DOCUMENTO DE SEGURIDAD

PROGRAMA DE PROTECCION DE DATOS

PERSONALES

INSTITUTO REGISTRAL DEL ESTADO DE CHIAPAS.

2026

Contenido

1.	Objetivo del Documento de Seguridad	Pag. 3
2.	Responsabilidades	Pag. 4
3.	Alcance del Documento de Seguridad	Pag. 07
4.	Desarrollo al Sistema de Gestion de Proteccion de datos personales	Pag. 09
4.1	Ciclo de vida de los Datos Personales	Pag 14
4.1.1	Obtención de Datos Personales	Pag. 14
4.1.2	Uso de los Datos Personales	Pag. 15
4.1.3	Eliminación de los datos personales	Pag. 16
5.	Inventario de Tratamientos de Datos Personales	Pag. 16
6.	Funciones y Responsabilidades del Tratamiento de Datos Personales	Pag 33
6.1.	Resguardo de los Soportes Fisicos y/o electrónicos de los Datos	Pag. 61
6.2	Bitácoras de Seguridad de los Datos Personales	Pag. 62
7.	Análisis de Riesgo y Brecha	Pag. 64
8.	Controles de Identificación y Autentificación de Usuarios	Pag. 96
9.	Los Procedimientos de respaldo y recuperación de datos personales	Pag. 96
10.	Plan de Contingencia	Pag. 97
11.	Plan de Trabajo	Pag. 98
12.	Mecanismos de monitoreo y revisión de las medidas de seguridad	Pag. 100
13.	Propuesta de Capacitación en materia de Datos Personales	Pag. 100

Presentación

Los artículos 6 y 16 de la Constitución Política de los Estados Unidos mexicanos establecen el derecho a la protección de los datos personales, así como al acceso, rectificación, cancelación y oposición en los términos que determine la ley.

En este sentido también la Constitución Política del Estado libre y Soberano de Chiapas en su artículo 5 fracción XVI establece el derecho a la protección de los datos personales; la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS) establece un conjunto de bases principios y procedimientos que garantizan el derecho a la protección de los datos con carácter personal en posesión de sujetos obligados; entre ellos el Instituto Registral del Estado de Chiapas.

En observancia de esta ley, se ha diseñado el presente documento de seguridad, cuyo propósito es establecer los parámetros que guían el tratamiento de los datos personales al interior del Instituto Registral del Estado de Chiapas, por las diferentes unidades administrativas que le conforman. Todo lo anterior, con base en el Artículo 25 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Todo lo anterior de conformidad al Decreto número 033, publicado en el Periódico Oficial número 077, por el cual se crea el Instituto Registral del Estado de Chiapas, como un Organismo Publico Descentralizado de la Administración Pública del Estado de Chiapas, derivado de lo anterior el presente instrumento se elabora por primera vez, buscando garantizar el manejo de los datos personales de conformidad a la normativa nacional y estatal del Estado.

Para su desarrollo se han identificado en primer lugar, los procesos que se llevan a cabo como parte de las competencias y facultades del Instituto, así como del

dictamen de creación por cada una de las áreas así como de sus 19 delegaciones, en los que se utilizan datos personales, para establecer líneas de acción como medidas de seguridad adoptadas a cada una de las áreas, a partir de las finalidades del tratamiento, con base en las funciones que desempeñan.

Lo que se busca es crear un sistema de gestión para el tratamiento de los datos personales que integre las acciones interrelacionadas para operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales tanto de los trámites registrales como de la atención cotidiana que se realiza al público y que por seguimiento de control y estadística de atención se le requiere información considerada como datos de particulares.

Esto implica el planteamiento de acciones pertinentes para evitar la alteración, pérdida, transmisión y acceso no autorizado de los datos mediante la implementación de medidas físicas, administrativas y técnicas, tendientes a garantizar la seguridad e integridad de dichos datos con el seguimiento y observancia continua. Incluye además acciones que permitan controlar y verificar que el tratamiento de los datos personales se realice de acuerdo con los principios establecidos para la protección de los datos personales, implicando un compromiso con las disposiciones previstas en la ley y en los lineamientos generales, por parte de los funcionarios involucrados.

Finalmente, ante la necesidad de mantener actualizado el documento de seguridad se ha de procurar la mejora continua, además, se ha procedido a la actualización de los elementos que integran el documento de seguridad; las medidas de seguridad adoptadas en su tratamiento, el análisis de riesgo y brecha, que permiten dar seguimiento a las medidas adoptadas, identificar las posibles vulneraciones y aminorar los riesgos. Todo lo anterior, acompañado del desarrollo del programa de capacitación que permita comprender la importancia de adoptar medidas para la prevención de las vulneraciones a los datos personales.

1.- Objetivos del Documento de Seguridad.

El presente Documento de Seguridad tiene como objetivos los siguientes:

1. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del Instituto Registral del Estado de Chiapas;
2. Cumplir con las obligaciones que establece, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del estado de Chiapas y los Lineamientos Generales, así como la normatividad que derive de los mismos;
3. Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, y
4. Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que el programa se haya implementado de manera integral en la organización, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos.

2.- Responsabilidades.

Con fundamento en lo dispuesto por los artículos 77 y 78, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, 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:

I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable de conformidad con lo previsto en la presente Ley y demás disposiciones aplicables en la materia.

II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los Derechos ARCO.

III. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los Datos Personales, o se niegue por cualquier causa, el ejercicio de alguno de los derechos ARCO.

IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y demás ordenamientos que resulten aplicables en la materia.

V. Supervisar, en coordinación con las áreas u órganos administrativos competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.

VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Órgano Desconcentrado de la Secretaria o la Autoridad Garante competente, según corresponda.

VII. Establecer programas de capacitación y actualización para las personas servidores públicos en materia de protección de datos personales.

VIII. Dar vista al órgano de control interno u homologo o equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realice el responsable.

Anualmente se presentará un informe, a finales del primer trimestre de cada año y referirá al año inmediato anterior. Algunos de los elementos que pueden incluirse en el informe son:

- ✓ Estadística e información general sobre el cumplimiento de las obligaciones señaladas en el Programa de Protección de Datos Personales por parte de los órganos administrativos;
- ✓ Acciones realizadas por el Comité de Transparencia y la Unidad de Transparencia para cumplir con las obligaciones específicas que establece el Programa de Protección de Datos Personales, y

- ✓ Los resultados de las revisiones y auditorías realizadas durante ese periodo
- ✓ El número de solicitudes y respuestas de Protección de Datos.

- Para ello resulta fundamental que el Programa se conozca al interior del sujeto obligado, por lo que el Comité de Transparencia se encargara de difundirlo y socializarlo entre el personal.

