

¿Elaboración de Documento de Seguridad?:

Contenido

¿Qué es Documento de Seguridad?.....	3
¿Cuáles son las finalidades del Documento de Seguridad?	6
¿Qué hacer para implementar de forma adecuada un Documento de Seguridad al interior de nuestro Sujeto obligado?.....	6
¿Cuáles son los pasos para la elaboración de un Documento de Seguridad?	7
¿Cuáles son los elementos indispensables del Documento de Seguridad?	8
¿Qué es un Inventario de Datos Personales y de sistemas de tratamiento?.....	7
FORMATO GUIA, Inventario De Datos Personales ?	11
¿Cómo establezco las funciones y obligaciones de las personas que traten datos personales?	16
¿Cómo se elabora la Bitácora de Responsables, Encargados y Usuarios de los Sistemas de Datos Personales?	16
Apartados destinados al establecimiento de roles y responsabilidades del personal en materia de protección de datos personales.....	17
I. Transmisiones de datos personales	17
II. Resguardo de sistemas de datos personales con soportes físicos *	19
III. Bitácora para accesos y operaciones cotidianas.....	20
IV. Registro de incidentes.....	21
V. Acceso a las instalaciones.....	21
VI. Actualización del sistema de datos personales	22
VII. Perfiles de usuario y contraseñas	23
VIII. Procedimientos de respaldo y recuperación de datos	24
¿Qué es y cómo se elabora un análisis de riesgo?.....	25
¿Qué es y cómo se elabora un análisis de brecha?.....	26
¿Cuáles son las partes finales del documento?.....	28
¿Funciones Y Obligaciones De Las Personas Que Traten Datos Personales?.....	30



¿Qué es Documento de Seguridad?

Es un instrumento interno que describe las medidas técnicas, físicas y administrativas adoptadas por una institución, empresa o sujeto obligado para garantizar la confidencialidad, integridad y disponibilidad de la información personal que posee y así poder cumplir el H. Ayuntamiento de Mazatán con lo dispuesto en el artículo 77 y 78 de la Ley.

que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones con relación a este programa:

- Aprobar, supervisar y evaluar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley y demás disposiciones que resulten aplicables en la materia.
- Coordinar, realizar y supervisar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la Ley y en las demás disposiciones que resulten aplicables en la materia en coordinación con el Oficial de Protección de Datos Personales, en caso de que se cuente con dicha figura que es opcional.
- Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes de datos personales o para el ejercicio de los derechos ARCOP.
- Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales o la improcedencia, por cualquier causa del ejercicio de alguno de los derechos ARCOP.
- Supervisar, en coordinación con las áreas u órganos administrativos competentes, el cumplimiento de las medidas, controles y acciones previstas en el Documento de Seguridad.
- Coordinar el seguimiento y cumplimiento de las resoluciones emitidas por la Autoridad Garante.
- 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.
- Asesorar a las unidades administrativas en la implementación de este Programa:

1. Sindicatura
2. Secretaría Municipal
3. Tesorería Municipal
4. Dirección de Obras Públicas
5. Oficialía Mayor
6. Seguridad Pública
7. COMSEP
8. Fomento Agropecuario
9. Empoderamiento de la Mujer
10. Dirección de Catastro Municipal
11. Dirección de Transparencia
12. Dirección de SAPAM

13. Salud Municipal
14. Protección Civil
15. Dirección de Vialidad
16. Dirección de Comunicación social
17. Dirección de Turismo
18. Servicios Públicos
19. Contraloría Municipal
20. Recursos Humanos
21. Prevención del Delito
22. Jurídico Municipal
23. Juez Municipal
24. Coordinador de COPLADEM
25. Delegado del Agua
26. Dirección de Alcoholes
27. Seguridad Alimentaria
28. Casa Día
29. Panadería y belleza
30. UBR
31. Unidad Deportiva
32. DIF

La intervención de Presidente Municipal Constitucional tendrá la finalidad única de impulsar la debida implementación del Programa al interior del sujeto obligado, pero no podrá suplir ni afectar las funciones que otorgan los artículos 77 y 78 de la LGPDPPSO al Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la organización.

Asimismo, para que la implementación del Programa tenga como resultado el cumplimiento integral de las obligaciones que establece la LGPDPPSO y los Lineamientos Generales, el Programa será de observancia obligatoria para todos los servidores públicos del sujeto obligado que en el ejercicio de sus funciones traten datos personales. Las unidades administrativas deberán realizar las acciones necesarias para cumplir con las obligaciones que establece este Programa, para lo cual deberán asignar los recursos materiales y humanos necesarios, y prever lo que se requiera en sus programas de trabajo.

