ESTE DOCUMENTO TIENE COMO PROPÓSITO CONTROLAR INTERNAMENTE LOS SISTEMAS DE DATOS PERSONALES.

QUE POSEE EL AYUNTAMIENTO DE ESCUINTLA; CHIAPAS

EL TIPO DE DATOS PERSONALES QUE CONTIENE CADA UNO, DE LOS RESPONSABLES, ENCARGADOS.

DOCUMENTO DE SEGUIDAD (DS)

PARA PROTECCIÓN DE DATOS PERSONALES

TRANSPARENCIA

	Página
PRESENTACIÓN	2
1. Objetivos del documento de seguridad	3
2. Responsabilidades	3
3. Alcance del documento de seguridad	5
4. Sistema de Gestión de los datos personales	6
5. Inventario de tratamientos y datos personales	9
6. Funciones y responsabilidades del tratamiento de datos personales	16
7. Análisis de riesgo y brecha	18
8. Análisis de la información	21
9. Medidas de seguridad	25
10. Monitoreo de medidas de seguridad	27
11. Programa de trabajo para la implementación de medidas de seguridad	27
12. Propuesta de capacitación en materia de datos personales	28
13. Actualización del documento de seguridad	29

PRESENTACIÓN

El documento de Seguridad para Sistemas (SD) Para el ayuntamiento de Escuintla, Chiapas. Es el instrumento Obligatorio que exige la ley para proteger la información confidencial de los ciudadanos y servidores públicos.

Los 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, se elabora de conformidad a lo establecido en el **artículo 55 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas,** el cual establece que el sujeto obligado es responsable de elaborar y aprobar un documento, el cual deberá de contener medidas de seguridad de carácter físico, técnico y administrativo.

Mediante este documento se busca fortalecer los sistemas administrativos, mejorando los procesos relativos a la confidencialidad, integridad y disponibilidad de la información. Es un instrumento que establecerá medidas, procedimientos administrativos, físicos y técnicos que serán aplicables a los sistemas de datos personales para garantizar que éstos sean tratados conforme a los principios de licitud, consentimiento, calidad de los datos, confidencialidad, seguridad, disponibilidad y temporalidad. El Documento de Seguridad expone con detalle la estructura del sujeto obligado, señalando los puestos, la jerarquía, el grado de autoridad y responsabilidad, lo cual permitirá adoptar medidas idóneas para el tratamiento de los datos personales.

Este Documento tiene como finalidad describir las medidas de seguridad, así como el personal autorizado y niveles jerárquicos del personal del sujeto obligado que tiene contacto con la información la cual variará en la medida que existan modificaciones al interior de este, por lo que es necesaria su revisión y actualización permanente para que se cumpla con el propósito para el cual fue suscrito.

1. 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 del municipio de Escuintla, 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

.

2. RESPONSABILIDADES

De conformidad con lo dispuesto por el artículo 113 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas (LPDPPSOCHIS), el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales, 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. Elaborar, aprobar, coordinar y supervisar el Programa, en conjunto con las áreas técnicas que estime necesario involucrar o consultar;
II. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
III. Dar a conocer el Programa al interior del sujeto obligado;
IV. Coordinar la implementación del Programa en las unidades administrativas del sujeto obligado;

V. Asesorar a las unidades administrativas en la implementación de este Programa, con el apoyo de la Dirección de Capacitación;
VI. Presentar un informe anual al titular de la institución, en el que se describan las acciones realizadas para cumplir con lo dispuesto por este Programa;
VII. Supervisar la correcta implementación del Programa;
VIII. Elaborar, aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con las áreas técnicas que estime necesario involucrar o consultar, y
IX. Las demás que de manera expresa señale el propio Programa.

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 del Pleno y la Presidencia del Instituto, a fin de que tomen las medidas necesarias para que el mismo se observe en este Instituto.

La intervención del Comisionado presidente 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.

Las unidades administrativas deberán 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.

3. ALCANCE DEL DOCUMENTO DE SEGURIDAD

El alcance de este documento de seguridad se relaciona con la identificación de sistemas de información o procesos administrados por parte de 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 medios electrónicos como en los espacios físicos en que se administran, operan y administran, con observancia de los principios, deberes y obligaciones que establece la ley.

Quedan exceptuados de la aplicación de este programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren el artículo 18 de la Ley de Transparencia y Acceso a la Información Pública del estado de Chiapas.

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

- ✓ **Presidencia Municipal**
- ✓ **Sindicatura Municipal**
- ✓ **Contraloría Municipal**
- ✓ **Secretaría Municipal**
- ✓ **Tesorería Municipal**
- ✓ **Dirección de Obras Publicas**
- ✓ **Fomento Agropecuario**
- ✓ **Fortalecimiento para la Gestión Institucional**
- ✓ **Unidad de Transparencia**
- ✓ **Protección Civil**
- ✓ **Secretario Ejecutivo de Seguridad Publica**
- ✓ **Seguridad Pública Municipal**
- ✓ **Juzgado Municipal**

La Unidad de Transparencia integra este documento de seguridad con base en la información generada por todas las unidades administrativas que conforman el H. Ayuntamiento de Escuintla, Chiapas.

4. SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES

Para el tratamiento de los datos personales que lleva a cabo el H. Ayuntamiento de Escuintla; Chiapas, garantiza el tratamiento de los datos personales que lleva a cabo como parte de sus funciones desde de su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable a los mismo; se realiza el establecimiento de políticas y métodos orientados a salvaguardar su confidencialidad, integridad y disponibilidad de estos datos, conforme a los preceptos previstos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley General de Transparencia y Acceso a la Información Pública.

Por lo anterior el H. Ayuntamiento de Escuintla inició un proceso de organización y planeación de los medios para la protección de datos, mediante la identificación de todos y cada uno de los procesos y tareas en los que, de acuerdo con el ámbito de funciones de las distintas áreas que conforman la institución, se involucra el tratamiento de datos personales. Para ello, se dispuso de un formato que facilitó a las diversas unidades administrativas, realizar el levantamiento de inventarios de los datos personales que se encuentran bajo 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, con el propósito de identificar entre otros aspectos, la categoría y tipo datos que son sometidos a 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, y 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.

En ese mismo sentido, el inventario ha contribuido para la consideración del **ciclo de vida** de los datos personales, entendiendo que una vez concluida la finalidad los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, lo que cobra especial relevancia en el marco del proceso de baja documental que las áreas realizan conforme a las disposiciones que regulan la gestión documental al interior del Ayuntamiento de Escuintla.

