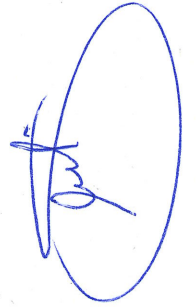
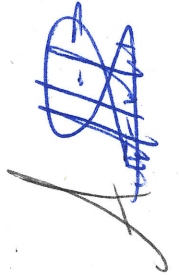
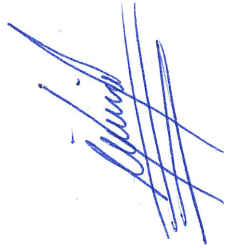


Documento de Seguridad del H. Ayuntamiento de Tuzantla, Michoacán.



INDICE.

Glosario.....	pág. 03
Prólogo	pág. 03
Objetivo	pág. 04
Justificación.....	pág. 04
Alcance	pág. 06
Desarrollo	pág. 07
I. Inventario de Tratamiento y Datos Personales	pág. 07
II. Funciones y Obligaciones de las Personas Servidoras Públicas que tratan Datos Personales	pág. 10
III. Análisis de Riesgo	pág. 14
IV. Análisis de Brecha.....	pág. 17
V. Plan de Trabajo	pág. 19
VI. Monitoreo de la las Medidas de Seguridad.....	pág. 24
VII. Programa General de Capacitación en Materia de Protección de Datos .	pág. 25
Bibliografía.....	pág. 25
Firmas del Comité de Transparencia.....	pág. 26



GLOSARIO.

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

Ley General de Transparencia. Ley General de Transparencia y Acceso a la Información Pública.

UT. Unidad de Transparencia.

PNT. Plataforma Nacional de Transparencia.

IMAIP. Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales.

INAI. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

PROLOGO.

La UT es la primer área u oficina de contacto que tiene el público en general cuando estos buscan información pública de un sujeto obligado, es por ello que es de suma importancia que su funcionamiento sea el de enlazar una consulta de información, realizada por el interesado, con el área que genere, administre y resguarde la información solicitada en dicha eventualidad. Ya que se debe de garantizar la transparencia de información a cualquier persona que la solicite, pero también se debe de garantizar la protección de datos personales.

Es así que en base a la Ley de Protección de datos Personales en su Cap. II Art. 35 De manera particular, el responsable deberá elaborar un documento de seguridad, el cual tiene como objetivo salvaguardar los datos que vulneren la identidad de las personas y que hagan identificable a la misma. Por lo que este Documento se centra en como salvaguardar la identidad de las personas ¿Qué y cómo se debe de hacer?

Tel que como lo define la Ley de Protección de Datos Personales el Documento de seguridad es el Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

OBJETIVO.

El presente documento tiene como objetivo primordial garantizar el correcto trato de los datos Personales en posesión del H. Ayuntamiento de Tuzantla, brindando las herramientas necesarias en base a lo estipulado en la Ley de Protección de Datos personales y así garantizar que los servidores públicos que manejan datos personales inherentes a su labores cotidianes, estos tengan un Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

JUSTIFICACIÓN.

Que como lo establece la Ley de Protección de Datos Personales en su Art. 83 El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales y que sus funciones serán las que siguen (Art. 84):

- Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;
- Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
- 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;
- Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;
- Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;
- Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto y los organismos garantes, según corresponda;
- Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y
- Dar vista al órgano interno de control o instancia 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; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.

Por lo que el Comité de Transparencia serán los encargados de vigilar el correcto trato de los Datos Personales, siendo estos la autoridad máxima en dicha materia.

Por lo que también en el TÍTULO SEGUNDO, PRINCIPIOS Y DEBERES, Cap. II De los Deberes. El responsable deberá establecer y mantener las medidas de

seguridad de carácter administrativo, físico y técnico para la protección de datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

En el Art. 35 de la presente Ley, se establecen que los sujetos obligados en posesión de datos personales y de manera particular, el responsable tendrá que elaborar un documento de seguridad, que contenga al menos lo siguiente:

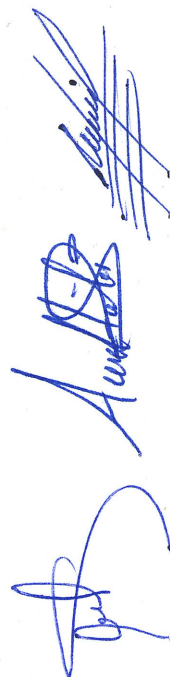
- I. El inventario de datos personales y de los sistemas de tratamiento;
- II. Las funciones y obligaciones de las personas que traten datos personales;
- III. El análisis de riesgos;
- IV. El análisis de brecha;
- V. El plan de trabajo;
- VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
- VII. El programa general de capacitación.

La protección de datos en posesión de Sujetos Obligados es primordial, debido a la gravedad en la que incurriría un servidor público si por alguna error comparte algún dato y si en dado caso hay vulnerabilidad con alguna base de datos de datos personales se tendrá que proceder como marca el Art. 37, dice que en caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

Además, conforme al Art. 39, las que incluyan la leyes y normatividad aplicable, también se considerará vulneración de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguiente:

- I. La pérdida o destrucción no autorizada;
- II. El robo, extravío o copia no autorizada;
- III. El uso, acceso o tratamiento no autorizado, o
- IV. El daño, la alteración o modificación no autorizada.

Cada que ocurra una vulneración de seguridad en los datos Personales, se tendrá que llevar una bitácora, con la finalidad de que el motivo por el cual se vulnero, no se vuelva a repetir.



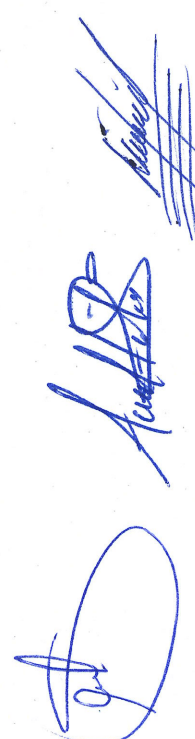
ALCANCE.