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

El personal del H. Ayuntamiento de Mazatán que tenga acceso a los datos personales está obligado a conocer y aplicar el presente Programa y es aplicable en todas y cada una de las fases del tratamiento de los datos personales, iniciando desde la obtención de estos y finalizando con su eliminación.

Las unidades administrativas que forman parte de la Unidad de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas y que deberán observar el Programa de Protección de Datos Personales son las siguientes:



- Sindicatura
- Secretaría Municipal
- Tesorería Municipal
- Dirección de Obras Públicas
- Oficialía Mayor
- Seguridad Pública
- COMSEP
- Fomento Agropecuario
- Empoderamiento de la Mujer
- Dirección de Catastro Municipal
- Dirección de Transparencia
- Dirección de SAPAM
- Protección Civil
- Dirección de Vialidad
- Dirección de Comunicación social
- Contraloría Municipal
- Recursos Humanos
- Jurídico Municipal
- UBR
- DIF

El tratamiento de datos personales que realicen las unidades administrativas deberá cumplir con los principios, deberes y obligaciones que prevé la LGPDPPSO, para lo cual este programa establecerá el marco de trabajo mínimo que se deberá seguir para alcanzar dicho objetivo.

Para ello, se identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las unidades administrativas, de acuerdo con lo que establece la LGPDPPSO y los Lineamientos Generales, y según el ciclo de vida de los datos personales.

¿Cuáles son las finalidades del Documento de Seguridad?

Identificar el universo de sistemas de datos personales que posee cada dependencia o entidad

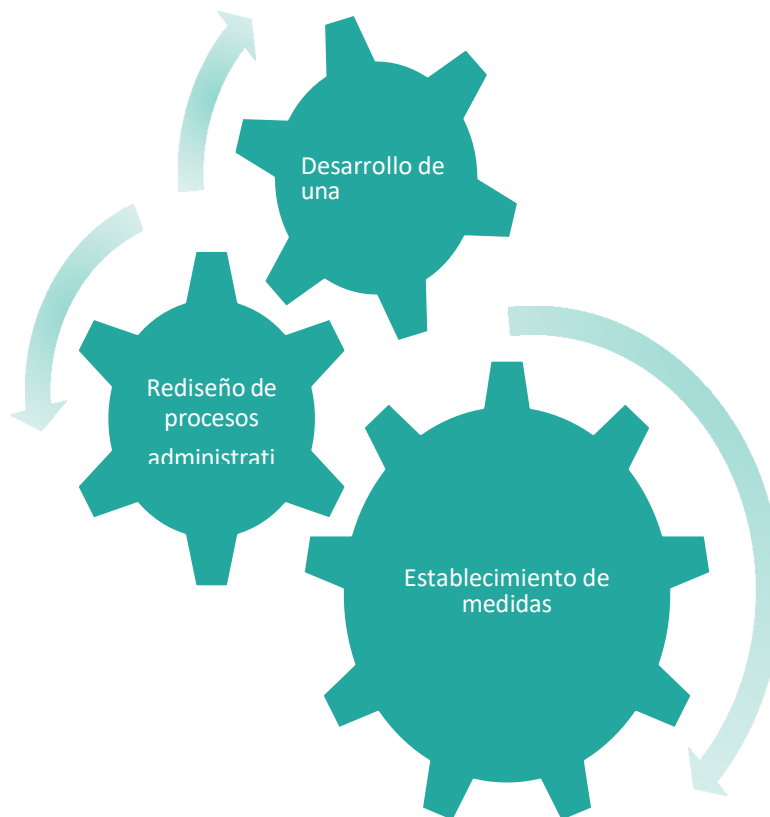
Clasificar el tipo de datos personales que contiene cada uno

Designar a los responsables, encargados, usuarios de cada sistema

Establecer las medidas de seguridad concretas implementadas



¿Qué hacer para implementar de forma adecuada un Documento de Seguridad al interior de nuestro Sujeto obligado?





¿Cuáles son los pasos para la elaboración de un Documento de Seguridad?

- Tratamiento a un sistema de datos personales
- Los sistemas de datos se agrupan a un sistema institucional
- Establecimiento de una política Institucional de Protección de datos personales
- Identificar el universo de sistema de datos personales que poseen.
- Identificar entre datos personales y datos personales sensibles.
- Designar responsables y encargados de cada sistema
- Establecer las medidas de seguridad necesarias para proteger los sistemas

¿Cuáles son los elementos indispensables del Documento de Seguridad?