De igual forma, Una vez integrados los inventarios de tratamientos y de datos, se dispuso de la metodología para el **análisis de riesgos**, con la intención de que se identificaran el valor de los datos de acuerdo a su categoría 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.

Con base en dicho análisis de riesgo, además de promover el reconocimiento de las medidas de seguridad administrativas, entendidas como el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información; físicas, que corresponden a las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento y, técnicas que se valen de la tecnología para proteger el entorno digital de la información, también se han registrado nuevas medidas de seguridad que deberán desarrollarse para fortalecer algunos de los controles que actualmente son implementados; es decir, el **análisis de brecha** a partir del cual será posible mitigar los riesgos a los que están expuestos los datos tratados, para que garanticen la seguridad de los datos, tanto administrativas, como físicas y técnicas.

A partir de esta identificación de potenciales 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; pueden ser intencionales o no, pero pondrían en riesgo los activos de información.

Tipos de amenazas:

- 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 de manera general 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; por lo que las medidas de seguridad por parte de las áreas comisionadas están orientadas a proteger los datos personales. A partir de la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que de acuerdo a la experiencia y mejores prácticas son monitoreadas para lograr la mejora continua por parte de todos los involucrados en el tratamiento.

En el marco del sistema de gestión y política de seguridad institucional, se procurará:

- Tratar datos personales de manera lícita, conforme a las disposiciones establecidas.
- Informar a los titulares del tratamiento de los datos y sus finalidades;
- Sujetar el tratamiento de datos personales al principio de consentimiento salvo las excepcionas previstas por la Ley;
- Procurar que los datos personales tratados sean correctos y estén actualizados;

- Suprimir los datos personales cuando hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron;
- Tratar los datos personales estrictamente para propósitos legales o legítimos para el cual fueron obtenidos y estrictamente los necesarios para las finalidades;
- No obtener datos personales a través de medios fraudulentos;
- 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 H. Ayuntamiento de Escuintla; Chiapas.
- Respetar los derechos de los titulares en relación con sus datos personales;
- Identificar a los servidores públicos del Ayuntamiento de Escuintla responsables del tratamiento de los datos personales;

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.

5. INVENTARIO DE TRATAMIENTOS Y DATOS PERSONALES

Para el debido cumplimiento de las obligaciones es necesario que cada una de las unidades administrativas realicen 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 municipio.

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

En tal virtud, en coordinación con las áreas, como resultado del proceso de actualización de la información, se logró identificar a las unidades administrativas que realizan tratamientos con datos personales; y estas son:

- ✓ **Presidencia Municipal**
- ✓ **Sindicatura Municipal**
- ✓ **Contraloría Municipal**
- ✓ **Secretaría Municipal**
- ✓ **Tesorería Municipal**
- ✓ **Dirección de Obras Publicas**
- ✓ **Fomento Agropecuario**
- ✓ **Fortalecimiento para la Gestión Institucional**
- ✓ **Unidad de Transparencia**
- ✓ **Protección Civil**
- ✓ **Secretario Ejecutivo de Seguridad Publica**
- ✓ **Seguridad Pública Municipal**
- ✓ **Juzgado Municipal**

Todos los tratamientos se realizan en apego a sus facultades y obligaciones que las normativas les confieren, a través de las diversas áreas que lo integran y permiten el desarrollo de los procesos que realizan para el cumplimiento de dichas funciones.

Con base a lo anterior, fue posible identificar 44 procesos que se desarrollan, que implican el tratamiento de datos personales, que a continuación se describen:

Unidad Administrativa	Area o Departamento	Proceso o Tratamiento
Presidencia Municipal	Presidencia Municipal	Atencion a la Ciudadanía
Sindicatura Municipal	Sindicatura Municipal	Juicios Laborales
		Juicios Administrativos
		Procedimientos Administrativos
Contraloría Municipal	Contraloría Municipal	Proceso de entrega-Recepción
		Declaración de situación patrimonial
Secretaria Municipal	Secretaria Municipal	Convenios
		Elaboración de Constancias
		Registro de Fierro Marcador
		Elaboración de nombramientos
		Actas de Cabildo
		Tramite de Cartilla de Servicio Militar
Tesorería Municipal	Tesorería Municipal	Nómina de Personal
		Expediente Único de Personal
		Comprobación para diferentes tipos de gastos
		Padrón de Proveedores
		Cobro de ingresos
Dirección de obras Publicas	Dirección de obras Publicas	Padrón de contratistas
		Elaboración de Contratos
		Expediente de obras
		Registro de contratistas
		Padrón de Beneficiarios
		Comprobaciones
		Supervisiones de obras
Fomento Agropecuario	Fomento Agropecuario	Padrón de Beneficiarios
		Comprobaciones
Fortalecimiento para la Gestión Institucional	Fortalecimiento para la Gestión Institucional	Capacitaciones Comité de COPLADEM
Unidad de transparencia	Unidad de transparencia	Atencion a las Solicitudes de Acceso a la Información y de Datos Personales
		Seguimiento al Directorio del Sujetos Obligado
		Actualización de las Obligaciones de Transparencia
		Seguimiento de denuncias por incumplimiento de las Obligaciones de Transparencia
Protección Civil	Protección Civil	Lista de Asistencia
		Expediente del Personal
Consejo Municipal de Seguridad Publica	Consejo Municipal de Seguridad Publica	Expediente Único de Personal
		Convenios y Contratos
		Tramite de carta laboral
		Certificado del centro estatal de control y confianza
Seguridad Pública Municipal	Seguridad Pública Municipal	Registro de Detenidos
		Notificaciones
		Requisitos para cumplir con los lineamientos (Nacionalidad)
		Alta de Elementos en el sistema
Juzgado Municipal	Juzgado Municipal	Actos Conciliatorios
		Asuntos Familiares (Separación, régimen de visitas, guarda y custodia)

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 Y CONTACTO:

Firma, Nombre de la Persona Física, Antecedentes Laborales, CURP, RFC, Estado Civil, Cedula Profesional, Año de nacimiento o Edad, Beneficiarios, Correo electrónico Personal, Curriculum Vitae, Datos Académicos, Datos contenidos en declaraciones patrimoniales, Datos de identificación, Datos de Salud, Domicilio, Huella Dactilar, Menor de Edad, Nacionalidad, Nivel Educativo, Ocupación, Sexo, Teléfono fijo o Celular, Títulos Profesionales.

