinar acciones para su protección y promoción.
Instituto Municipal De La Mujer	Promover la igualdad de género y el empoderamiento de las mujeres, implementar programas y políticas de apoyo a las mujeres.	Desarrollar y coordinar programas de apoyo a las mujeres, promover la igualdad de género, y ofrecer servicios de asesoría y apoyo a mujeres en situación de vulnerabilidad.

H. AYUNTAMIENTO 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

ANÁLISIS DE RIESGO

DOCUMENTO DE SEGURIDAD

ANÁLISIS DE RIESGO Y BRECHA

"Se testa el presente apartado (Análisis de Riesgo y Brecha), toda vez que contiene información que identifica de manera específica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el H. Ayuntamiento de Yajalón. Su divulgación pública representa un riesgo, ya que podría facilitar accesos no autorizados, derivar en vulneraciones a los sistemas de datos personales o comprometer gravemente la eficacia de los controles de seguridad físicos y lógicos de este Ayuntamiento.

La presente clasificación y reserva de información se realiza de conformidad con lo establecido en los Artículos 103, fracción II, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; 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."

DOCUMENTO DE SEGURIDAD

ANÁLISIS DE RIESGO Y BRECHA

"Se testa el presente apartado (Análisis de Riesgo y Brecha), toda vez que contiene información que identifica de manera específica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el H. Ayuntamiento de Yajalón. Su divulgación pública representa un riesgo, ya que podría facilitar accesos no autorizados, derivar en vulneraciones a los sistemas de datos personales o comprometer gravemente la eficacia de los controles de seguridad físicos y lógicos de este Ayuntamiento.

La presente clasificación y reserva de información se realiza de conformidad con lo establecido en los Artículos 103, fracción II, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; 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."

DOCUMENTO DE SEGURIDAD

ANÁLISIS DE RIESGO Y BRECHA

"Se testa el presente apartado (Análisis de Riesgo y Brecha), toda vez que contiene información que identifica de manera específica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el H. Ayuntamiento de Yajalón. Su divulgación pública representa un riesgo, ya que podría facilitar accesos no autorizados, derivar en vulneraciones a los sistemas de datos personales o comprometer gravemente la eficacia de los controles de seguridad físicos y lógicos de este Ayuntamiento.

La presente clasificación y reserva de información se realiza de conformidad con lo establecido en los Artículos 103, fracción II, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; 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."

DOCUMENTO DE SEGURIDAD

ANÁLISIS DE RIESGO Y BRECHA

"Se testa el presente apartado (Análisis de Riesgo y Brecha), toda vez que contiene información que identifica de manera específica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el H. Ayuntamiento de Yajalón. Su divulgación pública representa un riesgo, ya que podría facilitar accesos no autorizados, derivar en vulneraciones a los sistemas de datos personales o comprometer gravemente la eficacia de los controles de seguridad físicos y lógicos de este Ayuntamiento.

La presente clasificación y reserva de información se realiza de conformidad con lo establecido en los Artículos 103, fracción II, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; 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."

ANÁLISIS DE BRECHA

DOCUMENTO DE SEGURIDAD

ANÁLISIS DE RIESGO Y BRECHA

"Se testa el presente apartado (Análisis de Riesgo y Brecha), toda vez que contiene información que identifica de manera específica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el H. Ayuntamiento de Yajalón. Su divulgación pública representa un riesgo, ya que podría facilitar accesos no autorizados, derivar en vulneraciones a los sistemas de datos personales o comprometer gravemente la eficacia de los controles de seguridad físicos y lógicos de este Ayuntamiento.

La presente clasificación y reserva de información se realiza de conformidad con lo establecido en los Artículos 103, fracción II, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; 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."

DOCUMENTO DE SEGURIDAD

ANÁLISIS DE RIESGO Y BRECHA

"Se testa el presente apartado (Análisis de Riesgo y Brecha), toda vez que contiene información que identifica de manera específica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el H. Ayuntamiento de Yajalón. Su divulgación pública representa un riesgo, ya que podría facilitar accesos no autorizados, derivar en vulneraciones a los sistemas de datos personales o comprometer gravemente la eficacia de los controles de seguridad físicos y lógicos de este Ayuntamiento.