- El inventario de datos personales y de los sistemas de tratamiento
- Las Funciones y obligaciones de las personas que traten datos personales
- Los análisis de riesgo y brecha
- El plan de trabajo
- Los mecanismos de monitoreo y revisión de las medidas de seguridad
- El programa General de Capacitación

En relación con lo anterior, fue posible identificar 73 procesos que se desarrollan, que implican el tratamiento de datos personales. Mismas que a continuación se describen:

AREA	DEPARTAMENTO	PROCESO	No. PROCESO
SINDICATURA		RESOLUCION A SOLICITUDES QUE SE PRESENTEN	1
SECRETARIA MUNICIPAL	RECLUTAMIENTO	CARTILLA DE IDENTIDAD MILITAR	1
	COORDINACION DE ALCOHOLES	VERIFICACION Y CLAUSURA DE LOS ESTABLECIMIENTOS	1
	JUECES	CONTESTACION DE AMPAROS	1
		CERTIFICACIONES Y CONSTANCIAS	1
TESORERIA MUNICIPAL		ATAUDES	1
		CUESTIONARIO DE INGRESOS	1
		NOMINA Y VIATICOS	1
OBRAS PUBLICAS		ESTIMACIONES, ING CRISTIAN ALFREDO VILLARREAL ALTAMIRANO	1
		EXPEDIENTE TECNICO ARQ. FERNANDO DE LA CRUZ URBINA	1
		LEVANTAMIENTO TOPOGRAFICO ING. CARLOS BRANDON ITURBE ZEPEDA	1
		SUBDIVISIONES, LINEAMINETOS, PERMISOS DE COSNTRUCCION	1

		VERIFICACION DE OBRAS, ING. ADAN VAZQUEZ CALDERON	1
		CONTRATOS: ING. JOSE CARLOS MADRID MENDEZ	
OFICIALIA MAYOR		ADQUISICIONES	1
		FORMATOS DE DONACION	1
		ELABORACION DE CONTRATOS	1
		CONTRATO DE PERSONAL MORALES	1
SEGURIDAD PUBLICA		Registro de bitácora para ingresos a las instalaciones de seguridad publica	1
CONSEJO DE SEGURIDAD PUBLICA	PREVENCION DEL DELITO	Examen de control y confianza	1
		Lista de asistencia a las reuniones del consejo	1
FOMENTO AGROPECUARIO		Registro de proyectos productivos	1
		Proyectos productivos de peces	1
Empoderamiento de la mujer		Asesorías	1
		Talleres	1
		Platicas	1
Catastro Municipal		Pago de predial	1
Dirección de Transparencia		Solicitudes de la Plataforma nacional de Transparencia	1
SAPAM		Cambio de nombre del titular de servicio	1
		Contrato	1
		Reconexión y baja	1
		Atención a usuarios	1
		Convenio de pagos	1
Proteccion Civil		Conformacion de comités	1
		Atencion a llamadas de emergencia	1
		Actualizacion de refugios temporales	1
		Elaboracion técnica de seguridad y riesgo	1
			1
Direccion de Comunicación social		Elaboración de videos	1
		Fotografías	1
		Notas informativas	1
Contraloria Municipal		Declaraciones patrimoniales	1
		Atención a quejas y denuncias	1
RECURSOS HUMANOS		REGISTRO Y EVALUACION DE PERSONAL	1
		TRAMITE DE ALTA	1
JURIDICO MUNICIPAL		Acta de comparecencia	1
		Convenios	1

DIF		Contratos	1
		Actas administrativas	1
		CAIC	1
		TRABAJO SOCIAL	1
		CASA DIA	1
		DESAYUNOS ESCOLARES	1
		TRABAJO SOCIAL	1
		CENTRO DE REHABILITACION	1
		PSICOLOGIA	1
		PROCURADURIA	1
		SERVICIOS ESCOLARES	1

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

DE IDENTIFICACIÓN

Nombre, domicilio, CURP, fotografía, huella digital, edad, clave de elector, estado civil, RFC, correo electrónico personal, teléfono, sexo, información académica, fecha y lugar de nacimiento, cédula profesional, nacionalidad, beneficiarios, curriculum vitae, datos de identificación, nacionalidad, ocupación, sexo, títulos, profesionales.