PATRIMONIALES

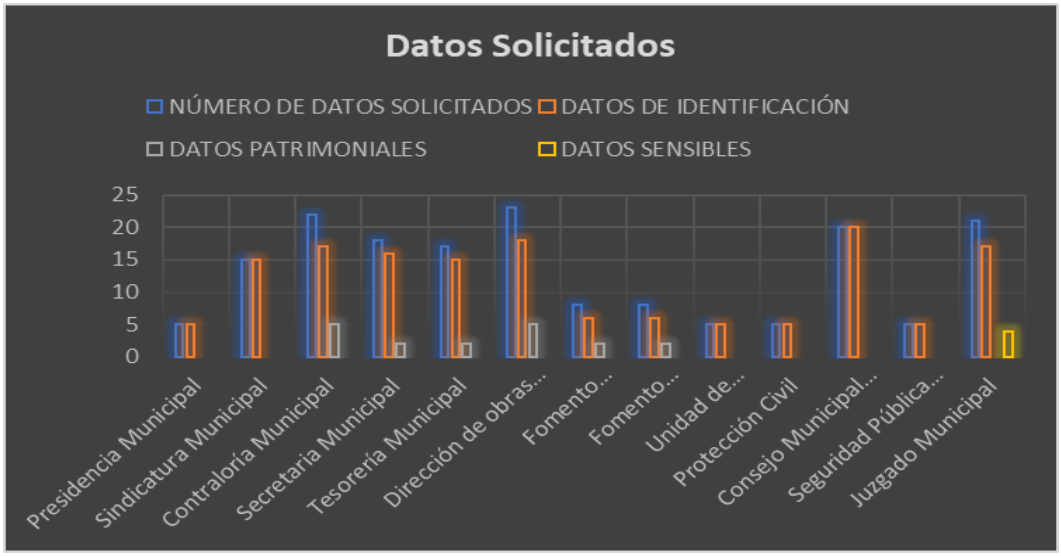
Número de Cuenta, Cuentas bancarias, estados de cuenta, CLABE interbancaria, institución bancaria, facturas, datos contenidos en declaraciones patrimoniales, descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil, entre otros).

SENSIBLES

Circunstancias socioeconómicas, creencias religiosas, filosóficas o morales, datos sobre procedimientos judiciales o seguidos en forma de juicio, discapacidad, estado de interdicción o incapacidad legal, información migratoria, lengua indígena.

Estos datos son utilizados en 44 procesos, de los cuales uno corresponde a presidencia, tres a sindicatura, dos a Contraloría, seis a Secretaría Municipal, cinco a Tesorería Municipal, siete a la Dirección de Obras Públicas Municipales, dos de Fomento Agropecuario, dos de Fomento Económico y Social, cuatro de Unidad de Transparencia, dos de Protección Civil, cuatro de secretario ejecutivo de Seguridad Pública, cuatro de Seguridad Pública, dos de Juzgado Municipal. Asimismo, en 44 procesos se utilizan datos personales de identificación, en 3 se utilizan datos personales patrimoniales y en dos procesos se utilizan datos sensibles.