2.-Alcance del documento de Seguridad

El presente programa aplicará a todas las áreas u órganos administrativos que realicen tratamiento de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que éstas efectúen en ejercicio de sus atribuciones, 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.

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 16 de la Ley de Protección de Datos en Posesión de Sujetos Obligados del estado de Chiapas.

Se cubrirán todos los principios, deberes y obligaciones lo anterior con fundamento en los artículos 10, 11, 12 de la LGPDPPSO del estado de Chiapas, se establecen lo siguiente:

Artículo 10.- El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los Datos Personales.

Artículo 11.- El tratamiento de Datos Personales por parte del responsable deberá sujetarse a las atribuciones que la normatividad aplicable le confiera.

Artículo 12.- Todo tratamiento de Datos Personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

El responsable podrá tratar Datos Personales para finalidades distintas a aquéllas establecidas en el Aviso de Privacidad, siempre y cuando cuente con atribuciones conferidas en la normatividad aplicable y medie el consentimiento de la persona titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

Es importante establecer que el manejo de datos personales son propios de las actividades de inscripción registrales, así como también para el proceso de atención al público, por lo que el tratamiento es diferenciado entro los que se utilizan para la actividad registral del cual deben de mantenerse vigente en los sistemas registrales y los que son susceptibles de eliminación posteriormente a la atención y la elaboración de datos estadísticos de las áreas de planeación y control.

Para cumplir con los objetivos y obligaciones que prevé la LGPDPPSO del estado de Chiapas, particularmente en materia de seguridad y, como parte del Sistema de Gestión de Seguridad de Datos Personales del Instituto Registral del Estado de Chiapas, se realizó un análisis de la estructura orgánica autorizada como consecuencia de la creación del Instituto Registral, para evaluar las distintas áreas que manejan datos personales en su actividad para la elaboración del presente documento, por lo que a continuación se presenta las instancias que llevan actualmente tratamiento con datos personales; mismas que deberán observar el presente Programa de Protección de Datos Personales y estas son:

- Dirección General **(DG)**
- **Dirección Operativa de Registro, Certificación y Gravámenes. (DO)**
    - Área de Asuntos Jurídicos **(AAJ)**
    - Área de Informática **(AI)**

- Unidad de Informática **(UI)**
- Delegación Administrativa **(DA)**
- 19 Delegaciones

El Comité de Transparencia del Instituto, en coordinación con las Unidades Administrativas integran este documento de seguridad con base en la información generada por las citadas con antelación dejando bajo su responsabilidad el contenido emitido por las mismas.

Asimismo, se advirtió que, el área que no lleva a cabo tratamiento de datos personales es:

- El área Planeación

4.-Desarrollo del Sistema de Gestión de protección de datos personales

La figura del Sistema de Gestión de Datos Personales está presente en el marco legal en materia de protección de datos personales mexicano y permite a las organizaciones, elevar el nivel de protección de los datos personales que tratan, facilitar el ejercicio de derechos ARCO y las transferencias de datos personales, complementar las disposiciones previstas en la ley en materia de datos personales además, como una forma de demostrar a la autoridad el cumplimiento con la normativa en materia de datos personales.

El sistema de gestión de datos personales es el medio por el cual el Instituto garantiza el tratamiento de los datos personales que lleva a cabo como parte de sus funciones, desde su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, difusión o cualquier otra operación correspondiente; para lo cual, se establecen políticas y métodos orientados a

salvaguardar la confidencialidad, integridad y disponibilidad de estos datos, de acuerdo con Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

Por lo anterior, se inició un proceso de organización y planeación de los medios para la protección de datos, tomando como punto de partida la identificación de los procesos y tareas en los que, dadas sus atribuciones, las distintas áreas del Instituto, desarrollan tratamientos de datos personales. Por lo que para ello sea consideró los trámites que requieren el uso de datos personales de los usuarios, el uso, la duración del uso, la pertinencia de conservación y/o destrucción en su caso, , considerando lo establecido en el artículo 27 de la Ley de Protección de Datos Personales del Estado de Chiapas; logrando con ello el levantamiento del inventario de datos, tratando de identificar, la categoría y tipo datos usados en cada 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 los datos físicos o las bases 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, difusión y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

Artículo 27.- Para establecer y mantener las medidas de seguridad para la protección de los Datos Personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

I. Crear políticas internas para la gestión y tratamiento de los Datos Personales que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los Datos Personales, es decir, su obtención, uso y posterior supresión;

II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de Datos Personales;

III. Elaborar un inventario de Datos Personales y de los sistemas de tratamiento;

IV. Realizar un análisis de riesgo de los Datos Personales, considerando las amenazas y vulnerabilidades existentes para los Datos Personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;

V. Elaborar un plan de trabajo para la implementación de las medidas de seguridad, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los Datos Personales;

VI. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los Datos Personales, y

VII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los Datos Personales.

Además, se ha considerado determinar que una vez concluida la finalidad del tratamiento de los datos personales, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión, eliminación o destrucción, vinculado con el proceso de gestión documental que se desarrolla al interior del Instituto.

Una vez integrados los inventarios de tratamientos y de datos, se estableció la metodología para el análisis de riesgo, con la intención de que se identificaran el valor de los datos y su ciclo de vida, así como el valor de exposición, las posibles consecuencias 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 establecer una proyección y estrategia para identificar la brecha entre las medidas de seguridad de la experiencia obtenida con algunos datos de la extinta Dirección del Registro Público de la Propiedad y del

Comercio del Estado de Chiapas y las posibilidades del mismo riesgo ante la creación del Instituto Registral del Estado de Chiapas, y las medidas de seguridad faltantes para que garanticen la seguridad de los datos, tanto administrativas, como físicas y técnicas.

A partir de esta identificación de posibles vulneraciones es factible prevenir y mitigar debilidades en la seguridad de los datos dentro de las áreas u órganos administrativos, aun cuando no haya existido un daño real, lo anterior es consecuencia de los reducidos o nulos controles de acceso físico y electrónicos, 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 vigilancia a los medios de seguridad y la inexistencia de mecanismos para garantizar la confidencialidad por parte del personal.

