Con fundamento en el artículo 50 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas.

Documento de Seguridad

INSTITUTO DE COMUNICACIÓN SOCIAL Y RELACIONES PÚBLICAS
GOBIERNO DE CHIAPAS

Rudy Alberto Orozco Ruiz-Responsable de la Unidad de Transparencia
Ruth Jaqueline Serrano Alfaro-Área de Apoyo Jurídico y UT.

Introducción

El derecho de protección de datos personales surge después de la Segunda Guerra Mundial, a partir del reconocimiento de la dignidad humana y los derechos humanos referidos en el artículo 12 de la Declaración Universal de los Derechos Humanos del 10 de diciembre de 1948; artículo 11 de la Convención Americana de Derechos Humanos de 1996; artículo 17 del Pacto Internacional de Derechos Civiles y Políticos del 19 de diciembre; artículo 8 del Convenio Europeo de Derechos Humanos del 4 de noviembre de 1950 y la Carta de los Derechos Fundamentales de la Unión Europea suscrita en Niza el 7 de diciembre de 2000.

En México se reconoce el derecho a la protección de datos personales el 11 de junio de 2002 con publicación de la Ley Federal de Acceso a la Información Pública Gubernamental publicada y en 2009 se realizaron reformas constitucionales de los artículos 16 y 73 en las cuales otorgaron reconocimiento pleno a la protección de datos personales como un derecho fundamental y autónomo; sin embargo dicha legislación no garantizaba los derechos de acceso, rectificación, cancelación y oposición por lo que se requería también crear una ley de protección de datos personales para el sector privado. Es así como el Congreso de la Unión emitió y publicó el 05 de julio de 2010 la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y el 26 de enero de 2017 la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSP) para armonizar la normatividad y que ambas legislaciones específicas contengan las obligaciones, deberes, procedimientos, sanciones y recursos de la materia, tanto para el sector público como privado.

Una vez teniendo la normatividad federal, el 30 de agosto de 2017 se publica en el periódico oficial No.315 2ª sección, la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas dando las pautas para aplicar en todos los organismos públicos de la entidad. En este contexto, el 26 de enero de 2018 se publicaron los Lineamientos Generales de Protección de Datos Personales para el Sector Público en los que se establecen las obligaciones exigibles del derecho a la protección de datos personales en el sector público federal y todas las dependencias y entidades, así como partidos políticos tienen que llevar el tratamiento de los datos personales de las personas físicas conforme a lo normado.

Es por ello que los artículos 35 de la LGPDPPSO y 49 a 50 de la LPDPPSOCHIS establecen como obligación la elaboración de un documento de seguridad, que se define según la fracción XIV del artículo 3 de la LGPDPPSO y la fracción XIII del artículo 5 de la LPDPPSOCHIS como el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Por lo anterior, este Instituto de Comunicación Social y Relaciones Públicas en cumplimiento a las leyes de la materia, elaboró el presente documento de seguridad en el cual se encuentran redactados los objetivos, responsabilidades, alcances, atribuciones y desarrollo de la protección de los datos personales que utiliza y se presenta de la siguiente manera:

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

Contenido

Glosario

Áreas, unidades administrativas u órganos administrativos:	Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, así como en las estructuras orgánicas u organigramas, que poseen y tratan los datos personales.
Autenticidad:	Busca asegurar la validez de la información en tiempo, forma y distribución, así como garantizar el origen de la misma, validando a la persona emisora para evitar suplantación de identidades.
Autodeterminación informativa:	Es un derecho fundamental de toda persona, a través del cual ésta puede ejercer un conjunto de controles sobre sus datos personales cuando éstos se encuentran en posesión de los llamados responsables (sujetos obligados en el sector público y sujetos regulados en el sector privado). Este derecho le permite a la persona titular de los datos personales conocer y controlar qué datos de su persona han sido recabados, para qué finalidad o motivo, cuál será el uso específico que se les dará, cuál será la vigencia de su uso y quién es el responsable de su tratamiento (recolección, integración, uso, resguardo, etc.), con el objetivo de poder proteger su intimidad, evitando el uso ilícito e indiscriminado de su información personal, y tener la posibilidad de otorgar su consentimiento expreso, si así lo considera pertinente, para la cesión y transferencia de dichos datos a terceros.
Autorizar:	Se considera como el acceso que se le permite a la persona que se ha identificado y autenticado apropiadamente, lo cual depende del permiso o los permisos que le conceda el responsable de autorizar los accesos.
Aviso de privacidad:	Documento físico, electrónico o en cualquier otro formato generado por las áreas del ICOSORP a disposición de las personas a partir del momento en el cual se recaban sus datos

	personales, con el objeto de informarles sobre la existencia, propósitos y características principales del tratamiento al que serán sometidos dichos datos, a fin de que puedan tomar decisiones informadas al respecto.
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 datos personales:	La identificación y conservación de los datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación, supresión o eliminación en la base de datos o sistema de datos personales que corresponda.
Categorías de datos personales:	De manera enunciativa, más no limitativa: **Datos de identificación** (nombre, CURP, RFC, nacionalidad, firma, etc.) **Datos de contacto** (domicilio, número telefónico, correo electrónico, etc.) **Datos laborales** (puesto, domicilio oficial, correo institucional, etc.) **Datos patrimoniales** (cuentas bancarias, información crediticia, etc.) **Datos académicos** (formación académica y número de cédula profesional) **Datos sobre salud física y/o mental** (enfermedades o padecimientos) **Datos biométricos** (rostro, huella digital o dactilar, iris, retina, etc.) **Datos sensibles** (origen étnico o racial, religión, preferencia sexual, etc.) **Datos de naturaleza pública** (nombre de personas servidoras públicas)
Comité de Transparencia:	Instancia a la que hacen referencia los artículos 83 de la LGPDPPSO y 113 de la LPDPPSOCHIS, así como los artículos 43 de la Ley General de Transparencia y Acceso a la Información Pública y 62 al 63 de la Ley de Transparencia y Acceso a la