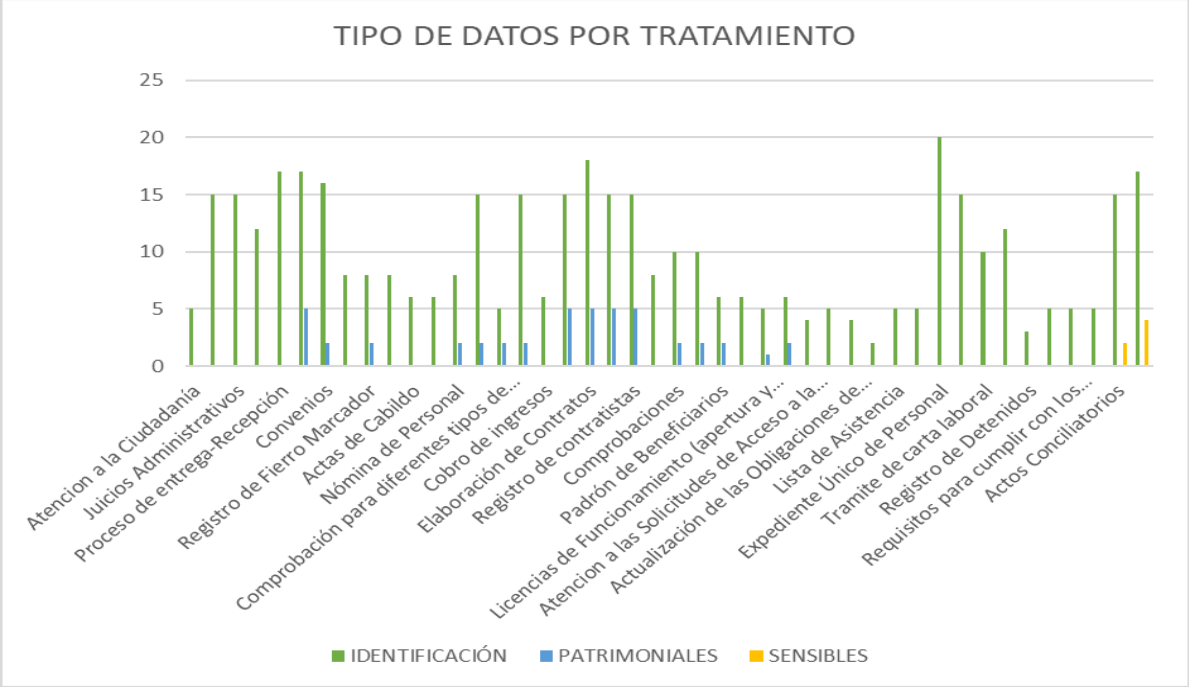
Procesos por Unidad Administrativa

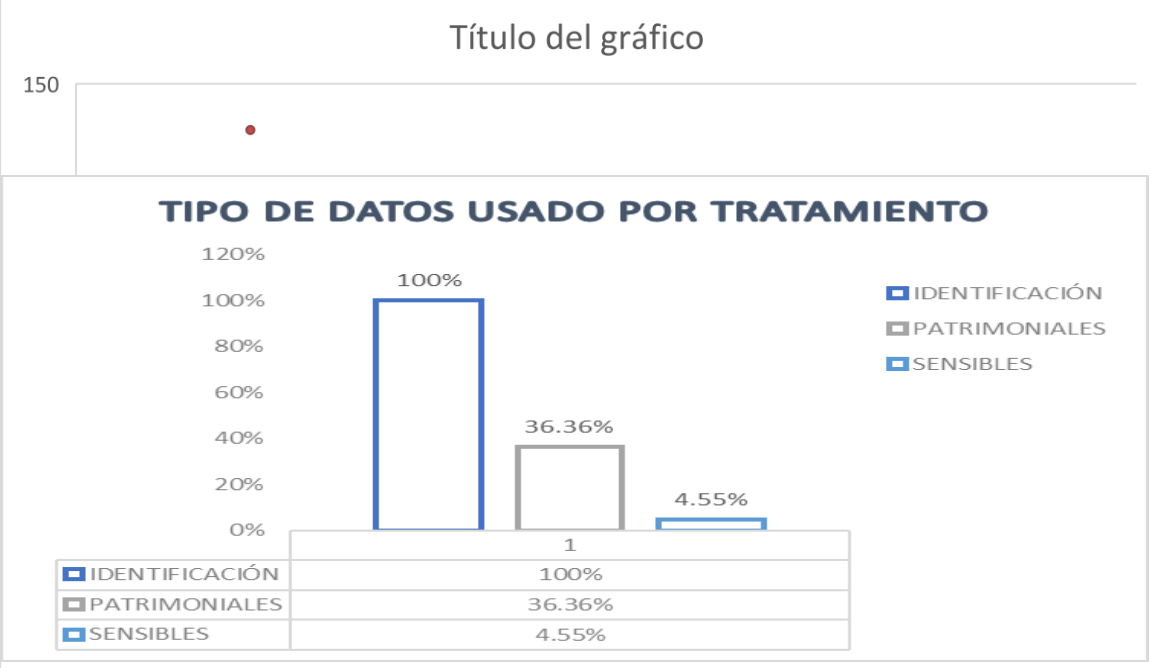


Como se puede observar en la gráfica, el área que desarrolla mayor número de procesos con datos personales, es el área de Obras Públicas, mientras que la Presidencia es la que menos procesos realiza al ser solamente uno en el área.

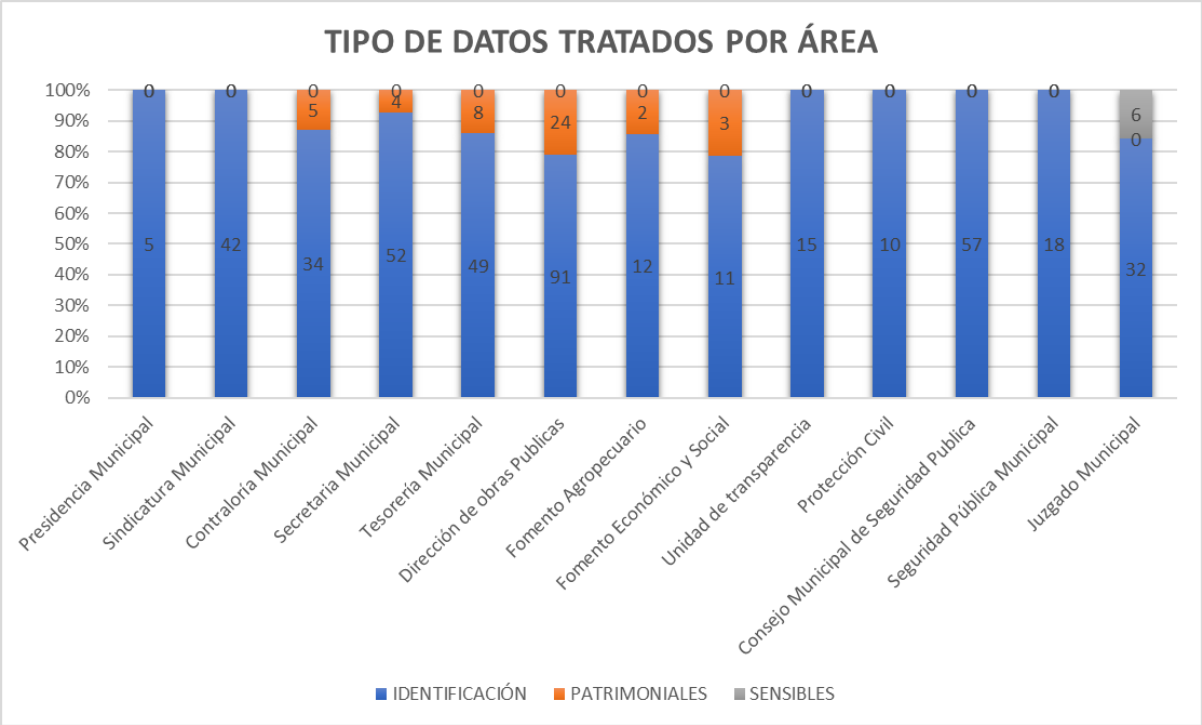
En relación a los datos solicitados, todas las áreas solicitan datos de identificación o contacto, mientras que las áreas de Fomento Agropecuario, Fomento Económico y Social, Contraloría Municipal, Secretaría Municipal y Tesorería Municipal, también solicitan datos patrimoniales y, únicamente, el Área de Juzgado municipal solicita datos sensibles; tal como se presenta en la gráfica

A partir de lo anterior, podemos identificar que la categoría de datos personales con mayor número procesos es la de carácter identificativo, en segundo término, los que incluyen datos patrimoniales y, en el caso de datos sensibles, contamos con dos tratamientos en los que se utilizan.





En relación con los procesos en los que se tratan datos personales, el 100 por ciento de los procesos usa datos identificativos, el 36.36 por ciento usa datos patrimoniales, y el 4.55 por ciento usa datos sensibles, como se muestra a continuación:


TIPO DE DATOS TRATADOS POR ÁREA
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Presidencia Municipal
Sindicatura Municipal
Contraloría Municipal
Secretaria Municipal
Tesorería Municipal
Dirección de obras Publicas
Fomento Agropecuario
Fomento Económico y Social
Unidad de transparencia
Protección Civil
Consejo Municipal de Seguridad Publica
Seguridad Pública Municipal
Juzgado Municipal
IDENTIFICACIÓN
PATRIMONIALES
SENSIBLES

Es posible observar que la Contraloría Municipal, la Secretaría Municipal, la Tesorería Municipal y la Dirección de Obras Publicas son las áreas que desarrollan el mayor número de procesos en los que se tratan datos personales, de acuerdo a sus atribuciones y obligaciones, lo anterior, debido a que las áreas que la integran se encuentran aquellas que 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.