Las amenazas que se busca prevenir pueden ser de diferente tipo:

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

El riesgo que puede presentarse en caso de que las amenazas señaladas expongan las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada comprometiendo su confidencialidad, disponibilidad e integridad; y en ese sentido, las medidas de seguridad por parte de cada área u órgano administrativo están orientadas justamente a proteger los datos personales. En el marco del sistema de gestión y política de seguridad institucional, se procurará:

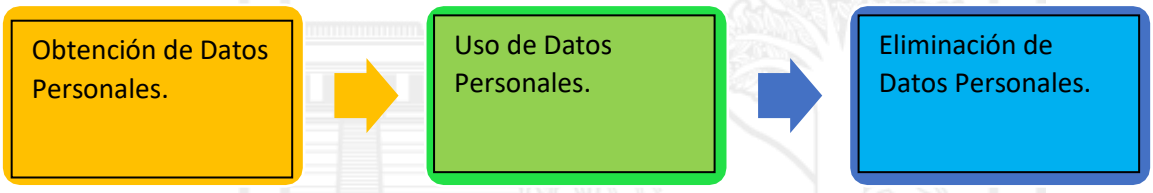
- Que los datos personales sean tratados conforme a la Ley;
- Identificar a los servidores públicos del Instituto responsables del tratamiento de los datos personales.

- Que los tratamientos de datos personales estén sujetos al principio de consentimiento siempre que la Ley lo permita;
- Responder al principio de información a los titulares sobre el uso que dará y sus finalidades;
- Procurar la actualización de los datos personales;
- Procurar la eliminación de los datos personales cuando haya concluido el proceso para el que fueron obtenidos;
- Procurar el tratamiento de los datos personales a las finalidades para la que fueron obtenidos y estrictamente los necesarios para las finalidades;
- Obtener datos personales a través de medios legales, respetando la privacidad del titular;
- 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;
- Mantener actualizado el inventario de datos personales que maneja el Instituto.

4.1.-Ciclo de vida de los datos personales.

El ciclo de vida de los datos es una secuencia de etapas por las que pasan los datos a lo largo de toda su vida útil. Los datos se separan en fases en función de diferentes criterios, y pasan por estas etapas a medida que completan diferentes tareas o cumplen ciertos requisitos.

Por lo que el análisis anterior es importante determinar que el uso de los datos en el Instituto, tienen el proceso siguiente:



4.1.1.-Obtención de datos personales

Los datos se obtienen con autorización tácita, expresa y/o por escrito de las personas propietarias de los datos personales con el consentimiento de los beneficiarios o usuarios, y una vez que se tiene la información correspondiente a la solicitud, se da el tratamiento correspondiente de acuerdo con el trámite a realizar y a la Delegación u área a donde se dirige la información a efectos de análisis, uso y resguardo de los datos.

4.1.2.- Uso de los datos personales

Se establece que las gestiones y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior eliminación.

En el tratamiento de los datos personales que efectúan las delegaciones o Unidades Administrativas, conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad previstos en el artículo 10 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

El uso de los datos personales por parte de las áreas del Instituto, son ingresadas, procesadas y usadas principalmente en los actos de inscripción de los distintos servicios registrales que se ofrecen a la ciudadanía, quedando dichos datos y soportes bajo resguardo de cada una de las delegaciones que realiza dichos actos registrales, así como en los distintos sistemas habilitados para la vigencia de los actos inscritos. Y para el caso de los documentos donde se solicita datos personales para atención al público éstos una vez obtenidos, atendidos se procede a realizar la cuantificación de estadística solicitados por las áreas normativas a efectos de control concluyendo con ello su funcionalidad, sin mayos necesidad de resguardo.

Es importante establecer que en todas las delegaciones en el área de recepción de

ventanilla y estrados se encuentran debidamente establecidos los avisos de privacidad, así como en los formatos que son solicitados en su oportunidad por el personal.

Para la realización de los trámites registrales en donde se solicitan diversos trámites registrales existen formatos pre establecido para ellos tanto en las ventanillas de las delegaciones que en su caso pueden ser de manera digital o físico, mismos que son usados para la calificación registral y resguardados como antecedentes de la vigencia de los actos que se inscriben, quedando debidamente almacenada dicha documentación en los archivos digitales y físicos en cada delegación del instituto, y para los casos de Transferencia de datos personales a otros organismos gubernamentales, que solicitan información y están autorizados por la ley para ello, se realiza por medio de Oficios y medios electrónicos oficiales para el envío de información, referentes para cumplimiento de tratamientos específicos, previamente en su mayoría de los casos mediante la firma de convenios que establece con claridad y precisión el objetivo, los rangos de información, el fundamento legal que les autoriza la firma y acceso a dicha información la secrecía de los mismos y el uso que habrá de dárseles y las personas responsables del manejo de dicha información.

La Disposición se encuentra sujeta al titular de los datos personales, mediante su derecho de Acceso, Rectificación, Cancelación y Oposición (ARCO) para ejercer al tratamiento de los mismos.

4.1.3. Eliminación y conservación de los datos personales.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser eliminados, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Los plazos de conservación de los datos personales no deberán exceder aquellos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, técnico, fiscales, jurídicos e históricos de los datos personales.

En caso de ser necesario para los trámites registrales que dicha información deba de quedar resguardada de manera física o digital, el mismo deberá de estar establecido en las disposiciones reguladores de los servicios registrales a efectos de determinar la vigencia del mismo y la necesidad y pertinencia legal de ser conservados, resguardados, clasificados y en su caso sustituidos para pasar a formar parte del histórico del tracto sucesivo registral.

Para el cumplimiento de lo anterior será necesario:

- Tener identificados los plazos de conservación de las series documentales que contienen datos personales.

- Realizar la eliminación de los documentos correspondientes a dichas series documentales cuando haya concluido el plazo de conservación respectivo.

- Conservarlos para efectos de soporte de la vigencia de la titularidad y del tracto sucesivo de los servicios registrales.

- Establecer de acuerdo a la normatividad interna el momento en que dichos datos serán sustituidos de conformidad a los servicios registrales, para ser sustituidos por los nuevos titulares de las inscripciones registrales.

- Establecer la conservación de los mismos como parte del tracto sucesivo de las inscripciones realizadas en el Instituto.

5.1.- Inventario de Tratamientos de Datos Personales

El Inventario de Tratamientos de Datos Personales es un control documentado y sistematizado en la mayoría de los casos, de los tratamientos que realizan las áreas competentes del Instituto con orden y precisión, de lo contrario, se desconoce donde se encuentran los datos, los riesgos a los que se enfrenta propiciando la vulnerabilidad de los mismos, por lo que de ser así en la mayoría de los casos se implementarán medidas de seguridad a ciegas, lo cual lo hará un blanco fácil ante cualquier ataque, filtración, uso o alteración de los datos resguardados.
Para el debido cumplimiento de las obligaciones que se establecen en este documento, fue necesario que cada una de las áreas u órganos administrativos realizaran 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 el Instituto. Por ***inventario de tratamientos de datos personales*** se entenderá el control documentado que se llevará de los tratamientos que realizan las áreas del Instituto, realizado con orden y precisión.

