



LA INDEPENDENCIA
»»» LA INDEPENDENCIA AVANZA «««
2024 - 2027

DOCUMENTO DE SEGURIDAD

**H. AYUNTAMIENTO MUNICIPAL DE LA
INDEPENDENCIA, CHIAPAS**

SEPTIEMBRE 2026



Palacio Municipal. Colonia Centro. La Independencia, Chiapas.



Tel: (963) 10 100



H. Ayuntamiento Constitucional

La Independencia, Chiapas

INDICE

Introducción



1. Objetivos del Documento de Seguridad.....	5
2. Responsabilidades.....	6
3. Alcance del Documento de Seguridad.....	10
4. Sistema de Gestión de los Datos Personales.....	11
5. Inventario de Tratamiento y Datos Personales.....	16
6. Análisis de Riesgo.....	22
7. Análisis de Brecha	26
8. Controles de Identificación y Autenticación de Usuarios.....	29
9. Destrucción Errónea de Medios de Almacenamiento físico.....	32
10. Analisis de la Información.....	39





H. Ayuntamiento Constitucional

La Independencia, Chiapas

11. Plan de Trabajo para la Para la Implementación de Medidas de Seguridad.....	39
12. Programa General de Capacitación.....	45
13. Monitoreos de las Medidas de Seguridad.....	46
14. Propuesta de Capacitación.....	48
15. Actualización del Documento de Seguridad.....	50



INTRODUCCION

En cumplimiento para el documento de Seguridad para Sistemas de Datos Personales en medios físicos (Documento) el H. Ayuntamiento de Municipal de la Independencia, Chiapas se dicta en cumplimiento de las disposiciones jurídicas vigentes, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen, se elabora de conformidad a lo establecido en el artículo 55 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, el cual establece que el sujeto obligado es responsable de elaborar y aprobar un documento, el cual deberá de contener medidas de seguridad de carácter físico, técnico y administrativo. Este documento comprende los siguientes apartados y anexos: Para el municipio de la Independencia, Chiapas, así como para su Unidad de Transparencia, la información representa un activo fundamental que debe ser protegido mediante un conjunto de procesos y sistemas administrados, ejecutados y preservados por la propia unidad de transparencia, así como por las distintas áreas del ayuntamiento y los organismos públicos descentralizados que los generan. En todo momento se debe asegurar la confidencialidad de la información, buscando mejorar continuamente los procesos y sistemas relacionados con la reserva, integridad y disponibilidad de la información, mientras se mitigan los riesgos asociados con su tratamiento de. Este Documento de Seguridad para Sistemas de Datos Personales, en formatos físicos y electrónicos, se elabora en cumplimiento de las disposiciones jurídicas vigentes con el objetivo de garantizar la integridad, confidencialidad y disponibilidad de la información personal que contienen dichos sistemas. El documento pretende ser una herramienta que brinde homogeneidad en la organización, procesos y sistemas a la Unidad de Transparencia, donde el Comité de Transparencia, en colaboración con las áreas del sujeto obligado y sus organismos públicos descentralizados, establecen las medidas de seguridad física a implementarse para proteger los sistemas de datos personales custodiados. Asimismo, este documento tiene como propósito asegurar el control de los sistemas de datos personales en posesión de la unidad,



especificando el tipo de datos personales que almacenan, los responsables, encargados y usuarios de cada sistema, así como las medidas de seguridad concretas implementadas.

1. OBJETIVO DEL DOCUMENTO DE SEGURIDAD.

El propósito primordial de este Documento de Seguridad tiene como objetivo establecer un marco integral para la protección de los datos personales administrados por el H. Ayuntamiento Municipal de la Independencia, Chiapas y su Unidad de Transparencia. Este marco tiene como objetivo principal salvaguardar la integridad, confidencialidad y disponibilidad de la información personal almacenada en sistemas físicos y electrónicos. En virtud de las obligaciones legales y éticas del ayuntamiento y su unidad de transparencia, este documento busca proporcionar una guía detallada y coherente para la gestión de la seguridad de la información. Su finalidad es promover una cultura de seguridad sólida dentro de la organización, donde todos los datos personales en posesión del H. Ayuntamiento del municipio de la Independencia, Chiapas, como un medio para cumplir con las obligaciones que establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas (LPDPPSOCHIS) y los Lineamientos Generales, así como la normatividad que derive de los mismos; estableciendo los elementos y actividades de gestión para la operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, además de promover la adopción de mejores prácticas en relación con la protección de datos personales, con la finalidad de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, emite el presente documento, en el cual los empleados, responsables y usuarios comprendan la importancia de proteger la privacidad y los derechos de las personas cuyos datos son procesados. Entre los objetivos específicos que este documento persigue, se incluyen: Definir y documentar claramente las políticas, procedimientos y controles de seguridad necesarios para proteger los datos personales bajo la custodia del Ayuntamiento Municipal de la Independencia y su unidad



de transparencia. Establecer roles y responsabilidades claros para la implementación, mantenimiento y supervisión de las medidas de seguridad contempladas en este documento. Proporcionar orientación y capacitación adecuadas a todo el personal involucrado en el manejo de datos personales, con el fin de fomentar buenas prácticas de seguridad y conciencia sobre los riesgos asociados con el tratamiento de la información. Garantizar el cumplimiento continuo de las leyes y regulaciones aplicables en materia de protección de datos personales, en particular la (LPDPPSOCHIS), así como cualquier otro marco normativo relevante. Establecer mecanismos efectivos de monitoreo, evaluación y mejora continua de las medidas de seguridad implementadas, con el fin de adaptarse a los cambios en el entorno operativo y a las nuevas amenazas y vulnerabilidades que puedan surgir. este Documento de Seguridad tiene como objetivo fundamental asegurar que los datos personales manejados por el H. Ayuntamiento Municipal de la Independencia y su Unidad de Transparencia sean tratados de manera responsable y segura, en cumplimiento con los más altos estándares de protección de la privacidad y la seguridad de la información.