PATRIMONIALES

Facturas, declaraciones patrimoniales.

SENSIBLES

Datos de salud.

Datos personales recabados.	Existente.	Necesario.	No necesario.
Datos de identificación y contacto.			
Nombre:		X	
Estado Civil:		X	
Registro Federal de Contribuyentes (RFC):		X	
Clave Única de Registro de Población (CURP):		X	
Lugar de nacimiento:		X	
Fecha de nacimiento:		X	
Nacionalidad:		X	
Domicilio:		X	



Teléfono particular:		X	
Teléfono celular:		X	
Correo electrónico:		X	
Firma autógrafa:		X	
Firma electrónica:			X
Edad:		X	

Inventario de datos personales: se refiere a qué **datos personales** se tienen, cuál tipo son (sensibles o no), cuántos sistemas de **datos** se tienen y en qué soportes se tiene la información, si es un documento físico o se encuentra en formato electrónico.

FORMATO GUÍA: INVENTARIO DE DATOS PERSONALES.

Marcar con una **X** los datos personales que existen y son necesarios o que existen más no son necesarios en los procesos administrativos de su Unidad Administrativa.

Fotografía:		X	
Referencias personales:		X	
Datos sobre características físicas.			
Color de piel:		X	
Color de cabello:		X	
Señas particulares:		X	
Estatura:		X	
Peso:		X	
Cicatrices:		X	
Tipo de sangre:		X	
Datos biométricos.			
Imagen del iris:			X
Huella dactilar:			X
Palma de la mano:			X
Datos laborales.			
Puesto o cargo que desempeña:		X	
Domicilio de trabajo:		X	
Correo electrónico institucional:		X	
Teléfono institucional:		X	
Referencias laborales:		X	
Información generada durante los procedimientos de reclutamiento, selección y contratación:		X	
Experiencia/Capacitación laboral:		X	
Datos académicos.			
Trayectoria educativa:		X	

Títulos:		X	
Cédula profesional:		X	
Certificados:		X	
Reconocimientos:		X	
Datos migratorios.			
Entrada al país:			X
Salida del país:			X
Tiempo de permanencia en el país:			X
Calidad migratoria:			X
Derechos de residencia:			X
Aseguramiento:			X
Repatriación.			X
Datos patrimoniales y/o financieros.			
Bienes muebles:		X	
Bienes inmuebles:		X	
Información fiscal:		X	
Historial crediticio/Buró de crédito:			X
Ingresos:			X
Egresos:			X
Cuentas bancarias:			X
Números de tarjetas de crédito:			X
Información adicional de tarjeta (fecha de vencimiento, códigos de seguridad, datos de banda magnética, pin):			X
Seguros:		X	
Afores:		X	



Datos sobre pasatiempos, entretenimiento y diversión.			
Pasatiempos:			X
Aficiones:			X
Deportes que practica:			X
Juegos de su interés:			X
Datos legales.			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros):			X
Otros datos personales (mencionar).			
Datos personales recabados:	Existente.	Necesario.	No necesario.

Datos personales recabados.	Existente.	Necesario.	No necesario.
Datos personales sensibles.			
Datos sobre la ideología.			
Posturas religiosas/ ideológicas/morales/ filosóficas:			X
Pertenencia a un partido/Posturas políticas:			X
Pertenencia a un sindicato:			X
Datos de salud.			
Estado de salud físico presente, pasado o futuro:		X	



Estado de salud mental presente, pasado o futuro:			X
Información genética:			X
Datos sobre vida sexual.			
Preferencias sexuales:			X
Prácticas o hábitos sexuales:			X
Datos de origen étnico o racial.			
Pertenencia a un pueblo, etnia o región:			X
Otros datos personales (mencionar).			



Descripción de los tipos de soporte de los Sistemas de Datos Personales

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	REGISTRO DE BASE DE DATOS PERSONAL MAZATAN
Tipo de Soporte: Físico o electrónico:	FISICO
Descripción del soporte:	DISCO DURO
Características del lugar donde se resguardan los soportes: [Describir el lugar en el que físicamente se encuentran los soportes del sistema]:	AREA DE ARCHIVO MUNICIPAL



¿Cómo establezco las funciones y obligaciones de las personas que traten datos personales?

Obligaciones comunes de todos los responsables de proteger datos personales.

- Conocer la privacidad de todos los **datos** que manejan y, por lo tanto, su obligación de mantener el secreto de dicha información.
- Hacer uso de los datos únicamente para los fines para los cuales han sido recabados.