La presente clasificación y reserva de información se realiza de conformidad con lo establecido en los Artículos 103, fracción II, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; 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."

DOCUMENTO DE SEGURIDAD
ANÁLISIS DE RIESGO Y BRECHA

La presente clasificación y reserva de información se realiza de conformidad con lo establecido en los Artículos 103, fracción II, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; 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."

BITÁCORAS DE REPORTE DE VULNERACIONES

Para mantener un sistema de seguridad confiable, es esencial contar con un protocolo de actuación claro y estructurado en caso de vulneraciones de datos personales. El H. Ayuntamiento de Yajalón, Chiapas, establece los siguientes componentes clave para gestionar adecuadamente estas situaciones:

- **Formato de Bitácora**:
  - La bitácora debe incluir secciones para:
    - Fecha y hora del incidente.
    - Descripción del incidente.
    - Sistemas y datos afectados.
    - Acciones iniciales de respuesta.
    - Resultado de la investigación.
    - Medidas de contención y recuperación.
    - Notificación a los titulares afectados.
    - Lecciones aprendidas y acciones de mejora.

- **Acceso y Seguridad de la Bitácora**:
  - La bitácora de reporte de vulneraciones debe ser accesible solo a personal autorizado.
  - Implementar controles de acceso y cifrado para proteger la información contenida en la bitácora.

H. AYUNTAMIENTO 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

En el Ayuntamiento de Yajalón, los sistemas tecnológicos son bastante básicos, por lo que no se aplican controles de identificación y autenticación de usuarios sofisticados. Actualmente, la única medida de seguridad implementada es el uso de contraseñas para el acceso a los equipos de cómputo, repositorios y cuentas de correo institucionales. Estas contraseñas son controladas por el coordinador de cada unidad administrativa.

Medidas Actuales

1. **Contraseñas para Acceso:**
    - **Equipos de Cómputo:** Cada equipo de cómputo está protegido por una contraseña que debe ser ingresada al iniciar sesión.
    - **Repositorios:** El acceso a repositorios de documentos y datos está protegido por contraseñas.
    - **Cuentas de Correo Institucionales:** Las cuentas de correo electrónico institucionales requieren una contraseña para acceder.
2. **Control de Contraseñas:**
    - **Coordinador de Unidad:** Cada coordinador de unidad es responsable de controlar y gestionar las contraseñas de acceso para su respectiva área.
    - **Cambio Periódico de Contraseñas:** Las contraseñas se deben cambiar periódicamente para aumentar la seguridad (se recomienda cada 90 días).

H. AYUNTAMIENTO MUNICIPAL 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

La correcta gestión de los datos personales incluye la implementación de mecanismos efectivos para la realización de copias de respaldo y la recuperación de la información en caso de pérdida o daño. A continuación, se describen los sistemas y técnicas utilizados por el H. Ayuntamiento de Yajalón, Chiapas, para el almacenaje y respaldo de la información, especialmente la generada en correos institucionales, la página web oficial, y medios analógicos como los archiveros.

Copias de Respaldo

1. **Frecuencia de Respaldo**:
    - **Diario**: Se realizan copias de respaldo diarias de los datos personales almacenados en servidores y bases de datos.
    - **Semanal**: Respaldo completo semanal que incluye todos los datos almacenados, así como las configuraciones del sistema.
    - **Mensual**: Respaldo mensual adicional que se almacena de forma segura en una ubicación externa.
2. **Métodos de Respaldo**:
    - **Automatización de Respaldo**: Utilización de software de respaldo automático para asegurar que las copias se realicen de manera constante y sin intervención manual.
    - **Respaldo Incremental**: Realización de copias de solo los datos modificados o añadidos desde el último respaldo completo, optimizando el tiempo y espacio de almacenamiento.
    - **Respaldo Completo**: Copia completa de todos los datos personales en intervalos regulares, garantizando la disponibilidad de una versión completa de la información.
3. **Almacenamiento de Respaldo**:
    - **Almacenamiento Local**: Utilización de servidores internos y dispositivos de almacenamiento conectados para el respaldo local.
    - **Almacenamiento Externo**: Uso de servicios de almacenamiento en la nube para guardar copias de respaldo en ubicaciones geográficas distintas, proporcionando una capa adicional de seguridad en caso de desastres locales.
    - **Medios Físicos**: Empleo de discos duros externos y otros medios físicos para el almacenamiento de copias de respaldo críticas que se mantienen en un lugar seguro y diferente del sitio principal de trabajo.