2. RESPONSABILIDADES

Las responsabilidades contenidas en este **documento de seguridad** del Ayuntamiento Municipal de la Independencia Chiapas se centran en garantizar la confidencialidad, integridad y disponibilidad de los datos personales en posesión de este sujeto obligado, cumpliendo con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

De conformidad con lo dispuesto por el artículo 113 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas (LPDPPSOCHIS), el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales, teniendo entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, en esa tesitura dicho órgano tiene las siguientes funciones con relación a este programa:



- **Inventario de datos y sistemas:** Establecer la relación exacta de los sistemas de tratamiento de información, ficheros y los tipos de datos personales (incluyendo los sensibles) que manejan las diferentes áreas del ayuntamiento de la Independencia, Chiapas.
- **Medidas de seguridad:** Describir y asignar las acciones de protección técnicas, físicas y administrativas que eviten daños, pérdidas, alteración, destrucción o uso no autorizado de la información.
- **Funciones y obligaciones del personal:** Delimitar claramente qué perfiles, áreas y servidores públicos tienen autorización para acceder, procesar o administrar los datos ciudadanos y registros internos dentro del Ayuntamiento Municipal.
- **Análisis de riesgos y brechas:** Evaluar de manera continua los posibles peligros y vulnerabilidades a los que se exponen los registros municipales para aplicar mejoras correctivas.
- **Capacitación y revisión:** Establecer programas obligatorios de formación para los trabajadores del ayuntamiento y calendarizar revisiones periódicas de los protocolos de seguridad
- **Elaborar, aprobar, coordinar y supervisar** el Programa, en conjunto con las áreas técnicas que estime necesario involucrar o consultar;
- **Proponer cambios y mejoras al Programa**, a partir de la experiencia de su implementación;
- **Dar a conocer** el Programa al interior del sujeto obligado;
- **Coordinar la implementación del Programa** en las unidades administrativas del sujeto obligado;
- **Supervisar** la correcta implementación del Programa;

H. Ayuntamiento Constitucional La Independencia, Chiapas

7

Las unidades administrativas, el área coordinadora de archivos y la unidad de transparencia tendrán las funciones y responsabilidades que se describen más adelante en este documento. Para que los objetivos planteados se logren con éxito, el Programa requiere del apoyo e impulso directo del más alto nivel de la institución. La intervención presidente tendrá la finalidad de impulsar la debida implementación del Programa al interior del sujeto obligado, pero no podrá suplir ni afectar las funciones del Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la organización.

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

Las unidades administrativas del Ayuntamiento Municipal de la Independencia, Chiapas, deberán realizar las acciones necesarias para cumplir con las obligaciones que establece este Programa, para lo cual deberán asignar los recursos materiales y humanos necesarios, y prever lo que se requiera en sus programas de trabajo. Para ello, resulta fundamental que el Programa se conozca al interior del sujeto obligado, por lo que el Comité de Transparencia se encargará de difundirlo y socializarlo entre el personal.

EL SERVIDOR PÚBLICO RESPONSABLE DE CADA SISTEMA, O EN SU CASO, EL TITULAR DE LA UNIDAD ADMINISTRATIVA RESPONSABLE DE CADA SISTEMA DEBERÁ:

- 1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad de H. Ayuntamiento Municipal de la Independencia., en el tratamiento de datos personales.
- 2) Implementar las medidas de seguridad que establece el documento de seguridad.
- 3) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.



- 4) Tomar por lo menos una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.
- 5) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda al H. Ayuntamiento Municipal de la Independencia.
- 6) Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales.
- 7) Informar H. Ayuntamiento Municipal de la Independencia, Chiapas sobre los cambios que sufran sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.
- 8) Monitorear la implementación de las medidas de seguridad.
- 9) Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de estas.
- 10) Dar aviso al Comité de Transparencia, y al H. Ayuntamiento Municipal de la Independencia, Chiapas sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de estas.
- 11) Presentar propuestas de mejora o modificación del documento de seguridad a través de H. Ayuntamiento Municipal de la Independencia, Chiapas.
- 12) Emitir reportes en relación con el tratamiento de los datos personales y la aplicación de medidas de seguridad, según sea requerido por el Comité de Transparencia a través del H. Ayuntamiento Municipal de la Independencia, Chiapas
- 13) Diseñar, desarrollar e implementar políticas públicas, procesos internos, y/o sistemas o plataformas tecnológicas necesarias para el ejercicio de sus funciones apegándose en todo



momento al documento de seguridad, las políticas o lineamientos que para el tratamiento de datos personales emita el Comité de Transparencia, así como a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del H. Ayuntamiento Municipal de la Independencia, Chiapas.

14) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del H. Ayuntamiento Municipal de la Independencia, Chiapas.

Son obligaciones del Responsable de la Unidad de Transparencia en relación al tratamiento de datos personales.

- 1) Difundir al interior los avisos de privacidad y el documento de seguridad.
- 2) Revisión física anual a dos unidades administrativas sobre el tratamiento de datos personales y la implementación de medidas de seguridad, mismas que serán sugeridas por el Comité de Transparencia.
- 3) Proponer al Comité de Transparencia actualizaciones o modificaciones al documento de seguridad.
- 4) Emitir un reporte anual al Comité de Transparencia sobre el ejercicio de estas funciones.

El Comité de Transparencia es la autoridad máxima en materia de protección de datos personales dentro del H. Ayuntamiento Municipal de la Independencia, Chiapas.

3. ALCANCE DEL DOCUMENTO DE SEGURIDAD

El alcance de este documento se relaciona con la identificación de sistemas de información o procesos administrados por parte del Instituto y áreas que conforman Unidad de Transparencia, en los que de acuerdo con su ámbito de funciones llevan a cabo el uso y tratamiento de datos personales, mismos que se encuentran bajo su estricta responsabilidad tanto en los medios electrónicos como en los espacios físicos en que se administran, operan y resguardan dichos datos personales. Quedan exceptuados de la



aplicación de este programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren el artículo 18 LPDPPSOCHIS.