Los roles y funciones del personal con respecto al tratamiento y protección de los datos personales deben estar descritos en una bitácora donde se establezcan los responsables, encargados y usuarios de los datos personales.

¿Cómo se elabora la Bitácora de Responsables, Encargados y Usuarios de los Sistemas de Datos Personales?

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	REGISTRO DE BASE DE DATOS PERSONAL MAZATAN
Responsable:	TRANSPARENCIA
Nombre:	MANOLO PEREZ MAGAÑA
Cargo:	DIRECTOR DE TRANSPARENCIA
Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema].	RECABAR ASI COMO CAPTURAR LA INFORMACION
Encargados:	
Nombre:	



Cargo:	
Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema].	
Usuarios:	
Nombre:	
Cargo:	
Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema].	

Apartados destinados al establecimiento de roles y responsabilidades del personal en materia de protección de datos personales

I. Transmisiones de datos personales PARA SOPORTES FÍSICOS.

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	REGISTRO DE BASE DE DATOS PERSONAL MAZATAN
I. Trasmisiones de Datos Personales.	Digitalización
1.1. Trasmisiones de Datos Personales en soportes físicos.	Digitalización Y Respaldo De Disco Duro
Descripción del soporte:	
Características del paquete:	Digitalización Y Respaldo De Disco Duro



Mecanismos para la entrega:	Físico así como digitalización y soporte en disco duro.
Mecanismos para la notificación de vulneraciones:	Deberá indicar si el remitente pide al destinatario que le informe en caso de que reciba el sobre o paquete con señas de apertura.
Acuse de recibido:	Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales.
Comunicación con el sistema de protección de datos del remitente:	Deberá señalar si el remitente registra la o las transmisiones en su bitácora, así como en el Sistema Persona.

PARA TRASLADO FÍSICO DE SOPORTES ELECTRÓNICOS

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	REGISTRO DE BASE DE DATOS PERSONAL MAZATÁN
I. Transmisiones de Datos Personales.	
1.2. Transmisiones de Datos Personales en soportes electrónicos, trasladados de forma física.	
Descripción del soporte:	Deberá señalar si el envío se realiza a través de mensajero oficial, mensajero privado o correspondencia ordinaria.
Características del paquete:	Deberá precisar si utiliza un sobre o paquete sellado de manera que sea perceptible si fue abierto antes de su entrega.
Mecanismos para la entrega:	Deberá manifestar si el sobre o paquete enviado es entregado en mano al destinatario, previa acreditación con identificación oficial.
Mecanismos para la notificación de vulneraciones:	Deberá indicar si el remitente pide al destinatario que le informe en caso de que reciba el sobre o paquete con señas de apertura.
Acuse de recibido:	Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales.
Comunicación con el sistema de protección de datos del remitente:	Deberá señalar si el remitente registra la o las transmisiones en su bitácora, así como en el Sistema Persona.
Tipo de cifrado:	Deberá precisar si los archivos electrónicos que contienen datos personales son cifrados antes de su envío y proporcionar detalles técnicos del cifrado tales como el



	tipo de algoritmo utilizado y la longitud de la llave (o clave).
--	--

PARA SOPORTES ELECTRÓNICOS

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	REGISTRO DE BASE DE DATOS PERSONAL MAZATÁN
I. Trasmisiones de Datos Personales.	
1.3. Trasmisiones de Datos Personales en soportes electrónicos.	
Procedimiento de Trasmisión:	
Tipo de cifrado:	Deberá precisar si los archivos electrónicos que contienen datos personales son cifrados antes de su envío y proporcionar detalles técnicos del cifrado tales como el tipo de algoritmo utilizado y la longitud de la llave (o clave).
Canal de Trasmisión:	Deberá precisar si utiliza un canal de comunicación dedicado o una red privada virtual especificando detalles técnicos relativos al cifrado de dicho canal como la longitud de llave (o clave); en su caso, deberá precisar si para dicho canal utiliza una red pública (como Internet) especificando el protocolo de transmisiones protegidas utilizado.
Mecanismos para detectar intrusiones:	Deberá manifestar si el remitente y/o el destinatario cuentan con dispositivos que faciliten la detección de intrusiones en el canal de comunicaciones.
Acuse de Recibido:	Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales.
Comunicación con el sistema de protección de datos del remitente:	Deberá señalar si el remitente registra la o las transmisiones en su bitácora, así como en el Sistema Persona



II. Resguardo de sistemas de datos personales con soportes físicos *

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	REGISTRO DE BASE DE DATOS PERSONAL MAZATAN
II. Tipo de Soporte del sistema:	Físico.
Medidas de seguridad implementadas:	Señalar las medidas de seguridad que ha implementado el sujeto obligado para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
Personal autorizado para el acceso al sistema:	Señalar en un listado las personas que tienen acceso a los soportes físicos del sistema.