Recuperación de Datos

1. **Plan de Recuperación de Datos**:
    - **Documentación**: Desarrollo de un plan documentado que detalle los pasos a seguir para la recuperación de datos en caso de pérdida.
    - **Roles y Responsabilidades**: Definición clara de los roles y responsabilidades del personal encargado de ejecutar el plan de recuperación.

H. AYUNTAMIENTO 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

- **Procedimientos de Prueba**: Realización de pruebas periódicas del plan de recuperación para asegurar su eficacia y actualizarlo según sea necesario.

2. **Técnicas de Recuperación**:

   - **Recuperación desde Respaldo**: Utilización de las copias de respaldo almacenadas para restaurar los datos personales en sus ubicaciones originales o en nuevas ubicaciones según el requerimiento.

   - **Recuperación de Correos Institucionales**: Implementación de herramientas específicas para la recuperación de correos electrónicos, asegurando que la información crítica contenida en los correos institucionales pueda ser restaurada rápidamente.

   - **Recuperación de la Página Web**: Uso de sistemas de gestión de contenido que permitan la recuperación rápida de la página web oficial del Ayuntamiento, incluyendo todas las bases de datos y archivos asociados.

3. **Seguridad en la Recuperación**:

   - **Autenticación y Autorización**: Implementación de procedimientos de autenticación y autorización para asegurar que solo el personal autorizado pueda acceder y recuperar los datos.

   - **Monitoreo y Registro**: Registro de todas las actividades de recuperación para mantener un control detallado y realizar auditorías posteriores si es necesario.

Gestión de Archivos en Medios Analógicos

1. **Almacenamiento y Organización de Archivos**:

   - **Archiveros**: Uso de archiveros físicos para el almacenamiento ordenado y seguro de documentos en papel que contienen datos personales.

   - **Clasificación**: Los documentos se clasifican y etiquetan adecuadamente para facilitar su localización y acceso.

   - **Condiciones de Almacenamiento**: Los archivos se almacenan en condiciones adecuadas de temperatura y humedad para prevenir el deterioro de los documentos.

2. **Respaldo y Digitalización**:

   - **Digitalización de Documentos**: Implementación de un proceso de digitalización de documentos importantes para crear copias de respaldo electrónicas que se almacenan en los sistemas digitales del Ayuntamiento.

H. AYUNTAMIENTO 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

- **Almacenamiento de Copias Digitales**: Las copias digitales se integran en los sistemas de respaldo regulares, asegurando que estén protegidas y sean recuperables en caso de pérdida o daño de los documentos físicos.

3. **Recuperación de Documentos Físicos**:

   - **Procedimientos de Acceso**: Establecimiento de procedimientos claros para el acceso y recuperación de documentos físicos desde los archiveros, garantizando que solo el personal autorizado pueda acceder a ellos.

   - **Registro de Acceso**: Mantenimiento de un registro de todos los accesos a los archivos físicos para asegurar un control adecuado y poder realizar auditorías si es necesario.

PLAN DE CONTINGENCIA

En el H. Ayuntamiento de Yajalón, Chiapas, el plan de contingencia se centra en la recuperación de datos almacenados en repositorios y unidades de almacenaje específicas de cada área, debido a la falta de un sistema tecnológico complejo.

Definición y Objetivos

El plan de contingencia del Ayuntamiento de Yajalón se define como la serie de acciones y recursos destinados a responder ante eventos intencionados o accidentales que puedan afectar los recursos informáticos o de transmisión de datos de la organización. Su objetivo principal es asegurar la continuidad operativa y la recuperación de datos críticos en caso de cualquier anomalía en el sistema de información.

Limitaciones y Consideraciones Específicas

Dado que el Ayuntamiento de Yajalón no cuenta con un sistema tecnológico complejo, el plan de contingencia se adapta a las medidas de seguridad específicas implementadas en cada área. Aunque no se ha diseñado un plan municipal formal en términos complejos, se asegura la capacidad de recuperación de datos a través de los repositorios y unidades de almacenaje disponibles.