Las unidades administrativas que forma parte este sujeto obligado que deberán observar el Programa de Protección de Datos Personales son las siguientes:

10

- ❖ Presidencia Municipal
- ❖ Sindicatura Municipal
- ❖ Contraloría Municipal
- ❖ Secretaría Municipal
- ❖ Tesorería Municipal
- ❖ Dirección de Obras Publicas
- ❖ Fomento Agropecuario
- ❖ Unidad de Transparencia
- ❖ Protección Civil
- ❖ Juzgado Municipal

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

4. SISTEMA DE GESTION DE DATOS PERSONALES

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



Por lo anterior el H. Ayuntamiento Municipal de La Independencia, Chiapas inició un proceso de organización y planeación de los medios para la protección de datos, mediante la identificación de todos y cada uno de los procesos y tareas en los que, de acuerdo con el ámbito de funciones de las distintas áreas que conforman la institución, se involucra el tratamiento de datos personales. Para ello, se dispuso de un formato que facilitó a las diversas unidades administrativas, realizar el levantamiento de inventarios de los datos personales que se encuentran bajo su responsabilidad, considerando lo establecido en el artículo 47 de la Ley de Protección de Datos Personales del Estado de Chiapas; logrando con ello el levantamiento del inventario de datos, con el propósito de identificar entre otros aspectos, la categoría y tipo de datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, y el nombre, cargo y adscripción de los servidores públicos que tienen acceso al tratamiento, además de si son objeto de la transferencia.

reconocimiento de las medidas de seguridad administrativas, entendidas como el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información; físicas, que corresponden a las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento y, técnicas que se valen de la tecnología para proteger el entorno digital de la información, también se han registrado nuevas medidas de seguridad que deberán desarrollarse para fortalecer algunos de los controles que actualmente son implementados; es decir, el análisis de brecha a partir del cual será posible mitigar los riesgos a los que están expuestos los datos tratados, para que garanticen la seguridad de los datos, tanto administrativas, como físicas y técnicas. A partir de esta identificación de potenciales vulneraciones es factible prevenir posibles debilidades en la seguridad de los datos y las áreas de oportunidad, aun cuando no haya existido un daño real, mediante la identificación de la ineficiencia de los

controles de acceso físico, electrónico y el inadecuado establecimiento de los esquemas de privilegios, sumado al poco conocimiento de procesos y responsabilidades en materia de protección de datos personales, además de la falta de definición de perfiles y roles, falta de seguimiento y monitoreo a las medidas de seguridad, así como la inexistencia de mecanismos para garantizar la confidencialidad por parte del personal.

A continuación, se presenta un listado de los sistemas y aplicaciones utilizados para el tratamiento de datos personales dentro del H. Ayuntamiento Municipal de la Independencia y su Unidad de Transparencia: Se utiliza para almacenar y gestionar información relacionada con el personal municipal, incluyendo datos de nómina, contratación y desempeño laboral de todos los empleados del Ayuntamiento. Plataforma de Atención Ciudadana: Utilizada para gestionar consultas, quejas y solicitudes de los ciudadanos, contiene datos personales de contacto y detalles sobre las interacciones.

Sistema de Transparencia y Acceso a la Información: Se utiliza para gestionar solicitudes de acceso a la información pública, que incluyen datos personales de los solicitantes.

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

De igual forma, Una vez integrados los inventarios de tratamientos y de datos, se dispuso de la metodología para el **análisis de riesgos**, con la intención de que se identificaran el valor de los datos de acuerdo con su categoría y su ciclo de vida, así como el valor de exposición, las posibles consecuencias para los titulares por el uso indebido y/o posible vulneración y las condiciones de riesgo



a los que podrían encontrarse expuestos por medidas de seguridad poco confiables. Lo anterior, permitió identificar la brecha entre las medidas de seguridad existentes y las medidas de seguridad faltantes para que garanticen la seguridad de los datos, tanto administrativas, como físicas y técnicas.

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

A partir de esta identificación de potenciales vulneraciones es factible prevenir posibles debilidades en la seguridad de los datos y las áreas de oportunidad, aun cuando no haya existido un daño real, mediante la identificación de la ineficiencia de los controles de acceso físico, electrónico

y el inadecuado establecimiento de los esquemas de privilegios, sumado al poco conocimiento de procesos y responsabilidades en materia de protección de datos personales, además de la falta de definición de perfiles y roles, falta de seguimiento y monitoreo a las medidas de seguridad, así como la inexistencia de mecanismos para garantizar la confidencialidad por parte del personal.

Las amenazas que se buscan prevenir pueden ser de diferentes tipos; pueden ser intencionales o no, pero pondrían en riesgo los activos de información.

Tipos de amenazas:

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

14

El riesgo que de manera general puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada comprometiendo su confidencialidad, disponibilidad e integridad; por lo que las medidas de seguridad por parte de las áreas comisionadas están orientadas a proteger los datos personales. A partir de la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que de acuerdo con la experiencia y mejores prácticas son monitoreadas para lograr la mejora continua por parte de todos los involucrados en el tratamiento.

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

- Tratar datos personales de manera lícita, conforme a las disposiciones establecidas.
- Informar a los titulares del tratamiento de los datos y sus finalidades;
- Sujetar el tratamiento de datos personales al principio de consentimiento salvo las excepciones previstas por la Ley;
- Procurar que los datos personales tratados sean correctos y estén actualizados;
- Suprimir los datos personales cuando hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron;
- Tratar los datos personales estrictamente para propósitos legales o legítimos para



el cual fueron obtenidos y estrictamente los necesarios para las finalidades;

- No obtener datos personales a través de medios fraudulentos;
- Velar por el cumplimiento de los principios, estableciendo y manteniendo medidas de seguridad y de confidencialidad durante el ciclo de vida de los datos personales, en estricto respeto de los derechos de los titulares;
- Mantener actualizado el inventario de datos personales que maneja el H. Ayuntamiento Municipal de la Independencia, Chiapas;
- Respetar los derechos de los titulares en relación con sus datos personales;
- Identificar a los servidores públicos del Ayuntamiento de la Independencia responsables del tratamiento de los datos personales.

15

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

5. INVENTARIO DE TRATAMIENTO Y DATOS PERSONALES

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

El diagnóstico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en este municipio.



