

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DEL INSTITUTO DEL CAFÉ DE CHIAPAS.

(Artículos 25 al 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y artículos 50 al 60 de los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados aún vigentes)

El presente Documento de Seguridad para la Protección de Datos Personales en Posesión del Instituto del Café de Chiapas, fue validado y aprobado en versión pública para su difusión mediante la Novena Sesión Ordinaria del Comité de Transparencia celebrado el día 20 de octubre de 2026.

INDICE.

1. Introducción.....	1
2. Responsabilidades.....	2
3. Glosario.....	4
4. Inventario de datos personales y de los sistemas de tratamiento.	8
5. Las funciones y obligaciones de las personas que traten Datos Personales.....	23
6. Análisis de riesgo.	31
7. Análisis de brecha.	35
8. Plan de trabajo.....	39
9. Los mecanismos de monitoreo y revisión de las medidas de seguridad.	43
10. Programa general de capacitación.	45

1. INTRODUCCIÓN.

El Instituto es un organismo descentralizado de la administración pública del Estado de Chiapas, con personalidad jurídica y patrimonio propio, según decreto publicado en el Periódico Oficial, número 276-2ª sección, tomo II, de fecha miércoles 01 de diciembre de 2004, de la publicación estatal, 1694-A-2004 Bis. De igual manera de su reforma publicada en el Periódico Oficial número 181, tomo III, de fecha miércoles 12 de agosto de 2009, publicación 1218-a-2009, así como de su estatuto orgánico, publicado en el Periódico Oficial número 065 de fecha 30 de octubre de 2019, publicación 0590-A-2019.

En correlación a su objetivo, el Instituto cuenta con diversas atribuciones legalmente conferidas, en cuyo ejercicio tiene acceso al tratamiento de datos personales de acuerdo a las actividades realizadas por los órganos administrativos, rigiéndose por los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, responsabilidad, deberes de seguridad y confidencialidad.

De conformidad con lo establecido en los artículos 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, el Instituto cuenta con la obligación de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los Datos Personales, contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, además de implementar controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los Datos Personales, guarden confidencialidad respecto de estos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

En virtud de lo anterior, el presente Documento de Seguridad tiene como objetivo que todas las personas servidoras públicas del Instituto que tengan acceso a los datos personales, estén obligadas a conocer y aplicar las medidas de seguridad propias en todas las fases del tratamiento en el que se concentren datos personales, iniciando desde la obtención de los mismos y finalizando con su eliminación.

2. RESPONSABILIDADES.

Con fundamento en lo dispuesto por los artículos 113 y 114 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, que señala que el Comité de Transparencia es la autoridad máxima 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 atribuciones, facultades, competencias o 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 disposiciones 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 Secretaría o la Autoridad Garante competente, según corresponda;

VII. Establecer programas de capacitación y actualización para las personas servidoras públicas en materia de protección de Datos Personales, y

VIII. Dar vista al órgano de control interno u homólogo 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.

Los Órganos Administrativos y el Responsable de la Unidad de Transparencia tendrán las funciones y responsabilidades que se describen en este Documento para asegurar la integridad, confidencialidad y disponibilidad de los datos personales recabados en las distintas acciones realizadas por el personal del Instituto del Café de Chiapas, en su carácter de Sujeto Obligado, garantizando la protección de los mismos, a través de mecanismos, procedimientos y procesos internos, delimitando las obligaciones de las

personas responsables, encargados y usuarios de cada sistema, así como las medidas de seguridad que deberán implementarse para el adecuado manejo de la información en posesión de cada órgano administrativo que integran la estructura de este Instituto.

El documento de seguridad, deberá aplicarse en todos los órganos administrativos y operativos considerando las necesidades de cada uno de ellos, a través del uso, registro, organización, conservación, elaboración, utilización, almacenamiento, posesión, acceso, manejo, aprovechamiento y transferencia, así como identificar las vulnerabilidades y amenazas que representan un riesgo, estableciendo mecanismos orientados al tratamiento de datos personales de conformidad a lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.



3. GLOSARIO

Análisis de brecha: Concentración de elementos específicos que pueden existir entre lo deseable y lo actual.

Análisis de riesgo: Sirve identificar peligros y estimar los riesgos, 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.