	Información Pública del Estado de Chiapas.
Consentimiento:	Manifestación de la voluntad libre, especifica e informada de la persona titular de los datos personales, mediante la cual se efectúa el tratamiento de éstos.
Control de acceso:	Medida de seguridad que permite el acceso únicamente a quien está autorizado para ello, una vez que se ha cumplido con el procedimiento de identificación y autentificación.
Datos personales:	Se trata de cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información como puede ser nombre, número de identificación, datos de localización, identificador en línea o uno o varios elementos de la identidad física, fisiológica, genética, psíquica, patrimonial, económica, cultural o social de la persona. Los datos personales pueden estar expresados de forma alfabética (letras), numérica (números), alfanumérica (letras y números), gráfica (imágenes) y acústica (sonido), etc.; como, por ejemplo: nombres y apellidos, edad, CURP o RFC, rostro y voz, etc.
Datos personales sensibles:	Se refiere a la información que pueda revelar aspectos íntimos de una persona, dar lugar a discriminación o que el uso indebido de la misma conlleve riesgos graves (origen racial o étnico, estado de salud física y/o mental, información genética, creencias religiosas, filosóficas y morales, opiniones políticas, preferencia sexual, entre otros).
Derechos ARCOP:	Derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales, todos ellos derechos humanos y fundamentales de rango constitucional.
Disociación:	El procedimiento mediante el cual los datos personales no pueden asociarse a la persona titular de los mismos ni permitir, por su estructura, contenido o grado de desagregación, la identificación de dicha persona.

Disponibilidad:	Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones, garantizando el acceso a la misma y a los recursos relacionados con ella, cada vez que se requiera.
Documentos o documentos de archivo:	Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas; o bien, cualquier otro registro que documente el ejercicio de las atribuciones, facultades y funciones de los sujetos obligados y las personas servidoras públicas adscritas a ellos, sin importar su fuente o fecha de elaboración. Dichos documentos podrán estar en cualquier tipo de soporte o medio existente, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico, o que se cree con posterioridad.
Documento de seguridad:	Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el ICOSORP para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.
Encargado:	La persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable.
Expediente:	Conjunto ordenado de documentos relacionados entre sí.
ICOSORP	Instituto de Comunicación Social y Relaciones Públicas.
Información:	Todo aquel conjunto organizado de datos que generan, obtiene, poseen o administran los sujetos obligados como consecuencia del ejercicio de sus atribuciones, facultades, competencias y funciones, cualquiera que sea su soporte y forma de expresión, los cuales se encuentran contenidos en documentos de archivo que generan, obtienen, adquieren, transforman o conservan por cualquier título.

ITAIPCH:	Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, el cual es el organismo garante local de dicha entidad federativa en materia de protección de datos personales en posesión de los sujetos obligados.
Integridad:	Garantizar la exactitud, totalidad y la confiabilidad de la información y los sistemas o métodos de procesamiento, de manera que éstos no puedan ser modificados sin autorización, ya sea accidental o intencionadamente.
Ley General o LGPDPPSO:	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Ley Local o Estatal o LPDPPSOCHIS:	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.
Lineamientos:	Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.
Medidas de seguridad:	Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.
Medidas de seguridad administrativas:	Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información o nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación 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 el hardware y el 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.
Oficial de Protección de Datos Personales:	Persona servidora pública especialista en protección de datos personales, adscrita a la Unidad de Transparencia, con suficiente jerarquía para implementar las disposiciones normativas en la materia al interior del sujeto obligado. Cabe precisar que la designación del Oficial de Protección de Datos Personales se encuentra prevista en una norma facultativa o potestativa, no imperativa, lo cual única y exclusivamente aplica tratándose de responsables que en el ejercicio de sus funciones sustantivas llevan a cabo tratamientos relevantes o intensivos, por lo que no es obligatorio ni necesario que todos los sujetos obligados cuenten con dicho Oficial, es opcional. La SESAECH no cuenta

	con esta figura en la actualidad.
Plataforma Nacional o PNT:	La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).
Principios y deberes:	**Calidad:** Los datos personales deben ser ciertos, exactos, completos, pertinentes, correctos y actualizados, en relación con la finalidad para la que fueron recabados. **Confidencialidad:** El responsable deberá establecer controles o mecanismos que permitan que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de que dichas personas finalicen su relación con el responsable. En cualquier caso, se deberá garantizar la secrecía y la no difusión de los datos personales sometidos a tratamiento. **Consentimiento:** Toda manifestación previa, de voluntad libre, específica, informada e inequívoca por la que la persona titular acepta, mediante declaración o acción afirmativa, el tratamiento de sus datos personales. **Finalidad:** El responsable está obligado a determinar las finalidades concretas, lícitas, explícitas y legítimas que motivan cada tratamiento de datos personales que efectúe, las cuales deberán ser acordes con las atribuciones, facultades y funciones que la normatividad aplicable le confiere y también deberán estar previstas en el aviso de privacidad que ponga a disposición de la persona titular de los datos personales. **Información:** El responsable deberá informar a la persona titular de los datos personales sobre la existencia y las características principales del tratamiento al que serán sometidos sus datos personales, a través del aviso de privacidad, a fin de que pueda tomar decisiones informadas al respecto. **Lealtad:** El tratamiento de los datos personales se realizará sin

	que medie dolo, engaño o medios fraudulentos, En todo momento el responsable debe privilegiar la protección de los intereses de la persona titular de los mismos y la expectativa razonable de privacidad, así como no vulnerar su confianza. **Licitud:** Todo tratamiento de datos personales efectuado por el responsable debe sujetarse a las atribuciones, facultades y funciones que la normativa aplicable le ha conferido. De conformidad con este principio, los datos personales deberán tratarse con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional. **Proporcionalidad:** El responsable tratará sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron y que se encuentren previstas en el aviso de privacidad. El responsable tendrá que realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios y limitar el periodo de tratamiento al mínimo indispensable. **Responsabilidad:** El responsable está obligado a implementar los mecanismos que considere convenientes para acreditar el cumplimiento de los principios rectores, deberes y obligaciones establecidas en la Ley, así como rendir cuentas sobre el tratamiento de datos personales en su posesión a la persona titular de los mismos y a las autoridades competentes. **Seguridad:** El responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.
Publicación:	La difusión en medios físicos o impresos y electrónicos o digitales de información contenida en documentos de archivo.
Remisión:	Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o