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

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

- ❖ Presidencia Municipal
- ❖ Sindicatura Municipal
- ❖ Contraloría Municipal
- ❖ Secretaría Municipal
- ❖ Tesorería Municipal
- ❖ Dirección de Obras Publicas
- ❖ Fomento Agropecuario
- ❖ Unidad de Transparencia
- ❖ Protección Civil
- ❖ Juzgado Municipal

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

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



UNIDAD ADMINISTRATIVA	AREA	TIPO DE TRATAMIENTO
Presidencia Municipal	Presidencia	Atención a la ciudadanía
Sindicatura Municipal	Sindicatura	Procedimiento Administrativos
Contraloría Municipal	Contraloría	Procesos de Entrega de Recepción y Declaración de Situación Patrimonial
Secretaría Municipal	Secretaría	Convenios, Elaboración de Constancias, Registro de Fierro Marcador, Elaboración de Nombramiento, Actas de Cabildo, Tramite de Cartilla Militar.
Tesorería Municipal	Tesorería	Nómina del Personal, Expediente Único del Personal, Comprobación para Diferentes Tipos de Gasto, Padrón de Proveedores, Cobro de Ingresos.
Obras Publicas Municipal	Obras Publicas	Padrón de Contratistas, Elaboración de Contratos, Expediente de Obras, Registro de Contratistas, Padrón de Beneficiarios, Comprobación y Supervisión de Obras



Fomento Agropecuario	Fomento Agropecuario	Padrón de Beneficiarios, Comprobaciones
Unidad de Transparencia Municipal	Unidad de transparencia	Atención de Solicitudes de Información y Datos Personales, Seguimiento al Directorio de Sujeto Obligado, Actualización de las Obligaciones de Transparencia.
Protección Civil Municipal	Protección Civil	Lista de Asistencia, Expediente de Personal,
Secretario Ejecutivo de Seguridad Publica	Secretario Ejecutivo	Expediente Único del Personal, Convenio y Contratos, Trámite de Carta Laboral, Certificado del Centro Estatal de Control y Confianza.
Juzgado Municipal	Juzgado Municipal	Actos Conciliatorios, Asuntos Familiares (separación, régimen de visitas, guardia y custodia)

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

DE IDENTIFICACION DE CONTACTO. Firma, Nombre de la Persona Física, Antecedentes Laborales, CURP, RFC, Estado Civil, Cedula Profesional, Año de nacimiento o Edad,

Beneficiarios, Correo electrónico Personal, Curriculum Vitae, Datos Académicos, Datos contenidos en declaraciones patrimoniales, Datos de identificación, Datos de Salud, Domicilio, Huella Dactilar, Menor de Edad, Nacionalidad, Nivel Educativo, Ocupación, Sexo, Teléfono fijo o Celular, Títulos Profesionales.

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

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

Es posible observar que la Contraloría Municipal, la Secretaría Municipal, la Tesorería Municipal y la Dirección de Obras Publicas son las áreas que desarrollan el mayor número de procesos en los que se tratan datos personales, de acuerdo a sus atribuciones y obligaciones, lo anterior, debido a que las áreas que la integran se encuentran aquellas que cuentan con atribuciones para administrar los recursos humanos, materiales y financieros del Ayuntamiento Municipal de la Independencia; lo cual implica que los procesos correspondientes a la protección de datos personales sean aplicados con mayor cuidado y puntualidad. por lo tanto, esas áreas que cuentan con mayor número de procesos, en materia de protección de datos deben contar con un enfoque de importancia en el desarrollo de las actividades. El inventario de datos personales del Ayuntamiento Municipal de la Independencia, se integra como un elemento del sistema de gestión de datos personales, con base a los hallazgos identificados en su actualización que junto con las medidas de seguridad representa un instrumento útil para la implementación de las medidas necesarias en materia de protección de datos personales.

Así mismo, ayuda a planear capacitaciones enfocados en materia protección de datos hacia los funcionarios del H. Ayuntamiento Municipal de la Independencia, teniendo como objetivo preparar y sensibilizar a los funcionarios para los tratamientos que ellos realizan de conformidad con los estándares nacionales e internacionales en la materia. En tal virtud se consolida el inventario de datos personales del H. Ayuntamiento de la Independencia, Chiapas, como un elemento de la política implementada para la observancia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados aportando con ello certeza a la ciudadanía sobre cuál es el motivo, y cuál es el destino, de los datos que se recaban por este Sujeto obligado.

6. ANALISIS DE RIESGO

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo

Se testa el apartado número 6, que contiene el Análisis de Riesgo, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo

Se testa el apartado número 6, que contiene el Análisis de Riesgo, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo

Se testa el apartado número 6, que contiene el Análisis de Riesgo, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo

Se testa el apartado número 6, que contiene el Análisis de Riesgo, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo

Se testa el apartado número 6, que contiene el Análisis de Riesgo, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

7. ANALISIS DE BRECHA

Sección Clasificada del Documento de Seguridad, apartado del 7. Análisis de Brecha

Se testa el apartado número 7, que contiene el Análisis de brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

Sección Clasificada del Documento de Seguridad, apartado del 7. Análisis de Brecha

Se testa el apartado número 7, que contiene el Análisis de brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

Sección Clasificada del Documento de Seguridad, apartado del 7. Análisis de Brecha

Se testa el apartado número 7, que contiene el Análisis de brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

27

8. CONTROLES DE IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS

Sección Clasificada del Documento de Seguridad, apartado del 8. Controles de Identificación y Autentificación de Usuarios

Se testa el apartado número 8, que contiene los Controles de Identificación y Autentificación de Usuarios, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

Sección Clasificada del Documento de Seguridad, apartado del 8. Controles de Identificación y Autenticación de Usuarios

Se testa el apartado número 8, que contiene los Controles de Identificación y Autenticación de Usuarios, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

Sección Clasificada del Documento de Seguridad, apartado del 8. Controles de Identificación y Autenticación de Usuarios

Se testa el apartado número 8, que contiene los Controles de Identificación y Autenticación de Usuarios, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

Sección Clasificada del Documento de Seguridad, apartado del 8. Controles de Identificación y Autenticación de Usuarios

Se testa el apartado número 8, que contiene los Controles de Identificación y Autenticación de Usuarios, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

9. DESTRUCCIÓN ERRÓNEA DE MEDIOS DE ALMACENAMIENTO FÍSICO

La destrucción manual: Romper archivos y documentos a mano, con tijeras o rasgarlos con un cúter es un método inseguro para desechar este tipo de activos. Este método permite que una persona mal intencionada pueda recuperar los fragmentos de la basura y los ensamble a modo de rompecabezas para extraer información importante.