Aviso de privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización. **Bloqueo de los datos personales (bloqueo):** Constituye una acción o etapa previa a la supresión o borrado de datos personales durante la cual se impide su tratamiento o posible reutilización por parte del responsable o encargado hasta en tanto prescribe cualquier acción relativa a posibles responsabilidades que pudieran surgir de la relación jurídica entre el titular y el responsable que motivó el tratamiento de dichos datos.

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular, mediante la cual autoriza el tratamiento de sus datos personales; que puede consistir entre otros en consentimiento expreso: la voluntad del titular se manifieste de forma verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología, en el entorno digital, podrá utilizarse la firma electrónica o cualquier mecanismo o procedimiento equivalente que permita identificar fehacientemente al titular, y a su vez, recabar su consentimiento de tal manera que se acredite la obtención del mismo y el consentimiento tácito: cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

Conservación de los datos (conservar): Consistente en el almacenamiento, mantenimiento y resguardo de datos personales, ya sea en soportes físicos o electrónicos, en cumplimiento a los plazos legalmente establecidos o períodos de retención determinados por el responsable.

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

Datos personales: Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica,

acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información.

Derecho de acceso (acceso): El derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el aviso de privacidad al que está sujeto el tratamiento. **Derecho de cancelación (cancelación):** Es el derecho fundamental reconocido al titular de los datos personales por el cual dispone que tiene, en todo momento, la prerrogativa de solicitar que todos o parte de sus datos personales se supriman o eliminen para que no estén en posesión del responsable y dejen de ser tratados.

Derecho de oposición (oposición): Es la prerrogativa con que cuenta el titular de los datos personales para, en todo momento y por causa legítima, oponerse al tratamiento de sus datos personales

Derecho de rectificación (rectificación): Consiste en poder solicitar, en todo momento, la rectificación de sus datos personales cuando sean inexactos, incompletos o no estén actualizados. **Derechos ARCO:** Son una garantía del derecho de autodeterminación de las personas como titulares de datos personales que les permite mantener el control y disponer de sus datos personales frente a los responsables pertenecientes al sector público y al privado.

Difusión: Publicar, extender y/o poner al alcance del público algo.

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad de carácter técnico, físico y administrativo adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Encargado: Prestador de servicios, que con el carácter de persona física o jurídica pública o privada, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste.

Instituto: Es un organismo descentralizado de la administración pública del Estado de Chiapas, con personalidad jurídica y patrimonio propio, denominado Instituto del Café de Chiapas.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel organizacional, la identificación, clasificación y borrado seguro de los datos personales, así como la sensibilización y capacitación del personal en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información; c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la

organización, y d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales.

Responsable de la Unidad de Transparencia: Instancia a que se refiere el artículo 41 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

Responsable: Cualquier autoridad, dependencia, entidad, órgano y organismos de los poderes Legislativo, Ejecutivo y Judicial, ayuntamientos, órganos constitucionales autónomos, fideicomisos y fondos públicos y partidos políticos locales, que decide y determina los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales.

Supresión de datos personales (supresión): Baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable. **Titular de los datos personales:** Es la persona física a quien corresponden o conciernen los datos personales sujetos a tratamiento y por tanto es a quien se considera como sujeto de protección del derecho a la protección de datos personales.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, transferencia y en general cualquier uso o disposición de datos personales.

4. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

Este Instituto, con la finalidad de establecer y mantener las medidas de seguridad de los datos personales, emite el presente inventario de datos personales y de los sistemas de tratamiento, de conformidad a lo establecido en los artículos 27, fracción III, 29, fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 27, fracción III, 29, fracción I, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, mismos que fueron generados con la información proporcionada por los órganos administrativos del Instituto.

Para el cumplimiento de las obligaciones establecidas en este, cada uno de los órganos administrativos realizaron un diagnóstico de los tratamientos de datos personales que llevan a cabo, dicho diagnóstico se encuentra basado en la elaboración básica de cada tratamiento de datos personales que se realizan en el Instituto, con el control documentado que se lleva a cabo en función de los tratamientos que realizan los órganos administrativos realizado con orden y precisión.

El tratamiento de datos personales que realicen los órganos administrativos deberá cumplir con los principios, deberes y obligaciones que prevé la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, para lo cual este documento establecerá el marco de trabajo que se deberá seguir para alcanzar ese objetivo, para ello se identificaran los requisitos y obligaciones de los tratamientos en el interior del Instituto se realicen en apego a lo estipulado en la normatividad de la materia y según el ciclo de vida de los datos personales los cuales una vez concluida la finalidad, estos deberán ser sometidos a un proceso de cancelación, supresión, eliminación o destrucción de acuerdo al proceso de gestión documental que se desarrolle en el interior del Instituto.