	fuera del territorio mexicano.
Responsable:	En el sector público son los "sujetos obligados" de las leyes de transparencia y acceso a la información (cualquier autoridad, dependencia, entidad, organismo u órgano de los poderes Ejecutivo, Legislativo y Judicial, así como los organismos u órganos autónomos, los fideicomisos y fondos públicos y los partidos políticos), excepto los sindicatos y las personas físicas y morales que reciban y ejerzan recursos públicos o que realicen o ejerzan actos de autoridad; mientras que en el sector privado son los llamados "sujetos regulados" (personas físicas y morales de carácter privado), excepto las sociedades de información crediticia en determinados supuestos y las personas físicas que lleven a cabo la recolección y almacenamiento de datos personales para uso exclusivamente personal y sin fines de divulgación o utilización comercial, los cuales deciden y determinan finalidades, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de los datos personales que poseen.
Responsable administrador o administrador responsable:	La persona servidora pública titular de un área, designada por la persona servidora pública titular del sujeto obligado, que decide sobre el tratamiento físico o automatizado de los datos personales en posesión del área, así como acerca del contenido y la finalidad de los sistemas de tratamiento o bases de datos personales con las que cuenta el área.
Responsable usuario:	La persona servidora pública que está autorizada para tratar datos personales.
Sistema(s) de tratamiento:	Todo conjunto organizado de archivos, registros, ficheros, bases o bancos de datos personales en posesión de alguna de las áreas del ICOSORP, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Existen dos tipos de sistemas de tratamiento:

	Físicos: Conjunto ordenado de datos que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos. **Automatizados:** Conjunto ordenado de datos que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.
Sujeto Obligado:	son sujetos obligados a transparentar y permitir el acceso a su información y proteger los datos personales que obren en su poder: cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en los ámbitos federal, de las Entidades Federativas y municipal.
Soportes físicos:	Los medios de almacenamiento identificables a simple vista, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados "a mano" o "a máquina", fotografías, placas radiológicas, carpetas y expedientes, entre otros.
Supresión:	La baja archivística de los datos personales conforme a la normatividad archivística vigente y aplicable, que resulta en la cancelación, eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.
Tecnología(s) de la información:	Se refiere al hardware y software operado por el sujeto obligado o por una tercera persona que procese información en su nombre, para llevar a cabo una función propia, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u cualquier otro tipo.

Titular:	La persona física a quien corresponden los datos personales, a ella pertenecen.
Transferencia:	Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado.
Transmisión de datos personales:	La entrega total o parcial de datos personales a cualquier persona distinta de la persona titular de los mismos, mediante el uso de medios físicos o electrónicos tales como la interconexión de equipos de cómputo o bases de datos y acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.
Transmisor:	Responsable que posee los datos personales objeto de la transmisión.
Tratamiento:	De manera enunciativa, mas no limitativa, cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, utilización, comunicación, difusión, almacenamiento, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de los mismos, hasta su cancelación, supresión o eliminación.
Unidad de Transparencia:	Instancia a la que hacen referencia los artículos 85 de la LGPDPPSO y 115 de la LPDPPSOCHIS, así como los artículos 45 de la Ley General de Transparencia y Acceso a la Información Pública y 67 al 69 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

Marco normativo

Para efectos del presente documento, la normatividad aplicable es la siguiente:

- Artículos 6, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM).

- Artículo 3 de la Constitución Política del Estado Libre y Soberano de Chiapas.

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS).

- Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (Lineamientos).

- Reglamento interior del Instituto de Comunicación Social y Relaciones Públicas del Estado de Chiapas.

Objetivo del documento de seguridad

El presente documento tiene por objeto ofrecer el marco de trabajo necesario para la protección de los datos personales en posesión del ICOSORP, como un medio para cumplir con las obligaciones que establecen la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS) y los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas que emitió el Pleno del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas (ITAIPCH), así como el resto de la normatividad que emane de dichos ordenamientos; estableciendo con ello los elementos y las actividades de gestión para la operación y control de los procesos que impliquen el tratamiento de los datos personales, a efecto de protegerlos de manera sistemática y continua, así como para promover la adopción de buenas prácticas.

A su vez, tiene los Objetivos específicos siguientes:

1.- Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del Instituto de Comunicación Social y Relaciones Públicas.

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 maneras sistemática y continua.

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 tratamiento específicos.

Responsabilidades dentro del Programa

Con fundamento en lo dispuesto por los artículos 83 de la LGPDPPSO, 113 y 114 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. Aprobar, supervisar y evaluar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la presente Ley y demás disposiciones que resulten aplicables en la materia.

II. Coordinar, realizar y supervisar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en las que resulten aplicables en la materia, en coordinación con el oficial de protección de datos personales, en su caso.

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

IV. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se declare improcedente, por cualquier causa, el ejercicio de alguno de los derechos ARCO.

V. 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.

VI. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.

VII. Coordinar el seguimiento y cumplimiento de las resoluciones emitidas por el Instituto.

VIII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales.

IX. Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales.

Anualmente se presentará un informe, en el primer trimestre (a finales del mes de marzo) 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 las unidades administrativas.
- ✓ 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
- ✓ Los resultados de las revisiones por parte del Órgano Garante.

Para que los objetivos planteados en la primera sección se logren con éxito, el Programa requiere del apoyo e impulso directo del más alto nivel de la Institución. En ese sentido, el Programa se deberá hacer del conocimiento del Director General, a fin de que tome las medidas necesarias para que el mismo se observe en Instituto de Comunicación Social y Relaciones Públicas.

La intervención del Director General tendrá la finalidad única de impulsar la debida implementación del Programa al interior del sujeto obligado, pero no podrá suplir ni afectar las funciones que otorgan los artículos 113 y 114 de la LPDPPSO de Chiapas al Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la institución.

Así mismo, para que la implementación del programa tenga como resultado el cumplimiento integral de las obligaciones que establece la LPDPPSO de Chiapas y los Lineamientos correspondientes, el programa será de observancia obligatoria para todos los servidores públicos del sujeto obligado que en el ejercicio de sus funciones traten datos personales.

