

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES DEL HONORABLE AYUNTAMIENTO MUNICIPAL DE IXTAPA CHIAPAS.

VERSIÓN PÚBLICA.

**PALACIO MUNICIPAL: 1ª PONIENTE Y AVENIDA CENTRAL S/N COL. CENTRO
IXTAPA, CHIAPAS.
C.P.: 29340**

DOCUMENTO DE SEGURIDAD.

1. PRESENTACIÓN	3
2. OBJETIVO DEL DOCUMENTO SEGURIDAD	4
3. RESPONSABILIDADES	5
4. ALCANCE DE DOCUMENTO DE SEGURIDAD	7
5. MARCO JURÍDICO	8
6. PRINCIPIOS Y DEBERES	9
7. INVENTARIO DE DATOS PERSONALES Y SISTEMAS DE TRATAMIENTO	11
8. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES	18
9. ANÁLISIS DE BRECHA Y RIESGO	19
10. CUADRO DE ANÁLISIS DE BRECHA	21
11. CUADRO DE IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS	24
12. MEDIDAS DE SEGURIDAD GENERALES	27
13. PLAN DE TRABAJO	35
14. PROPUESTA DE CAPACITACIÓN	40

1. PRESENTACIÓN

En el presente documento se detallan las medidas de seguridad administrativas, físicas y técnicas con las que se contara en el H. Ayuntamiento de Ixtapa, Chiapas, para garantizar el debido tratamiento y protección de los datos personales que poseen las Dependencias y Unidades Administrativas que conforman a este sujeto obligado.

Su contenido se formula conforme al marco jurídico vigente en materia de protección de Datos Personales y, particularmente, a los artículos 25 a 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como a los artículos correlativo de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

El propósito de este documento es establecer los parámetros que guían el tratamiento de los datos personales al interior del H. Ayuntamiento de Ixtapa, Chiapas, por las diferentes dependencias que integran la Administración Municipal.

El documento constituye un instrumento interno de observancia obligatoria para las personas servidoras públicas, áreas administrativas, encargadas y demás personas que intervengan en cualquier fase del tratamiento de Datos Personales.

Su elaboración se realiza en cumplimiento de las obligaciones establecidas en la legislación vigente en materia de protección de Datos Personales, particularmente de los artículos 25 al 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

2. OBJETIVO DEL DOCUMENTO DE SEGURIDAD

Establecer las políticas, procedimientos, controles y medidas de seguridad administrativa, físicas y técnicas necesarias para garantizar la confidencialidad, integridad y disponibilidad de los Datos Personales tratados por el H. Ayuntamiento Municipal de Ixtapa, Chiapas.

Asimismo, tiene como objetivo:

1. Prevenir daños, pérdidas, alteraciones, destrucciones o accesos no autorizados.
2. Identificar y administrar los riesgos relacionados con el tratamiento de Datos Personales.
3. Establecer responsabilidades para las personas servidoras públicas que intervienen en el tratamiento.
4. Implementar medidas preventivas y correctivas.
5. Establecer mecanismos de respuestas ante vulneraciones de seguridad.
6. Garantizar la continuidad de los servicios relacionados con el tratamiento de Datos Personales.
7. Promover una cultura institucional de protección de Datos Personales.

3. RESPONSABILIDADES

Con fundamento en lo dispuesto por los artículos 77 y 78 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, el Comité de Transparencia es la máxima autoridad al interior del H. Ayuntamiento Municipal de Ixtapa, Chiapas, en materia de protección de Datos Personales.

En termino del articulo 78 de la Ley, corresponde al Comité de Transparencia coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los Datos Personales en la organización del responsable, así como supervisar, en coordinación con las áreas u órganos administrativos competentes, el cumplimiento de las medidas, controles y acciones previstas en el Documento de Seguridad.

Para el cumplimiento de sus atribuciones en materia de protección de Datos Personales, el Comité de Transparencia tendrá las siguientes funciones:

- I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los Datos Personales en la organización del H. Ayuntamiento Municipal de Ixtapa, Chiapas, de conformidad con la Ley y demás disposiciones aplicables;
- II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los Derechos ARCO;
- III. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los Datos Personales o se niegue, por cualquier causa, el ejercicio de alguno de los Derechos ARCO;

- 
- IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de legislación en materia de protección de Datos Personales;
 - V. Supervisar, en coordinación con las áreas u órganos administrativos competentes, el cumplimiento de las medidas, controles y acciones previstas en el presente Documento de Seguridad;
 - VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Organo Desconcentrado de la Secretaría a la Autoridad Garante competente, según corresponda;
 - VII. Establecer programas de capacitación y actualización para las personas servidoras publicas en materia de protección de Datos Personales;
 - VIII. Dar vista al órgano de control interno u homologo o equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de Datos Personales; y
 - IX. Las demás atribuciones, facultades, competencia o funciones que establezcan la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y demás disposiciones jurídicas aplicables.

4. ALCANCE DE DOCUMENTO DE SEGURIDAD.

El presente Documento de Seguridad será aplicable a todas las áreas, unidades administrativas, personas servidoras públicas, presentadoras de servicios, encargados y demás personas que, por razón de sus funciones, tenga acceso o intervengan en el tratamiento de Datos Personales en posesión del H. Ayuntamiento.

Comprenderá los tratamientos realizados mediante:

- Expedientes físicos.
- Archivos administrativos.
- Sistemas informáticos,
- Bases de datos.
- Equipos de cómputo.
- Dispositivos electrónicos.
- Sistemas de almacenamiento.
- Correos electrónicos institucionales.
- Plataformas digitales.
- Medios removibles.
- Cualquier otro medio mediante el cual se obtengan, utilicen, almacenen, consulten, comuniquen o supriman Datos Personales.