III. Bitácoras para accesos y operación cotidiana

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	REGISTRO DE BASE DE DATOS PERSONAL MAZATAN
III. Bitácoras para accesos y operación cotidiana.	
Los datos que se registran en las bitácoras:	
Datos de acceso:	Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida.
Soporte físico:	Número o clave del expediente utilizado.
Soporte Electrónico:	Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.



IV. Registro de incidentes

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	REGISTRO DE BASE DE DATOS PERSONAL MAZATAN
IV. Registro de Incidentes.	
Persona que resolvió el incidente:	
Metodología aplicada:	Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida.
Soporte físico:	Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados.
Soporte Electrónico:	Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados.
Autorización a la recuperación de datos:	Nombre del responsable quien autoriza la recuperación de los datos.

V. Acceso a las instalaciones

PARA DESCRIBIR LA SEGURIDAD PERIMETRAL

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	REGISTRO DE BASE DE DATOS PERSONAL MAZATAN
V. Acceso a las instalaciones.	



Descripción de las medidas generales de seguridad perimetral:	
Proceso de identificación para el ingreso:	
Proceso de autenticación para el ingreso:	
Proceso de autorización para el ingreso:	

PARA DESCRIBIR LA SEGURIDAD AL INTERIOR

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	REGISTRO DE BASE DE DATOS PERSONAL MAZATAN
V. Acceso a las instalaciones.	
Descripción de las medidas generales de seguridad al interior:	
Proceso de identificación para el ingreso:	
Proceso de autenticación para el ingreso:	
Proceso de autorización para el ingreso:	

Actualización del sistema de datos personales

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	REGISTRO DE BASE DE DATOS PERSONAL MAZATAN
VI. Mecanismo de actualización del sistema.	
Descripción del mecanismo:	Establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenido en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

VI. Perfiles de usuario y contraseñas

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	REGISTRO DE BASE DE DATOS PERSONAL MAZATAN
VII. Perfiles de usuario y contraseñas.	ADMINISTRADOR
Modelo de control de acceso:	¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? ¿Es discrecional (matriz de control de acceso)? ¿Está basado en roles (perfiles) o grupos? ¿Está basado en reglas?
Perfiles de usuario y contraseñas en el sistema operativo de red:	¿Cuenta con un sistema operativo de red instalado en sus equipos? ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuándo los almacena?
Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales:	¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Administración de perfiles de usuario y contraseñas:	¿Quién da de alta nuevos perfiles? ¿Quién autoriza la creación de nuevos perfiles? ¿Se lleva registro de la creación de nuevos perfiles?
Acceso remoto al sistema de datos personales:	¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? ¿Cómo se evita el acceso remoto no autorizado?



VII. Procedimientos de respaldo y recuperación de datos

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	REGISTRO DE BASE DE DATOS PERSONAL MAZATAN
VIII. Procedimiento de respaldo y recuperación de los datos.	DISCO DURO
Tipo de respaldo:	Señalar si realiza respaldos completos, diferenciales o incrementales.
Tipo de medios:	El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad.
Especificaciones sobre el almacenamiento:	Cómo y dónde archiva esos medios.
Nombre del responsable de las operaciones de respaldo:	

Una vez que hemos establecido esto, debemos analizar el estado actual y futuro de nuestros sistemas de datos personales. Esto significa realizar un análisis de riesgo y un análisis de brecha.

¿Qué es y cómo se elabora un análisis de riesgo?

Análisis previo que se debe de dar a todo nuevo tratamiento de **datos personales** con la principal finalidad de establecer los controles y medidas de seguridad adecuadas que garanticen las libertades y los derechos de las personas afectadas.

MATRIZ DE ANÁLISIS DE RIESGOS.