Alcances del Programa

El presente programa aplicará a todas las unidades administrativas 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.

Se cubrirán todos los principios, deberes y obligaciones de la LPDPPSO:

Artículo 12.- En todo tratamiento de datos personales, el responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

Artículo 13.- El responsable deberá tratar los datos personales en su posesión con estricto apego y cumplimiento de lo dispuesto por la presente Ley, la legislación mexicana que resulte aplicable y, en su caso, el derecho internacional, respetando los derechos y libertades del titular; debiendo para tales efectos sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

Artículo 14.- Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, explícitas, lícitas y legítimas, relacionadas con las atribuciones expresas que la normatividad aplicable le confiera.

Para efectos de la presente Ley, se entenderá que las finalidades son:

I. Concretas: Cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que sea posible la existencia de finalidades genéricas que puedan confundir al titular.

II. Explícitas: Cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad, y;

III. Lícitas y legítimas: Cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones expresas del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable.

Las Unidades Administrativas involucradas son:

A. Unidad de Apoyo Administrativo y Servicios
B. Área de Recursos Financieros
C. Área de Apoyo Jurídico y Unidad de Transparencia

Sistema de Gestión de los datos personales

El sistema de gestión es la herramienta que garantiza el tratamiento de los datos personales que ICOSORP lleva a cabo como parte del ejercicio de sus atribuciones, facultades y funciones, desde su obtención, uso, registro, organización, conservación, utilización, comunicación, difusión, almacenamiento, acceso, manejo, aprovechamiento, divulgación, transferencia, remisión o disposición de los mismos, hasta su cancelación, supresión o eliminación; o bien, cualquier otra operación correspondiente, para lo cual se establecen políticas y métodos orientados a salvaguardar la confidencialidad, integridad y disponibilidad de tales datos, de conformidad con lo previsto en la LGPDPPSO y en la LPDPPSOCHIS, así como en los Lineamientos.

Es por ello que se realizó un proceso de organización y planeación de los medios para la protección de datos, considerando las facultades y atribuciones de los órganos administrativos de este Instituto y, en consecuencia, realizan o efectúan tratamientos de datos personales. A través de un diagnóstico con formatos entregados a cada órgano administrativo que conforma el ICOSORP, se obtuvo el inventarios de datos personales y de los sistemas de tratamiento o bases de datos personales que tienen bajo de su responsabilidad, considerando lo establecido en la fracción III de los artículos 33 de la LGPDPPSO y 47 de la LPDPPSOCHIS, en este trabajo en coordinación, se identificaron la categoría y el tipo de datos usados en cada tratamiento, incluyendo los de carácter sensible, así como los medios a través de los cuales se obtienen dichos datos; el sistema físico 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 las personas servidoras públicas que tienen acceso a los datos, además de si son objeto de transferencias y la identificación de los receptores de los mismos, así como las causas que lo justifican.

Todo lo anterior ha contribuido para la consideración del ciclo de vida de los datos personales, entendiendo que, una vez concluida la finalidad, 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 ICOSORP.

A partir de la información recolectada de los datos personales y su forma de tratamiento en cada área de este Instituto, se procedió a elaborar la metodología para el análisis de riesgos, con el objetivo de identificar el valor de los datos personales y su ciclo de vida, así como el valor de exposición y las consecuencias para las personas titulares de los datos, por el uso indebido o posible vulneración de riesgo a los que podrían exponerse; así mismo se prevé identificar la brecha entre las medidas de seguridad existentes y las medidas de seguridad faltantes para que se garantice la seguridad de los datos personales en posesión de este Sujeto Obligado. Esto ayudará a prevenir posibles debilidades en la seguridad de los datos y las áreas de oportunidad, aun cuando no haya existido un daño real, mediante la identificación de la ineficiencia de los controles de acceso físico 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 y de seguimiento y monitoreo 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 los siguientes tipos:

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

El riesgo que puede presentarse en caso de que las amenazas señaladas detonen las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada comprometiendo su confidencialidad, disponibilidad e integridad; en este sentido, las medidas de seguridad por parte de cada órgano administrativo del ICOSORP están orientadas a proteger los datos personales. Por lo anterior, este Instituto implementará para su protección las siguientes acciones:

- ✓ Los datos personales serán tratados conforme a lo establecido en la normatividad vigente.
- ✓ Identificar a las personas servidoras públicas responsables del tratamiento de los datos personales.
- ✓ Los tratamientos de datos personales estén sujetos al principio de consentimiento siempre que la Ley lo permita.
- ✓ Responder al principio de información a las personas titulares de los datos personales sobre la existencia, propósitos y características principales del tratamiento al que serán sometidos dichos datos, a fin de que puedan tomar decisiones informadas al respecto.
- ✓ Procurar la actualización y pertinencia de los datos personales.
- ✓ Procurar la supresión de los datos personales cuando haya concluido el proceso para el que fueron obtenidos
- ✓ Sujetar el tratamiento de los datos personales a las finalidades para las que fueron obtenidos y que sean estrictamente los necesarios para las finalidades por las cuales se obtuvieron.
- ✓ Obtener datos personales a través de medios legales, con respeto a la expectativa razonable de privacidad de la persona titular de los mismos.
- ✓ Velar por el cumplimiento de los principios, deberes y obligaciones, estableciendo y manteniendo medidas de seguridad y de confidencialidad durante el ciclo de vida de los datos personales, en estricto respeto de los derechos de las personas a quienes pertenecen.
- ✓ Mantener actualizado el inventario de datos personales y de los sistemas de tratamiento o bases de datos personales en posesión del ICOSORP.

Con la finalidad de logar la salvaguarda de los derechos a la privacidad y a la protección de los datos personales, se han determinado las líneas de acción para el personal encargado de tratamiento de datos, con el propósito de generar mecanismos para el resguardo adecuado, actuando en apego a lo establecido en la LGPDPPSO y en la LPDPPSOCHIS, así como en los Lineamientos establecidos en la materia.

Inventario de datos personales y de los sistemas de tratamiento o bases de datos personales.