5. MARCO JURÍDICO.

El presente Documento de Seguridad se fundamenta, entre otras disposiciones aplicables, en:

1. Constitución Política de los Estados Unidos Mexicanos, artículo 16, segundo párrafo.
2. Ley General de Protección de Datos Personales en Posesión de sujetos Obligados.
3. Ley General de Transparencia y Acceso a la Información Pública.
4. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.
5. Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.
6. Ley de Archivos del Estado de Chiapas.
7. Ley de Responsabilidades Administrativas para el Estado de Chiapas.
8. Demás disposiciones, lineamientos y normativa aplicable en materia de protección de Datos Personales, transparencia, archivos, seguridad de la información y responsabilidades administrativas.

La legislación estatal vigente reconoce expresamente a los Ayuntamientos como sujetos obligados en materia de protección de Datos Personales.

6. PRINCIPIOS Y DEBERES.

El H. Ayuntamiento Municipal de Ixtapa, Chiapas, en su carácter de responsable del tratamiento de Datos Personales, deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, establecidos en el artículo 10 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

En el tratamiento de Datos Personales, las áreas de Tesorería Municipal, Contraloría Municipal, Secretaría de Ayuntamiento, Obras Públicas, Oficialía y Unidad de Transparencia, así como las personas servidoras públicas que intervengan en dicho tratamiento, deberán observar lo siguiente:

1. Licitud.

Los Datos Personales deberán ser tratados de conformidad con las atribuciones y facultades que correspondan al Ayuntamiento y a cada una de sus áreas, conforme a la normatividad aplicable.

2. Finalidad.

Los Datos Personales deberán ser tratados para finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones del Ayuntamiento y del área que realice el tratamiento.

3. Lealtad.

Los Datos Personales no deberán obtenerse ni tratarse mediante medios engañosos o fraudulentos, debido a que se respetará la expectativa razonable de privacidad de las personas titulares.

4. Consentimiento.

Cuando resulte exigible conforme la legislación aplicable, deberá obtenerse el consentimiento de la persona titular para el tratamiento de sus Datos Personales, salvo los casos de excepción establecidos por la propia Ley.

5. Calidad.

Los Datos Personales deberán ser exactos, complementos, correctos y actualizados, cuando así corresponda, procurando que sean adecuados para la finalidad para las cuales fueron recabados.

6. Proporcionalidad.

El Ayuntamiento deberá tratar únicamente los Datos Personales que resulten adecuados, relevantes y necesarios para las finalidades que justifican su tratamiento, evitando la recopilación o utilización excesiva de información.

7. Información.

El Ayuntamiento deberá informar a las personas titulares, mediante los avisos de privacidad correspondientes, sobre las características principales de tratamiento de sus Datos Personales, de conformidad con la legislación aplicable.

8. Responsabilidad.

El Ayuntamiento deberá implementar mecanismos y acciones que permitan acreditar el cumplimiento de los principios, deberes y obligaciones en materia de protección de Datos Personales.

7. INVENTARIO DE DATOS PERSONALES Y SISTEMAS DE TRATAMIENTO.

El H. Ayuntamiento Municipal de Ixtapa, Chiapas, identificar y documenta los Datos Personales que son objeto de tratamiento en las distintas áreas administrativas, así como los sistemas, medios físicos y electrónicos utilizados para su recopilación, almacenamiento, consulta, utilización, transferencia, conservación y, en su caso, supresión.

El inventario se encuentra sujeto a actualización cuando existan modificaciones sustanciales en el tratamiento de los Datos Personales, que impliquen un cambio en el nivel de riesgo, conforme a lo establecido en la legislación aplicable.

➤ Inventario general.

ÁREA RESPONSABLE	DATOS PERSONALES TRATADOS	TIPO DE DATOS	TITULARES	FINALIDAD DEL TRATAMIENTO	MEDIO O SISTEMA DE TRATAMIENTO.	SOPORTE
TESORERIA MUNICIPAL	Nombre, domicilio, teléfono, correo electrónico, RFC, CURP, firma, identificación oficial, datos fiscales, datos bancarios y datos relacionados con pagos.	Identificativos, contacto, fiscales, patrimoniales y financieros	Servidores públicos, contribuyentes, proveedores, contratistas y particulares.	Recaudación, administración financiera, pagos, comprobación de gastos, nómina, proveedores y cumplimiento de obligaciones fiscales y administrativas.	Recopilación, registro, organización, consulta, utilización, almacenamiento, transferencia y conservación.	Expedientes físicos, archivos electrónicos, computadoras, sistemas administrativos y medios institucionales.
CONTRALORIA MUNICIPAL	Nombre, domicilio, teléfono, correo electrónico, CURP, RFC, identificación oficial, firma, datos laborales, patrimoniales y los contenidos en declaraciones, quejas, denuncias y procedimientos administrativos.	Identificativos, contacto, laborales, patrimoniales y administrativos.	Servidores públicos, particulares, denunciantes, quejosos y personas relacionadas con procedimientos administrativos.	Auditorías, revisiones, investigaciones, control interno, recepción y seguimiento de quejas y denuncias y procedimientos administrativos.	Recopilación, registro, consulta, análisis, utilización, conservación y archivo.	Expedientes físicos, archivos electrónicos, computadoras y sistemas institucionales.
SECRETARIA DEL AYUNTAMIENTO	Nombre, domicilio, teléfono, correo electrónico, firma, identificación oficial, CURP y datos contenidos en actas, certificaciones, constancias, solicitudes y documentación oficial.	Identificativos, contacto y administrativos.	Ciudadanía, servidores públicos, representantes y particulares.	Elaboración de actas, certificaciones, constancias, correspondencia oficial, atención de solicitudes y demás funciones administrativas.	Recepción, registro, consulta, utilización, reproducción, almacenamiento y conservación.	Libros, expedientes físicos, archivos electrónicos, computadoras y medios institucionales.