Tirar documentos de forma íntegra a la basura: Arrojar a la basura documentos con información valiosa o utilizarlos como papel de reciclaje es una conducta aún más riesgosa que la anterior.



destrucción errónea de medios de almacenamiento electrónico Los sistemas operativos de los equipos de cómputo o dispositivos ordenan la información en archivos dentro de sus medios de almacenamiento (por ejemplo, en un disco duro). Para encontrar estos archivos en el espacio correspondiente, el sistema operativo acude a la “lista de archivos”, donde se indica tanto el nombre del archivo como su ubicación dentro del espacio de almacenamiento de es Ayuntamiento Municipal de la Independencia. Cuando se utilizan métodos de borrado dispuestos por el propio sistema operativo, la eliminación se realiza exclusivamente en la “lista de archivos” sin que se borre realmente el contenido del archivo que permanece en la zona de almacenamiento hasta que se reutilice este espacio con un nuevo archivo. Por tanto, toda aquella acción que no conlleve la eliminación, tanto de la información de la “lista de archivos” como del contenido del mismo, no consigue destruir eficazmente dicha información de forma específica: **Los comandos de borrado por defecto de los sistemas operativos:** Cuando se utiliza un comando o el botón de “borrar” o “eliminar”, lo único que se está quitando de esa tabla es la referencia al archivo, pero la información permanece en el medio de almacenamiento, hasta que se reutilice este espacio con un nuevo archivo. Así que, con la simple utilización de algún software (en ocasiones gratuito), se podrían recuperar todos los archivos “borrados”.

“Formatear”: Cuando se formatea un medio de almacenamiento, se eliminan las tablas o listas de archivos mencionadas anteriormente, pero igual que en el caso anterior, la información sigue en el dispositivo y puede recuperarse con el uso de software.

¿Cómo borrar de manera segura los datos personales? para La destrucción y borrado de información es un tema de vital importancia proteger la confidencialidad, integridad y disponibilidad de la información, y en particular de los datos personales, por esta razón, el Ayuntamiento Municipal de la Independencia, debe analizar los medios más eficaces que conviene implementar para evitar que se pueda recuperar la información que ya no requieren. Las técnicas de borrado seguro buscan que no sea posible recuperar la información tanto física como electrónica y evitan que personas no autorizadas puedan

tener acceso a esos datos. De acuerdo con estándares internacionales en la materia, las características para este tipo de destrucción son:

- Irreversibilidad. Se debe garantizar que no existe un proceso que permita recuperar la información.
- Seguridad y confidencialidad. Los medios de almacenamiento se deben tratar durante el borrado con la misma seguridad con que se han mantenido durante su existencia.
- Favorable al medio ambiente. El método de borrado debe producir el mínimo de emisiones y desperdicios que afecten el medio ambiente. A continuación, se detallan los diferentes métodos de Borrado Seguro, a fin de que los responsables de borrado seguro puedan seleccionar aquéllos que mejor se ajusten a sus necesidades.

32

Métodos Físicos de Borrado

Los Métodos Físicos son aquellos que implican un daño irreversible o la destrucción total de los medios de almacenamiento, tanto físico como electrónico.

a) Destrucción de los medios de almacenamiento físico Dentro de las técnicas de destrucción para los medios de almacenamiento físico se encuentran:

1) Trituración Uno de los procesos más intuitivos para la destrucción de activos, tales como documentos, carpetas o archivos, es la trituración.

Las principales características que se deben considerar para la adquisición de una trituradora son el tipo y tamaño del corte o “partícula”, así como la capacidad de la trituradora. Considerando el tipo de corte, existen dos tipos principales de trituradoras: En línea recta o tiras: Cortan el documento en tiras delgadas. Se recomienda usar el corte en tiras de 2 mm de ancho o menos, a fin de evitar que la información pueda ser recuperada rearmando los fragmentos. y En corte cruzado o en partículas: Corta el documento de forma vertical horizontal generando fragmentos diminutos, denominados “partículas”, lo cual hace prácticamente imposible que se puedan unir, es decir, el valor significativo tanto para



los titulares y responsables, como para cualquier persona no autorizada que pudiera beneficiarse de ellos. A continuación, se ofrecen ejemplos de categorías para los sistemas de tratamiento de datos personales según su riesgo inherente: a) Nivel estándar Esta categoría considera información de identificación, contacto, datos laborales y académicos de una persona física identificada o identificable, tal como: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo, experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.

b) Nivel sensible Esta categoría contempla los datos que permiten conocer la ubicación física de la persona, tales como la dirección física e información relativa al tránsito de las personas dentro y fuera del país. También son datos de nivel sensible aquéllos que permitan inferir el patrimonio de una persona, que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores y fianzas. Incluye el número de tarjeta bancaria de crédito y/o débito. Son considerados también los datos de autenticación con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica y cualquier otro que permita autenticar a una persona. Dentro de esta categoría se toman en cuenta los datos jurídicos tales como antecedentes penales, amparos, demandas, contratos.

Política para el Borrado Seguro de Datos cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa. Finalmente, se contemplan los datos personales sensibles de la Ley, es decir, aquéllos que afecten a la esfera más íntima de su titular. Por ejemplo, se consideran sensibles los que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente y futuro,



información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave a la integridad del titular.

c) Nivel especial Esta categoría corresponde a los datos cuya naturaleza única, o bien debido a un cambio excepcional en el contexto de las operaciones usuales de la organización, pueden causar daño directo a los titulares, por ejemplo la Información adicional de tarjeta bancaria que considera el número de la tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido en la misma, por ejemplo fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN). Las categorías antes descritas de la Guía para el SGSDP son sólo una orientación, ya que el Pleno del INAI no ha emitido criterios institucionales al respecto, además de que ciertos datos personales que en principio no se consideran sensibles o de alto riesgo, podrían llegar a serlo dependiendo del contexto en que se trate la información.