En resumen, el enfoque del plan de contingencia del Ayuntamiento de Yajalón se centra en la recuperación efectiva de datos críticos mediante los recursos locales disponibles, garantizando así la continuidad operativa ante cualquier eventualidad en el sistema de información.

TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES

La supresión y el borrado seguro de los datos personales es una parte esencial de la gestión de la información en el H. Ayuntamiento de Yajalón, Chiapas. Estos procesos aseguran que los datos personales sean eliminados de manera irreversible una vez que se haya cumplido con la finalidad de su utilización, protegiendo así la privacidad de los titulares de los datos.

Mecanismos de Supresión y Borrado Seguro

1. **Borrado Seguro en Sistemas Digitales**:
    - **Borrado Criptográfico**: Eliminación de datos cifrados mediante la destrucción de las claves de cifrado, haciendo que los datos sean ininteligibles y, por lo tanto, inútiles.
    - **Formateo Seguro**: Empleo de herramientas de formateo seguro que no solo eliminan los datos, sino que también reescriben la estructura del disco para prevenir la recuperación de datos.
    - **Borrado de Archivos en Nube**: Uso de las opciones de eliminación segura proporcionadas por los servicios de almacenamiento en la nube, asegurando que los datos eliminados no sean recuperables desde los servidores remotos.
2. **Borrado de Datos en Bases de Datos**:
    - **Purga de Bases de Datos**: Implementación de procesos de purga que eliminan completamente los registros y cualquier índice asociado, seguido de una reconstrucción de índices para asegurar que los datos no sean recuperables.
3. **Destrucción de Documentos Físicos**:
    - **Trituración de Documentos**: Uso de trituradoras de alta seguridad que convierten los documentos en tiras o partículas finas, asegurando que los datos no puedan ser reconstruidos.
    - **Reciclaje Seguro**: Proceso de reciclaje que incluye la trituración de documentos antes de su reciclaje, garantizando la destrucción de los datos personales.

Implementación de sistemas de supresión y borrado

H. AYUNTAMIENTO 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

El H. Ayuntamiento de Yajalón, Chiapas, cuenta con un sistema de técnicas para la supresión y borrado seguro de los datos personales, implementado a través de los siguientes mecanismos:

1. **Políticas y Procedimientos**:
   - Desarrollo de políticas claras para la eliminación de datos personales, alineadas con las regulaciones y mejores prácticas.
2. **Capacitación del Personal**:
   - Formación regular del personal sobre las técnicas y procedimientos para la eliminación segura de datos.
   - Sensibilización sobre la importancia de la privacidad y la protección de datos personales.
3. **Herramientas y Tecnología**:
   - Adopción de herramientas de software específicas para el borrado seguro de datos en dispositivos digitales.
   - Uso de equipos de trituración de alta seguridad para la destrucción de documentos físicos.
4. **Auditorías y Verificación**:
   - Realización de auditorías periódicas para verificar el cumplimiento de las políticas y procedimientos de eliminación de datos.
   - Monitoreo y registro de todas las actividades de supresión y destrucción de datos para asegurar la trazabilidad y responsabilidad.

En caso de no contar con un sistema específico de técnicas para la supresión y borrado seguro de datos, el Ayuntamiento implementa procedimientos manuales y utiliza herramientas de terceros confiables para asegurar la eliminación efectiva de la información, adaptándose a las mejores prácticas y normativas vigentes para la protección de datos personales.

GESTIÓN DE VULNERACIONES DE SEGURIDAD DE LA INFORMACIÓN

La gestión de vulneraciones de seguridad de la información se refiere a la respuesta organizada y planificada ante cualquier incidente de seguridad que afecte los datos personales. Estos incidentes pueden incluir pérdida, destrucción no autorizada, robo, extravío o copia no autorizada de datos personales, entre otros.

Procedimientos de Identificación y Notificación de Vulneraciones

1. **Identificación de Vulneraciones**:
   - Monitoreo continuo de los sistemas y procesos de tratamiento de datos para detectar incidentes de seguridad.
   - Establecimiento de indicadores de riesgo y alertas tempranas.
   - Evaluación periódica de vulnerabilidades y pruebas de penetración.