Para que el objetivo de este documento de seguridad se lleve a cabo, se requiere del impulso de más alto nivel de cada sujeto Obligado, en este caso, del presidente Municipal, para que se tomen las medidas necesarias para que sea de observancia obligatorias para todas las áreas del H. Ayuntamiento de Tuzantla, que dentro de sus funciones traten con datos personales. Además, como el Comité de Transparencia es la Autoridad Máxima para este Documento, deberán de apoyar la instrucción que girará el presidente Municipal de que el presente documento sea de observancia Obligatoria para las oficinas citadas, es decir, el presidente gira la instrucción y el Comité de Transparencia se encargara de darlo a conocer en todas las áreas.

A continuación, se enlistan las áreas del H. Ayuntamiento de Tuzantla para las cuales será obligatorio conocer y apegarse a este Documento de Seguridad:

1. Presidencia
2. Sindicatura
3. Obras Públicas
4. Tesorería
5. Contraloría
6. Desarrollo Rural
7. Desarrollo Social
8. Dirección de Salud
9. Secretaría
10. Dirección de la Mujer
11. Atención al Migrante
12. DIF
13. Oficialía Mayor
14. Servicios Municipales.
15. Seguridad Pública

En caso de que no quieran apegarse a las indicaciones aquí descritas, se tendrán que apegar a lo que dicta la Ley de Protección de Datos en su Título Décimo Tercero Medidas de Apremio y Responsabilidad del art. 152 al 168.



DESARROLLO.

Para realizar el desarrollo de este documento partimos de los conceptos que se refieren a datos personales.

Los datos Personales son Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Tomando en cuenta lo anterior, se realizó un diagnóstico en conjunto con las áreas del H. Ayuntamiento de Tuzantla, para verificar que oficinas manejan Datos Personales y que sean inherentes a sus funciones, dando como resultado las áreas que arriba se citaron (Listado de áreas para las que será obligatorio la observancia de este documento).

I. Inventario de Tratamiento y Datos Personales.

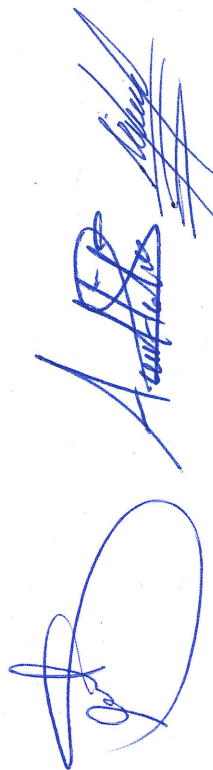
Por inventario de Tratamiento de Datos Personales, entenderemos que es el control documental que se lleva a cabo por las áreas del H. Ayuntamiento de Tuzantla con la finalidad de desempeñar funciones inherentes al cargo público que se desempeña.

Con respecto al análisis y alcance que se realizó de este documento de seguridad, hemos identificado 39 cantidad de Tratamientos de datos Personales, los cuales se especifican en la siguiente tabla:

Área del Ayuntamiento.	Tratamiento.
Presidencia.	<ul style="list-style-type: none"> • Celebrar Convenios con Personas Morales o Físicas. • Recepción de Solicitudes de Apoyo.
Sindicatura	<ul style="list-style-type: none"> • Celebrar Convenios/Contratos de Compraventa y audiencias de conciliación entre Particulares. • Recibir Demandas ciudadanas. • Mandar notificaciones de demandas a título personal.
Obras Públicas	<ul style="list-style-type: none"> • Comité ciudadano de la localidad beneficiada para cada obra pública. • Solicitudes de apoyo con maquinaria pesada.
Tesorería	<ul style="list-style-type: none"> • Otorgamiento de Apoyo y Subsidios para personas Físicas o Morales. Generando padrones por cada



	<p>programa de subsidios al que se haya hecho acreedor el titular de los datos personales.</p> <ul style="list-style-type: none"> • Emisión de Licencias de Funcionamiento (documentación solicitada para su emisión). • Padrón de Pagos del Impuesto Predial, ISA y altas en el padrón. • Nóminas de Servidores Públicos/empleados (INE, comprobante de domicilio, etc.) • Padrón de Proveedores.
Contraloría	<ul style="list-style-type: none"> • Declaraciones Patrimoniales.
Desarrollo Rural	<ul style="list-style-type: none"> • Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.
Desarrollo Social	<ul style="list-style-type: none"> • Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.
Dirección de Salud	<ul style="list-style-type: none"> • Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.
Secretaría	<ul style="list-style-type: none"> • Trámites y servicios de: Cartilla Militar, Constancias de Identidad, Comprobante de residencia, de domicilio, de bajos recursos y de buena conducta, Carta de recomendación, constancia de ingresos, de origen, de pertenencia, de residencia, de origen y vecindad, de modo honesto de vivir, de no adeudo y Permisos para eventos sociales.
Dirección de la Mujer	<ul style="list-style-type: none"> • Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.
Atención al Migrante	<ul style="list-style-type: none"> • Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.
DIF	<ul style="list-style-type: none"> • Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.
Oficialía Mayor	<ul style="list-style-type: none"> • Expedientes de los trabajadores del ayuntamiento. • Permisos de Incapacidad.
Servicios Municipales	<ul style="list-style-type: none"> • Solicitudes de apoyo para la reparación de algún servicio (Luz, agua, tala de árboles y drenaje)
Seguridad Pública	<ul style="list-style-type: none"> • Resguardo y/o entrega de Citatorios o Expedientes girados por alguna dependencia gubernamental para la prevención del delito. • Resguardo de Individuos sospechosos de incurrir en algún tipo de delito.



Los datos Personales recabados por estas áreas del ayuntamiento, según el análisis de los mismos, los podremos clasificar como sigue:

De identificación: Nombre, sexo, nacionalidad, fecha de nacimiento, antecedentes laborales, correo electrónico personal, CV, datos familiares, estado civil, ocupación, firma, CURP, RFC, número de seguridad social, Identificación oficial del propietario, clave de elector, fotografía del propietario, huella digital o dactilar, entre otros.