Nivel de riesgo por sistema de tratamiento	Nivel del estándar	Tamaño máximo del fragmento	Tipo de documento
No recomendable	General	Tiras de 12 mm de ancho.	Documentos generales que deben hacerse ilegibles
No recomendable	Interno	Tiras de 6 mm de ancho	Documentos internos que deben hacerse ilegibles
Estándar	Confidencial	Tiras de 2 mm de ancho.	Partículas de 4x80 mm. Documentos confidenciales.
Estándar	Secreto	Partículas de 2x15 mm.	Documentos de importancia vital para la organización que deben mantenerse en secreto.

Especial	Secreto	Partículas de 0.8x12 mm.	Documentos clasificados para los que rigen exigencias de seguridad muy elevadas.
-----------------	---------	--------------------------	--

En general, para la protección de los datos personales, se recomienda utilizar la clasificación que sugiere la Guía para el SGSDP, respecto a los sistemas de tratamiento de datos personales según su riesgo inherente, en combinación con la norma DIN 32757, o cualquier otro estándar internacional o mejores prácticas en la materia.

2) Incineración La incineración de medios de almacenamiento físico consiste en su destrucción a través del uso del fuego. Actualmente la práctica de la incineración no es muy recomendable por cuestiones relacionadas con el cuidado del medio ambiente, sin embargo, es una opción segura para la destrucción de los datos personales, siempre y cuando se valide que el activo se redujo a cenizas.

3) Químicos En algunos casos también es posible destruir documentos por medio de químicos, sin embargo esta opción tampoco es muy recomendable por temas ecológicos.

b) Destrucción de los medios de almacenamiento electrónicos La destrucción de medios de almacenamiento electrónico utiliza técnicas tales como:

- Desintegración. Separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.
- Trituración o Pulverización. Procedimiento mediante el cual un cuerpo sólido se convierte en pequeñas partículas.
- Abrasión. Acción de arrancar, desgastar o pulir algo por rozamiento o fricción.
- Fundición o Fusión. Paso de un cuerpo del estado sólido al líquido por la acción del calor.

La destrucción de medios de almacenamiento electrónico tiene el carácter de un proceso industrial robusto, por lo que el H. Ayuntamiento Municipal de la Independencia Chiapas, les puede resultar más práctico la subcontratación del servicio, además de que la eliminación definitiva del activo puede contar con opciones de tratamiento de desperdicios y de reciclaje para hacer que el proceso sea más amigable con el ambiente. Cuando se trate de un proceso más pequeño, por ejemplo el de desechar un disco duro del equipo personal, es recomendable aplicar algún método lógico (que se verán en la siguiente sección) y posteriormente realizar una destrucción minuciosa del dispositivo (por ejemplo, haciendo varios hoyos en el dispositivo con un taladro), antes de enviarlo a un centro de reciclaje o depositarlo en algún contenedor genérico de “basura electrónica”.

10. ANALISIS DE LA INFORMACION.

En el resultado del levantamiento de información para el análisis de riesgo y de brecha, se identifica que el Ayuntamiento Municipal de la Independencia, Chiapas, cuenta con 8 áreas que realizan tratamientos de datos personales para el desarrollo de procesos

Uno corresponde a presidencia, tres a sindicatura, dos a Contraloría, seis a Secretaría Municipal, cinco a Tesorería Municipal, siete a la Dirección de Obras Públicas Municipales, dos de Fomento Agropecuario, dos de Fomento Económico y Social, cuatro de Unidad de Transparencia, dos de Protección Civil, cuatro del Consejo Municipal de Seguridad Pública, cuatro de Seguridad Pública, dos de Juzgado Municipal. Asimismo, en los procesos se utilizan datos personales de identificación, en 4 se utilizan datos personales patrimoniales y en dos procesos se utilizan datos sensibles.

La unidad administrativa que observa mayor estado de vulnerabilidad y riesgo de los datos personales es el Juzgado Municipal de riesgo, seguida en orden descendente por la Tesorería Municipal, la Dirección de obras Públicas, y Fomento agropecuario, la



Contraloría Municipal, mientras que la Presidencia Municipal, Sindicatura Municipal, Secretaria Municipal, Unidad de transparencia, Protección Civil, no poseen tanto riesgo.

11. PLAN DE TRABAJO PARA LA IMPLEMENTACION DE MEDIDAS DE SEGURIDAD.

El plan de trabajo se elaborará para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales. Este plan de trabajo deberá elaborarse de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer. Se deben seleccionar los controles de seguridad faltantes identificados en el análisis de brecha y en el plan de tratamiento del riesgo, tomando en cuenta la ponderación hecha en la valoración.

Existen cuatro posibilidades comunes para tratar el riesgo:

- 1.- Mitigar o reducir el riesgo.
- 2.- Retener el riesgo.
- 3.- Evitar el riesgo.
- 4.- Compartir el riesgo.

Las opciones de tratamiento del riesgo serán seleccionadas con base en el resultado de la valoración del riesgo, los costos estimados, y los beneficios esperados de implementar estas opciones. Si se obtiene una considerable reducción del riesgo con un costo relativamente bajo, esto es una combinación para considerar para implementar los controles. En general, las consecuencias adversas de los riesgos deben reducirse lo más razonablemente posible con independencia de cualquier criterio absoluto, por ejemplo, se deben considerar los riesgos que no ocurren con frecuencia pero que serían severos, en cuyo caso también se deben implementar controles. Los cuatro tipos de tratamiento de riesgo no son



mutuamente excluyentes, a veces las organizaciones pueden beneficiarse sustancialmente de la combinación de opciones, como reducir la probabilidad de un riesgo, reducir sus consecuencias, compartir o retener el riesgo residual. Algunos tratamientos pueden atender a más de un riesgo, por ejemplo, el entrenamiento y concienciación del personal. El plan de tratamiento del riesgo tiene que establecer prioridades de atención de riesgos específicos y su periodo, dicha prioridad puede establecerse equilibrando la valoración del riesgo y el análisis costo-beneficio de la implementación en relación con el presupuesto.