La fracción III de los artículos 33 de la LGPDPPSO y 47 de la LPDPPSOCHIS establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de los datos personales, la elaboración de un inventario de datos personales y de los sistemas de tratamiento o bases de datos personales.

De acuerdo con la fracción I del artículo 35 de la LGPDPPSO y las fracciones I y IV del artículo 50 de la LPDPPSOCHIS, dicho inventario forma parte del documento de seguridad y se basa un diagnóstico realizado por cada una las áreas que efectúan tratamientos de datos personales en ejercicio de sus atribuciones, facultades o funciones. El diagnóstico en mención contiene información básica de cada tratamiento de datos personales que se realiza en la SESAECH.

Por inventario de datos personales se entenderá el control documentado que se llevará de los tratamientos que realizan las áreas de la Secretaría Ejecutiva, realizado con orden y precisión. Sobre el particular, los artículos 53 y 54 de los Lineamientos establecen lo siguiente:

Inventario de datos personales.

> *Artículo 53.- Con relación a lo previsto en el artículo 47, fracción III, de la Ley Estatal, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:*
>
> *I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;*
>
> *II. Las finalidades de cada tratamiento de datos personales;*
>
> *III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;*
>
> *IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;*
>
> *V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;*

VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y

VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

Ciclo de vida de los datos personales en el inventario.

Artículo 54.- Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:

I. La obtención de los datos personales;

II. El almacenamiento de los datos personales;

III. El uso de los datos personales conforme a su acceso, manejo, (SIC)

IV. Aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin; (SIC)

V. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;

VI. El bloqueo de los datos personales, en su caso, y

VII. La cancelación, supresión o destrucción de los datos personales.

Por lo anterior, el ICOSORP realizó los inventarios de los tratamientos de datos personales que realizan los órganos administrativos, identificados de acuerdo a lo establecido en el artículo 50 de la LPDPPSOCHIS y 53 de los Lineamientos, basado en el ciclo de vida de los datos personales, tal como lo requiere el artículo 54 de ésta última norma.

No.	Órgano Administrativo	Número de inventarios	Sistemas de tratamiento o base de datos personales
1	Unidad de Apoyo Administrativo y Servicios	3	1.- Complemento del Expediente Único de Datos Personales 2.- Datos Biométricos Huella Dactilar y Rostro. 3.- Proceso de Integración de solicitudes de pago a proveedores.
2	Área de Recursos Financieros	2	1.- Elaboración de contratos y subsecuente trámite de pago para personas físicas. 2.- Elaboración de contratos y subsecuente trámite de pago para personas morales.
3	Área de Apoyo Jurídico	2	1.- Unidad de Transparencia. 2.- Cursos de capacitación
Total		**7**	

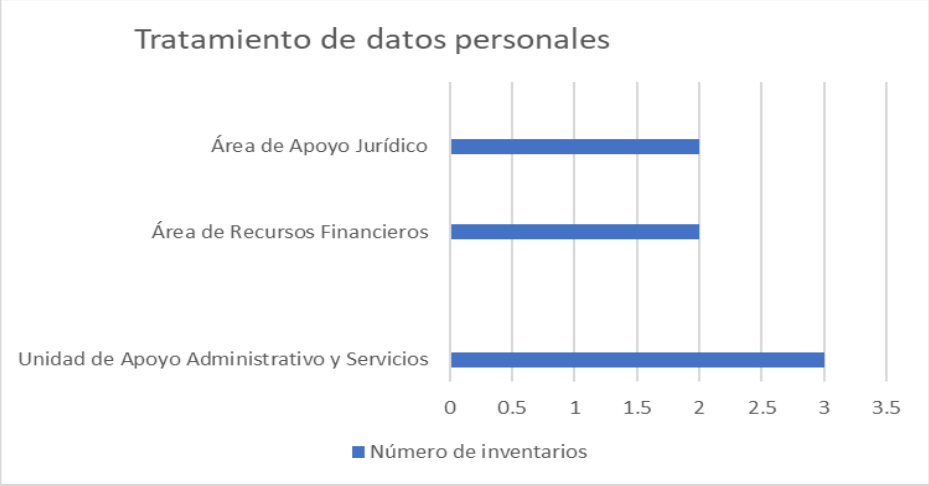
Como resultado del proceso de análisis realizado, se logró identificar que las áreas del ICOSORP que efectúan tratamientos de datos personales en ejercicio de sus atribuciones, facultades y funciones según lo establecido en el decreto de creación, reglamento interior, manual de procedimientos de este Instituto; son la Unidad de Apoyo Administrativo y Servicios, el área de recursos financieros y el área de apoyo jurídico.

En consecuencia, se hace mención de los datos personales identificados, de la siguiente manera:

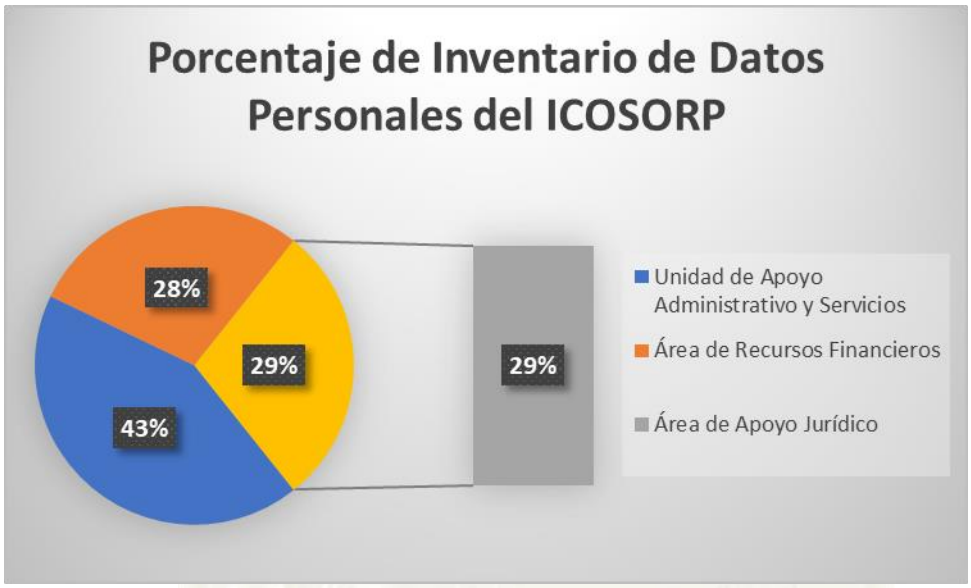
Tipo de datos	Datos personales
De identificación o identificativos	Nombre, apellido, sexo, nacionalidad, año y lugar de nacimiento, edad, firma autógrafa, clave única de registro de población (CURP), Registro Federal de Contribuyentes (RFC), domicilio particular, número telefónico, correo electrónico, datos personales