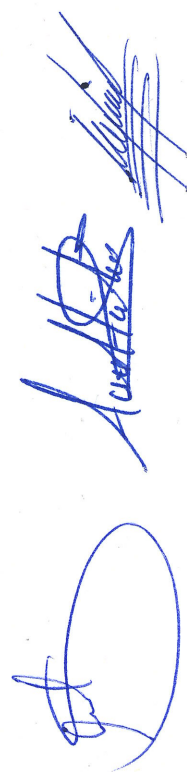
Patrimoniales: Numero de Cuentas bancarias, estado de cuentas, clave interbancaria, institución bancaria, datos contenidos en declaraciones patrimoniales, Ahorro para vivienda, descuentos por algún crédito adquirido por el titular, etc.

Sensibles: Creencias Religiosas, filosóficas o morales, datos de salud, datos sobre procedimientos judiciales, discapacidad, información genética, migratorias, origen étnico o racial.

Con lo que cada unidad Administrativa cuenta con la siguiente cantidad de tratamientos.

Área del Ayuntamiento.	Cantidad de Tratamiento.
Presidencia.	2
Sindicatura	3
Obras Públicas	2
Tesorería	5
Contraloría	1
Desarrollo Rural	1
Desarrollo Social	1
Dirección de Salud	1
Secretaria	15
Dirección de la Mujer	1
Atención al Migrante	1
DIF	1
Oficialía Mayor	2
Servicios Municipales	1
Seguridad Pública	2

Dando, así como secretaria el área donde más se realizan tratamientos de seguridad, por la cantidad de trámites y servicios, aunque también, el área de Tesorería que está ubicada en segundo lugar, el manejo de la cantidad de datos Personales que protege es en mayor volumen que secretaria.



II. Funciones y Obligaciones de la Personas Servidoras Públicas que tratan Datos Personales.

Proteger los datos personales en posesión de los sujetos obligados es obligatorio para los servidores públicos que los administran y resguardan, y con ello apegarse a lo que dictamina La ley de Protección de Datos. Para garantizar la protección de los datos personales que se administran en cada área de este Ayuntamiento de Tuzantla, se designaron los responsables de cada tratamiento, enlistándolos como sigue:

No.	Área Administrativa	Nombre del responsable	Cargo dentro del Sujeto Obligado	Tratamiento.
1	Presidencia.	Arturo Serrato Suárez	Presidente Municipal	Celebrar Convenios con Personas Morales o Físicas
		Anayeli Vázquez Villafaña	Secretaria	
2	Presidencia.	Arturo Serrato Suárez	Presidente Municipal	Recepción de Solicitudes de Apoyo.
		Anayeli Vázquez Villafaña	Secretaria	
		Álvaro Hidalgo López	Secretario Particular	
3	Sindicatura	María de la Cruz Villafaña Robles	Síndico Municipal	Celebrar Convenios/Contratos de Compraventa y audiencias de conciliación entre Particulares.
		Pedro Delgado Delgado	Asesor Jurídico	
		Anayeli Osorio García	Auxiliar	
4	Sindicatura	María de la Cruz Villafaña Robles	Síndico Municipal	Recibir Demandas ciudadanas.
		Pedro Delgado Delgado	Asesor Jurídico	
		Anayeli Osorio García	Auxiliar	
5	Sindicatura	María de la Cruz Villafaña Robles	Síndico Municipal	Mandar notificaciones de demandas a título personal.
		Pedro Delgado Delgado	Asesor Jurídico	
		Anayeli Osorio García	Auxiliar	
6	Obras Públicas	Nemesio Pérez Mondragón	Director	Comité ciudadano de la localidad beneficiada para cada obra pública.
		María de Lourdes Vargas Loza	Secretaria	
7	Obras Públicas	Nemesio Pérez Mondragón	Director	Solicitudes de apoyo con maquinaria pesada.
		María de Lourdes Vargas Loza	Secretaria	
8	Tesorería	Fernando Ocampo Mercado	Tesorero Municipal	Otorgamiento de Apoyo y Subsidios para

[Handwritten signatures and initials in blue ink, including a large signature that appears to be 'Arturo Serrato' and another signature below it.]

		Blanca Estela Camacho Ynistra	Contadora	personas Físicas o Morales. Generando padrones por cada programa de subsidios al que se haya hecho acreedor el titular de los datos personales.
		Bonfilio Bucio González	Contador	
		Teresa Camacho Brito	Contadora	
9	Tesorería	Fernando Ocampo Mercado	Tesorero Municipal	Emisión de Licencias de Funcionamiento (documentación solicitada para su emisión).
		Adriana Tavira Santana	Encargada de Ingresos	
10	Tesorería	Fernando Ocampo Mercado	Tesorero Municipal	Padrón de Pagos del Impuesto Predial, ISA y altas en el padrón.
		Adriana Tavira Santana	Encargada de Ingresos	
11	Tesorería	Fernando Ocampo Mercado	Tesorero Municipal	Nóminas de Servidores Públicos/empleados (INE, comprobante de domicilio, etc.)
		Bonfilio Bucio González	Contador	
12	Tesorería	Fernando Ocampo Mercado	Tesorero Municipal	Padrón de Proveedores.
		Teresa Camacho Brito	Contadora	
13	Contraloría	Abimael Albarrán Avilés	Contralor	Declaraciones Patrimoniales
		Yareli Arzate López	Secretaria	
		Almadeni Toledo Arellano	Secretaria	
14	Desarrollo Rural	Sandra Mariana Pereznegron Cabrera	Directora	Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.
		Yomara Sandoval Almaraz	Secretaria	
15	Desarrollo Social	Alicia Gabriela San Román Rodríguez	Directora	Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.
		Yanet Suarez Reyes	Secretaria	
16	Dirección de Salud	Imelda Sánchez Bautista	Directora	Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.
		Rubí Yareli Castro Toledo	Secretaria	
17	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Tramites de Cartilla Militar.
		Luis Eduardo Sandoval Nateras	Auxiliar	





TUZANTLA
"Un gobierno para el pueblo"