OBRAS PUBLICAS	Nombre, domicilio, teléfono, correo electrónico, RFC, CURP, identificación oficial, firma y datos de contratistas, proveedores, representantes y beneficiarios.	Identificativos, contacto, fiscales, patrimoniales y laborales.	Contratistas, proveedores, representantes, beneficiarios y ciudadanía relacionada con obras y programas.	Integración de expedientes de obras, contratación, supervisión, seguimiento de programas, permisos, licencias y atención de beneficiarios.	Recopilación, registro, consulta, utilización, almacenamiento, transferencia y conservación.	Expedientes físicos, archivos electrónicos, computadoras, sistemas administrativos y archivos digitales.
OFICIALÍA MAYOR	Nombre, domicilio, teléfono, correo electrónico, firma, identificación oficial y datos contenidos en documentos recibidos por el Ayuntamiento.	Identificativos, contacto y administrativos.	Ciudadanía, servidores públicos, representantes, proveedores y particulares.	Recepción, registro, control, distribución, archivo y seguimiento de documentación oficial.	Recepción, registro, clasificación, distribución, consulta, archivo y conservación.	Libros y registros físicos, expedientes, archivos electrónicos y computadoras.
UNIDAD DE TRANSPARENCIA	Nombre, domicilio o medio para recibir notificaciones, correo electrónico, teléfono, firma y datos contenidos en solicitudes de acceso a la información y solicitudes de derechos ARCO.	Identificativos, contacto y administrativos.	Solicitantes, titulares de Datos Personales, representantes y terceros que aparezcan en la documentación.	Atención de solicitudes de acceso a la información, ejercicio de derechos ARCO, asesoría, seguimiento y cumplimiento de obligaciones de transparencia y protección de Datos Personales.	Recopilación, registro, consulta, análisis, respuesta, almacenamiento, transferencia y conservación.	Plataforma Nacional de Transparencia, expedientes físicos, archivos electrónicos, computadoras y medios institucionales.

➤ **Clasificación de los Datos Personales**

Para efectos de identificación y gestión de riesgos, los Datos Personales tratados por el Ayuntamiento podrán clasificarse de acuerdo con su naturaleza en:

A) Datos identificativos	B) Datos de contacto	C) Datos laborales	D) Datos patrimoniales y financieros	E) Datos fiscales	F) Datos contenidos en procedimientos administrativos
- Nombre. - CURP. - RFC. - Edad. - Sexo, cuando resulte aplicable. - Firma. - Fotografía, cuando corresponda. - Número de identificación oficial.	- Domicilio. - Teléfono. - Correo electrónico. - Domicilio para recibir notificaciones.	- Puesto. - Área de adscripción. - Información relacionada con la relación laboral. - Datos contenidos en expedientes de servidores públicos.	- Información relacionada con pagos. - Datos bancarios. - Información de proveedores y contratistas. - Información patrimonial cuando legalmente corresponda.	- RFC. - Constancias y documentación fiscal. - Información relacionada con obligaciones fiscales.	- Quejas. - Denuncias. - Declaraciones. - Documentación relacionada con auditorías. - Información contenida en expedientes administrativos.

Nota: La clasificación anterior se realizará únicamente cuando los datos sean efectivamente recabados y tratados por el área correspondiente.

➤ **Titulares de los Datos Personales**

Los principales titulares de los Datos Personales tratados por el Ayuntamiento pueden comprender:

- Servidores públicos municipales.
- Ciudadanía.
- Contribuyentes.
- Proveedores.
- Contratistas.
- Beneficiarios de programas y obras.
- Representantes legales.
- Solicitantes de información.
- Titulares que ejerzan derechos ARCO.
- Personas relacionadas con procedimientos administrativos.
- Particulares que presenten escritos, solicitudes, quejas o denuncias.

- **Sistemas y medios de tratamiento**

Los Datos Personales podrán ser tratados mediante sistemas **físicos, electrónicos o mixtos**, dependiendo de las funciones de cada área.

- **Tratamiento físico**

Comprende, entre otros:

- Expedientes.
- Oficios.
- Solicitudes.
- Formatos.
- Libros y registros.
- Contratos.
- Convenios.
- Actas.
- Identificaciones.
- Comprobantes.
- Documentación administrativa.
- Expedientes de proveedores, contratistas y beneficiarios.

- **Tratamiento electrónico**

Comprende, entre otros:

- Computadoras institucionales.
- Archivos digitales.
- Hojas de cálculo.
- Bases de datos.
- Sistemas administrativos.
- Correo electrónico institucional.
- Plataformas oficiales.
- Dispositivos de almacenamiento autorizados.
- Plataforma Nacional de Transparencia.

- **Ciclo de vida de los Datos Personales**

El tratamiento podrá comprender las siguientes etapas:

1.Obtención:

Los Datos Personales son recabados directamente de sus titulares o mediante los mecanismos legalmente establecidos.

2.Registro:

Los datos son incorporados a expedientes, formatos, sistemas o bases de datos.

3.Organización y almacenamiento:

Los datos son clasificados y resguardados en soportes físicos o electrónicos.

4. Uso y consulta:

Los servidores públicos autorizados acceden a los datos exclusivamente para el cumplimiento de sus funciones.

5.Transferencia:

Cuando legalmente corresponda, los Datos Personales podrán ser comunicados a otras autoridades, instituciones o terceros, atendiendo a las disposiciones legales aplicables.

6.Conservación:

Los datos serán conservados durante el periodo necesario para cumplir con la finalidad del tratamiento y las obligaciones legales correspondientes.