A. [Denominación de la Unidad administrativa A].

IDENTIFICACIÓN		ANÁLISIS		EVALUACIÓN		TRATAMIENTO O CONTROL OPERACIONAL
A1. [Nombre del sistema A1]	RIESGO	PROBABILIDAD	GRAVEDAD	CALIFICACIÓN	NIVEL DEL RIESGO	
REGISTRO DE BASE DE DATOS PERSONAL MAZATAN.	NINGUNO DADO QUE SE RESPALDA RA EN EL PORTAL WEB	1 POCO PROBABLE	1 NADA GRAVE.	1	BAJO.	1 SE TENDRA LOS CUIDADOS TANTO DE PERSONAS QUE MANEJARAN LOS DATOS COMO LOS RESPALDOS.

Nivel de riesgo

<i>Valor de Gravedad (1-4)</i>	4	8	12	16	ALTO (12-16)
	3	6	9	12	MEDIO (8-9)
	2	4	6	8	BAJO (1-6)
	1	2	3	4	
<i>Valor de Probabilidad (1-4)</i>					

¿Qué es y cómo se elabora un análisis de brecha?

Análisis de las medidas de seguridad existentes y aquellas faltantes, que resultan necesarias para la protección de los datos personales.

Análisis de Brecha.			
A. [Denominación de la Unidad administrativa A].			
A1. [Nombre del sistema A1].			
(Medidas de seguridad existentes VS medidas de seguridad faltantes).			
Pregunta o Control.	¿Existente?		
	SI	NO	Observaciones.
Medidas de seguridad basadas en la cultura del personal.			
¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?	X		
Política de escritorio limpio.	X		
Hábitos de cierre y resguardo.	X		
Impresoras, escáneres, copiadoras y buzones limpios.	X		
¿Tienes mecanismos para eliminar de manera segura la información?	X		
Destrucción segura de documentos.	X		
Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico.	X		
Fijar periodos de retención y destrucción de información.	X		
Tomar precauciones con los procedimientos de reutilización.	X		
Informar al personal sobre sus deberes mínimos de seguridad y protección de datos.	X		
Fomentar la cultura de la seguridad de la información.	X		
Asegurar la protección de datos personales en subcontrataciones.	X		

¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?	X		
Tener un procedimiento de notificación.	X		
¿Realizas respaldos periódicos de los datos personales?	X		
Medidas de seguridad en el entorno de trabajo físico.			
¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?	X		
Mantener registros del personal con acceso al entorno de trabajo.	X		
¿Tienes medidas de seguridad para evitar el robo?	X		
Cerraduras y candados.	X		
Elementos disuasorios.	X		
¿Cuidas el movimiento de información en entornos de trabajo físicos?	X		
Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico.	X		
Mantener en movimiento sólo copias de la información, no el elemento original.	X		
Usar mensajería certificada.	X		
Medidas de seguridad en el entorno de trabajo digital.			
¿Realizas actualizaciones al equipo de cómputo?	X		
¿Revisas periódicamente el software instalado en el equipo de cómputo?	X		
¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?	X		
Uso de contraseñas y/o cifrado.	X		
Bloqueo y cierre de sesiones.	X		
Administrar usuarios y accesos.	X		
¿Revisas la configuración de seguridad del equipo de cómputo?	X		
¿Tienes medidas de seguridad para navegar en entornos digitales?	X		



Reglas de navegación segura.	X		
Uso de conexiones seguras.	X		
¿Cuidas el movimiento de información en entornos de trabajo digitales?	X		
Seguridad de la información enviada y recibida.	X		

Finalmente, se debe establecer un plan de trabajo que incluya: un programa de contingencias, un programa de capacitaciones y un programa de vigilancia y auditorías.

¿Cuáles son las partes finales del documento?



Programa de contingencia.

Programa de contingencia	
Programa de contingencia:	Se cuenta con el equipo de cómputo y sistema de digitalización optimo así como área de trabajo para realizar los trabajos de la mejor manera.
Mecanismos para probar su eficacia:	Modelos, simulacros, ataques controlados, simulaciones.
Sitios alternos de resguardo:	Es un área climatizada y cuenta con lo necesario para realizar los trabajos.
Procedimiento detallado ante vulneraciones y contingencias:	Se cuenta con cámaras de seguridad que permite el control de acceso a el área y equipos aparte de la seguridad municipal
Tiempo de reacción:	20 minutos

Programa de capacitación.

A. [Denom Programa de Capacitación Unidad administrativa A]	
Programa de capacitación:	
Periodicidad:	Trimestral
Unidades administrativas a las que va dirigido:	Transparencia Municipal
Temas para abordar y cronograma:	Se están estructurando
Responsable del programa:	Manolo Pérez Magaña
Medios de verificación del aprendizaje:	

Programa de auditorías y vigilancias.