CICLO DE VIDA DE LOS DATOS PERSONALES

- 1.** Obtención (licitud, información, consentimiento, proporcionalidad, seguridad, confidencialidad)
- 2.** Uso: registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia, disposición. (Calidad, finalidad, seguridad, confidencialidad.)
- 3.** Eliminación: calidad y seguridad.

Durante el ciclo de vida de los datos personales que sean recabados por los órganos administrativos que conforman la estructura del Instituto, deberá dar cumplimiento a la actualización en la identificación de los mismos, avisos de privacidad integrales, simplificados y documento de seguridad.

Para el debido cumplimiento de las obligaciones que se establecen en este apartado, 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 basó en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en el instituto. El inventario de datos personales al que hace referencia los artículos 27, fracción III, 29, fracción I, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, y 58 de los Lineamientos Generales, identificará los siguientes elementos relevantes:

1. ¿Qué tratamientos de datos personales realiza el órgano administrativo?
2. ¿Qué órgano administrativo está a cargo de estos procesos y que por tanto sea la administradora de las bases de datos o archivos que se generen con motivo de dichos tratamientos?

Una vez que identificados los tratamientos de los cuales está a cargo cada órgano administrativo, será necesario determinar lo siguiente, de acuerdo con el ciclo de vida de los datos personales:

3. ¿Cómo se obtienen los datos personales?
4. ¿Qué tipo de datos personales se tratan? ¿Son sensibles?
5. ¿Dónde se almacenan y realiza el tratamiento de los datos personales?
6. ¿Para qué finalidades se utilizan los datos personales?
7. ¿Quién tiene acceso a la base de datos o archivos (sistemas de tratamiento) y a quién se comunican los datos personales al interior del sujeto obligado?
8. ¿Intervienen encargados en el tratamiento de los datos personales?
9. ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?
10. ¿Se difunden los datos personales?

El inventario completo forma parte integral del presente Documento de Seguridad y constituye la base para la determinación de riesgos y la implementación de medidas de seguridad diferenciadas, especialmente en aquellos tratamientos que involucran datos sensibles relacionados con salud, origen étnico, orientación sexual, entre otros. Cada órgano administrativo realiza los tratamientos de datos personales con diversas finalidades, conforme a la estructura orgánica de este Instituto y a las disposiciones normativas que rigen el actuar del mismo, de acuerdo a lo señalado en el siguiente cuadro:

Órgano Administrativo	Tratamiento(s) o Proceso (s)	Finalidad	Base de Datos Personales
Unidad de Apoyo Administrativo	Lista de Asistencia.	1. Registrar la asistencia de los servidores públicos en las capacitaciones que se llevan a cabo en materia de datos personales. 2. Emisión de constancia de participación o asistencia de acuerdo a la modalidad de que se trate; 3. Generar	• Nombre Completo • Sexo • Área de Adscripción

2026, "Año de Jaime Sabines Gutiérrez"

**UNIDAD DE TRANSPARENCIA.
UNIDAD DE APOYO JURIDICO**

		estadísticas para informes obligatorios del Instituto ante otros organismos públicos o privados. 4. Registrar la asistencia de los servidores públicos que pertenecen a los grupos y comités de este organismo.	• Correo electrónico • Teléfono fijo o celular • Cargo • Firma Autógrafa
Unidad de Apoyo Administrativo	Comité de Ética.	Los datos que se recolectan a través del Formato de primer contacto para la presentación de quejas y denuncias ante el Comité de Ética y de Prevención de Conflictos de Interés, serán utilizados con la finalidad de integrar el expediente de denuncia que será presentado a los miembros del Comité para su análisis, así como contar con los datos de contacto del personal, mismos que deben ser actualizados en caso de requerirse establecer comunicación	• Nombre completo. • Correo electrónico • Número telefónico • Firma autógrafa
Unidad de Apoyo Administrativo	Expediente Único Personal.	Integrar el expediente único personal de las y los servidores públicos del Instituto del Café de Chiapas para realizar los trámites administrativos y fiscales correspondientes	• Nombre completo • Fecha de nacimiento • Lugar de nacimiento • Nacionalidad • Escolaridad • Domicilio • Registro Federal de Contribuyente • Número telefónico • Correo electrónico • Clave Única de Registro de Población • Clave de credencial de elector • Datos familiares (padres, cónyuge, hijos) • Número de seguridad social. • Curriculum Vitae • Acta de Nacimiento • Certificado Médico
Unidad de Apoyo Administrativo	Nómina de Pago de Personal.	Integrar la nómina de pago, realizar los trámites administrativos y fiscales de las y los servidores públicos del Instituto del Café de Chiapas	• Nombre completo. • Registro Federal del Contribuyente. • Número de Seguridad Social. • Clave Única de Registro de Población. • Número de cuenta bancaria (en su caso).