Finalmente, el plan de trabajo se podrá elaborar, hasta que el sistema de gestión de seguridad de datos personales (SGSDP) se encuentre en pleno funcionamiento como resultado de las medidas de seguridad faltantes. Lo anterior, considerando:

- Los recursos designados;
- El personal interno y externo, y
- Las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

En el contexto actual de avances tecnológicos y crecientes desafíos en materia de seguridad y protección de datos, el H. Ayuntamiento Municipal de la Independencia, Chiapas. reconoce la importancia fundamental de garantizar la integridad, confidencialidad y disponibilidad de la información, así como la salvaguarda de los datos personales de sus ciudadanos. Con el objetivo de fortalecer la seguridad y protección de datos en todas sus operaciones y servicios, se ha desarrollado el presente plan de trabajo. El principal objetivo de este plan es implementar medidas efectivas que mejoren la seguridad de la información y protejan los datos personales dentro del H. Ayuntamiento Municipal de La Independencia y su Unidad de Transparencia. A través de una evaluación exhaustiva, identificaremos las áreas de riesgo y vulnerabilidad, desarrollaremos estrategias para mitigar dichos riesgos y fortaleceremos la infraestructura de seguridad, incluyendo los sistemas de vigilancia, para garantizar un entorno seguro y confiable para nuestros ciudadanos y colaboradores.



El Artículo 38 fracción V de la ley general establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la Realización de plan de trabajo para mejorar el tratamiento de datos personales.

Evaluación Integral de Seguridad: Iniciar con una evaluación exhaustiva de la seguridad de la información y de las instalaciones del H. Ayuntamiento de Municipal de la Independencia, incluyendo la revisión de políticas, procedimientos y controles de seguridad existentes. Esta evaluación abarcará también la infraestructura de las cámaras de vigilancia para asegurar su adecuada configuración y funcionamiento.

Implementación de Medidas Correctivas y Preventivas: Desarrollar e implementar un plan de acción para abordar las brechas identificadas, priorizando aquellas áreas que representen un mayor riesgo para la seguridad de la información y la protección de datos personales. Esto incluirá la actualización de políticas y procedimientos, la realización de capacitaciones específicas para el personal, así como la mejora y ampliación de los controles de seguridad, incluyendo los relacionados con las cámaras de vigilancia.

Mejora Continua y Monitoreo: Establecer mecanismos de monitoreo continuo para supervisar la efectividad de las medidas implementadas y detectar cualquier cambio en el entorno de seguridad. Esto incluirá la revisión periódica de los controles de seguridad, la realización de pruebas de vulnerabilidad y la actualización regular de las políticas y procedimientos en función de las lecciones aprendidas y las nuevas amenazas identificadas.

Plan de trabajo en materia de datos personales

MEDIDA FALTANTE	CATEGORIA	DESCRIPCION DE LA ACTIVIDAD	FORMAS DE IMPLEMENTACION	AREAS INVOLUCRADAS

VULNERACIÓN DE DATOS PERSONALES PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD

La gestión de incidentes es el proceso de planeación, comunicación y capacidad de acción cuando ocurre un incidente de seguridad. Por lo tanto, elaborar un plan de respuesta a incidentes es probablemente una de las tareas más complejas en seguridad de la información. Por lo anterior, en este apartado se presenta el documento de Bitácora de Vulneraciones de Datos Personales para atender incidentes de seguridad, a fin de prevenir y mitigar las vulneraciones a la seguridad de los datos personales. Los activos, las amenazas y las vulnerabilidades se combinan para generar riesgos. Cuando un riesgo se materializa, ocurre un incidente de seguridad, el cual se traduce en una violación a las medidas de seguridad.

RIESGO = Amenaza que genera una acción o evento no deseado y que trata de explotar vulnerabilidades de los archivos “Un incidente de seguridad es un riesgo materializado” Para identificar un incidente de seguridad, se requiere de la detección y/o registro de alertas de seguridad, los cuales son advertencias respecto a cambios en los sistemas de

tratamiento. Sin embargo, dichas alertas no siempre implican que haya ocurrido un incidente de seguridad. Además, si no se tienen suficientes medidas de seguridad, puede ocurrir un incidente sin que éste se detecte. A continuación, se presenta una lista de alertas de seguridad, que pueden advertir de una anomalía o cambio no deseado en los activos:

EJEMPLOS DE ALERTAS DE SEGURIDAD	
ENTORNO	TIPO DE ALERTA
fisico	Alarmas para desastres como incendios o terremotos.
fisico	Alarmas automatizadas contra robos o intrusos en instalaciones
fisico	Alertas del personal de vigilancia o a través de circuito cerrado de video.
fisico	Aviso de desaparición o extravío de equipos de cómputo, medios de almacenamiento o documentos.
fisico	Avisos del personal, justiciables, proveedores, autoridades o reportes en medios de comunicación masivos.
fisico	Anomalías o accesos no autorizados identificados en bitácoras de los sistemas de tratamiento físicos.

	EJEMPLOS DE ALERTAS DE SEGURIDAD
ENTORNO	TIPO DE ALERTA
electronico	Notificaciones sobre software malicioso o vulnerabilidades técnicas descubiertas, preferentemente de fuentes confiables como agencias nacionales o firmas especializadas en riesgos o seguridad.
electronico	Alertas de sistemas automatizados como firewalls, antivirus, filtros de contenido, sistemas de detección de intrusos (IDS = Intrusion Detection System, por sus siglas en inglés) o gestores de seguridad de la información y eventos (SIEM = Security Information and Event Management, por sus siglas en inglés).
electronico	Anomalías o accesos no autorizados identificados en bitácoras de los sistemas de tratamiento automatizados, medios de almacenamiento y equipos de cómputo

Cuando se identifica o reporta una alerta de seguridad que involucra información comprometida o daño a los activos, se habla de un incidente de seguridad.

12. PROGRAMA GENERAL DE CAPACITACIÓN

Se manejarán las capacitaciones de conformidad con las necesidades de las unidades administrativas obligadas en cuanto a la implementación y aplicación del sistema de manejo de datos personales, en posesión del sujeto obligado, trabajando de manera coordinada con el Ayuntamiento Municipal de la Independencia. Las fechas exactas se les notificarán a los encargados que sean designados con al menos una semana de anticipación a las fechas estimadas con la intención de que éstos las difundan con los interesados en asistir a las capacitaciones.