En tal virtud, el Instituto Registral del Estado de Chiapas, inició el desarrollo de un instrumento homogéneo y estandarizado, mediante el cual se llevó a cabo el levantamiento del inventario de datos, con el propósito de identificar, entre otros aspectos, la categoría y tipo datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo,

aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, y el nombre, cargo y adscripción de los servidores públicos que tienen acceso al tratamiento, además de si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

Como resultado del proceso de análisis y actualización de la información, se logró **identificar** que, en general las 19 delegaciones del Instituto, así como las 4 áreas administrativas del Instituto, **realizan tratamientos con datos personales**; y estas son:

- Dirección General **(DG)**
- **Dirección Operativa de Registro, Certificación y Gravámenes. (DO)**
- Área de Asuntos Jurídicos **(AAJ)**
- Área de Informática **(AI)**
- Unidad de Informática **(UI)**
- Delegación Administrativa **(DA)**
- 19 delegaciones

Asimismo, se advirtió que, la Unidad o área Administrativa del Instituto que **no lleva a cabo tratamientos de datos personales** es:

- Unidad de Planeación

Los tratamientos de datos personales se realizan en absoluto apego a sus funciones, a través de las diversas áreas que las integran y permiten el desarrollo de los procesos que realizan para el cumplimiento de dichas funciones.

En relación con lo anterior, fue posible identificar los procesos que se desarrollan y que implican el **Tratamientos de Datos Personales**, mismas que a continuación se describen:

UNIDAD ADMINISTRATIVA	PERSONA, DEPARTAMENTO O ÁREA RESPONSABLE	TRATAMIENTO(S) O PROCESO(S)
Dirección General (DG)	Asistente	1.- Solicitudes de Audiencia 2.- Solicitudes de revisión o atención registral.
Dirección Operativa, de Registro, Certificación y Gravámenes. **(DO)**	Director.	1.- Proceso de Inscripción de Actos de Comercio en el SIGER. 2.- Atención al Público.
Delegación Administrativa (DA)	**Personal de la Unidad con Actividad de Recursos Humanos**	1. Requerimientos para contratación de personal. 2.- Gestión de nómina para el pago de sueldo al personal.
	Personal de la Unidad con Actividad de Recursos Financieros	3.- Pago a proveedores, prestadores de servicios, viáticos a servidores públicos, impuestos y derechos, los sistemas habilitados
		4.- Captura de las transacciones financieras y presupuestales diarias realizadas por el en el Sistema Integral de Gestión Hacendaria y Administrativa de Chiapas (SIGHA)
		5.- Elaboración de información contable del en el Sistema Integral de Gestión Hacendaria y Administrativa de Chiapas (SIGHA)
	Personal de la Unidad con Actividad de Recursos Materiales.	6.- Alta de Empleados en el SIAPE (Suite Integral
		7.- Compras menores de bienes
		8.- Mantenimiento Vehicular
Área de Asuntos Jurídicos (UAJ)	**Personal del área.**	1.- Comparecencia
		2.- Actas Administrativa
		3.- Notificaciones
		4.- Recepción y contestación de Demandas y Recursos.
		5.- Convenios y Contratos
		6.- Expedición de Certificaciones.

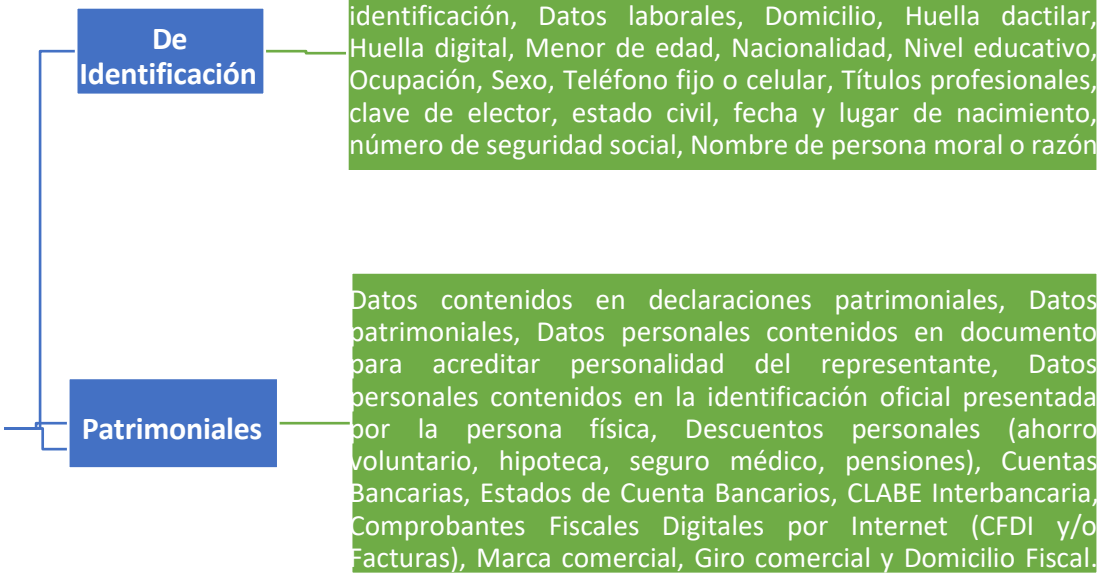
		7.- Solicitudes de acceso a la información y protección de datos personales 8.- Asesorías y Atención al Público mediante el Sistema SIGOF. 9. -Registro de Firma y Sello Notarios.
Unidad de Informática (UI)	**Personal del área.**	1.- Expedición de las firmas electrónicas y Altas de Sistema personal del Instituto en SIREC WEB. 2.- Expedición de claves, firmas y accesos a Notarios en el SIREC WEB. 3.- Expedición de claves, firmas y accesos a Instituciones vía colaboración mediante convenio en el SIREC WEB.
9 delegaciones	**Personal de Delegación.**	1.- Atención al Usuario. 2.- Solicitud de Inscripción de Servicios Registrales vía Ventanilla Física o SIREC WEB. 3.- Registra de Inscripción de datos Registrales. 4.- Solicitud de Verificación de Datos Registrales en Ventanilla.

Categorías de Datos Personales
dos dentro del Sistema DIP Chiapas

A efecto de ejemplificar lo anterior de manera cuantitativa en el manejo de los datos personales, se presenta el concentrado siguiente:

Area	Número de Procesos
Dirección General	2
Dirección Operativa, Registro, Certificaciones y Gravámenes.	2
Delegación Administrativa	8
Área de Asuntos Jurídicos	9
Área de Informática	3
Delegaciones	4
Total de Procesos	**28**

Durante el proceso de análisis y sistematización, se observó que los datos personales cuyo tratamiento se lleva a cabo en los **28 procesos** identificados, corresponden a las siguientes 2 categorías:



A partir de lo anterior, el Inventario de Datos Personales del Instituto posibilitó la identificación de hallazgos en relación con el tratamiento de datos personales, aportando los elementos que permiten focalizar las áreas con mayor incidencia en el tratamiento de éstos, y con ello, enfocar los trabajos de atención e implementación para el cumplimiento de las disposiciones jurídicas en materia de protección de datos.