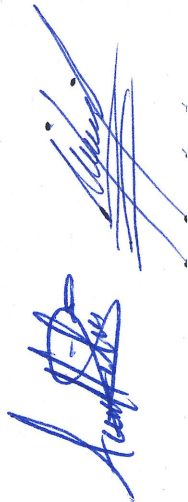
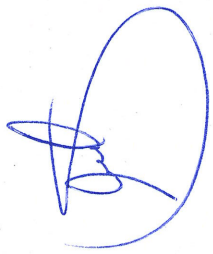
18	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Trámite de constancias de Identidad.
		Alma Rosa Machuca Quiroz	Secretaria	
		Luis Eduardo Sandoval Nateras	Auxiliar	
19	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Trámite de Comprobante de residencia.
		Alma Rosa Machuca Quiroz	Secretaria	
		Luis Eduardo Sandoval Nateras	Auxiliar	
20	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Trámite de Comprobante de domicilio.
		Alma Rosa Machuca Quiroz	Secretaria	
		Luis Eduardo Sandoval Nateras	Auxiliar	
21	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Trámite de Comprobante de bajos recursos.
		Alma Rosa Machuca Quiroz	Secretaria	
		Luis Eduardo Sandoval Nateras	Auxiliar	
22	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Trámite de Constancia de buena conducta.
		Alma Rosa Machuca Quiroz	Secretaria	
		Luis Eduardo Sandoval Nateras	Auxiliar	
23	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Trámite de Carta de recomendación.
		Alma Rosa Machuca Quiroz	Secretaria	
		Luis Eduardo Sandoval Nateras	Auxiliar	
24	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Trámite de constancia de ingresos.
		Alma Rosa Machuca Quiroz	Secretaria	
		Luis Eduardo Sandoval Nateras	Auxiliar	
25	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Trámite de Constancia de origen y vecindad.
		Alma Rosa Machuca Quiroz	Secretaria	
		Luis Eduardo Sandoval Nateras	Auxiliar	
26	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Trámite de pertenencia.
		Alma Rosa Machuca Quiroz	Secretaria	

[Handwritten signatures and marks in blue ink on the right side of the page]

		Luis Eduardo Sandoval Nateras	Auxiliar	
27	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Trámite de Constancia de residencia.
		Alma Rosa Machuca Quiroz	Secretaria	
		Luis Eduardo Sandoval Nateras	Auxiliar	
28	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Trámite de Constancia de modo honesto de vivir.
		Alma Rosa Machuca Quiroz	Secretaria	
		Luis Eduardo Sandoval Nateras	Auxiliar	
29	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Trámite de Constancia de no adeudo.
		Alma Rosa Machuca Quiroz	Secretaria	
		Luis Eduardo Sandoval Nateras	Auxiliar	
30	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Trámite de Constancia de misma persona.
		Alma Rosa Machuca Quiroz	Secretaria	
		Luis Eduardo Sandoval Nateras	Auxiliar	
31	Secretaría	Víctor Manuel Ocampo Córdova	Secretario	Permisos para eventos sociales.
		Alma Rosa Machuca Quiroz	Secretaria	
		Luis Eduardo Sandoval Nateras	Auxiliar	
32	Dirección de la Mujer	Esmeralda García Sanchez	Directora	Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.
33	Atención al Migrante	Erika Pacheco Arriaga	Directora	Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.
34	DIF	Rosa Elia Serrato Suárez	Directora	Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.
		Yuliana Samudio Vieyra	Secretaria	
35	Oficialía Mayor	Pedro García Montillo	Oficial Mayor	Expedientes de los trabajadores del ayuntamiento.
		Olivia Toledo Pérez	Secretaria	
36		Pedro García Montillo	Oficial Mayor	

[Handwritten signatures in blue ink]

	Oficialía Mayor	Olivia Toledo Pérez	Secretaria	Permisos de Incapacidad.
37	Servicios Municipales	Fermin Leyva Carmona	Director	Solicitudes de apoyo para la reparación de algún servicio (Luz, agua, tala de árboles y drenaje)
38	Seguridad Pública	Arturo Sánchez Rodríguez	Director	Resguardo y/o entrega de Citatorios o Expedientes girados por alguna dependencia gubernamental para la prevención del delito.
		Maribel Moreno Cardozo	Secretaria	
39	Seguridad Pública	Arturo Sánchez Rodríguez	Director	Resguardo de Individuos sospechosos de incurrir en algún tipo de delito.
		Maribel Moreno Cardozo	Secretaria	

III. Análisis de riesgo.

El análisis de riesgo es parte fundamental de este documento de seguridad, ya que es donde se analiza de fondo como se pueden identificar las medidas de seguridad implementadas para salvaguardar la integridad de los Datos personales en Posesión del H. Ayuntamiento de Tuzantla. Que como se establece en el Art. 33 fracc. IV. Se deberá realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.

Dicho análisis sirve para identificar el riesgo inherente a los datos personales en el tratamiento a que son sometidos en el ejercicio de las funciones del H. Ayuntamiento de Tuzantla con respecto a la integridad de las personas. Es así como la Evaluación de riesgos de los datos personales forman parte de la serie de elementos que integran el documento de seguridad, del cual su propósito es garantizar la confidencialidad, integridad y disponibilidad de los datos personales en posesión del Ayuntamiento.

Es así que se deberá considerar que, para realizar un Análisis de riesgo sobre la protección de datos, se deberá tener en cuenta lo siguiente:

- I. El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida.
- II. El valor y exposición de los activos involucrados en el tratamiento de datos personales.

- III. Los requerimientos regulatorios, código de conducta o mejores prácticas de un sector específico.
- IV. Las consecuencias y negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.
- V. Además, lo que se dispone en el Art. 32 de esta Ley de Protección de datos personales

Es así que, para maximizar la Protección de Datos Personales por el H. Ayuntamiento de Tuzantla, se aplicó un instrumento para Clasificar los datos utilizados, a partir de lo que marca la Ley (como se menciona en la pág. 8 Clasificación de los datos Personales). Se mencionan a continuación para resaltar a cuál clasificación se hace referencia:

- De identificación.
- Patrimoniales.
- Sensibles.

De esta clasificación de datos Personales, se identificó que con los que más se cuentan son con la Clasificación de Datos Personales y después la de Datos Sensibles, quedando en último, pero no menos importante los Datos Patrimoniales, la razón de que sea baja, radica en su clasificación ya que es lo que menos se maneja de Datos Personales en el H. Ayuntamiento de Tuzantla.