7.Supresión:

Una vez concluido el periodo de conservación y cuando legalmente proceda, se realizará la supresión, bloqueo o destino final correspondiente, aplicando medidas de seguridad para evitar recuperación o acceso no autorizado.

- **Plazos de conservación**

Los periodos de conservación de los Datos Personales deberán determinarse de acuerdo con:

- La finalidad para la cual fueron recabados.
- Las obligaciones legales y administrativas aplicables.
- Los plazos establecidos en los instrumentos archivísticos del Ayuntamiento.
- Las disposiciones en materia de archivos.
- La existencia de procedimientos administrativos, jurídicos o de fiscalización.
- La necesidad de conservar documentación como evidencia del cumplimiento de obligaciones.

Cada área deberá identificar los plazos correspondientes a sus expedientes y evitar conservar Datos Personales durante periodos superiores a los necesarios o legalmente establecidos.

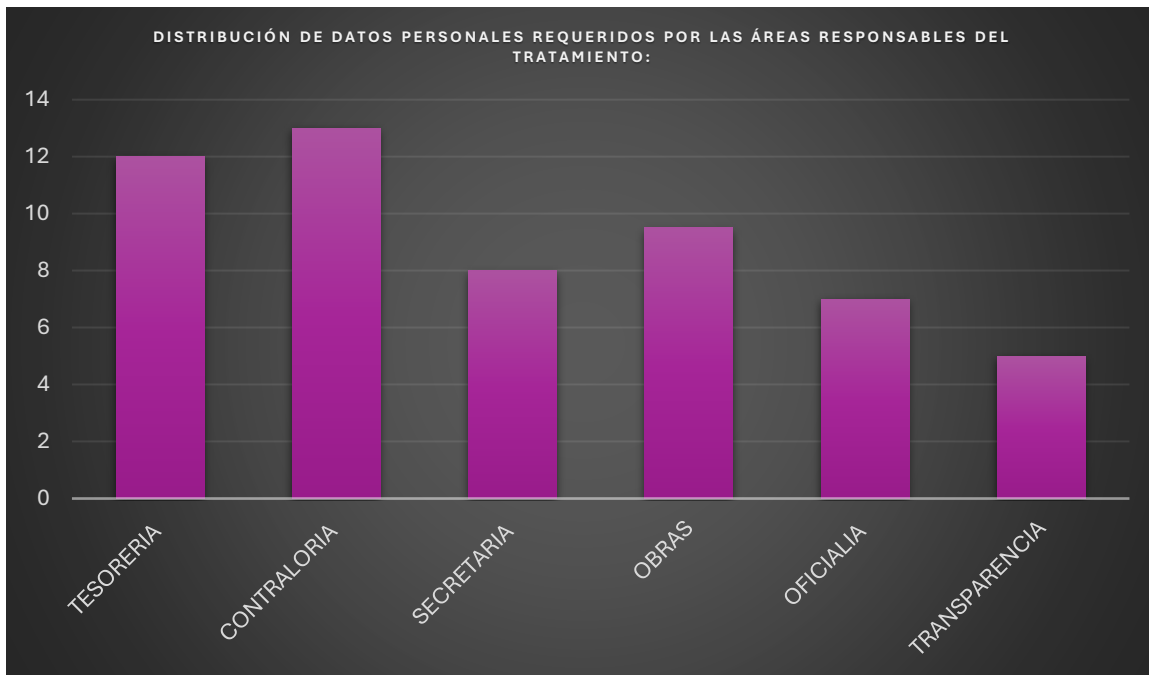
- **Nivel de riesgo por área**

**SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL
ANÁLISIS DE RIESGO Y BRECHA.**

Se testea el apartado número 10, que contiene el Análisis de Riesgo y Brecha, con fundamento en los artículos 25, 26, 27 fracciones IV y V, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, vigente, se determina que la información contenida en el presente apartado será objeto de testeo únicamente respecto de aquellos elementos cuya divulgación pudiera comprometer la seguridad de los datos personales, los sistemas de tratamiento o las medidas de seguridad implementadas por el H. Ayuntamiento Municipal de Ixtapa, Chiapas.

A partir de lo anterior, el Inventario de Datos Personales del H. Ayuntamiento de Ixtapa, Chiapas, posibilitó la identificación de hallazgos en relación con el tratamiento de datos personales, aportando los elementos que permiten focalizar las áreas con mayor incidencia en el tratamiento de estos, y con ello, enforzar los trabajos de atención para el cumplimiento de las disposiciones jurídicas en materia de protección de datos.

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



Gráfica 1. Distribución de Datos Personales por Área Responsable del Tratamiento.
Como resultado de la integración del inventario preliminar de Datos Personales del H. Ayuntamiento Municipal de Ixtapa, Chiapas, se identificaron diversas categorías de información personal que son objeto de tratamiento por las áreas administrativas, de acuerdo con las atribuciones y funciones que desempeñan. La cantidad señalada corresponde a las categorías identificadas en el inventario y deberá actualizarse cuando se modifiquen los tratamientos o se incorporen nuevos datos personales.

8. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN 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 ayuntamiento, resulta importante definir estas actividades con las funciones y facultades establecidas en la normatividad interna. Que otorga a las personas servidoras as publicas responsables de dicho tratamiento; lo anterior, a fin de dar cumplimiento al principio de legalidad que debe atender todos servidor público.

El H. Ayuntamiento Municipal de Ixtapa, Chiapas, establecerá y mantendrá las medidas administrativas, técnicas y físicas necesarias para garantizar la protección de los datos personales que sean objeto de tratamiento, procurando en todo momento su confidencialidad, integridad y disponibilidad.