2026, "Año de Jaime Sabines Gutiérrez"

**UNIDAD DE TRANSPARENCIA.
UNIDAD DE APOYO JURIDICO**

Unidad de Apoyo Administrativo	Declaración Patrimonial.	Integrar el expediente de la presentación de la declaración de situación patrimonial de las y los servidores públicos del Instituto del Café de Chiapas para realizar los trámites administrativos y fiscales correspondientes.	• Nombre completo • Lugar y fecha de nacimiento • Nacionalidad • Escolaridad • Domicilio • RFC • Número telefónico • Género • Correo electrónico • Clave Única de Registro de Población • Estado Civil • Ingresos netos
Unidad de Apoyo Administrativo	Control de Asistencia.	Registrar y controlar la asistencia de los servidores públicos del Instituto del Café de Chiapas	• Nombre completo • Huella
Unidad de Apoyo Jurídico.	Solicitudes de datos personales o para el ejercicio de los derechos ARCOP.	Registrar y gestionar internamente las solicitudes de datos personales o para el ejercicio de los derechos ARCOP y realizar las notificaciones correspondientes a las personas titulares de los datos personales, quien las represente o quien acredite el interés jurídico, así como generar información estadística para integrar informes o reportes que el responsable Unidad de Transparencia rinde o podría rendir ante el Comité de Transparencia del INCAFECH	• Nombre(s) y apellidos de la persona titular de los datos personales • Condición particular del titular (persona menor de edad, en estado de interdicción o incapacidad – sensible- o fallecida); • Datos y documentación proporcionados en la descripción de la solicitud y para acreditar la identidad de la persona titular de los datos personales o de su representante, así como la personalidad de este último; • Documentos que se presenten en caso de que la persona titular de los datos personales sea menor de edad, se encuentre en estado de interdicción o incapacidad o haya fallecido (algunos de estos documentos podrían contener datos sensibles); • Lugar o medio para recibir notificaciones (cuenta de correo electrónico personal o domicilio particular); • Datos adicionales de contacto (número telefónico de teléfono fijo o celular y cuenta de correo electrónico personal); • En caso de que así lo proporcione, lengua indígena que hable (sensible) y especificaciones de las preferencias de accesibilidad (lugar de estacionamiento para persona

2026, "Año de Jaime Sabines Gutiérrez"

**UNIDAD DE TRANSPARENCIA.
UNIDAD DE APOYO JURIDICO**

			con discapacidad, acceso para perros guías o animales de apoyo, ayuda de lectura a documentos, etc. -sensibles); • En caso de que así lo proporcione, la solicitud para no cubrir el pago de derechos por concepto de costos de reproducción y gastos de envío (sensible) y los solicitados con fines estadísticos.
Unidad de Apoyo Jurídico.	Solicitudes de acceso a la información dirigidas al Instituto del Café de Chiapas	Registrar y gestionar internamente las solicitudes de acceso a la información y realizar las notificaciones correspondientes a las personas solicitantes, así como generar información estadística para integrar informes o reportes que el responsable Unidad de Transparencia rinde o podría rendir ante el Comité de Transparencia del INCAFECH	• Nombre(s) y/o apellido(s) (paterno y/o materno), • Domicilio particular, • Cuenta de correo electrónico personal y cualquier otro que las propias personas solicitantes incorporen de forma voluntaria en el texto de las solicitudes o que obre en los documentos que adjunten.
Unidad de Apoyo Jurídico.	Recursos de revisión en materia de datos personales.	Remitir al Órgano Administrativo Desconcentrado denominado Transparencia para el Pueblo de Chiapas los recursos de revisión en materia de Datos Personales que sean presentados, promovidos o interpuestos ante el responsable de la Unidad de Transparencia del INCAFECH.	• Los mismos que hayan proporcionado las personas solicitantes al presentar sus solicitudes de datos personales o para el ejercicio de los derechos ARCO • Condición particular del titular (persona menor de edad, en estado de interdicción o incapacidad – sensible- o fallecida); • Datos y documentación proporcionados para acreditar la identidad • Documentos que se presenten en caso de que la persona titular de los datos personales sea menor de edad, se encuentre en estado de interdicción o incapacidad o haya fallecido (algunos de estos documentos podrían contener datos sensibles); • Lugar o medio para recibir notificaciones (cuenta de correo electrónico personal o domicilio particular); • Datos adicionales de contacto m(número telefónico de teléfono fijo o celular y cuenta de correo electrónico personal); • En caso de que así lo proporcione, lengua indígena que hable (sensible) y especificaciones de las preferencias de accesibilidad (lugar de estacionamiento para persona con discapacidad, acceso para perros guías o animales de apoyo, ayuda de lectura a documentos, etc. -sensibles); • En caso de que así lo proporcione y la solicitud para no cubrir el pago de derechos por concepto de costos de reproducción y gastos de envío