Lo anterior, permite advertir que la categoría de datos personales con mayor número de áreas y procesos son los de carácter identificativo, seguida por los sensibles y, en casos muy específicos, los datos de naturaleza patrimonial. Sin embargo, es preciso indicar que se detectaron procesos en los que se realiza tratamiento de datos tanto identificativos, patrimoniales y sensibles, otros identificativos y sensibles, y únicamente identificativos, en un mismo proceso.

También, se identificó que cada área tiene un medio propio para obtener los datos

personales, por tal motivo, podemos identificar que de manera general el agrupamiento de la obtención de los datos, así como su uso y conservación se realiza de la manera siguiente:

- Obtención de Información de manera física y Directa. (Formatos de audiencia, solicitudes, recursos administrativos)
- Obtención de Información mediante el Ingreso a los Sistemas. (SIREC, SIGOF)
- Obtención de información en otros Sistemas. (Correo electrónicos)

Por tal motivo, las áreas administrativas del Instituto en materia de protección de datos deben contar con un enfoque de importancia en el desarrollo de las actividades y desarrollar estrategias para la protección de los datos personales, mediante archivos o bases de datos electrónicas simples resguardadas en las computadoras de los funcionarios.

En tal virtud, el Inventario de Datos Personales del Instituto se inscribe como un elemento más de la política para el cumplimiento de las directrices determinadas por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, aportando con ello certeza a la ciudadanía de cuáles son y cuál es el destino de los datos recabados, por lo que es importante para desarrollar e implementar la finalidad del presente documento como una guía de aplicación al personal, establecer cuales son los proceso que se deben de observar como servidores públicos en los datos proporcionados por la ciudadanía, mismos que se explican en el apartado siguiente.

6.- Funciones y Responsabilidades del Tratamiento de Datos Personales.

Como fue referido previamente, uno de los objetivos que se busca con este documento, es permear en las y los servidores públicos de Instituto, la importancia que tiene el adecuado tratamiento de los datos personales y, con ello, sensibilizarlos

para garantizar la efectiva protección de la información personal que manejen, conforme al ámbito de sus atribuciones.

A raíz de los procesos determinados en el Inventario de Datos Personales, por las áreas que integran las unidades administrativas que realizan tratamiento de éstos, resultó necesario asociar dichas actividades con las facultades que el Código Civil para el Estado de Chiapas, en el Capítulo que regula las funciones del extinto Registro Púbico de la Propiedad y del Comercio del Estado, hoy Instituto Registral del Estado, que regula las funciones registrales; Reglamento Interior, otorga a los servidores públicos responsables de dicho tratamiento, a efecto de generar certeza y dar cumplimiento al principio de legalidad que debe atender todo servidor público, en el presente caso para el control de los datos personales.

Es importante establecer que los manuales aún se encuentran en proceso de elaboración toda vez que el nuevo Reglamento del Instituto aún se encuentra en validación por las áreas respectivas, no omitiendo precisar que de conformidad la Ley de General para el Fortalecimiento y Armonización Catastral y Registral, que deberán de entrar en vigor a partir del 01 de enero de 2027, en toda la República es pertinente regular toda la función Registral mediante la expedición de sus leyes secundarias que impulsarán la actualización de los servicios registrales, los requisitos y en consecuencia el manejo de la información de datos, las bases de almacenamiento y la durabilidad de resguardo de los mismos, por ello en el presente documento se presentan las atribuciones establecidas en el Decreto de Creación del Instituto Registral, el dictamen de estructura orgánica por funciones de cada área y del Reglamento, para la elaboración del presente documento.

Bajo ese contexto, a continuación, se precisan las funciones otorgadas por el ordenamiento jurídico a los servidores públicos que llevan a cabo tratamiento de datos personales dentro de las áreas administrativas que conforman la estructura orgánica del Instituto:

UNIDAD ADMINISTRATIVA	DEPARTAMENTO/ ÁREA RESPONSABLE	NOMBRE Y CARGO DE LAS PERSONAS O FUNCIONARIOS QUE TRABAJAN DATOS PERSONALES	FUNCIONES	ACCIONES
Dirección General	N/A	• Daniela Martínez Gómez; Secretaria	La recepción de solicitudes de audiencia con la directora. Recepción de documentos en ejercicio del derecho de petición del ciudadano	• Registro y control de Audiencias con Directora.
			Art. 25 del Decreto de Creación del Instituto Registral del Estado de Chiapas, número 33 de fecha 9 de diciembre de 2025.	
Delegación de Apoyo Administrativo	Administración de Recursos Humanos.	• Lic. Alfonso Diaz Fonseca. Delegado.	Registrar l o s movimientos nominales del personal de confianza y eventual; así como las incidencias, descuentos, periodos vacacionales y demás medidas disciplinarias del personal en el Sistema de Nómina del Estado de Chiapas, para la elaboración de la nómina por parte de la Secretaría de Hacienda. Tramitar oportunamente la inscripción, modificación salarial y baja del personal en el Instituto. Elaborar el Capítulo 1000 Servicios Personales para su integración al proyecto de Presupuesto de Egresos.	• Nómina de pago de personal
	Administración Financiera.		Ejercer el presupuesto asignados al Instituto, con racionalidad y disciplina presupuestaria, con la finalidad de cubrir los requerimientos y necesidades de los diferentes órganos administrativos del mismo.	• Pago a proveedores, prestadores de servicios, viáticos a servidores públicos, impuestos y derechos, en el Sistema Integral de Gestión de Estados. • Captura de las transacciones financieras mensuales realizadas. • Elaboración de información contable.