2. **Notificación de Vulneraciones**:
   - En caso de detectar una vulneración, se debe notificar de inmediato al responsable de la seguridad de la información.
   - La notificación interna debe incluir una descripción del incidente, los datos personales comprometidos y las medidas inmediatas adoptadas para contener la vulneración.
   - Conforme al artículo 52 de la LPDPPSOECH, se debe notificar a la autoridad de protección de datos en un plazo máximo de 72 horas desde la detección del incidente, salvo que sea improbable que la vulneración constituya un riesgo para los derechos y libertades de los titulares de los datos.

Medidas de Contención y Remediación

1. **Medidas Inmediatas**:
   - Aislar el sistema afectado para prevenir la propagación del incidente.
   - Cambiar credenciales y contraseñas comprometidas.
   - Implementar soluciones de emergencia para proteger los datos restantes.

2. **Investigación del Incidente**:
   - Realizar una investigación detallada para determinar la causa raíz del incidente.
   - Documentar todas las acciones tomadas y los hallazgos de la investigación.

3. **Medidas Correctivas**:
   - Reparar vulnerabilidades explotadas durante el incidente.
   - Reforzar las políticas de seguridad y actualizar los protocolos de protección de datos.
   - Implementar mejoras en los sistemas y procesos de seguridad para prevenir futuras vulneraciones.

Comunicación a los Titulares de los Datos

1. **Información a los Titulares**:
   - En caso de que la vulneración pueda resultar en un alto riesgo para los derechos y libertades de los titulares de los datos, se les debe informar de manera clara y oportuna.
   - La comunicación debe incluir la naturaleza de la vulneración, las posibles consecuencias y las medidas adoptadas para mitigar los efectos adversos.

Registro y Evaluación de Vulneraciones

1. **Registro de Incidentes**:

- Mantener un registro detallado de todas las vulneraciones de datos personales, independientemente de su gravedad.
- El registro debe incluir información sobre la naturaleza del incidente, los datos comprometidos, las acciones tomadas y las lecciones aprendidas.

2. **Evaluación Post-Incidente**:
   - Realizar una evaluación posterior al incidente para analizar la eficacia de la respuesta y mejorar los procedimientos de gestión de vulneraciones.
   - Ajustar las estrategias de seguridad y los planes de contingencia basados en los resultados de la evaluación.

El H. Ayuntamiento de Yajalón, Chiapas, se compromete a mantener altos estándares de seguridad en el tratamiento de datos personales, implementando medidas proactivas y reactivas para gestionar cualquier vulneración de manera eficaz y conforme a la normativa vigente.

PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN

DOCUMENTO DE SEGURIDAD
PLAN DE TRABAJO PARA LA IMPLEMENTACION

"Se testa el presente apartado (Análisis de Riesgo y Brecha), toda vez que contiene información que identifica de manera específica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el H. Ayuntamiento de Yajalón. Su divulgación pública representa un riesgo, ya que podría facilitar accesos no autorizados, derivar en vulneraciones a los sistemas de datos personales o comprometer gravemente la eficacia de los controles de seguridad físicos y lógicos de este Ayuntamiento.

La presente clasificación y reserva de información se realiza de conformidad con lo establecido en los Artículos 103, fracción II, y 112, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; 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."

[redacted]

MEDIDAS DE SEGURIDAD

La normatividad establece que se entenderá como medidas de seguridad al conjunto de acciones, actividades, controles o mecanismos administrativos, físicos y técnicos que permiten proteger los datos personales.

LAS MEDIDAS DE SEGURIDAD ADMINISTRATIVAS. Se traducen en políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación clasificación y borrado seguro de la información; así como la sensibilización y capacitación del personal en materia de protección de datos personales.