2026, "Año de Jaime Sabines Gutiérrez"

**UNIDAD DE TRANSPARENCIA.
UNIDAD DE APOYO JURIDICO**

			(sensible)], así como cualquier otro que las propias personas recurrentes incorporen de forma voluntaria en el texto de sus recursos de revisión en materia de datos personales o que obre en los documentos que adjunten al presentarlos, promoverlos o interponerlos.
Unidad de Apoyo Jurídico.	Recursos de revisión en materia de acceso a la información.	Remitir al Órgano Administrativo Desconcentrado denominado Transparencia para el Pueblo de Chiapas los recursos de revisión en materia de acceso a la información que sean presentados, promovidos o interpuestos ante el responsable de la Unidad de Transparencia del INCAFECH.	• Los mismos que hayan proporcionado las personas solicitantes al presentar sus solicitudes de acceso a la información • Domicilio particular, • Cuenta de correo electrónico personal y cualquier otro que las propias personas solicitantes incorporen de forma voluntaria en el texto de sus recursos de revisión en materia de acceso a la información o que obre en los documentos que adjunten al presentarlos, promoverlos o interponerlos.

5. LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES.

En cumplimiento con lo establecido en los artículos 27, fracción II, y 29 fracción II de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; los servidores públicos del Instituto que traten datos personales en el ejercicio de sus funciones y de las atribuciones del órgano administrativo a la que se encuentran adscritos observarán al menos las medidas de seguridad técnicas siguientes:

- 1.** Prevenir el acceso no autorizado al perímetro del órgano administrativo, sus instalaciones físicas, áreas críticas, recursos e información;
- 2.** Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas del órgano administrativo, recursos e información;
- 3.** Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir del órgano administrativo;
- 4.** Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.
- 5.** Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- 6.** Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- 7.** Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware;
- 8.** Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Adicionalmente, los servidores públicos del Instituto, al tratar datos personales, observarán las siguientes funciones y obligaciones:

- a).** Resguardar los datos personales a los que tenga acceso en el ejercicio de sus atribuciones.
- b).** Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos se encuentren actualizados.
- c).** Llevar un registro de los servidores públicos que accedan a los datos personales y llevar a cabo las acciones necesarias para la autenticación de los usuarios.
- d).** Mantener actualizada la relación de usuarios que traten datos personales.
- e).** En caso de presentarse algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, deberán informarlo al Responsable de la Unidad de Transparencia del Instituto.

- f).** Llevar a cabo permanentemente las medidas de seguridad de carácter administrativo, físico y técnico necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- g).** Atender los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.
- h).** Cumplir con la normatividad de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, garantizando la seguridad y confidencialidad de los datos.
- i).** Llevar a cabo las medidas de seguridad administrativas, técnicas y físicas para proteger los datos contra accesos no autorizados, pérdida, alteración o destrucción.
- j).** Responder a las solicitudes de derechos ARCO de forma eficiente y oportuna.
- k).** Actuar con transparencia y responsabilidad, asegurando que los datos sean exactos, completos, correctos y actualizados.
- l).** Proteger los datos contra accesos no autorizados, pérdida, alteración o destrucción y respetar la privacidad de los titulares.
- m).** Informar a los titulares sobre el tratamiento de sus datos mediante el aviso de privacidad, especificando las características principales del mismo, para que puedan tomar decisiones informadas.
- n).** Cumplir con todas las disposiciones legales en materia de protección de datos personales.
- o).** Mantener la seguridad de los datos personales durante en ejercicio de las funciones del puesto.
- p).** Respetar la privacidad del titular, obteniendo su consentimiento para el tratamiento de sus datos.
- q).** No tratar los datos de forma engañosa o fraudulenta y tratar los datos de forma transparente y honesta, evitando cualquier manipulación.
- r).** Mantener los datos personales completos, correctos y actualizados.
- s).** Tramitar las consultas, solicitudes y reclamos relacionados con el tratamiento de los datos.
- t).** No transferir datos personales salvo aquellas estrictamente necesarias para atender requerimientos de información de diversas autoridades fiscales, de seguridad social, fiscalizadoras, investigadoras, judiciales y administrativas.
- u)** Documentar roles y responsabilidades de las personas que tratan datos personales, así como la cadena de rendición de cuentas, según el sistema de gestión implementado. Esto