13. MONITOREOS DE LAS MEDIDAS DE SEGURIDAD

El compromiso con la seguridad de la información y la protección de datos personales, el H. Ayuntamiento Municipal de la Independencia ha establecido la implementación de mecanismos de monitoreo y revisión. Estos mecanismos buscan asegurar la eficacia de las medidas de seguridad ya implementadas, a través de un monitoreo continuo, garantizar que las medidas de seguridad en el tratamiento de datos personales sean efectivas y estén actualizadas. Esto permitirá al H. Ayuntamiento Municipal de la Independencia identificar y abordar rápidamente cualquier vulnerabilidad o riesgo potencial, protegiendo así la privacidad y la confidencialidad de la información manejada.

El Artículo 38 fracción VI de la ley general establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, los Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad, así como las amenazas y vulneraciones que están sujetas a los datos personales y mejorar el tratamiento de los mismos.

Capacitación y Concientización: Impartir programas de capacitación y concientización sobre seguridad de la información y protección de datos personales dirigidos al personal del H. Ayuntamiento de la Independencia, Chiapas con el objetivo de fomentar una cultura de seguridad y privacidad en toda la organización. Esto incluirá la formación sobre el manejo adecuado de la información, el reconocimiento de amenazas y la respuesta ante incidentes de seguridad.

Fortalecimiento de la Infraestructura de Seguridad: Realizar mejoras en la infraestructura de seguridad, incluyendo la optimización de las cámaras de vigilancia y su integración con sistemas de monitoreo centralizado, para garantizar una cobertura efectiva de las áreas críticas y una respuesta rápida ante incidentes.

Auditorías y Certificaciones: Realizar auditorías internas y externas de seguridad de manera periódica para verificar el cumplimiento de las políticas y estándares de seguridad



H. Ayuntamiento Constitucional La Independencia, Chiapas

establecidos, así como para obtener certificaciones relevantes que demuestren el compromiso del H. Ayuntamiento Municipal de la Independencia con la protección de datos personales y la seguridad de la información.

Evaluación de Incidentes de Seguridad: Estableceremos un proceso formal para la evaluación de incidentes de seguridad, que incluirá la investigación de cualquier incidente reportado o detectado, la determinación de su causa raíz y la implementación de medidas correctivas para prevenir futuros incidentes similares. Este proceso garantizará una respuesta rápida y efectiva ante cualquier amenaza o violación de seguridad.

Evaluación de Desempeño de Sistemas de Videovigilancia: Implementaremos un sistema de evaluación de desempeño para los sistemas de videovigilancia, que incluirá la revisión regular de la calidad de las imágenes capturadas, la funcionalidad de las cámaras y la integridad de los datos almacenados. Cualquier anomalía o problema detectado será abordado de manera oportuna para garantizar la efectividad continua de la vigilancia.

MECANISMOS	MEDIDAS
Monitoreo y revisión	Cada una de las cámaras está agregada a un NVR, es cual almacena todos los videos de todas las cámaras que tenga asignadas hasta que se llena todo su espacio de disco duro, a partir de allí comienza a sobrescribir los videos más viejos con los videos más nuevos que se vayan generando.
Monitoreo	Tienen acceso Solo el personal de las Jefaturas de Redes y TI, el director de área de Redes y TI, el Director General de Sistemas y el personal de C2 en Seguridad Pública
Monitoreo y revisión	Cada cámara tiene un usuario y una contraseña de acceso, las que solo tienen el personal de las Jefaturas de Redes y TI, el director de área de Redes y TI.
Revisión	La Dirección de Patrimonio tiene los resguardos, y la seguridad de los sistemas los maneja la Dirección General de Sistemas
Revisión	Se realizan mantenimientos preventivos a todos los equipos de cómputo, impresoras, enlaces inalámbricos, servicios gratuitos de internet y cámaras de seguridad. Licencias de programas Se han estado llevando a cabo procesos de licenciamientos, con el cual ya la mayoría de las computadoras tienen sus licencias de Windows Resguardo de Servidores Se tienen resguardados todos los servidores bajo llave Control de resguardo El control de los resguardos los tiene la Dirección de Patrimonio

14. PROPUESTA DE CAPACITACION EN MATERIA DE DATOS PERSONALES

La aplicación del programa de protección de datos personales en el ayuntamiento Municipal de la Independencia, requiere como un factor esencial, la formación y sensibilización de las personas que aquí laboran, de tal forma que pueda garantizarse la actualización y mejora continua del inventario de datos personales, la observancia



de la normatividad y Ley, por lo que se propone un programa de capacitación en el tema de protección de datos personales que favorezca la profundización en el conocimiento del tema por parte de quienes intervienen en el tratamiento de datos personales. A manera de propuesta, se han considerado el siguiente tema.

46

- I. La Ley de protección de datos personales en posesión de sujetos obligados en Chiapas.
 - Antecedentes
 - Principios.
 - Alcances
 - Objetivo
 - Implicaciones
- II. Obligaciones en la observancia de la LPDPPSOCHIS
 - Deberes.
 - Medidas de seguridad.
 - Procedimientos y sanciones/Derechos ARCO (acceso, rectificación, cancelación y oposición).
 - Medios de defensa.
- III. El programa de protección de datos personales
 - Sistemas de datos personales.
 - Inventario y Base de Datos.
 - Medidas de seguridad.
 - Análisis de brecha y de riesgo.
 - Funciones y obligaciones.
- IV. El principio de información: Avisos de Privacidad en el marco del programa de protección de datos personales.

- Contenido: Integral, simplificado
- Consentimiento.
- Deber de información.
- Finalidades del tratamiento de los datos

15. ACTUALIZACION DEL DOCUMENTO DE SEGURIDAD

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

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

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





H. Ayuntamiento Constitucional

La Independencia, Chiapas

PRESIDENCIA DEL COMITÉ DE TRANSPARENCIA SECRETARIA DEL COMITÉ DE TRANSPARENCIA

48

Lic. Joel Hernández López

Director de Asuntos Jurídicos

Ing. Alba Rubí García López

Responsable de la Unidad de Transparencia

VOCAL DEL COMITÉ DE TRANSPARENCIA

Ing. Kareli Amivery García Velasco

Coordinadora de Archivo Municipal



Palacio Municipal. Colonia Centro. La Independencia, Chiapas.



Tel: (963) 10 100