Se logró identificar que las áreas tienen un medio diferente entre sí, para obtener los datos personales, y estos son: físicamente, USB, correo electrónico y WhatsApp; siempre directamente con el titular. No existe un sistema de base de datos del Ayuntamiento donde se puedan guardar los datos personales; si no que cada área se encarga de buscar y desarrollar estrategias para brindarle 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 Escuintla, se integra como un elemento del sistema de gestión de datos personales, con 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, ayuda a planear capacitaciones enfocados en materia protección de datos hacia los funcionarios del H. Ayuntamiento de Escuintla, 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 Escuintla, Chiapas, como un elemento de la política implementada para la observancia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados aportando con ello certeza a la ciudadanía sobre cuál es el motivo, y cuál es el destino, de los datos que se recaban por este Sujeto obligado.

6. FUNCIONES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES

Como resultado de la identificación de los procesos en los que intervienen datos personales, relacionado en el Inventario de Datos Personales, por las áreas que integran las unidades administrativas correspondientes al interior del H. Ayuntamiento de Escuintla, Chiapas, es de suma importancia definir estas actividades con 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 responsabilidad en todo tratamiento que realicen; lo anterior, a fin de dar cumplimiento al principio de legalidad que debe atender todo servidor público.

Por lo anterior, a continuación, se ilustran las atribuciones y funciones otorgadas por la Ley de Desarrollo Constitucional en Materia de Gobierno y

Administración Municipal del Estado de Chiapas a quienes llevan a cabo tratamiento de datos personales

Unidad Administrativa	Nombre y cargo de la(s) persona(s) funcionaria(s) que trata(n) datos personales	Proceso o Tratamiento
Presidencia Municipal	Lic. Gerardo Javier García Hilerio Secretario Técnico	Atención a la Ciudadanía
Sindicatura Municipal	Profa. Georgina gordillo ordoñez Sindica Municipal Lic. Gerardo coutiño dominguez Director Jurídico	Juicios Laborales
		Juicios Administrativos
		Procedimientos Administrativos
Contraloría Municipal	C.P. Rosalio ibarias escobar Contralora Municipal	Declaración de situación patrimonial
Secretaria Municipal	Lic. Gerardo Javier Gracia Hilerio	Convenios
		Elaboración de Constancias
		Registro de Fierro Marcador
		Elaboración de nombramientos
		Actas de Cabildo
		Tramite de Cartilla de Servicio Militar
Tesorería Municipal	LIC. GIEZI SALLU JIMENEZ VAZAQUEZ	Nómina de Personal
		Expediente Único de Personal
		Comprobación para diferentes tipos de gastos
		Padrón de Proveedores
		Cobro de ingresos
Dirección de obras Publicas	Ing. ING. MANUEL ROJAS RAMOS Director de Obras Públicas Ing. JORGE LUIS CRUZ GIRON Subdirector de Obras Públicas	Padrón de contratistas
		Elaboración de Contratos
		Expediente de obras
		Registro de contratistas
		Padrón de Beneficiarios
		Comprobaciones
		Supervisiones de obras
Fomento Agropecuario	Ing.Luis Enrique Vázquez Domínguez Director de Fomento Agropecuario Biol. Santiago de Jesús Estudillo Ramos Proyectista Ing. Zureima Ojendis García Proyectista	Padrón de Beneficiarios
		Comprobaciones

Director de planeación L I C . A n t o n i o r o b l e r o		**Comités de comunitarios de copladem**
Unidad de transparencia	**Ing. Mayra Vanessa Díaz Hernández** coordinadora de la Unidad de Transparencia Municipal	**Información y de Datos Personales** **Seguimiento al Directorio del Sujetos Obligado** **Actualización de las Obligaciones de Transparencia** **Seguimiento de denuncias por incumplimiento de las Obligaciones de Transparencia**
Protección Civil	**Ing. Miguel gallegos vera** Director de Protección Civil	**Lista de Asistencia** **Expediente del Personal**
Consejo Municipal de Seguridad Publica	**Lic. Julio Roberto Suarez Martínez** Secretario Ejecutivo del Consejo Municipal de Seguridad Pública	**Expediente Único de Personal** **Convenios y Contratos** **Tramite de carta laboral** **Certificado del centro estatal de control y confianza**
Seguridad Pública Municipal	C. Aaron perez hernandez director de Seguridad Pública Municipal	**Registro de Detenidos** **Notificaciones** **Requisitos para cumplir con los lineamientos (Nacionalidad)** **Alta de Elementos en el sistema**
Juzgado Municipal	**Lic. Yasmin Santiago ovando**	**Actos Conciliatorios** **Asuntos Familiares (Separación, régimen de visitas, guarda y custodia)**

7. ANÁLISIS DE RIESGO Y BRECHA

El análisis de riesgo y de brecha es parte del documento de seguridad, De acuerdo con el artículo 50 de la LPDPPSOCHIS, es una forma de identificar las medidas de seguridad implementadas y, con respecto a ello, las amenazas de vulneración en que se encuentran los datos personales.

El análisis de brecha que ayudarán a los responsables autorizados a identificar las medidas de seguridad implementadas para proteger datos personales recabados, realizando un diagnóstico de las prácticas de

seguridad de la información con las que cuenta, en ese momento, el sujeto obligado y las que deberían de tenerse con base a las mejores prácticas.

El análisis permite detectar el riesgo inherente a los datos personales en el tratamiento a que son sometidos en el ejercicio de las funciones del H. Ayuntamiento de Escuintla, Chiapas, en relación a la integridad de las personas.

La valoración de los riesgos de los datos personales forma parte de la serie de elementos que integran el documento de seguridad, cuyo propósito es garantizar la confidencialidad, integridad y disponibilidad de los datos personales en posesión del H. Ayuntamiento de Escuintla, Chiapas.

Por otra parte, para el análisis de riesgo se tomó en cuenta lo establecido en el lineamiento para la protección de datos personales del estado de Chiapas, que en su artículo 55, define que para el cumplimiento al artículo

47 fracción IV de la Ley Estatal, el responsable deberá realizar un análisis de riesgo de los datos personales tratados considerando lo siguiente:

a) Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
b) El valor de los datos personales de acuerdo con su clasificación previamente definitiva y su ciclo de vida;
c) El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
d) Las consecuencias y negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; y
e) Los factores previstos en el artículo 47 de la Ley Estatal.