incluye la identificación de los perfiles de puesto y la definición de las responsabilidades de cada persona.

v). Poner a disposición del titular de los datos personales el aviso de privacidad previo iniciar el uso de los datos personales para la finalidad para la que se obtuvieron.

w). Ubicar el aviso de privacidad en un lugar visible, que facilite su consulta, con independencia del medio de difusión o reproducción que se utilice.

x). Notificar oportunamente cualquier incidente de seguridad.

Como resultado de la identificación de los procesos en los que intervienen datos personales, relacionado en el Inventario de Datos Personales, por las áreas que integran los órganos administrativos correspondientes al interior del Instituto, resulta importante definir estas actividades con las funciones y facultades establecidas en la normatividad interna, que otorga a las personas servidoras públicas responsables de dicho tratamiento; lo anterior, a fin de dar cumplimiento al principio de legalidad que debe atender todo servidor público.

Por lo anterior, a continuación, se ilustran las funciones otorgadas por el reglamento interior de este Instituto a quienes llevan a cabo tratamientos de datos personales

Órgano Administrativo	Órgano Administrativo Responsable	Tratamiento(s) o Proceso (s)	Nombre y Cargo de las Personas Servidoras Públicas que Tratan los Datos Personales
Unidad de Apoyo Administrativo	Área de Recursos Humanos	Lista de Asistencia.	Las áreas testadas son las que corresponden a los nombres de las personas servidoras públicas reserva en referencia al servidor público que tiene bajo su tutela la protección de los datos personales es para salvaguardar su seguridad en caso de que personas malintencionadas quieran tener acercamiento para obtener información que solo corresponde a la persona titular del derecho; se fundamenta en los artículos 103, fracción II, 112 fracción IV, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, vinculándose con el artículo Vigésimo Tercero de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.
		Comité de Ética.	
		Expediente Único Personal.	
		Nómina de Pago de Personal.	
		Declaración Patrimonial.	
		Control de Asistencia	
Unidad de Apoyo Jurídico	Responsable de la Unidad de Transparencia	Solicitudes de datos personales o para el ejercicio de los derechos ARCOP.	Las áreas testadas son las que corresponden a los nombres de las personas servidoras públicas reserva en referencia al servidor público que tiene bajo su tutela la protección de los datos personales es para salvaguardar su seguridad en caso de que personas malintencionadas quieran tener acercamiento para obtener información que solo corresponde a la persona titular del derecho; se fundamenta en los artículos 103, fracción II, 112 fracción IV, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, vinculándose con el artículo Vigésimo Tercero
		Solicitudes de acceso a la información dirigidas al Instituto del Instituto del Café de Chiapas.	
		Recursos de revisión en materia de datos personales.	

2026, "Año de Jaime Sabines Gutiérrez"

**UNIDAD DE TRANSPARENCIA.
UNIDAD DE APOYO JURIDICO**

		Recursos de revisión en materia de acceso a la información.	de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.
	Unidad de Apoyo Jurídico	Contratos, convenios.	Las áreas testadas son las que corresponden a los nombres de las personas servidoras públicas reserva en referencia al servidor público que tiene bajo su tutela la protección de los datos personales es para salvaguardar su seguridad en caso de que personas malintencionadas quieran tener acercamiento para obtener información que solo corresponde a la persona titular del derecho; se fundamenta en los artículos 103, fracción II, 112 fracción IV, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, vinculándose con el artículo Vigésimo Tercero de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.
		Demandas	

6. ANÁLISIS DE RIESGO.

Sección Clasificada del Documento de Seguridad, apartado del 6.