Se presenta la siguiente tabla, donde se hace la clasificación del tratamiento de Datos Personales en el H. Ayuntamiento de Tuzantla.

No	Tratamiento.	Tipo de Clasificación de Datos Personales.
1	Celebrar Convenios con Personas Morales o Físicas	De identificación.
2	Recepción de Solicitudes de Apoyo.	De identificación.
3	Celebrar Convenios/Contratos de Compraventa y audiencias de conciliación entre Particulares.	De identificación.
4	Recibir Demandas ciudadanas.	Datos Sensibles
5	Mandar notificaciones de demandas a título personal.	Datos Sensibles
6	Comité ciudadano de la localidad beneficiada para cada obra pública.	De identificación.
7	Solicitudes de apoyo con maquinaria pesada.	De identificación.
8	Otorgamiento de Apoyo y Subsidios para personas Físicas o Morales. Generando padrones por cada programa de subsidios al que se haya hecho acreedor el titular de los datos personales.	De identificación.
9	Emisión de Licencias de Funcionamiento (documentación solicitada para su emisión).	De identificación.
10	Padrón de Pagos del Impuesto Predial, ISA y altas en el padrón.	Patrimoniales
11	Nóminas de Servidores Públicos/empleados (INE, comprobante de domicilio, etc.)	Patrimoniales
12	Padrón de Proveedores.	De identificación
13	Declaraciones Patrimoniales	Patrimoniales
14	Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.	De identificación

15	Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.	De identificación
16	Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.	De identificación
17	Tramites de Cartilla Militar.	De identificación
18	Tramite de constancias de Identidad.	De identificación
19	Trámite de Comprobante de residencia.	Sensibles
20	Trámite de Comprobante de domicilio.	De identificación
21	Trámite de Comprobante de bajos recursos.	De identificación
22	Trámite de Constancia de buena conducta.	De identificación
23	Trámite de Carta de recomendación.	De identificación
24	Trámite de constancia de ingresos.	De identificación
25	Trámite de Constancia de origen y vecindad.	De identificación
26	Trámite de pertenencia.	De identificación
27	Trámite de Constancia de residencia.	De identificación
28	Trámite de Constancia de modo honesto de vivir.	De identificación
29	Trámite de Constancia de no adeudo.	De identificación
30	Trámite de Constancia de misma persona.	De identificación
31	Permisos para eventos sociales.	De identificación
32	Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.	De identificación
33	Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.	De identificación
34	Padrón de los beneficiarios de los programas sociales que otorga esta esta dirección.	De identificación
35	Expedientes de los trabajadores del ayuntamiento.	De identificación
36	Permisos de Incapacidad.	Sensibles
37	Solicitudes de apoyo para la reparación de algún servicio (Luz, agua, tala de árboles y drenaje)	De identificación
38	Resguardo y/o entrega de Citatorios o Expedientes girados por alguna dependencia gubernamental para la prevención del delito.	Sensibles
39	Resguardo de Individuos sospechosos de incurrir en algún tipo de delito.	Sensibles

[Handwritten signatures and initials in blue ink on the right margin of the table]

De identificación son: 30 tratamientos, de Datos Sensibles son 6 y 3 de Datos Patrimoniales.

También se valoró la probabilidad y el impacto que pudiera tener para el titular, en caso de que ocurriera uno o más factores (amenazas) durante el ciclo de vida de los datos sometidos a tratamiento (obtención, almacenamiento, transferencia, remisión, bloqueo y/o supresión). Y aunado a lo anterior, la Presente Ley de Protección de Datos Personales en su Art. 38 establece que se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

- I. La pérdida o destrucción no autorizada;
- II. El robo, extravío o copia no autorizada;
- III. El uso, acceso o tratamiento no autorizado, o
- IV. El daño, la alteración o modificación no autorizada.

Siendo estos son los que presentan mayor riesgo de vulneración, dentro de los sujetos obligados, pero, el que presenta una probabilidad mayor de ser vulnerado es el de robo, extravió o copia no autorizada.

Una vez realizado el análisis de riesgo, se puede presentar que la dependencia que presenta mayor riesgo en vulneración de datos es: secretaria, por la cantidad de tratamientos que maneja y en segundo lugar es Tesorería, ya que al ser el área que tiene la segunda cantidad mayor de tratamientos, aumenta el riesgo de vulneración, pero si comparamos el volumen de datos personales que se manejan en cada área; Tesorería maneja 60% más de datos Personales. Para las áreas que cuentan con menos riesgo de vulneración, son: Desarrollo Social y Dirección de salud, esto por el volumen tan bajo de Datos Personales que manejan, en comparación con Tesorería (que es la que más maneja datos Personales), cuentan con tan solo un 5% de los datos totales, además, los datos que manejan son solo identificativos.

IV. Análisis de brecha

Independiente del sistema en el que se encuentren los datos personales o el tipo de tratamiento que se realice, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales. Dichas medidas deberán protegerlos en contra de daño, pérdida, destrucción o su uso, acceso o tratamiento no autorizado y a su vez deberá garantizar su confidencialidad, integridad y disponibilidad (cuando aplique), todo esto conforme se establece en el Art. 31 de la presente Ley. Las medidas implementadas son las siguientes:

- **MEDIDAS FÍSICAS.**

1. Restringir el acceso a Personas no autorizadas a las distintas áreas del H. Ayuntamiento, donde se resguarden datos personales.
2. Contar con instalaciones que tengan cerradura con llave, para dejar cerradas las oficinas, cada que el responsable de la protección de los datos personales que se resguardan en esa área, salga.
3. Entregar una copia de este Documento de Seguridad para que el personal que maneja, administra o resguarda datos personales, tenga conocimiento de la importancia de que no se vulneren estos.

- **MEDIDAS ADMINISTRATIVAS.**

1. Compartir las capacitaciones impartidas por parte del IMAIP e INAI, en materia de Protección de Datos Personales e invitarlos a que durante las capacitaciones expresen sus dudas para que estas sean disipadas que si bien, hay alguna duda específica, llamar al IMAIP con el especialista en Protección de Datos y realizar la consulta.