Por lo anterior, a continuación, se ilustra las funciones otorgadas por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, a quienes llevan a cabo tratamiento de datos personales:

UNIDAD ADMINISTRATIVA	NOMBRE Y CARGO DE LAS PERSONAS SERVIDORAS PUBLICAS QUE TRATAN LOS DATOS PERSONALES	PROCESO O TRATAMIENTO
TESORERIA MUNICIPAL	Lic. Aarón Alberto Salazar Cisneros/ Tesorero Municipal Luis Emilio Acero Vazquez/ Contador General Hugo Alberto Gómez Nucamendi/ Auxiliar de Recursos Federales.	- Integración de la cuenta publica. - Pagos a proveedores. - Pagos a contratistas. - Integración de gastos de diferentes ramos.
CONTRALORIA MUNICIPAL	Lic. Miguel Ángel Vera Gómez/ Contralor Municipal Jorge Erwin López Pinot/ Jurídico Municipal	- Notificación por Memorándum a las áreas. - Capacitación para el llenado de Declaraciones. - Recepción y control de Declaraciones Patrimoniales. - Resguardo de documentación de Presidencia y Personal.

OBRAS PÚBLICAS	Ing. Juan Carlos Tipá Martínez/ Director de Obras Públicas Fredy Rodríguez Nucamendi/ Subdirector de Obras Públicas.	- Traslado a comunidad en donde se realiza proyecto. - Programar. - Finiquitar el proceso constructivo.
SECRETARÍA MUNICIPAL	Lic. Carlos Antonio Méndez Solís/ Secretario Municipal	- Resguardo y protección de datos personales referente a las constancias de: identidad, residencia, origen, dependencia económica, ingresos económicos, planilla de juez, producto activo, fierro marcador, alumbramiento, madre soltera). - Resguardo protección de datos administrativos referente al ayuntamiento
OFICIALÍA MAYOR	Lic. José de Jesús Artot Penagos/ Oficial Mayor	- Gestión de personal. - Control de recursos materiales. - Control de asistencia y disciplina. - Contrataciones altas y bajas. - Administración de recursos materiales y adquisiciones compras. - Control de inventario y patrimonio. - Bajas y enajenaciones. - Mantenimiento de inmuebles. - Almacenes. - Apoyo institucional y logística y eventos institucionales.
UNIDAD DE TRANSPARENCIA	Lic. Cristal Guadalupe Ocaña López/ Jefa de la Unidad de Transparencia	- Obtención y recepción de datos personales. - Registro y captura. - Clasificación y organización. - Consulta y utilización. - Remisión a las áreas administrativas. - Atención de solicitud de derechos ARCO. - Elaboración y entrega de respuestas. - Conservación y resguardo. - Transferencia o comunicación. - Atención de incidentes de seguridad.

9. ANÁLISIS DE BRECHA Y RIESGO.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.

Se testea el apartado número 10, que contiene el Análisis de Riesgo y Brecha, con fundamento en los artículos 25, 26, 27 fracciones IV y V, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, vigente, se determina que la información contenida en el presente apartado será objeto de testeo únicamente respecto de aquellos elementos cuya divulgación pudiera comprometer la seguridad de los datos personales, los sistemas de tratamiento o las medidas de seguridad implementadas por el H. Ayuntamiento Municipal de Ixtapa, Chiapas.

**SECCIÓN CLASIFICADA DEL DOCUMENTO DE
SEGURIDAD, APARTADO DEL ANÁLISIS DE
RIESGO Y BRECHA.**

Se testea el apartado número 10, que contiene el Análisis de Riesgo y Brecha, con fundamento en los artículos 25, 26, 27 fracciones IV y V, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, vigente, se determina que la información contenida en el presente apartado será objeto de testeo únicamente respecto de aquellos elementos cuya divulgación pudiera comprometer la seguridad de los datos personales, los sistemas de tratamiento o las medidas de seguridad implementadas por el H. Ayuntamiento Municipal de Ixtapa, Chiapas.

10. CUADRO DE ANÁLISIS DE BRECHA

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.

Se testea el apartado número 10, que contiene el Análisis de Riesgo y Brecha, con fundamento en los artículos 25, 26, 27 fracciones IV y V, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, vigente, se determina que la información contenida en el presente apartado será objeto de testeo únicamente respecto de aquellos elementos cuya divulgación pudiera comprometer la seguridad de los datos personales, los sistemas de tratamiento o las medidas de seguridad implementadas por el H. Ayuntamiento Municipal de Ixtapa, Chiapas.

**SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD,
APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.**

Se testea el apartado número 10, que contiene el Análisis de Riesgo y Brecha, con fundamento en los artículos 25, 26, 27 fracciones IV y V, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, vigente, se determina que la información contenida en el presente apartado será objeto de testeo únicamente respecto de aquellos elementos cuya divulgación pudiera comprometer la seguridad de los datos personales, los sistemas de tratamiento o las medidas de seguridad implementadas por el H. Ayuntamiento Municipal de Ixtapa, Chiapas.

**SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD,
APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.**

Se testea el apartado número 10, que contiene el Análisis de Riesgo y Brecha, con fundamento en los artículos 25, 26, 27 fracciones IV y V, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, vigente, se determina que la información contenida en el presente apartado será objeto de testeo únicamente respecto de aquellos elementos cuya divulgación pudiera comprometer la seguridad de los datos personales, los sistemas de tratamiento o las medidas de seguridad implementadas por el H. Ayuntamiento Municipal de Ixtapa, Chiapas.

**SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD,
APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.**

Se testea el apartado número 10, que contiene el Análisis de Riesgo y Brecha, con fundamento en los artículos 25, 26, 27 fracciones IV y V, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, vigente, se determina que la información contenida en el presente apartado será objeto de testeo únicamente respecto de aquellos elementos cuya divulgación pudiera comprometer la seguridad de los datos personales, los sistemas de tratamiento o las medidas de seguridad implementadas por el H. Ayuntamiento Municipal de Ixtapa, Chiapas.

**SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD,
APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.**

Se testea el apartado número 10, que contiene el Análisis de Riesgo y Brecha, con fundamento en los artículos 25, 26, 27 fracciones IV y V, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, vigente, se determina que la información contenida en el presente apartado será objeto de testeo únicamente respecto de aquellos elementos cuya divulgación pudiera comprometer la seguridad de los datos personales, los sistemas de tratamiento o las medidas de seguridad implementadas por el H. Ayuntamiento Municipal de Ixtapa, Chiapas.

**SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL
ANÁLISIS DE RIESGO Y BRECHA.**

Se testea el apartado número 10, que contiene el Análisis de Riesgo y Brecha, con fundamento en los artículos 25, 26, 27 fracciones IV y V, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, vigente, se determina que la información contenida en el presente apartado será objeto de testeo únicamente respecto de aquellos elementos cuya divulgación pudiera comprometer la seguridad de los datos personales, los sistemas de tratamiento o las medidas de seguridad implementadas por el H. Ayuntamiento Municipal de Ixtapa, Chiapas.

12. MEDIDAS DE SEGURIDAD GENERALES.

Con base en los resultados obtenidos en el análisis de brecha y riesgo, la Unidad de Transparencia del H. Ayuntamiento Municipal de Ixtapa, Chiapas, establece y mantiene medidas de seguridad orientadas a prevenir, detectar y reducir los riesgos que pudieran afectar los datos personales que son objeto de tratamiento durante el desarrollo de sus funciones.

Las medidas de seguridad tienen como finalidad proteger los datos personales contra daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado, así como garantizar que la información se encuentre disponible únicamente para las personas que, de acuerdo con sus funciones y atribuciones, requieran tener acceso a ella.

Las medidas implementadas consideran las características de los datos personales tratados, la naturaleza de los procedimientos realizados por la Unidad de Transparencia, los medios utilizados para el almacenamiento y manejo de la información, así como los riesgos identificados en el presente análisis.

De manera general, la Unidad de Transparencia contempla las siguientes medidas de seguridad:

- **Control de acceso a la información:** se procura que únicamente el personal autorizado tenga acceso a los expedientes, documentos, archivos y sistemas que contengan datos personales, de acuerdo con las funciones que desempeñe.
- **Resguardo de documentación física:** los expedientes y documentos que contengan datos personales deberán mantenerse en espacios destinados

para su conservación, evitando su exposición, extravió o consulta por personas no autorizadas.

- **Protección de información electrónica:** los archivos digitales que contengan datos personales deberán mantenerse bajo mecanismos de acceso controlado, procurando el uso de contraseñas y equipos institucionales para su consulta y procesamiento.
- **Confidencialidad:** el personal que intervengan en el tratamiento de datos personales deberá guardar confidencialidad respecto de la información a la que tenga acceso con motivo de sus funciones, incluso después de concluir su relación laboral o sus actividades dentro del área.
- **Clasificación y tratamiento de la información:** antes de proporcionar información que pudiera contener datos personales, se deberá revisar su naturaleza y, cuando corresponda, aplicar las medidas necesarias para evitar la divulgación de información que no debe hacerse publica.
- **Capacitación y concientización:** se promoverá que el personal conozca sus responsabilidades en materia de protección de datos personales, seguridad de información y confidencialidad.
- **Atención de incidentes:** cualquier pérdida, acceso no autorizado, divulgación, alteración o situación que pueda comprometer la seguridad de los datos personales deberá ser identificada, comunicada y atendida conforme a los procedimientos internos correspondientes.
- **Revisión y actualización:** las medidas de seguridad deberán revisarse y, en su caso, actualizarse cuando existan cambios en los procesos, sistemas, personal, tecnologías utilizadas o en los tipos de datos personales tratados por la Unidad de transparencia.

MEDIDAS ADMINISTRATIVAS.

Las medidas de seguridad administrativas comprenden las acciones, políticas, procedimientos y controles establecidos por la Unidad de Transparencia para organizar y regular el tratamiento de los datos personales durante el desarrollo de sus funciones.

La Unidad de Transparencia establece que el tratamiento de datos personales deberá realizarse únicamente para el cumplimiento de las atribuciones y funciones que correspondan al área, procurando que el personal que tenga acceso a dicha información conozca y cumpla con las obligaciones de confidencialidad y protección de datos personales.

Como parte de estas medidas, se consideran las siguientes acciones:

- Identificar y mantener actualizado el inventario de datos personales y de los sistemas de tratamiento utilizados por el área.
- Determinar las funciones y responsabilidades del personal que interviene en el tratamiento de datos personales.
- Limitar el acceso a la información exclusivamente al personal que lo requiera para el desempeño de sus funciones.
- Mantener procedimientos internos para la recepción, registro, atención y seguimiento de solicitudes de información y solicitudes relacionadas con datos personales
- Aplicar criterios de revisión de la información antes de su entrega o publicación, con el propósito de evitar la divulgación indebida de datos personales.

- Promover la capacitación y sensibilización del personal respecto de las obligaciones en materia de protección de datos personales y seguridad de la información.
- Mantener mecanismos para identificar y comunicar posibles incidentes de seguridad.
- Realizar revisiones periódicas de las medidas de seguridad implementadas y de los riesgos identificados.
- Actualizar las medidas de seguridad cuando existan modificaciones en los procesos, sistemas, personal o tipos de datos personales tratados.
- Procurar que el personal que tenga acceso a datos personales conozca las consecuencias administrativas derivadas de un tratamiento indebido de la información.
- Estas medidas buscan establecer una organización adecuada de las actividades relacionadas con la protección de datos personales y reducir los riesgos derivados de errores humanos, accesos indebidos o incumplimiento de los procedimientos establecidos.