Análisis de riesgo y 7. Análisis de brecha.

Se testan los apartados números 6. Análisis de riesgo y 7. Análisis de brecha, en virtud que contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado y su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad; bajo este precepto se protege todo aquello que sirva para desactivar una amenaza antes de que se materialice; se fundamenta en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, vinculándose con el artículo Vigésimo Sexto primer párrafo, 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 6.

Análisis de riesgo y 7. Análisis de brecha.

Se testan los apartados números 6. Análisis de riesgo y 7. Análisis de brecha, en virtud que contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado y su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad; bajo este precepto se protege todo aquello que sirva para desactivar una amenaza antes de que se materialice; se fundamenta en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, vinculándose con el artículo Vigésimo Sexto primer párrafo, 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 6.

Análisis de riesgo y 7. Análisis de brecha.

Se testan los apartados números 6. Análisis de riesgo y 7. Análisis de brecha, en virtud que contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado y su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad; bajo este precepto se protege todo aquello que sirva para desactivar una amenaza antes de que se materialice; se fundamenta en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, vinculándose con el artículo Vigésimo Sexto primer párrafo, 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 6.

Análisis de riesgo y 7. Análisis de brecha.

Se testan los apartados números 6. Análisis de riesgo y 7. Análisis de brecha, en virtud que contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado y su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad; bajo este precepto se protege todo aquello que sirva para desactivar una amenaza antes de que se materialice; se fundamenta en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, vinculándose con el artículo Vigésimo Sexto primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

7. ANÁLISIS DE BRECHA.

Sección Clasificada del Documento de Seguridad, apartado del 6.

Análisis de riesgo y 7. Análisis de brecha.

Se testan los apartados números 6. Análisis de riesgo y 7. Análisis de brecha, en virtud que contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado y su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad; bajo este precepto se protege todo aquello que sirva para desactivar una amenaza antes de que se materialice; se fundamenta en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, vinculándose con el artículo Vigésimo Sexto primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

r

Sección Clasificada del Documento de Seguridad, apartado del 6.

Análisis de riesgo y 7. Análisis de brecha.

Se testan los apartados números 6. Análisis de riesgo y 7. Análisis de brecha, en virtud que contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado y su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad; bajo este precepto se protege todo aquello que sirva para desactivar una amenaza antes de que se materialice; se fundamenta en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, vinculándose con el artículo Vigésimo Sexto primer párrafo, 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 6.

Análisis de riesgo y 7. Análisis de brecha.

Se testan los apartados números 6. Análisis de riesgo y 7. Análisis de brecha, en virtud que contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado y su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad; bajo este precepto se protege todo aquello que sirva para desactivar una amenaza antes de que se materialice; se fundamenta en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, vinculándose con el artículo Vigésimo Sexto primer párrafo, 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 6.

Análisis de riesgo y 7. Análisis de brecha.

Se testan los apartados números 6. Análisis de riesgo y 7. Análisis de brecha, en virtud que contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado y su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad; bajo este precepto se protege todo aquello que sirva para desactivar una amenaza antes de que se materialice; se fundamenta en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, vinculándose con el artículo Vigésimo Sexto primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

8. PLAN DE TRABAJO.

Sección Clasificada del Documento de Seguridad, apartado del 8.

Plan de trabajo.

Se testan el apartado con numeral 8. Plan de trabajo, en virtud de que su contenido corresponde a las acciones a implementar derivado del análisis de riesgo y análisis de brecha, en el que se establecen las acciones específicas que este Instituto del Café de Chiapas implementará para corregir las deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de los datos personales; se fundamenta en 103, fracciones II y III, 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 primer párrafo, 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.

Plan de trabajo.

Se testan el apartado con numeral 8. Plan de trabajo, en virtud de que su contenido corresponde a las acciones a implementar derivado del análisis. de riesgo y análisis de brecha, en el que se establecen las acciones específicas que este Instituto del Café de Chiapas implementará para corregir las deficiencias, fortalecer controles y reducir los riesgos , identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de los datos personales; se fundamenta en 103, fracciones II y III, 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 primer párrafo, 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.

Plan de trabajo.