	contenidos en la identificación oficial, acta de nacimiento.
Laborales	Curriculum vitae
Patrimoniales	Número de cuenta bancaria, CLABE interbancaria, Cotización, Opinión de cumplimiento de obligaciones, constancia de no adeudos fiscales, registro al padrón de proveedores, acta constitutiva y sus modificaciones (para personas morales), poder legal del representante legal.
Biométricos	Rostro, huella dactilar y firma autógrafa.
Sensibles	Salud, tipo de religión, estado civil.

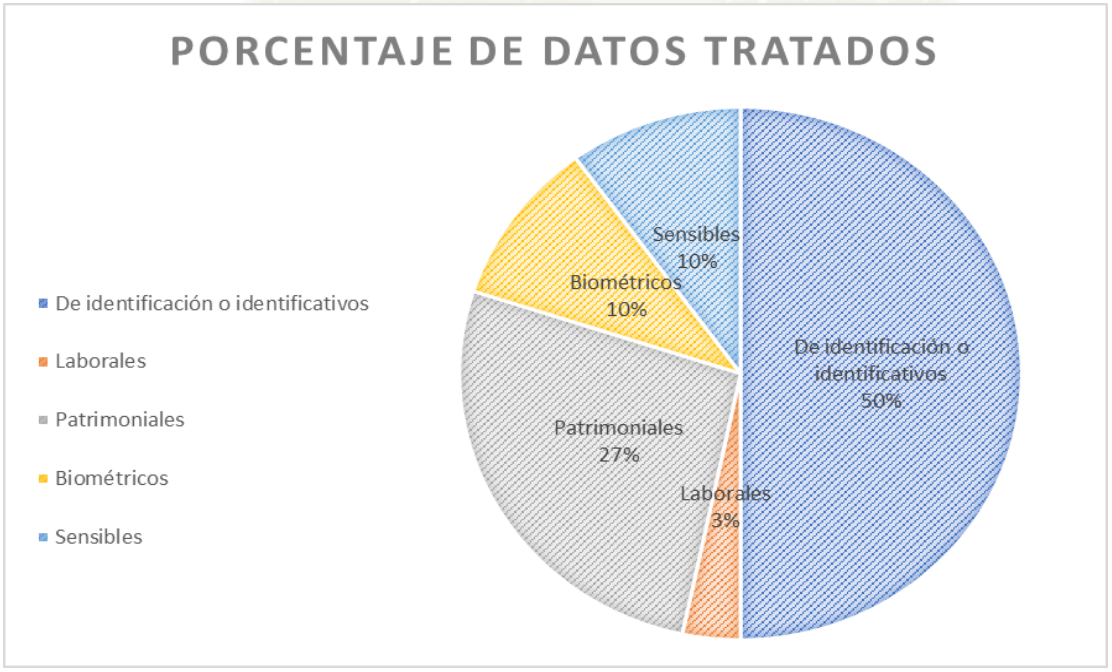
Los datos personales citados anteriormente son utilizados en los siete avisos de privacidad que utilizan las áreas, tres de la Unidad de Apoyo Administrativo y Servicios, dos del área de recursos financieros y dos del área de apoyo jurídico considerando la naturaleza de sus funciones, actividades y atribuciones que le son conferidas a través del marco normativo que rige a este Instituto.



La unidad de apoyo administrativo y servicios es el órgano administrativo que solicita y resguarda datos sensibles, así como datos biométricos para llevar a cabo el registro de asistencia tanto entrada como salida de sus labores.

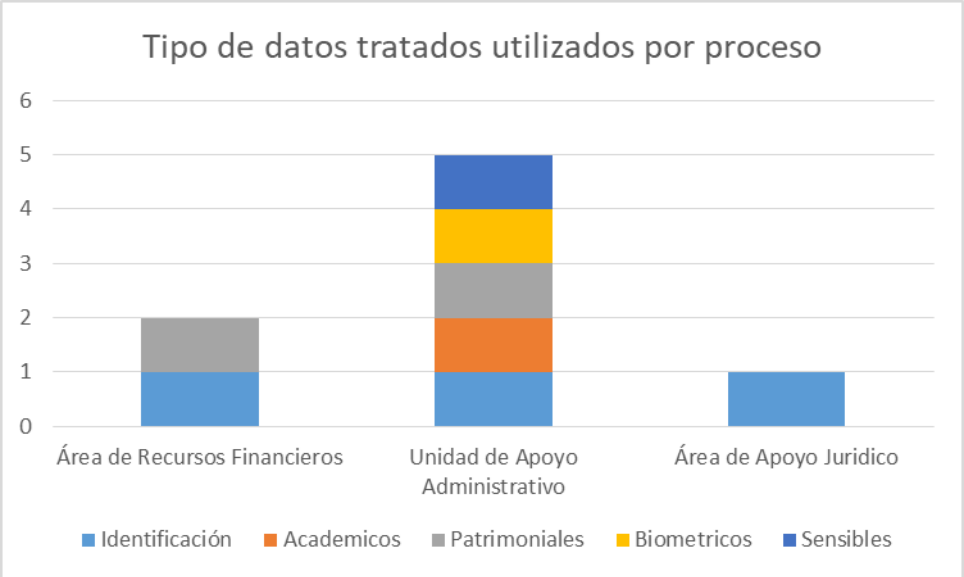


Referente a los tipos de datos que utiliza cada área que conforma el ICOSORP, se estima que el 50% son datos de identificación o identificativos, el 27% son datos patrimoniales, el 10% son datos sensibles, otro 10% son datos biométricos y el 3% son datos laborales que se recaban para el tratamiento correspondiente a cada órgnao administrativo.