	Administración de Recursos Materiales.		Proveer de las necesidades del Instituto para su buen funcionamiento.	Compra de bienes y/o contratación de servicios. Pago de Proveedores.
			Artículo 5º. y 13 del Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Chiapas.	
Área de Asuntos Jurídicos.	Jefe de Área	• Lic. Carlos Daniel Conde Ramírez. Jefe de área	Conocer y Turnar al Órgano Interno de Control, las actas administrativas que se levanten a los trabajadores del Instituto, derivadas de la violación a las disposiciones laborales aplicables. Habilitar al personal para que realice notificaciones de oficios, acuerdos, y resoluciones de los procedimientos jurídicos Substanciar los procedimientos administrativos a los que se encuentren sujetos los servidores públicos Instituto. Contestar Demandas de Amparo, Administrativas y Civiles. Resolver Recursos Administrativos.	• Comparecencia • Actas Administrativas • Notificaciones
			Expedir constancias y certificar documentos oficiales que obren en los archivos impresos y/o digitales del DIF-Chiapas. Reglamento Interior del Sistema DIF-Chiapas.	• Expedición de Constancia de asistencia social a las A.C.
			Representar legalmente al Instituto, en el ámbito de su competencia, ante toda clase de autoridades judiciales, administrativas, del trabajo, militares, fiscales y del fuero federal, estatal o municipal; así como ante Comisiones de Derechos Humanos, sociedades, asociaciones y particulares en los procedimientos de cualquier índole, con las atribuciones generales y especiales de un mandato para pleitos y cobranzas.	• Recepción y Contestación de Demandas.
			Participar en la celebración y suscripción de Contratos, Convenios, Acuerdos, y demás actos jurídicos relacionados con los asuntos competencia del DIF-Chiapas.	• Convenios y Contratos

			Las demás atribuciones que en el ámbito de su competencia le sean encomendadas por el Director General, así como las que le confieran las disposiciones legales, administrativas y reglamentarias aplicables. Reglamento Interior del Sistema DIF-Chiapas.	• Solicitudes de Acceso a la Información y Protección de Datos Personales
			Artículo 5 y 12 del Reglamento del Registro Público de la Propiedad y del Comercio del Estado de Chiapas.	
Unidad de Informática	Jefe de Área.	• David Bautista Narcía. Jefe de Área.	Contribuir en el otorgamiento de los servicios de Firma Electrónica Avanzada a servidores públicos del Instituto, Notarios, -Chiapas, a través de los Agentes Certificadores, con base en sus obligaciones, en coordinación con la Dependencia Normativa.	• Expedición de las firmas electrónicas y accesos a sistema registrales y de consulta histórica.
			Artículo 5º. y 14 Reglamento Interno del Registro Público de la Propiedad y del Comercio en el Estado.	
19 Delegaciones.	Delegados	• Lic. Edson Miguel Romero Coutiño. (Tuxtla) • Lic. Juan Manuel de la Cruz Juárez. (Acapetahua) • Lic. Emiliano Díaz López (Bochil) • Lic. Sergio Hernández Cabrera. (Playas de Catazajá) • Lic. Fernando Toledo Tort. (Cintalapa) • Lic. José Augusto González Dominguez. (Comitán) • Lic. María Raquel Zamudio Lara. (Chiapa de Corzo) • Lic. María Esther Martínez Senteno. (Copainalá) • Lic. Humberto Hernández Flores Posada. (Huixtla) • Carlos Omar Pérez Velázquez. (Motozintla) • Lic. Heber Antonio Mayorga Zepeda. (Ocosingo) • Juan Carlos Quevedo	Recepción de Solicitudes de Trámites Registrales. Atención al Público para asesorías y aclaración. Inscripción de Trámites Registrales. Expedición de Certificados. Resguardo de Archivos de documentación de Servicios Registrales.	• Inscripción de Actos Registrales.

		Rodríguez. Pichucalco) • Yolanda Rodríguez Madrazo. (Salto de Agua) • Lic. Elías Peñaloza Landa. (San Cristóbal de las Casas) • Lic. Renan Galán Gómez. (Tapachula) • Lic. Ada Hena Torres de la Rosa. (Tonalá) • Lic. Raquel Hernández Coello. (Venustiano Carranza) • Lic. Dimas Cruz Ruíz. (Villaflores) • Lic. Milton Aronai Trujillo Recinos. (Yajalón)	Resguardo y Administración de los Sistemas Registrales.	
			Articulo 5o. y 15 del Reglamento del Registro Público de la Propiedad y del Comercio en el Estado.	

6.1.- Resguardo de los Soportes Físicos y/o electrónicos de los Datos.

Resguardos Físicos

- Por área ordena, archiva y/o digitaliza los datos recabados en folders, recopiladores y estantes.
- Por área ordena y archiva los datos recabados en cajas de archivo.
- Los soportes físicos documentales se encuentran resguardados en archiveros de cada área.
- Los archivos soporte de trámites históricos y vigente de servicios registrales se encuentran archivados físicamente bajo la responsabilidad de las delegaciones.

- Los Escritorios y archiveros donde se maneja datos cuentan con llave.

- **Resguardos Electrónicos**

- Los datos recabados en algunos casos se digitalizan y posteriormente son resguardados en los equipos de cómputo del personal responsable.
- Las computadoras mediante las cuales se manejan los datos personales cuentan con contraseña, las cuales únicamente tienen conocimiento y acceso el responsable del área.
- clasificación en subcarpetas electrónicas que facilitan localizar la información.
- memorias digitales para respaldo de la información y resguardarlas.
- Se aplican respaldos informáticos para blindaje y resguardo digital.
- Los actos registrales que requieren soporte digital de datos, formas precodificadas, anexos, escrituras son digitalizados y resguardados por cada una de las delegaciones en los sistemas habilitados para ello.

6.2. Bitácoras de seguridad de los datos personales.

Las Áreas Administrativas con que cuenta el Instituto Registral del Estado de Chiapas realiza controles para el acceso de información que maneja, por lo que tanto bitácoras físicas y electrónicas para acceso de operación cotidiana, que contenga los siguientes datos de acuerdo al Artículo 33 de la LPDPPSOCHIS.

Los datos que se registrarán en las bitácoras de las áreas del Instituto serán:

- 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;
- Para soportes físicos: Número o clave del expediente utilizado
- Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

Las áreas determinaran que tipo de bitácora son la que realizaran de acuerdo a sus necesidades, si serán en soporte físico o en soporte electrónico, determinarán el lugar donde las almacenaran, por cuanto tiempo y la manera en que aseguren la integridad de las mismas.

Respecto del análisis de las bitácoras:

- Se determinará que Dirección, Unidad o persona será la responsable de analizarlas y cada cuanto tiempo las analizará.
- Las bitácoras que estén en soporte electrónico: se determinará las herramientas de análisis que serán utilizadas.

Formato de Bitácora Física.

Bitácora Física

No	FECHA	HORA DE ENTRADA	NOMBRE COMPLETO	AREA	DOCUMENTO O INFORMACION CONSULTADA	HORA DE SALIDA	FIRMA	OBSERVACIONES

7.- Análisis de riesgos y de brecha.