2. Que como lo marca el Art. 37 de esta Ley, en caso de que ocurra una vulneración el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.
3. Elaborar y aplicar un formato para solicitar algún documento que se encuentre en el área de archivo, este con la finalidad de que, si hay alguna vulneración de datos, poder rastrear posibles responsables y a su vez que se tenga un mayor control de los archivos que entran y salen del área de Archivo.
4. Diseñar e implementar un documento (carta) responsivo (a) donde se comprometan a cumplir con el deber de confidencialidad por parte de la persona que administre y/o resguarde datos personales.

- **MEDIDAS TÉCNICAS.**

1. Al usar el correo electrónico, siempre utilizar el correo electrónico institucional y nunca el personal para uso de las actividades laborales, con minimizando la fuga de datos personales.
2. Verificar que, al fin de la jornada laboral, no se queden en las impresoras del área alguna impresión olvidada que contenga datos personales que se puedan vulnerar por el descuido.
3. Cuando se esté recabando copias de datos personales identificables y estas se saquen mal o tengan error de impresión, cuando se detecte esta situación hay que destruir la copia con los datos personales, para con ello, garantizar la protección de los datos que en el documento se encontraban.
4. Cuando se creen cuentas para el respaldo de datos, garantizar la protección de datos personales creando contraseñas con Caracteres especiales, fáciles de recordar, pero, difícil de descifrar por terceros. Es importante que los usuarios y contraseñas creados, sean de uso exclusivamente individual, evitando compartirlos con los compañeros, porque esto aumenta el riesgo de vulnerar los datos personales.
5. Cuando se percate de que su usuario o contraseña han sido usados por terceros, inmediatamente comunicarse con el área de informática de este H. Ayuntamiento de Tuzantla, el técnico en informática evaluará la posible violación y les brindará la mejor solución para el caso.

- **CONTROLES DE IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS.**

En el H. Ayuntamiento de Tuzantla los sistemas que se manejan son de carácter básicos, el sistema más complejo que se maneja es en Tesorería, el Sistema Contable y Armonizado, de este, a cada contador se le asigno su usuario en su



equipo de cómputo y se realiza el respaldo diario del sistema, con esto evitando la pérdida de datos importante y Maxime de datos personales. En lo que concierne a los demás equipos de cómputo del Ayuntamiento, la medida de seguridad que se implemente es ponerle contraseña de inicio a cada computadora, esto con la finalidad de que terceros no accedan a las mismas y pueda sustraer información y entre ella, datos personales. Como se mencionó en las medidas Técnicas, si el usuario del equipo de cómputo detecta algo inusual en su ordenador, deberá llamar al encargado de sistemas para que evalúe la posible violación en carácter de seguridad.

- **RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.**

El respaldo de la información generado por cada área del H. Ayuntamiento de Tuzantla se realiza en un medio de almacenamiento digital, como puede ser: Memoria USB, disco, Nube o Disco duro; aunque se recomienda que se respalde de preferencia en USB o Disco duro externo, al menos una vez a la semana; en la nube no se recomienda tanto, ya que el Ayuntamiento no cuenta con el servicio de almacenamiento y al que acceden los servidores públicos es a la versión de prueba o gratis que otorgan ciertas plataformas como son Google, Dropbox, entre otras; Al ser prueba, la información que respaldan en la nube, no está segura o del todo accesible, esto porque pueden cambiar las políticas de uso y perder el acceso a la cuenta y con ello, la información.

La recuperación de la información que por alguna razón se eliminó del ordenador o se extravió, la realiza el encargado de sistemas, pero es importante hacer mención que, no siempre es posible recuperar la totalidad de la información, es por ello que recomendamos a los responsables de la información que se genera o recaba, que los respaldos los hagan periódicamente para que, en el peor de los casos, se pierda la menos información posible.

V. Plan de trabajo

En lo que concierne al Plan de Trabajo de H. Ayuntamiento de Tuzantla, es la serie de casos hipotéticos que se pudieran llegar a presentar y como les haremos frente.

- **PLAN DE CONTINGENCIA PARA LA PROTECCIÓN DE LA INFORMACIÓN.**

Para desarrollar un plan ante las posibles contingencias que se pudieran presentar, se parte de la clasificación de las mismas en función de su grado de afectación:

Grado 1: Son las de menor impacto y son las que van desde las fallas eléctricas, fallas en la conexión de internet, las cuales pueden ser atendidas por el mismo personal de Ayuntamiento.



Grado 2: La presentación de estas contingencias, son de afectación media y para corregirlas o minimizar su impacto, se requiere el apoyo del Personal del Ayuntamiento, así como personal externo. Algunas de estas eventualidades podrán ser un incendio y se requeriría del apoyo de protección civil y de los bomberos.

Grado 3: Son contingencias que, por su grado de afectación, afectan severamente la operatividad del Instituto y se requiere el apoyo externo del personal calificado para la eventualidad que se haya presentado.

Consideraciones Principales:

1. Se deberá efectuar una evaluación después de que haya paso la eventualidad.
2. Dentro del plan de contingencia, se debe de contar con un responsable general, quien será el que organice a los demás para ejecutar el plan.
3. En cada área del H. Ayuntamiento deberá de existir un encargado, este debe de conocer el plan de contingencia y además deberá de contar con conocimientos en el uso de extintores, hidrante, entre otros.
4. Es importante, que cuando se tenga el plan de contingencia, se realicen simulacros, como los que se realizan para los sismos.
5. Los encargados de cada área y el encargado general, deben reunirse periódicamente para capacitarse y evaluarse, así como también formar las brigadas y mantenerlas vigentes.
6. Revisar el plan de contingencia, una vez ya analizado, se emitirán recomendaciones y decisiones tomadas en base al aprendizaje adquirido de implementar dicho plan.
7. Una vez completo el Plan y aprobado, este se tendrá que dar la difusión correspondiente para que todos los servidores públicos del H. Ayuntamiento de Tuzantla lo conozcan.

Lugar alternativo de trabajo:

Esta posibilidad se debe de considerar, ya que los desastres naturales (Sismos, Inundaciones e incendios) no Esta posibilidad se debe de considerar, ya que los desastres naturales (Sismos, Inundaciones e incendios) no son predecible y pueden tomar por sorpresa a los trabajadores y público en general. Es por ello que se debe de considerar un lugar alerno para realizar las labores inherentes al cargo, este lugar alerno puede ser propio, mediante una colaboración o rentado (si hay el presupuesto).