El área que recaba mayores datos personales es la Unidad de Apoyo Administrativo y Servicios (UAAyS) por parte de lo que refiere a la plantilla de personal y por el cual se crea el aviso de privacidad de complemento de expediente Único de Datos Personales así mismo es el órgano administrativo que recaba Datos Biométricos Huella Dactilar y Rostro para el registro de asistencia a la platilla de personal en cumplimiento a lo establecido en el artículo 17 del reglamento interior del Instituto de Comunicación Social y Relaciones Públicas.

De lo anterior se desprende también que el área de recursos financieros utiliza datos de identificación y patrimoniales para poder elaborar los contratos y/o convenios correspondientes, así como el pago correspondiente por el tipo de servicio contratado. Esto se puede apreciar gráficamente en la siguiente gráfica.



Es importante mencionar que los datos personales recabados se hacen por medio de correo electrónico, vía telefónica, escrito o formato presentado directamente en esta Institución. Es por ello que el inventario de datos personales y de los sistemas de tratamiento o base de datos personales de este Instituto de Comunicación Social y Relaciones Públicas, a partir de la información que procesa cada órgano administrativo, se integra como un elemento del sistema de gestión de datos personales que representa junto con las medidas de seguridad, un instrumento útil para la implementación de las medidas correspondientes en materia de protección de datos personales.

Por lo anteriormente descrito, el inventario de datos personales y de los sistemas de tratamiento o bases de datos personales del ICOSORP se consolida como un elemento más de la política implementada para la observancia de la LGPDPPSO, de la LPDPPSOCHIS y de los Lineamientos, dando certeza a todas las personas titulares de los datos personales sobre el destino de sus datos recabados por este sujeto obligado. Es así que de conformidad con lo dispuesto en el artículo 50 de la LPDPPSOCHIS, este documento de seguridad contiene:

I. El nombre de los sistemas de tratamiento o base de datos personales.

II. El nombre, cargo y adscripción del administrador de cada sistema de tratamiento y/o base de datos personales.

III. Las funciones y obligaciones del responsable, encargados y todas las personas que traten datos personales.

IV. El inventario de los datos personales tratados en cada sistema de tratamiento y/o base de datos personales.

V. La estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan.

VI. Los controles y mecanismos de seguridad para las transferencias, que en su caso, se efectúen.

VII. El resguardo de los soportes físicos y/o electrónicos de los datos personales.

VIII. Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales.

IX. El análisis de riesgos.

X. El análisis de brecha.

XI. La gestión de vulneraciones.

XII. Las medidas de seguridad físicas aplicadas a las instalaciones.

XIII. Los controles de identificación y autenticación de usuarios.

XIV. Los procedimientos de respaldo y recuperación de datos personales.

XV. El plan de contingencia.

XVI. Las técnicas utilizadas para la supresión y borrado seguro de los datos personales.

XVII. El plan de trabajo.

XVIII. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y

XIX. El programa general de capacitación.

Sin embargo, las funciones del administrador y usuario responsable que se consideran en este instrumento, son las estrictamente concernientes al tratamiento de los datos personales o la finalidad para la cual fueron recabados y las obligaciones que consideran son exclusivamente las tienen que ver con el tratamiento de los datos personales, es decir las establecidas en las fracciones descritas en líneas anteriores.

NOTA: Para todos los sistemas de tratamiento o bases de datos personales aplica lo siguiente:

El acceso a la persona titular de los datos personales se dará en todo momento, por sí o a través de su representante, mediante escrito libre presentado ante la Unidad de Transparencia del ICOSORP, ubicado en Boulevard Andrés Serra Rojas 1090, Anexo 2B Torre Chiapas, Colonia Paso Limón, C.P. 29045, Tuxtla Gutiérrez, Chiapas, México; a través del Sistema de Solicitudes (SISAI) de la Plataforma Nacional de Transparencia (PNT, en adelante) [http://www.plataformadetransparencia.org.mx], en la sección denominada "Solicitudes", así como vía correo electrónico dirigido a icosorp@transparencia.chiapas.gob.mx o bien, mediante cualquier otro medio que al efecto establezca o apruebe el Pleno del ITAIPCH, conforme a lo establecido en el Título Tercero de la LGPDPPSO y la LPDPPSOCHIS.

El acceso, rectificación, cancelación, oposición y portabilidad de los datos personales se podrá solicitar en todo momento. Las solicitudes de datos personales o para el ejercicio de los derechos ARCOP serán analizadas por las áreas competentes, a fin de determinar la procedencia de dichos requerimientos, de acuerdo con lo previsto en los artículos 52 de la LGPDPPSO y 78 de la LPDPPSOCHIS.

Asimismo, que las personas que ejerzan dichos derechos tienen derecho a presentar un recurso de revisión ante el ITAIPCH cuando no estén conformes con la respuesta a su solicitud, lo cual podrán hacerlo a través de la propia PNT por sí mismas o a través de su representante y dentro de un plazo que no podrá exceder de quince días hábiles contados a partir del siguiente a la fecha de la notificación de la respuesta o a la fecha en que haya vencido el plazo para dar respuesta, en la sección y opción denominadas "Quejas de respuestas" y "Queja", respectivamente; o bien, de presentarse alguna inconsistencia podrán enviar su recurso de revisión a la cuenta oficial de correo electrónico recursosderevision@itaipchiapas.org.mx o presentarlo por escrito directamente en las instalaciones del ITAIPCH o ante la Unidad de Transparencia del ICOSORP, la cual lo canalizará al ITAIPCH al día hábil siguiente de haberlo recibido, ya que es la autoridad facultada para sustanciarlo y resolverlo. Para más información, las personas interesadas podrán consultar la dirección electrónica www.itaipchiapas.org.mx o comunicarse a los números telefónicos 9616112346 y/o 9615500760 del organismo garante local del estado de Chiapas.