El presente análisis identifica el riesgo inherente a los datos personales en el tratamiento que reciben por el Instituto Registral del Estado de Chiapas al ejercer sus atribuciones, de manera que pueda ser controlado por la institución para satisfacer el derecho humano a la autodeterminación informativa.

La LGPDPPSO en sus artículos 32, fracción I, y 33, fracción IV, considera que el determinar el riesgo inherente a los datos personales tratados es un deber de los sujetos obligados en la adopción de medidas de seguridad, para lo que deben realizar un análisis que considere las amenazas y vulnerabilidades para los datos, así como los recursos involucrados en el tratamiento.

Con base en la LGPDPPSO, la valoración de los riesgos de los datos personales forma parte de los elementos mínimos que debe contener el instrumento que describe y da cuenta, en lo general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas (Documento de seguridad), en este caso, por el Instituto, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de ese tipo de datos bajo su posesión.

Aunado a lo anterior, los Lineamientos Generales de Protección de Datos Personales para el Sector Público, emitidos por Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INT), indican en su artículo 60 que el análisis de riesgos de los datos personales tratados debe contemplar los siguientes aspectos:

- Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.
- El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.

El valor y exposición de los activos involucrados en el tratamiento de los datos personales.

- Las consecuencias negativas para los titulares de los datos personales, que puedan derivar en una vulneración de seguridad.
- El riesgo inherente, la sensibilidad, las posibles consecuencias de vulneración para los titulares, las

transferencias y vulneraciones previas ocurridas sobre los datos personales, así como el número de titulares de éstos y el riesgo por su valor potencial, además del desarrollo tecnológico.

7.1 Elementos para el análisis de riesgos.

La seguridad de los datos personales que se tratan en el Instituto, demanda conocer y entender los riesgos a los que se encuentran expuestos en los distintos procesos que realizan las unidades administrativas, lo que permitiría afrontarlos de manera adecuada y oportuna.

Para analizar los riegos de los datos personales que son objeto de tratamiento, se elaboró un instrumento que, a partir de considerar su objeto y atribuciones constitucionales, clasifica los datos en dos tipos, tal y como ha sido referenciado con antelación.

1) **De identificación**, que se refieren a información por la que se identifica a una persona y/o permiten su contacto tales como, Nombre de persona física, Antecedentes laborales, CURP, RFC, Firma, Cédula profesional, Año de nacimiento o edad, Beneficiarios, Fotografía, Características físicas, Correo electrónico, Currículum Vitae, Datos académicos, Datos de identificación, Datos laborales, Domicilio, Huella dactilar, Huella digital, Menor de edad, Nacionalidad, Nivel educativo, Ocupación, Sexo, Teléfono fijo o celular, Títulos profesionales, clave de elector, estado civil, fecha y lugar de nacimiento, número de seguridad social, Datos personales.
2) **Patrimonial,** se refieren a la información de las propiedades o bienes inmuebles, que son sujetas de inscripción, así como el titular del mismo debidamente identificado con datos como el nombre, teléfono, CURP, Credencial de Elector, Domicilio, RFC, Sexo, correo electrónica, actividad laboral, así como todos los datos que identifiquen la propiedad como son el domicilio, clave catastral, avalúos, permisos de subdivisión y de traslado.

Se testa el apartado número 7, que contiene el análisis de riesgo que contiene la Gestión de vulneraciones, y Plan de Contingencia toda vez, que contiene información sensible sobre la forma que el sujeto obligado previene, contine, procesa, detecta, responde, recupera la operación ante incidentes de seguridad de conformidad a lo dispuesto en los artículos 103, Fracción II, 112 Fracción VI, de la Ley de

Transparencia, y acceso a la información pública del Estado y la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; en los artículos 3º. Fracción IX y 6 párrafo tercero de la Ley de Protección de Datos Personales en posesión de sujetos obligados del Estado de Chiapas; así como en el artículo vigésimo de los lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

8.- Los Controles de identificación y autentificación de usuarios

Los sistemas tecnológicos del Instituto, únicamente cuentan con controles de ID y Autentificación mediante credenciales personalizadas para cada usuario con el nombre de usuario y contraseña individualizada.

9.- Los Procedimientos de respaldo y recuperación de datos personales.

El Sistema Instituto cuenta con mecanismos establecidos con periodicidad definida para el respaldo de la información de algunos equipos; así como de su recuperación en casos necesarios, para lo cual tiene programados respaldos locales y en la nube diario y semanales según los tipos de información.

10.- El plan de contingencia.

El plan de contingencia consiste en acciones definidas para la vuelta a la normalidad en caso de contingencias derivadas de emergencia o desastre, a través del restablecimiento de los datos que sufra algún percance o siniestro.

El plan debe considerar todos los componentes del sistema, datos críticos, equipo lógico de base, aplicaciones, equipos físicos, de comunicaciones, documentación y personal, además debe contemplar también todos los recursos auxiliares sin los cuales el funcionamiento de los sistemas podría verse seriamente comprometido: suministro de potencia, sistemas de climatización, e instalaciones.

Respaldos y recuperación

1.- Realizar respaldo

2.- Verificar respaldo

3.- Registrar respaldo.

Recuperación de respaldos ante desastres.

4.- Solicitar respaldos

5.- Utilizar Respaldos.

6.- Verificar respaldos.

7.- Solicitar equipos

8.- Configurar equipos

11.- El plan de Trabajo

Para una correcta y permanente eficiencia de la aplicación del Programa de Protección de Datos Personales del Instituto, es necesaria la formación constante de los servidores públicos, que garantice la actualización y mejora continua del tratamiento de datos personales, así como el cumplimiento de la normatividad establecida, por ello se propone realizar las siguientes capacitaciones de acuerdo al calendario que se desarrolla en el presente capitulo, mismas que tendrán el objetivo de instruir y profundizar los conocimientos en la materia, por parte del personal que interviene en el tratamiento de los datos personales.

Lo anterior bajo el siguiente esquema de trabajo.

1.- A partir del día 6 de noviembre de 2026, se hará de conocimiento al personal del presente instrumento guía.

2.- La siguiente capacitación será el día viernes 13 de noviembre 2026, será sobre las obligaciones de la Ley Federal de Protección de Datos personales en posesión de Particulares.

3.- La siguiente capacitación será el día viernes 20 de noviembre 2026, será sobre las obligaciones de la Ley de Transparencia y Acceso a la información Pública del Estado de Chiapas.

4.- La siguiente capacitación será el día viernes 27 de noviembre 2026, será sobre Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas.

12.- Mecanismos de monitoreo y revisión de las medidas de seguridad.

Como parte de las medidas es importante la supervisión de las medidas de seguridad técnicas y físicas que permitan definir nuevas formas de monitoreo de acuerdo a las necesidades.