En caso de que se cuente con un lugar alerno, este deberá por lo menos contar con los siguientes recursos:

- Mesas para los monitores, CPU's y teclados de los servidores principales.
- Sillas.

- Conexiones Eléctricas.
- Conexión a internet.
- Teléfono.
- Extinguidor
- Útiles de oficina.
- Servicios básicos (Agua, Luz y WC).

Medidas preventivas ante Siniestros.

Medidas de prevención y conservación de los archivos:

1. El Archivo de concentración o histórico debe situarse en el primer piso del edificio (no sótano).
2. El espacio donde se almacenan los archivos de contar con luz natural y sin humedad.
3. Los muebles utilizados, deberán ser los óptimos para el almacenamiento de los archivos, para garantizar la conservación y uniformidad de los mismos.
4. Se debe de evitar archivar documentación cerca de los aparatos eléctricos y las instalaciones eléctricas se deben de encontrar en condiciones óptimas, ya que estas podrían ocasionar un siniestro.
5. Los estantes de archivo deberán de estar entre 10 y 15 cm del suelo, para que faciliten la limpieza y así eviten a su vez la acumulación de humedad y proliferación de plagas.
6. Todos los equipos eléctricos cuando finalice la jornada laboral, deberán quedar apagados y desconectados.
7. Se recomienda no colocar vasos con líquido que puedan derramarse fácilmente sobre los aparatos electrónicos o sobre algún expediente, esto podría dañarlo.

INCENDIOS

En caso de que se presente un incendio, hay que acatar las indicaciones de los encargados del plan de contingencia y de Protección Civil.

Sobre el resguardo de la información:

1. La información deberá estar resguardada en las zonas clasificadas como seguras, donde el calor del incendio no alcance los dispositivos, esto generalmente es cerca de un extintor. La información se sugiere que se resguarde en un Disco duro externo, Memoria USB y CD.
2. Tener identificados los documentos con mayor relevancia, para que estos sean resguardados en una zona segura, ya sea en cajas de seguridad o realizar digitalización de esto y guardarlos como se sugiere en el anterior paso.

TERREMOTOS.

En este caso, cuando ocurre un terremoto lo que principalmente se daña son las estructuras (edificios) y con ellos los archivos que se encontraban en físico pueden quedar destruidos e imposibilitando la extracción de datos, es por ello que, si los tenemos almacenados en Memorias USB, discos Externos o CD, en cuanto se tenga acceso a la oficina, estos se pueden rescatar y obtener la información que allí habíamos respaldado. Es importante tener en cuenta que las medidas de prevención para un Sismo, son las que acatamos durante los simulacros.

INUNDACIONES POR LLUVIAS.

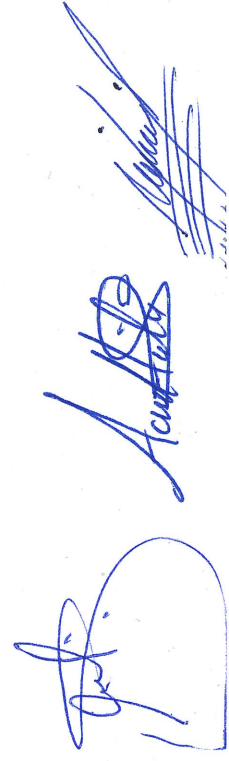
En la temporada de lluvias es importante estar al pendiente de la información meteorológica que comparten los medios de comunicación, esto con la finalidad de estar prevenidos ante dicha eventualidad. En dado caso si llegara a ocurrir cuando estamos en nuestra área de trabajo, deberemos acatar las medidas que nos ha compartido Protección Civil y salvaguardar nuestra integridad.

Después de la inundación y cuando las autoridades competentes permitan el ingreso a las oficinas, deberemos resguardar nuestros medios de almacenamiento (Memorias USB, CD y Discos Duros), estos no hay que conectarlos directamente a un ordenador, hay que solicitar al encargado de sistemas que evalúe el dispositivo y esperar a su recomendación. Ya que, si se conecta sin haber realizado lo anterior, podremos genera un corto y perder la información almacenada, así como también, descomponer el ordenador del que estemos trabajando. En el caso de la documentación en físico (diferentes tipos de papel) que se encuentre mojada, está la podemos intentar rescatar por el método de congelación, el cual se encuentra disponible en varias páginas de internet para su consulta, si así se llegara a requerir.

AMENAZAS INFORMÁTICAS.

Las distintas áreas que cuentan con un ordenador (computadora) deberán de contar con al menos una persona (encargada del equipo) que cuente con los conocimientos básicos de los componentes de este y así como su operatividad. Esto con la finalidad de que el daño al equipo no sea por negligencia o ignorancia en como operarlo.

Los equipos de cómputo deberán contar con sus mantenimientos preventivos al menos 1 vez al año, esto incluye limpieza de hardware y software, también deberán contar con una conexión eléctrica estable mediante un regulador de corriente, para así evitar un corto circuito y perdida de la información. Cuando el equipo con el que trabaja presente una anomalía de inmediato deberá llamar al técnico en sistemas y expresarle la situación para que este pueda tomar la mejor decisión respecto al equipo.



Hackeo Informático.

Si ha detectado que alguien más ha usado su computadora o que esta es controlada vía remota sin su autorización, proceda a apagarla. Pero si la violación es en un sistema que dependa de la conexión a internet para acceder, lo primero que debe de realizar es cambiar la contraseña, la cual no deberá tener datos que lo relacionen a usted con la contraseña, como pueden ser: fecha de cumpleaños, nombre del cónyuge, combinación sucesiva de números, entre otras. Las contraseñas deben de ser algo fácil de recordar para usted, pero, deberá de combinarlas con caracteres especiales y de al menos 8 dígitos, para con esto, elevar el grado de seguridad de la misma y así evitar otro hackeo.