MEDIDAS DE SEGURIDAD FISICAS.

Las medidas de seguridad físicas tienen como finalidad proteger los documentos, equipos, instalaciones y demás recursos materiales utilizados para el tratamiento de datos personales, evitando su pérdida, daño, deterioro, sustracción, acceso o utilización por personas no autorizadas.

Para tal efecto, la Unidad de Transparencia considera las siguientes medidas:

- Mantener los expedientes y documentos físicos que contengan datos personales en espacios destinados para su resguardo.
- Evitar que los documentos con datos personales permanezcan expuestos o al alcance de personas ajenas al área.
- Controlar el acceso físico al espacio donde se resguarda documentación que contenga datos personales.
- Procurar que los expedientes sean consultados únicamente por personal autorizado y durante el tiempo necesario para realizar las actividades correspondientes.
- Mantener los documentos organizados e identificados para facilitar su localización y evitar extravíos.
- Evitar dejar sobre escritorios, impresoras, copiadoras u otros espacios de uso común documentos que contengan datos personales.
- Adoptar medidas para prevenir daños ocasionados por humedad, polvo, agua, incendios, fallas eléctricas u otros factores ambientales que puedan afectar la documentación o los equipos.
- Procurar que los equipos de cómputo utilizados para el tratamiento de datos personales se encuentren ubicados en espacios bajo control del personal autorizado.
- Resguardar adecuadamente dispositivos, medios de almacenamiento y documentos que contengan información personal.
- En caso de destrucción o eliminación de documentos que contengan datos personales, procurar que se realice mediante mecanismos que impidan su recuperación o reconstrucción.

Estas medidas tienen como propósito mantener la integridad y disponibilidad de los documentos y recursos utilizados por la Unidad de Transparencia, reduciendo las posibilidades de pérdida, deterioro, sustracción o acceso físico no autorizado.

MEDIDAS DE SEGURIDAD TECNICAS.

Las medidas de seguridad técnicas comprenden los mecanismos y controles tecnológicos utilizados para proteger los datos personales tratados mediante equipos de cómputo, sistemas, archivos digitales y otros medios electrónicos.

La Unidad de Transparencia considera necesario mantener controles que permitan prevenir accesos no autorizados, pérdida de información, modificación indebida o divulgación de archivos electrónicos que contengan datos personales.

Entre las medidas consideradas se encuentran:

- Utilizar cuentas y contraseñas para controlar el acceso a los equipos y sistemas utilizados para el tratamiento de información.
- Procurar que las contraseñas sean de uso personal y no sean compartidas con personas no autorizadas.
- Bloquear o cerrar la sesión de los equipos cuando el personal se retire de su lugar de trabajo.
- Limitar el acceso a carpetas y archivos digitales que contengan datos personales de acuerdo con las funciones del personal autorizado.
- Mantener actualizados, en la medida de las posibilidades institucionales, los sistemas operativos, programas y herramientas de seguridad utilizados en los equipos.

- Utilizar mecanismos de protección contra software malicioso y otras amenazas informáticas.
- Realizar respaldos periódicos de la información electrónica que resulte necesaria para el funcionamiento de la Unidad de Transparencia.
- Procurar que los respaldos se mantengan en medios seguros y con acceso restringido.
- Evitar almacenar o transferir datos personales mediante dispositivos o medios electrónicos no autorizados.
- Verificar los archivos y destinatarios antes de enviar información que pudiera contener datos personales por medios electrónicos.
- Mantener controles de acceso a los archivos digitales para evitar modificaciones o eliminaciones no autorizadas.
- Reportar cualquier falla, pérdida de información, acceso inusual o incidente relacionado con los equipos y sistemas utilizados para el tratamiento de datos personales.
- Las medidas técnicas deberán revisarse periódicamente y fortalecerse de acuerdo con las necesidades del área, los recursos tecnológicos disponibles y los riesgos identificados en el análisis de brecha y riesgo.

CONSIDERACIÓN FINAL.

Las medidas administrativas, físicas y técnicas descritas deberán aplicarse de manera complementaria, debido a que la protección de los datos personales requiere la combinación de controles organizativos, físicos y tecnológicos.

La Unidad de Transparencia deberá mantener una revisión periódica de estas medidas con el propósito de identificar nuevas vulnerabilidades, atender las brechas detectadas y fortalecer los controles existentes, procurando que las medidas implementadas sean proporcionales a los riesgos asociados con el tratamiento de los datos personales bajo su responsabilidad.

13. PLAN DE TRABAJO.

**SECCIÓN CLASIFICADA DEL DOCUMENTO DE
SEGURIDAD, APARTADO DEL PLAN DE TRABAJO.**

Se testea el apartado número 13, que contiene el Plan de Trabajo, con fundamento en los artículos 25, 26, 27, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se determina que el Plan de Trabajo podrá ser objeto de testeo respecto de aquella información específica cuya divulgación pudiera comprometer la seguridad de los datos personales o de los sistemas de tratamiento.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL PLAN DE TRABAJO.

Se testea el apartado número 13, que contiene el Plan de Trabajo, con fundamento en los artículos 25, 26, 27, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se determina que el Plan de Trabajo podrá ser objeto de testeo respecto de aquella información específica cuya divulgación pudiera comprometer la seguridad de los datos personales o de los sistemas de tratamiento.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL PLAN DE TRABAJO.