Bajo esta premisa, para analizar los riegos de los datos personales que son objeto de tratamiento por el Ayuntamiento de Escuintla, se aplicó un instrumento para clasificar los datos utilizados, a partir de la categorización existente en la ley:

- **De identificación o contacto**, que se refieren a cualquier dato que podría identificar potencialmente a un individuo específico y/o permiten su contacto como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población o la edad. Cualquier información que puede ser utilizada para distinguir una persona de otra, y que puede ser usada para quitarle el anonimato a los datos anónimos.

- **Patrimoniales**, contiene información que se encuentran vinculados al patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.
- **Sensibles**, Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, por ejemplo, el origen étnico, el estado de salud presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

De los anteriores, se identificó que se trabaja sobre todo con dos categorías: Datos de Identificación y datos patrimoniales, ya que como datos sensibles se recaban únicamente Circunstancias socioeconómicas, discapacidad, estado de interdicción o incapacidad legal y lengua indígena.

para la determinación del riesgo sobre esa tipología de datos personales se valoró la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación (ciclo de vida), en correspondencia con la cantidad de datos involucrados, se materialice uno o más factores que pueden causar un daño a su titular (amenaza).

Para el desarrollo del análisis, se recuperaron cuatro tipos de amenazas sustentados en la Ley:

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

A partir de lo anterior, se consideró una probabilidad baja, media o alta de que la amenaza suceda en las distintas etapas de vida y tipo de datos personales. Además, se tomó en cuenta la consecuencia desfavorable que podría sufrir el titular en caso de vulneración, la cual puede ser leve, moderada o grave.

En cuanto a la valoración del riesgo por el tipo de dato en cada proceso en el que las áreas del ayuntamiento de Escuintla, tratan datos personales, se señaló una escala del 0 al 2, representándose de la forma siguiente:

TIPO DE DATO	RIESGO INHERENTE	NIVEL DE RIESGO
Datos identificativos	Bajo	1
Datos laborales, de domicilio laborales, patrimoniales, procedimientos administrativos	Medio	2
Datos de tránsito y movimientos migratorios; de salud, biométricos	Medio	3
Datos sensibles	Alto	4

Sección Clasificada del Documento de Seguridad

Análisis de Riesgo y Brecha

Se testa el apartado, que 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 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

Análisis de Riesgo y Brecha

Se testa el apartado, que 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 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

Análisis de Riesgo y Brecha

Se testa el apartado, que 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 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

Gestión y Notificación de las Vulneraciones

Se testa el apartado, que contiene la Gestión y notificación de Vulneraciones 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 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

Plan de Contingencia

Se testa el apartado, que contiene el 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 conformidad con 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

Plan de Contingencia

Se testa el apartado, que contiene el 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 conformidad con 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

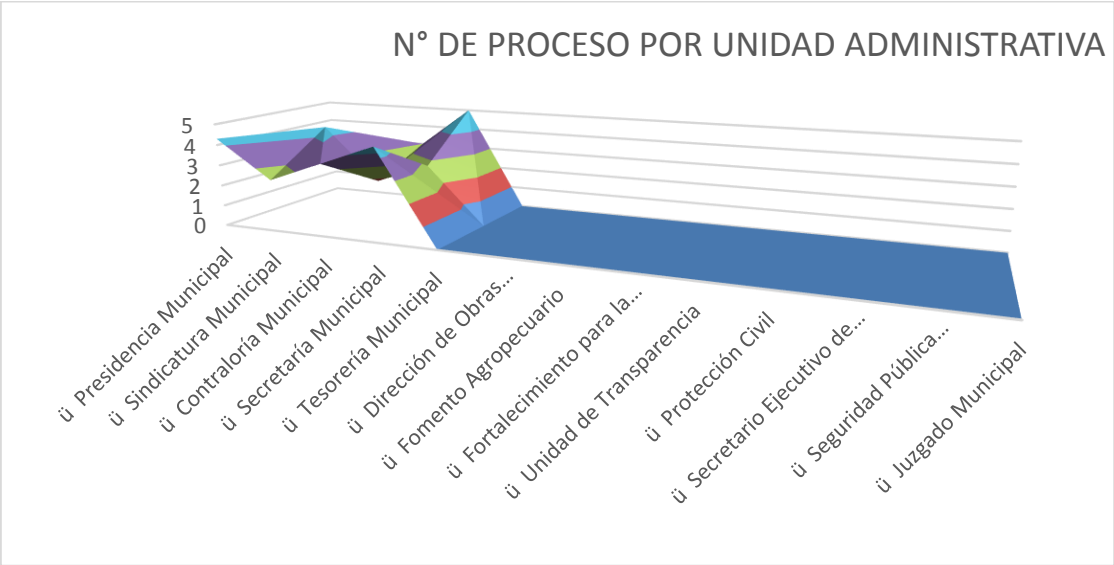
Plan de Contingencia

Se testa el apartado, que contiene el 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 conformidad con 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.

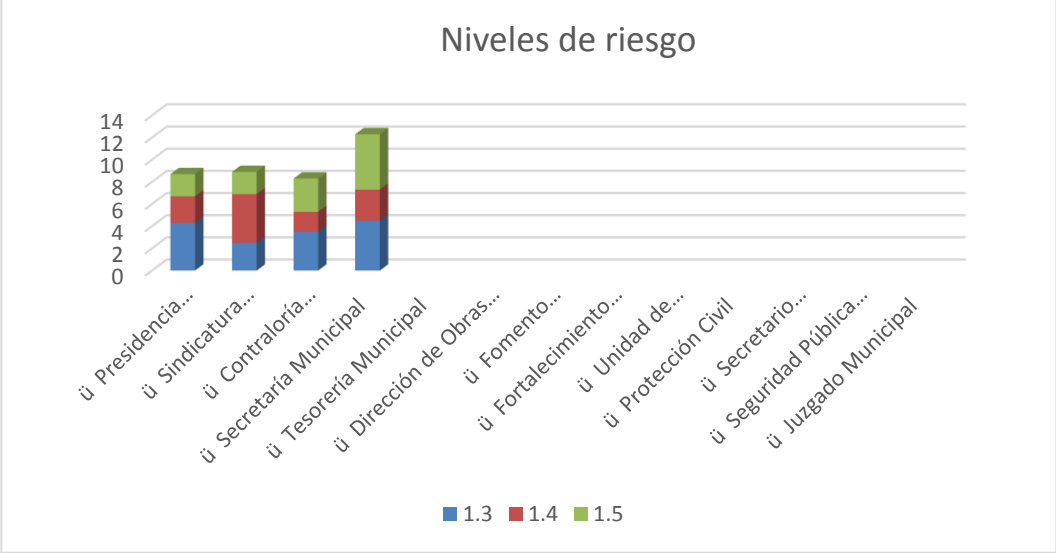
8. ANÁLISIS DE LA INFORMACIÓN

En el resultado del levantamiento de información para el análisis de riesgo y de brecha, se identifica que el Ayuntamiento de Escuintla, Chiapas, cuenta con 13 áreas que realizan tratamientos de datos personales para el desarrollo de los 44 procesos como se ilustra a continuación:

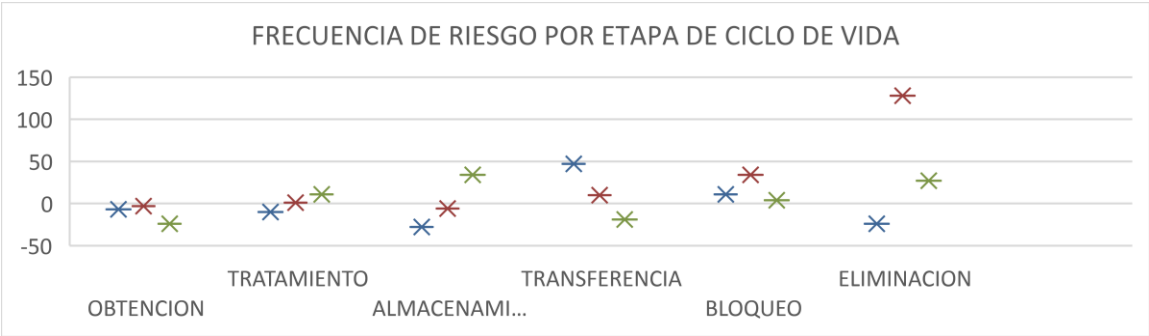
Uno corresponde a presidencia, tres a sindicatura, dos a Contraloría, seis a Secretaría Municipal, cinco a Tesorería Municipal, siete a la Dirección de Obras Públicas Municipales, dos de Fomento Agropecuario, dos de Fortalecimiento, cuatro de Unidad de Transparencia, dos de Protección Civil, cuatro del Consejo Municipal de Seguridad Pública, cuatro de Seguridad Pública, dos de Juzgado Municipal. Asimismo, en 44 procesos se utilizan datos personales de identificación, en 16 se utilizan datos personales patrimoniales y en dos procesos se utilizan datos sensibles.



La unidad administrativa que observa mayor estado de vulnerabilidad y riesgo de los datos personales es el Juzgado Municipal con 1.8 de riesgo, seguida en orden descendente por la Tesorería Municipal, la Dirección de obras Públicas, y Fomento Agropecuario con 1.5 de riesgo, la Contraloría Municipal y Fortalecimiento con 1.4 de riesgo, mientras que la Presidencia Municipal, Sindicatura Municipal, Secretaria Municipal, Unidad de transparencia, Protección Civil, Consejo Municipal de Seguridad Publica y Seguridad Pública Municipal poseen 1.3 de riesgo.



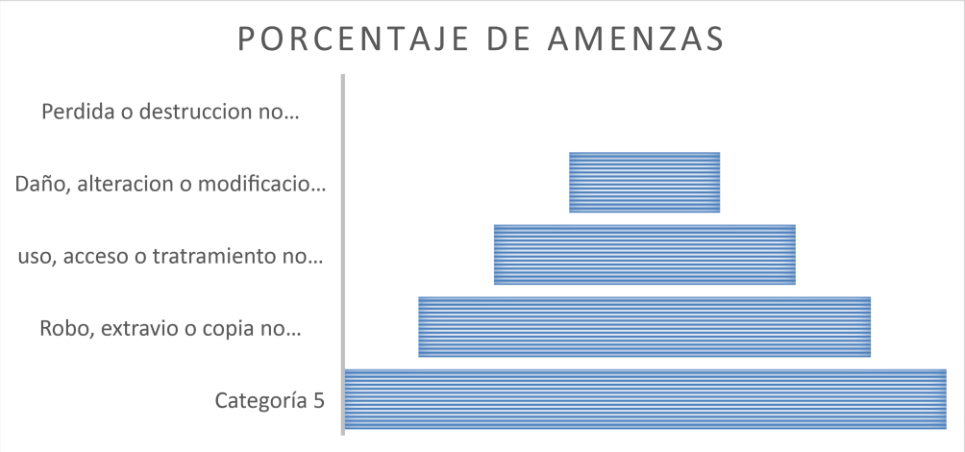
Por otra parte, hay que señalar además que la etapa del ciclo de vida (obtención, tratamiento, almacenamiento, transferencia, bloqueo y eliminación) en la que los datos personales se encuentran más vulnerables, es en el periodo de almacenamiento en un 35%; mientras que el periodo que implica menor riesgo es el de bloqueo con un 2%.



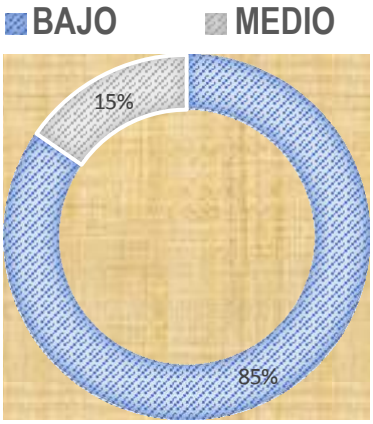
Las amenazas a las que se ven expuestos son básicamente:

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

Siendo la más alta, la de pérdida o destrucción no autorizada y la de menor riesgo es daño, alteración o modificación no autorizada, como se muestra en la tabla siguiente:



Finalmente, como parte del análisis es posible establecer que el nivel de riesgo es mayormente medio, debido que se trabaja sobre todo con datos de identificación, en algunos casos con datos patrimoniales y únicamente en dos tratamientos se solicitan datos sensibles. Asimismo, los datos personales corresponden a menos de 1000 personas, lo que reduce el nivel de riesgo y se mantienen a resguardo en computadoras personales con contraseña y en archiveros con llave para ampliar el margen de seguridad. El nivel de riesgo se ilustra en la siguiente tabla:



9. MEDIDAS DE SEGURIDAD

Las medidas de seguridad administrativas, físicas y técnicas que actualmente se aplican en el ayuntamiento de Escuintla para mantener la confidencialidad e integralidad de la información, protegiendo los datos personales contra daño, pérdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado, e impedir la divulgación no autorizada, son las siguientes:

A. Medidas administrativas

i. Diseño y desarrollo de un modelo de capacitación permanente en materia de la Ley de Protección de Datos Personales en posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), impartido a quienes colaboran en el H. Ayuntamiento de Escuintla, Chiapas.
ii. Diseño y ejecución de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.
iii. Aplicación de estrategias de seguridad, para el resguardo de los expedientes, con observancia de criterios vinculados con el sistema de gestión documental.
iv. Diseño e implementación de una carta responsiva por parte del personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.

v. Previsión de reportes de incidencias, mediante la elaboración e implementación de los formularios correspondientes.

B. *Medidas Físicas*

i. Protección de documentos e información resguardándolos en archivos físicos de trámite y concentración, asegurados con llave.
ii. Disponer de instalaciones aseguradas con llave para mantener control de acceso de personas a espacios de resguardo de información.
iii. Aplicar la firma de cartas de confidencialidad con el personal que trata datos personales

C. *Medidas técnicas*

i. Garantizar la seguridad de los datos personales, utilizando claves de usuario y contraseñas de manera individual y evitar compartirlas, prestarlas o registradas a la vista de otras personas. Y que estas sean seguras al incluir: caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero.
ii. Cuando se identifique algún caso en el que las claves de usuario y/o contraseña hayan sido utilizadas por un tercero, notificar de manera inmediata a la Dirección de verificación y tecnologías de la información, para las prevenciones conducentes.
iii. Procurar la utilización de una cuenta de correo electrónico oficial para fines relacionados con las actividades laborales, evitando remitir datos personales.
iv. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de restringir el acceso a los datos personales que pudieran mantenerse en archivos y equipos.
v. Cuidar que en los equipos de impresión no se dejen olvidados documentos que contengan datos personales.

10. MONITOREO DE LAS MEDIDAS DE SEGURIDAD

Como parte del programa de protección de datos personales, es importante la supervisión de las medidas de seguridad técnicas y físicas, como un elemento para la mejora continua, que permite definir nuevas formas de monitoreo, de acuerdo con las necesidades surgidas al interior del ayuntamiento de Escuintla, Chiapas, entre las que podemos señalar las siguientes:

1. Revisión y actualización permanente de las contraseñas utilizadas para resguardar los datos personales en equipos de cómputo.

2. Revisar de manera permanente el cumplimiento de protocolos implementados para la protección de los datos personales.

3. Vigilar que el ingreso de personas sea a través de los accesos correspondientes, plenamente identificados.

11. PROGRAMA DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

Conforme al análisis de brecha, existen algunas medidas de seguridad que se requiere implementar, por lo que a continuación se presentan las actividades generales que se planea realizar:

- Celebración de reuniones de trabajo con los jefes de área a efecto identificar alternativas de solución técnicas, físicas y administrativas a desarrollar en el mediano y largo plazo.
- Promover un sistema de gestión y administración de datos personales que permita centralizar mediante la identificación de datos por categorías, asociando los diversos tratamientos y procesos a las políticas de seguridad que resultan aplicables a cada caso, conforme a los estándares y mejores prácticas en la materia.
- Implementar mecanismos de divulgación y conocimiento de las políticas generales de seguridad y, verificar de manera continua su cumplimiento.
- Fortalecer los mecanismos de control de documentos e información en las distintas unidades administrativas, a efecto de evitar posibles vulneraciones

12. PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

La aplicación del programa de protección de datos personales en el ayuntamiento de Escuintla, requiere como un factor esencial, la formación y sensibilización de las personas que aquí laboran, de tal forma que pueda garantizarse la actualización y mejora continua del inventario de datos personales, la observancia de la normatividad y Ley, por lo que se propone un programa de capacitación en el tema de protección de datos personales que favorezca la profundización en el conocimiento del tema por parte de quienes intervienen en el tratamiento de datos personales. A manera de propuesta, se han considerado los siguientes temas:

I. La Ley de protección de datos personales en posesión de sujetos obligados en Chiapas.
   - Antecedentes
   - Principios.
   - Alcances
   - Objetivo
   - Implicaciones

II. Obligaciones en la observancia de la LPDPPSOCHIS
   - Deberes.
   - Medidas de seguridad.
   - Procedimientos y sanciones/ Derechos ARCO (acceso, rectificación, cancelación y oposición).
   - Medios de defensa.

III. El programa de protección de datos personales
   - Sistemas de datos personales.
   - Inventario y Base de Datos.
   - Medidas de seguridad.
   - Análisis de brecha y de riesgo.
   - Funciones y obligaciones.

IV. El principio de información: Avisos de Privacidad en el marco del programa de protección de datos personales.
   - Contenido: Integral, simplificado
   - Consentimiento.
   - Deber de información.
   - Finalidades del tratamiento de los datos

13. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD.

En términos de lo previsto en el artículo 51 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas, este Ayuntamiento actualizará el Documento de Seguridad de manera constante como resultado de una mejora continua y como consecuencia del monitoreo y revisión que se lleve a cabo a través de su sistema de gestión, asimismo, cuando ocurran los siguientes eventos:

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

- Por lo anterior, con el propósito de mantener una mejora continua en el Documento de Seguridad se informa que la periodicidad de la revisión y en su caso actualización se efectuará anualmente. En caso de que se lleve a cabo alguna actualización al Documento de Seguridad, éste se someterá nuevamente para su aprobación al Comité de Transparencia del H. Ayuntamiento de Escuintla, Chiapas.

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

PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

La adecuada protección de los datos personales dentro del H. Ayuntamiento Municipal de Escuintla, 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 Escuintla; 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 Escuintla, 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 Escuintla, 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 Escuintla, 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 Escuintla, 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.

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

ELABORO:
LIC. ING. MAYRA VANESSA DIAZ HERNANDEZ
RESPONSABLE DE LA UNIDAD DE TRANSPARENCIA

FECHA DE ÚLTIMA ACTUAIZACION DEL DOCUMENTO DE SEGURIDAD:
29 DE SEPTIEMBRE DE 2026