Se cuenta con consolas remotas para el monitoreo y revisión constante de los sistemas de seguridad que protegen los sistemas de información y las bases de datos manejadas por los mismos..

Como parte de las medidas es importante la supervisión de las medidas de seguridad técnicas y físicas que permitan definir nuevas formas de monitoreo de acuerdo a las necesidades.

Se cuenta con consolas remotas para el monitoreo y revisión constante de los sistemas de seguridad que protegen los sistemas de información y las bases de datos manejadas por los mismos.

12.-Mecanismos de monitoreo y revisión de las medidas de seguridad.

Como parte de las medidas es importante la supervisión de las medidas de seguridad técnicas y físicas que permitan definir nuevas formas de monitoreo de acuerdo a las necesidades.

Se cuenta con consolas remotas para el monitoreo y revisión constante de los sistemas de seguridad que protegen los sistemas de información y las bases de datos manejadas por los mismos.

12. Propuesta de capacitación en materia de Datos Personales

Para una correcta y permanente eficiencia de la aplicación del Programa de Protección de Datos Personales en el Sistema DIF Chiapas, es necesaria la formación constante de los servidores públicos, que garantice la actualización y mejora continua del tratamiento de datos personales, así como el cumplimiento de la normatividad establecida, por ello se propone realizar las siguientes dos capacitaciones con un espacio de 6 meses aproximadamente entre cada uno de ellas, mismas que tendrán el objetivo de instruir y profundizar los conocimientos en la materia, por parte del personal que interviene en el tratamiento de los datos personales.

Capacitación 1

Fecha sugerida: Noviembre 2026.

- Módulo 1. Sensibilización en materia de Protección de Datos Personales
- Objetivo.- Sensibilizar a los servidores públicos del Instituto Chiapas sobre el derecho a la protección de datos personales
- Temario:

    1) Derecho a la Protección de Datos Personales

    2) Relación y distinción entre el Derecho a la Protección de Datos Personales con la Protección de la Privacidad de las Personas

    3) El derecho a la Protección de Datos Personales en la Constitución Política de los Estados Unidos Mexicanos.

    4) Instrumentos normativos de protección de datos personales.

    5) Evaluación de aprendizaje

- Módulo 2. Tratamiento para la protección de Datos Personales

- Objetivo.- Profundizar en los conocimientos referentes a los contenidos básicos y prácticos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y establecer las bases y condiciones que rigen el tratamiento de los datos personales.
- Temario.

1) Conceptos básicos para el tratamiento de los Datos Personales.

2) Principios, deberes y obligaciones para el cumplimiento efectivo del tratamiento de Datos Personales.

3) Sanciones por el indebido tratamiento de datos personales.

4) Evaluación de aprendizaje.

- Módulo 3. Ejercicio de Derechos ARCO

- Objetivo.- Distinguir el contenido y el alcance de los derechos de Acceso, Rectificación, Cancelación y Oposición.
- Temario.

1) Derechos de Acceso, Rectificación, Cancelación y Oposición.

2) Personas facultadas para el ejercicio de los derechos ARCO.

3) Solicitudes para el ejercicio de los derechos ARCO.

4) Respuesta de la solicitud del ejercicio de los derechos ARCO.

5) Causas de improcedencia del ejercicio de los derechos ARCO.

6) Incompetencia e inexistencia de los datos personales.

7) Evaluación de aprendizaje

Capacitación 2

Fecha sugerida: Noviembre 2026

- Módulo 1. Aviso de Privacidad en el Sistema DIF Chiapas
- Objetivo.- Que los servidores públicos dispongan de una herramienta que facilite el cumplimiento de emitir y poner a disposición el Aviso de Privacidad con los elementos necesarios en términos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.
- Temario.

1) Objetivo del Aviso de Privacidad y su vinculación con el principio de información.

2) Características, modalidades y contenido que debe contener el Aviso de Privacidad.

3) Momentos para la puesta a disposición del Aviso de Privacidad.

4) Medios de difusión del Aviso de Privacidad

5) Casos en los que se requiere un nuevo Aviso de Privacidad o actualización del Aviso de Privacidad existente.

6) Sugerencia para su estructura, diseño y redacción.

7) Evaluación de aprendizaje.

- Módulo 2. Medidas de Seguridad Administrativas, Técnicas y Físicas para la Protección de Datos Personales
- Objetivo.- Que las y los servidores públicos conozcan los objetivos y alcances en materia de seguridad la protección que tiene bajo su responsabilidad.
- Temario.

1) Conceptos fundamentales para las medidas de seguridad.

2) Obligaciones y responsabilidades sobre las medidas de seguridad en los datos personales.

3) Medidas administrativas.

4) Medidas físicas

5) Medidas técnicas

6) Sistemas de Gestión

7) Medidas de seguridad en los Datos personales en el Sistema DIF Chiapas

8) Evaluación del aprendizaje.

Sección Clasificada del Documento de Seguridad,

Apartado del Análisis de Riesgo y Brecha

Se testa los apartados 7,8,910,11,12 y 13, que contienen el Análisis de Riesgo Brecha, Medidas de mitigación, recuperación de la información, Evaluación y Monitoreo de Información, Recuperación de la Información que identifica las vulnerabilidades, debilidad amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obliga Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personale afectar la eficiencia de los controles de seguridad, de conformidad con lo dispuesto en artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Informac Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiap así como en el artículo vigésimo sexto de los Lineamientos generales en materia clasificación y desclasificación de la información, así como para la elaboración de versio públicas.

Sección Clasificada del Documento de Seguridad,

Apartado del Análisis de Riesgo y Brecha

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

Sección Clasificada del Documento de Seguridad,

Apartado del Análisis de Riesgo y Brecha

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

Sección Clasificada del Documento de Seguridad,

Apartado del Análisis de Riesgo y Brecha

Se testa el apartado número 7, que contiene el Análisis de Riesgo y 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 eficiencia 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 y Brecha

Se testa el apartado número 7, que contiene el Análisis de Riesgo y 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 eficiencia 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.

GOBIERNO DEL ESTADO DE CHIAPAS

Sección Clasificada del Documento de Seguridad,

Apartado del Análisis de Riesgo y Brecha

Se testa el apartado número 7, que contiene el Análisis de Riesgo y 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 eficiencia 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.

GOBIERNO DEL ESTADO DE

Sección Clasificada del Documento de Seguridad,

Apartado del Análisis de Riesgo y Brecha

Se testa el apartado número 7, que contiene el Análisis de Riesgo y 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 eficiencia 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 y Brecha

Se testa el apartado número 7, 8,9,10,11,12 y 13, que contiene el Análisis de Riesgo y 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 eficiencia 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.