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

Destruir y borrar la información es un proceso importantísimo para proteger la privacidad, confidencialidad, integridad y disponibilidad de la información y en particular de los Datos Personales. Esto se deberá llevar a cabo con procedimientos que garanticen que fueron en su totalidad eliminados y que estos no podrán recuperarse bajo ningún método. Así, los métodos para eliminar la información son los siguiente:

- a) En caso de que el almacenamiento sea en un medio digital, se apoyaran del técnico en sistemas para que los oriente en el correcto procedimiento de eliminación de información y que no quede rastro de ella o que de alguna forma se pueda recuperar. Si en dado caso se requiere destruir el medio de almacenamiento, bastara con separar los componentes y desecharlos por separados para que estos no se puedan reconstruir y obtener la información almacenada, aunque esto es muy poco probable.
- b) Con respecto a la información en físico (por lo general es algún tipo de papel), esta información se puede destruir cortando en modo cruzado o en partículas. Para realizar esto, podremos apoyarnos de aparatos electrónicos (triturados de papel) para garantizar la correcta destrucción de la información. Si es de un solo corte (horizontal) se da vuelta a las tiras de papel que salen para que queden pequeños pedazos de pale y esto haga imposible su reconstrucción.

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

Con respecto al Análisis de Brecha, es importante generar acciones que permitan la seguridad de la información, así como de su localización, para resolver de manera eficaz el acceso, rectificación, corrección u oposición de las personas titulares de la

información. Por lo que a continuación se presenta una serie de acciones a realizar para cumplir con el cometido:

- a) Realizar mesas de trabajo en las cuales nos reunamos las personas que manejamos datos personales en el Ayuntamiento y analizar la presente Ley para así, crear una cultura y conciencia sobre la Protección de datos personales.
- b) Elaborar pequeñas pruebas de trabajo para poder mediante un ejercicio sencillo, identificar el tipo de Dato personal que se está recabando y su sensibilidad.
- c) Fomentar la creación de un sistema de gestión y administración de datos personales para que cuando se recaben los Datos personales, el encargado sepa cómo manejarlos y la confidencialidad en la que se comprometerá.
- d) Elaborar un consentimiento informado sobre el uso que se le dará a los datos recabados por cada área y según el objetivo con el que los esté proporcionando el propietario.
- e) Fortalecer los mecanismos de control de documentos e información en las distintas áreas del ayuntamiento, para así minimizar el riesgo de posibles vulneraciones.



VI. Monitoreo de las Medidas de Seguridad.

Es de vital importancia la supervisión de las medidas de seguridad técnicas, administrativas y físicas, ya que este seguimiento nos permitirá avanzar en la construcción de una mejor cultura en la Protección de Datos Personales y a su vez nos permitirá proponer nuevas estrategias/medidas que nos permitan minimizar la probabilidad de vulneración de datos personales. Es por ello que se realizaran las siguientes acciones con la finalidad de llevar un seguimiento a dichas medidas:

- Vigilar que, al término de las labores dentro del ayuntamiento, las oficinas se queden cerradas con llave, para evitar cualquier extravío de información u objeto de valor.
- Verificar que los compañeros recuerden sus contraseñas y estas las actualicen conforme a su necesidad, a su vez, verificar que las mismas cuenten al menos con los criterios de seguridad anteriormente mencionados en este documento.
- Verificar que las áreas cuenten con su respaldo digital de la información que manejen y en dado caso de que no cuenten con él, incentivarlos a que lo realicen.

- Corroborar que los encargados de la protección de Datos Personales de cada área estén accediendo a las capacitaciones impartidas por el IMAIP e INAI en materia de Protección de Datos.

VII. Programa General de Capacitación en Materia de Protección de Datos Personales.

La capacitación continua en Materia de Protección de Datos Personales es de vital importancia para los servidores públicos del H. Ayuntamiento de Tuzantla, ya que es la única forma en la que se logrará crear consciencia de la importancia que tiene este tema y lo fundamental que es para construir una sociedad equitativa y de respeto hacia los derechos del prójimo.

Es así que mediante el siguiente programa se pretende sensibilizar sobre la importancia de la Protección de datos Personales.

- a) ¿Qué es un dato persona y cómo lo clasifico?
- b) Lectura y Análisis de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.
- c) ¡Como garantizar el Derecho de la Protección de Datos Personales? y medidas de apremio en la vulneración de datos Personales.

REFERENCIAS BIBLIOGRÁFICAS:

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

<https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>

Documento de Seguridad del IMAIP.

file:///E:/TRANSPARENCIA/Denuncias/IMAIP_VERIFICACI%C3%93N_DP_002_2024/DOCUMENTO%20DE%20SEGURIDAD/DOCUMENTO-DE-SEGURIDAD-DEL-IMAIP.pdf

Documento de Seguridad del H. Ayuntamiento de Sahuayo.

file:///E:/TRANSPARENCIA/Denuncias/IMAIP_VERIFICACI%C3%93N_DP_002_2024/DOCUMENTO%20DE%20SEGURIDAD/6a-7723cl-1.pdf

FIRMAN EL PRESENTE DOCUMENTO DE SEGURIDAD, LOS INTEGRANTES DEL COMITÉ DE TRANSPARENCIA DEL H. AYUNTAMIENTO DE TUZANTLA.

LIC. VÍCTOR MANUEL OCAMPO CÓRDOBA
SECRETARIO DEL H. AYUNTAMIENTO



PRESIDENTE DEL COMITÉ DE TRANSPARENCIA

C. ADRIANA TAVIRA SANTANA
ENCARGADA DE INGRESOS



SECRETARIA TÉCNICA DEL COMITÉ DE TRANSPARENCIA

C. ÁLVARO HIDALGO LÓPEZ.
SECRETARIO PARTICULAR.



PRIMER VOCAL DEL COMITÉ DE TRANSPARENCIA

LAS PRESENTES FIRMAS FORMAN PARTE DEL DOCUMENTO DE SEGURIDAD DEL H. AYUNTAMIENTO DE TUZANTLA, APROBADO EN LA TERCER ACTA EXTRAORDINARIA (ACTA NÚMERO 3) DEL COMITÉ DE TRANSPARENCIA, CELEBRADA EL 9 (NUEVE) DE ENERO DEL 2024 Y CONSTA DE 26 PAGINAS INCLUIDA LA PRESENTE.