Se testea el apartado número 13, que contiene el Plan de Trabajo, con fundamento en los artículos 25, 26, 27, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se determina que el Plan de Trabajo podrá ser objeto de testeo respecto de aquella información específica cuya divulgación pudiera comprometer la seguridad de los datos personales o de los sistemas de tratamiento.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL PLAN DE TRABAJO.

Se testea el apartado número 13, que contiene el Plan de Trabajo, con fundamento en los artículos 25, 26, 27, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se determina que el Plan de Trabajo podrá ser objeto de testeo respecto de aquella información específica cuya divulgación pudiera comprometer la seguridad de los datos personales o de los sistemas de tratamiento.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL PLAN DE TRABAJO.

Se testea el apartado número 13, que contiene el Plan de Trabajo, con fundamento en los artículos 25, 26, 27, 28, 29, 30, 31, 32 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se determina que el Plan de Trabajo podrá ser objeto de testeo respecto de aquella información específica cuya divulgación pudiera comprometer la seguridad de los datos personales o de los sistemas de tratamiento.

14. PROPUESTA DE CAPACITACIÓN

La capacitación constituye una herramienta fundamental para fortalecer la protección de los datos personales dentro del H. Ayuntamiento Municipal de Ixtapa, Chiapas, ya que permite que las personas servidoras públicas que intervienen en el tratamiento de datos personales conozcan sus responsabilidades y desarrollen los conocimientos necesarios para realizar sus funciones de manera adecuada y segura.

En materia de protección de datos personales, la capacitación deberá contribuir al fortalecimiento de las medidas de seguridad administrativas, físicas y técnicas implementadas por las diferentes áreas del Ayuntamiento, así como al adecuado cumplimiento de los principios, deberes y obligaciones relacionados con el tratamiento de datos personales.

Asimismo, permitirá fortalecer las capacidades del personal encargado de recibir, registrar, consultar, organizar, almacenar, utilizar, transferir, resguardar o, en su caso, publicar información que pueda contener datos personales, procurando que dichas actividades se realicen exclusivamente para las finalidades que correspondan al ejercicio de sus funciones.

En este sentido, la Unidad de Transparencia propone implementar un **Programa Institucional de Capacitación en Materia de Protección de Datos Personales**, dirigido a las personas servidoras públicas de las diferentes áreas municipales que intervienen en el tratamiento de datos personales.

El programa tendrá como finalidad proporcionar conocimientos básicos y prácticos sobre la protección de datos personales, así como establecer criterios comunes para su manejo, resguardo y protección dentro del Ayuntamiento.

La capacitación podrá realizarse mediante cursos, reuniones de trabajo, talleres, pláticas informativas y material de apoyo, de acuerdo con las necesidades y disponibilidad del Ayuntamiento.

PERIODICIDAD Y MECANISMO.

La capacitación en materia de protección de datos personales se realizará de manera periódica y estará dirigida a las personas servidoras públicas de las diferentes áreas del H. Ayuntamiento Municipal de Ixtapa, Chiapas, que intervengan en cualquier etapa del tratamiento de datos personales.

Como parte de las acciones de capacitación, se considerará la participación de las personas servidoras públicas responsables de la Unidad de Transparencia en las capacitaciones, cursos, talleres, reuniones de trabajo y demás actividades de actualización que sean impartidas por **la Autoridad de Transparencia para el Pueblo de Chiapas**, así como por las instituciones o autoridades competentes en materia de transparencia y protección de datos personales.

Una vez que la Unidad de Transparencia participe en dichas actividades de capacitación, las personas encargadas de la Unidad de Transparencia realizarán la difusión y réplica de los conocimientos adquiridos ante las diferentes áreas del H. Ayuntamiento, con la finalidad de que las personas servidoras públicas conozcan los principios, deberes, obligaciones y medidas de seguridad aplicables al tratamiento de datos personales.

Estas capacitaciones internas tendrán como finalidad que las áreas municipales conozcan y apliquen correctamente las medidas necesarias para el manejo, tratamiento, conservación, resguardo, consulta y protección de los datos personales que se encuentren bajo su responsabilidad.

Asimismo, la Unidad de Transparencia podrá establecer reuniones de orientación con las áreas municipales cuando se detecten necesidades específicas, nuevas obligaciones, cambios normativos, nuevos sistemas de tratamiento, modificaciones en los procedimientos internos o riesgos que requieran ser atendidos mediante capacitación.

La participación en las actividades de capacitación podrá acreditarse mediante listas de asistencia, convocatorias, material utilizado, presentaciones, constancias, fotografías, evaluaciones o informes de capacitación, según corresponda.

De esta manera, la Unidad de Transparencia contribuirá a mantener una capacitación continua y coordinada dentro del Ayuntamiento, procurando que las personas servidoras públicas que intervienen en el tratamiento de datos personales cuenten con los conocimientos necesarios para realizar sus funciones de manera segura y conforme a las disposiciones aplicables.

DOCUMENTO DE SEGURIDAD	
SISTEMA DE DATOS PERSONALES DE IXTAPA, CHIAPAS	
FECHA DE ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD	FECHA DE ÚLTIMA ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD:
23 DE SEPTIEMBRE DEL 2026	23 DE SEPTIEMBRE DEL 2026
ELABORO: LIC. CRISTAL GUADALUPE OCAÑA LÓPEZ. JEFA DE LA UNIDAD DE TRANSPARENCIA.	
APROBÓ: LIC. MIGUEL ÁNGEL VERA GÓMEZ. PRESIDENTE DEL COMITÉ. LIC. CRISTAL GUADALUPE OCAÑA LÓPEZ. SECRETARIA DEL COMITÉ. C. NORMA DINA HERNÁNDEZ HERNÁNDEZ. VOCAL DEL COMITÉ.	