A. [Denom Programa de Auditoria y vigilancia Unidad administrativa A]	
Programa de Auditoría y vigilancia:	
Periodicidad:	Trimestral.
Unidades administrativas a las que va dirigido:	Unidad de Transparencia
Responsable de la ejecución:	Manolo Pérez Magaña
Manejo de la información reportada:	Manolo Pérez Magaña

FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN 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 ITAIPCH, resulta importante definir estas actividades con las funciones y facultades establecidas en el reglamento Interior, que otorga a los servidores públicos responsables de dicho tratamiento; lo anterior, a fin de dar cumplimiento al principio de legalidad que debe atender todo servidor público. Por lo anterior, a continuación, se ilustran las funciones otorgadas por el reglamento interior del ITAIPCH a quienes llevan a cabo tratamiento de datos personales. Como lo demuestra la siguiente tabla:

AREA	NOMBRE Y CARGO DE LAS PERSONAS FUNCIONARIAS QUE TRATAN DATOS	FUNCIONES	ACCIONES
SINDICATURA		RESOLUCION A SOLICITUDES QUE SE PRESENTEN	RESOLUCION A SOLICITUDES QUE SE PRESENTEN
SECRETARIA MUNICIPAL	RECLUTAMIENTO	CARTILLA DE IDENTIDAD MILITAR	1
	COORDINACION DE ALCOHOLES	VERIFICACION Y CLAUSURA DE LOS ESTABLECIMIENTOS	1
	JUECES	CONTESTACION DE AMPAROS	1
		CERTIFICACIONES Y CONSTANCIAS	1
TESORERIA MUNICIPAL		ATAUDES	1
		CUESTIONARIO DE INGRESOS	1
		NOMINA Y VIATICOS	1
OBRAS PUBLICAS		ESTIMACIONES	1
		EXPEDIENTE TECNICO	1
		LEVANTAMIENTO TOPOGRAFICO	1
		MANTENIMIENTO Y ALCANTARILLADO	1
		VERIFICACION DE OBRAS	1
OFICIALIA MAYOR	MAURICIO LOPEZ VELAZQUEZ	ADQUISICIONES	1
		FORMATOS DE DONACION	1
		ELABORACION DE CONTRATOS	1
		CONTRATO DE PERSONAL MORALES	1
SEGURIDAD PUBLICA	JUAN GABRIEL ARVIZU JONGUITUD	Registro de bitácora para ingresos a las instalaciones de seguridad publica	1
CONSEJO DE SEGURIDAD PUBLICA	MANOLO PEREZ MAGAÑA	Examen de control y confianza	1
		Lista de asistencia a las reuniones del consejo	1
FOMENTO AGROPECUARIO		Registro de proyectos productivos	1
		Proyectos productivos de peces	1



Empoderamiento de la mujer		Asesorías	1
		Talleres	1
		Pláticas	1
Catastro Municipal	MIREYA SANDOVAL LOPEZ	Pago de predial	1
Dirección de Transparencia	MANOLO PEREZ MAGAÑA	Solicitudes de la Plataforma nacional de Transparencia	Solicitudes de la Plataforma nacional de Transparencia
SAPAM	LILIANA RODRIGUEZ	Cambio de nombre del titular de servicio	1
		Contrato	1
		Reconexión y baja	1
		Atención a usuarios	1
		Convenio de pagos	1
Proteccion Civil	VICTOR DE JESUS CORTEZ DE LA CRUZ	Conformacion de comités	1
		Atencion a llamadas de emergencia	1
		Actualizacion de refugios temporales	1
		Elaboracion técnica de seguridad y riesgo	1
			1
Direccion de Comunicación social		Elaboración de videos	1
		Fotografías	1
		Notas informativas	1
Contraloria Municipal		Declaraciones patrimoniales	1
		Atención a quejas y denuncias	1
RECURSOS HUMANOS		REGISTRO Y EVALUACION DE PERSONAL	1
		TRAMITE DE ALTA	1
JURIDICO MUNICIPAL		Acta de comparecencia	1
		Convenios	1
		Contratos	1
		Actas administrativas	1
DIF		CAIC	1
		TRABAJO SOCIAL	1
		CASA DIA	1
		DESAYUNOS ESCOLARES	1
		TRABAJO SOCIAL	1
		CENTRO DE REHABILITACION	1
		PSICOLOGIA	1
		PROCURADURIA	1
		SERVICIOS ESCOLARES	1