LAS MEDIDAS DE SEGURIDAD FÍSICAS. Son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

MEDIDAS DE SEGURIDAD TÉCNICAS. Son el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con el hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

En tal sentido y de manera general en el H. Ayuntamiento de Municipal de Yajalón, Chiapas, se cuenta con las medidas de seguridad siguientes:

DE TIPO FÍSICO. La Dirección de Protección Civil del H. Ayuntamiento de Yajalón y la Secretaría de Administración salvaguardan la integridad y seguridad de las personas, bienes, activos e instalaciones del H. Ayuntamiento del Municipio de Yajalón, Chiapas,

Mediante procedimientos y mecanismos institucionales de identificación y prevención de riesgos de seguridad, como:

- Prevenir el acceso no autorizado al perímetro de organización de las dependencias, sus instalaciones físicas, áreas críticas, recursos e información: mediante control de accesos, de recepción, vigilancia, control de estacionamientos.

- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas, recursos e información, contando con procedimientos y medidas de seguridad integradas en el

programa de protección civil: protocolos de acceso a las áreas estratégicas, ante manifestaciones, amenazas de bomba, sismos y de incendio.

- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que puedan salir de las oficinas. Se cuenta con acciones y mecanismos que permiten proteger e identificar los equipos móviles y portátiles; mobiliario, documentos y materiales mediante controles tales como pases de salida autorizado por el director del área.

DE TIPO TÉCNICO: Son las que se consideran aplicables para los sistemas de tratamiento tyde datos en soporte electrónico (Hardware y Software).

- Para prevenir que el acceso a las bases de datos o a la información y a los recursos, sea realizado solo por usuarios identificados y autorizados. El acceso a las bases de datos de cada unidad administrativa es exclusivo para personal de su adscripción, incluido el personal que da soporte, y aquellos autorizados. El acceso se efectúa a través de segmento de red.

- Para generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones. Las funciones del usuario de los sistemas de información institucionales son definidas por las áreas responsables de los procesos correspondientes, así como de validar su perfil.

- Para revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del hardware y software.

- Para gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos. Mediante revisión de sistemas de información, que identifiquen aquellos que estén fuera de servicio.

H. AYUNTAMIENTO 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

La implementación de un Programa de Protección de Datos Personales en el H. Ayuntamiento de Yajalón, Chiapas, es fundamental para garantizar el resguardo de la información y la conformidad con la normativa vigente. Este programa se basa en la formación y sensibilización continua de los servidores públicos para mejorar la gestión de datos personales. A continuación, se presenta una propuesta de capacitación diseñada para profundizar el conocimiento de quienes intervienen en el tratamiento de datos personales.

Objetivo del Programa de Capacitación

El objetivo es proporcionar a los servidores públicos del Ayuntamiento las herramientas y conocimientos necesarios para proteger adecuadamente los datos personales bajo su

responsabilidad, asegurando el cumplimiento de la normatividad y la implementación de las mejores prácticas de seguridad.

Estructura del Programa de Capacitación

La capacitación se desarrollará en módulos temáticos que abordarán diferentes aspectos de la protección de datos personales. Se proponen las siguientes áreas temáticas para las sesiones de capacitación:

Objetivos de la Capacitación

1. **Concienciar a los Empleados**: Aumentar la concienciación sobre la importancia de proteger los datos personales y las consecuencias legales y éticas de las violaciones de datos.
2. **Desarrollar Competencias**: Proveer a los empleados con las habilidades y conocimientos necesarios para manejar los datos personales de manera segura y conforme a la ley.
3. **Implementar Buenas Prácticas**: Fomentar la adopción de buenas prácticas en la gestión y protección de datos personales.
4. **Cumplir con la Legislación**: Asegurar que todos los empleados comprendan y cumplan con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOECH).

Contenido del Programa de Capacitación

1. **Introducción a la Protección de Datos Personales**
   - Definición de datos personales y datos sensibles.
   - Importancia de la protección de datos personales.
   - Principios y derechos de los titulares de los datos personales.
2. **Marco Legal y Normativo**
   - Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOECH).
   - Reglamentos y directrices aplicables.
   - Obligaciones del Ayuntamiento y de los empleados.
3. **Gestión de Datos Personales**
   - Ciclo de vida de los datos personales: recolección, uso, almacenamiento, y eliminación.
   - Procedimientos seguros para la recolección y tratamiento de datos.
   - Mecanismos de consentimiento informado.
4. **Seguridad de la Información**
   - Medidas técnicas y organizativas para proteger los datos personales.
   - Gestión de contraseñas y autenticación.
   - Protección de datos en dispositivos móviles y almacenamiento en la nube.