Se testan el apartado con numeral 8. Plan de trabajo, en virtud de que su contenido corresponde a las acciones a implementar derivado del análisis de riesgo y análisis de brecha, en el que se establecen las acciones específicas que este Instituto del Café de Chiapas implementará para corregir las deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de los datos personales; se fundamenta en 103, fracciones II y III, 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 primer párrafo, 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.

Plan de trabajo.

Se testan el apartado con numeral 8. Plan de trabajo, en virtud de que su contenido corresponde a las acciones a implementar derivado del análisis de riesgo y análisis de brecha, en el que se establecen las acciones específicas que este Instituto del Café de Chiapas implementará para corregir las deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de los datos personales; se fundamenta en 103, fracciones II y III, 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 primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

9. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

En cumplimiento con lo establecido en los artículos 27, fracción VII, y 29 fracción VI, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, con la finalidad de mantener un monitoreo y revisión de las medidas de seguridad, se llevarán a cabo de manera permanente las siguientes acciones:

1. El Responsable de la Unidad de Transparencia llevará un monitoreo del cumplimiento por parte de los servidores públicos que intervengan en las actividades detalladas en el Plan de trabajo.
2. Se mantendrá actualizado el inventario de datos personales y de los sistemas de tratamiento de los mismos.
3. El Área de Informática mantendrá monitoreados los esquemas de seguridad implementados para la infraestructura tecnológica, que permita garantizar conexiones seguras, tanto al exterior como en el interior del Instituto.
4. Para garantizar el cumplimiento de las políticas en materia de protección de datos personales establecidas en el presente documento, el mismo será publicado en el Portal de Transparencia del Instituto y se notificado a los servidores públicos que integran cada órgano administrativo, a través del Responsable de la Unidad de Transparencia.
5. Se llevarán a cabo diversas medidas de seguridad físicas para proteger el entorno de los datos personales y de los recursos involucrados en su tratamiento mediante las siguientes actividades:
 -) Prevenir el acceso no autorizado al perímetro del lugar en que se resguarden los datos Personales.
 -) Prevenir el daño o interferencia a las instalaciones, recursos e información que contenga datos personales.
 -) Proteger los recursos móviles y cualquier soporte físico o electrónico que pueda salir de las instalaciones del Instituto.
 -) Proveer a los equipos que contienen o almacenan datos personales, de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.
 -) Proteger los documentos físicos, conforme al desarrollo de las tareas que desempeñan o a las funciones que se les encomiendan.

6. SERÁN MONITOREADAS LAS SIGUIENTES ACCIONES:

-) La migración tecnológica.
-) La transferencia de información entre sujetos obligados y entre servidores públicos del Instituto.
-) Establecer medidas para limitar el acceso a los datos personales a personas autorizadas.
-) Verificar las políticas y procedimientos de protección de datos personales se estén aplicando correctamente.
-) Configurar las cuentas y perfiles con contraseñas robustas y cambiarlas frecuentemente, como un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.

7. Identificación, clasificación y borrado seguro de la información, el Instituto implementará mecanismos para identificar, clasificar, conservar y en su caso, eliminar de manera segura la información que contenga datos personales, atendiendo a las disposiciones legales y archivísticas aplicables. Asimismo, cuando se proceda la baja documental o eliminación de información, esta se realizará mediante mecanismos que garanticen su borrado o destrucción segura, de conformidad con las disposiciones en materia de archivos y protección de datos personales.

10. PROGRAMA GENERAL DE CAPACITACIÓN.

En cumplimiento con lo establecido en los artículos 27, fracción VIII, y 29 fracción VII, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, la aplicación del programa de protección de datos personales en el Instituto, requiere como un factor esencial, la formación y sensibilización de las personas que ahí laboran de tal forma que pueda garantizarse la actualización y mejora continua del inventario de datos personales, la observancia de la normatividad, 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 los siguientes temas:

TEMA			
Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.	Obligaciones en la Observancia de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.	El programa de protección de datos personales.	El principio de información: Avisos de Privacidad en el marco del programa de protección de datos personales.
CONTENIDO			
) Antecedentes) Principios.) Alcances.) Objetivos.) Implicaciones	) Deberes) Medidas de seguridad) Procedimientos y sanciones/Derechos ARCO.) Medios de defensa	) Sistema de datos personales.) Inventario y Base de datos.) Medidas de seguridad.) Análisis de brecha y riesgo.) Funciones y obligaciones	) Contenido: integral y simplificado.) Consentimiento) Deber de información.) Finalidades del tratamiento de los datos.