5. **Gestión de Vulneraciones**
   - Identificación y reporte de incidentes de seguridad.
   - Protocolo de actuación en caso de vulneración de datos personales.
   - Registro y documentación de incidentes.
6. **Derechos de los Titulares de Datos Personales**
   - Acceso, rectificación, cancelación y oposición (ARCO).
   - Procedimientos para atender solicitudes de los titulares.
   - Transparencia y comunicación con los titulares de datos.
7. **Destrucción Segura de Datos Personales**
   - Técnicas de supresión y borrado seguro de datos.
   - Procedimientos para la eliminación segura de documentos físicos y digitales.
   - Mantenimiento de registros de destrucción de datos.

Modalidades de Capacitación

1. **Talleres Presenciales**
   - Sesiones interactivas con ejercicios prácticos y estudios de caso.
   - Oportunidad para discusión y aclaración de dudas.
2. **Cursos en Línea**
   - Módulos de aprendizaje a través de una plataforma de e-learning.
   - Flexibilidad para que los empleados completen los cursos a su propio ritmo.
3. **Seminarios y Conferencias**
   - Invitación a expertos en protección de datos y seguridad de la información para impartir charlas y conferencias.
   - Actualización sobre tendencias y mejores prácticas en protección de datos.
4. **Material de Apoyo y Recursos**
   - Manuales y guías prácticas sobre protección de datos personales.
   - Boletines informativos y actualizaciones periódicas sobre cambios legislativos y nuevas amenazas.

Evaluación y Seguimiento

1. **Evaluaciones Periódicas**
   - Pruebas y cuestionarios para evaluar el conocimiento adquirido.
   - Evaluaciones prácticas para medir la aplicación de los conocimientos en situaciones reales.
2. **Retroalimentación Continua**
   - Encuestas y feedback de los participantes para mejorar los programas de capacitación.
   - Sesiones de retroalimentación con los responsables de cada área para identificar necesidades específicas de capacitación.
3. **Certificación**
   - Emisión de certificados de participación y cumplimiento al finalizar los cursos.
   - Reconocimiento a los empleados que demuestren un alto nivel de competencia en protección de datos.

H. AYUNTAMIENTO 2024-2027
YAJALÓN
CONTINUIDAD Y DESARROLLO POR UN YAJALÓN UNIDO

Plan de Implementación

1. **Diagnóstico Inicial**
   - Evaluación de las necesidades de capacitación y el nivel actual de conocimiento en protección de datos personales.
2. **Desarrollo de Contenidos**
   - Creación de materiales de capacitación adaptados a las necesidades del Ayuntamiento y sus empleados.
3. **Calendario de Capacitación**
   - Planificación de sesiones de capacitación presenciales y en línea a lo largo del año.
   - Priorización de áreas y departamentos con mayor exposición a datos personales.
4. **Monitoreo y Ajuste**
   - Seguimiento continuo del progreso del programa de capacitación.
   - Ajustes y mejoras basadas en los resultados de las evaluaciones y la retroalimentación recibida.

DOCUMENTO DE SEGURIDAD	
SISTEMA DE DATOS PERSONALES DEL H. AYUNTAMIENTO YAJALÓN, CHIAPAS.	
FECHA DE ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD : 20 DE AGOSTO DE DEL 2026	FECHA DE ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD : 20 DE AGOSTO DE DEL 2026
ELABORÓ:	**APROBÓ:**
UNIDAD DE TRANSPARENCIA DEL H. AYUNTAMIENTO DE YAJALÓN, CHIAPAS	COMTE DE TRANSPARENCIA DEL H. AYUNTAMIENTO DE YAJALÓN, CHIAPAS. 28 DE AGOSTO DEL 2026
LIC. JOSUE ENRIQUE RODRÍGUEZ BONIFAZ OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	**PRESIDENTE:** LIC. MIGUEL ÁNGEL UTRILLA ROBLES **SECRETARIO:** LIC. MARÍA ISABEL CAMPAÑA MARTÍNEZ **VOCAL:** LIC. JOSUÉ ENRIQUE RODRÍGUEZ BONIFAZ