Las personas que deseen conocer el procedimiento para el ejercicio de estos derechos podrán acudir a la Unidad de Transparencia del ICOSORP. Las transferencias de los datos personales se darán únicamente entre responsables, como se señala en el glosario del presente documento, de acuerdo con los trámites respectivos.

La remisión de los datos personales se dará únicamente entre el responsable y los encargados (personas físicas o morales, privadas o públicas, con las que se contrate), de acuerdo con los trámites correspondientes.

Funciones y obligaciones de las personas que tratan datos personales

La fracción II de los artículos 33 de la LGPDPPSO y 47 de la LPDPPSOCHIS establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de los datos personales, la definición de las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

> ***Artículo 33.*** *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. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*
> *VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;*
> *VII. 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*
> *VIII. 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.*

> ***Artículo 47.-*** *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable en la medida de sus posibilidades 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 los datos personales y/o 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. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.*
> *VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.*
> *VII. 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*
> *VIII. Diseñar y aplicar diferentes niveles de capacitación de su personal, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales*

De acuerdo con las funciones y obligaciones de las personas que traten datos personales establecidas en la fracción II del artículo 35 de la LGPDPPSO y la fracción III del artículo 50 de la LPDPPSOCHIS, este elemento informativo también forma parte del documento de seguridad.

Sobre el particular, el artículo 52 de los Lineamientos establece lo siguiente:

> *Artículo 52.- Con relación a lo dispuesto en el artículo 47, fracción II, de la Ley Estatal, el responsable deberá establecer y documentar los roles y*

responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.

El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.

Siendo así que el inventario de datos personales y de los sistemas de tratamiento o bases de datos personales contienen información donde se identifican las personas que intervienen en el tratamiento de cada uno de los datos personales, como se presenta a continuación:

Área de adscripción	Cargo de la persona que trata los datos personales	Funciones
Unidad de Apoyo Administrativo y Servicios	Analista G	-Elaboración del expediente único de personal. - Realizar y supervisar las altas, bajas, modificación de salarios, así como el cálculo de las cuotas obrero patronal ante del Instituto Mexicano del Seguro Social
Unidad de Apoyo Administrativo y Servicios	Jefa de Unidad	Supervisar la correcta administración y aplicación del presupuesto autorizado al Instituto para el cumplimiento de las metas establecidas. Supervisar el funcionamiento de la estructura organizacional y la aplicación de los instrumentos de organización de trabajo para el cumplimiento de los objetivos del Instituto. Supervisar y coordinar la integración del anteproyecto de presupuesto de egresos y la cuenta pública del Instituto para su

		presentación ante la instancia normativa correspondiente.
Unidad de Apoyo Administrativo y Servicios	Enlace D	Realizar y supervisar las altas, bajas, modificación de salarios, así como el cálculo de las cuotas obrero patronal ante INFONAVIT.
Unidad de Apoyo Administrativo y Servicios	Auxiliar administrativo C	Controlar la asistencia del personal de acuerdo a las políticas y lineamientos establecidos por la Secretaría de Hacienda y la Unidad de Apoyo Administrativo y Servicios.
Unidad de Apoyo Administrativo y Servicios	Analista G	Elaborar requisiciones de compras y solicitudes de pago de las adquisiciones realizadas a los proveedores, y compras directas ante el comité de adquisiciones de la Secretaria de Hacienda.
Área de recursos financieros	Jefe de Área	Solicitar la documentación legal de los prestadores de servicio para su contratación.
Área de recursos financieros	Auxiliar administrativo C	Revisión de la documentación legal presentada por los prestadores de servicios
Área de recursos financieros	Analista G	Elaboración de contratos de prestadores de servicios.
Área de recursos financieros	Analista D	Elaboración de órdenes de pago y trámite ante la secretaria de hacienda para su pago correspondiente.
Área de Apoyo Jurídico	Asesor Jurídico	Responsable de la Unidad de Transparencia.
Área de Apoyo Jurídico	Analista G	Responsable de atender las obligaciones en materia de transparencia, capacitaciones, oficial de datos personales.

Análisis de riesgos, análisis de brecha y plan de trabajo

De acuerdo a lo establecido en la fracción IV, V y VI de los artículos 33 de la LGPDPPSO y 47 de la LPDPPSOCHIS establecen como actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la realización de los análisis de riesgos y de brecha, así como un plan de trabajo. En ese sentido, los lineamientos para la protección de datos personales también lo establecen a través de los artículos 55, 56 y 57.

Por lo anterior se recurre a las disposiciones de los artículos 32 de la LGPDPPSO y 46 de la LPDPPSOCHIS que a la letra dicen:

Artículo 32. *Las medidas de seguridad adoptadas por el responsable deberán considerar:*

I. El riesgo inherente a los datos personales tratados;

II. La sensibilidad de los datos personales tratados;

III. El desarrollo tecnológico;

IV. Las posibles consecuencias de una vulneración para los titulares;

V. Las transferencias de datos personales que se realicen;

VI. El número de titulares;

VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y

VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Artículo 46.- Las medidas de seguridad adoptadas por el responsable deberán considerar:

I. El riesgo inherente a los datos personales tratados.

II. La sensibilidad de los datos personales tratados.

III. El desarrollo tecnológico.

IV. Las posibles consecuencias de una vulneración para los titulares.

V. Las transferencias de datos personales que se realicen.

VI. El número de titulares, y

VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento.

Resultado de los trabajos coordinados con las unidades administrativas que recaban y utilizan los datos personales para el ejercicio de sus funciones, le localizaron que se trabaja con quince datos de identificación, uno laboral, ocho patrimonial, tres biométricos y tres datos sensibles.

Por lo tanto, al realizar el análisis de riesgos que existen en el tratamiento por el que son sometidos los datos anteriormente mencionados, este Instituto cuida la integridad de las personas titulares de los datos personales considerando las amenazas y vulnerabilidades a las que éstos podrían estar expuestos; por ello se consideran medidas de seguridad físicas, técnicas y administrativas para su protección; garantizando la confidencialidad, integridad y disponibilidad de los datos personales en posesión de este sujeto obligado (ICOSORP).

De lo anterior, se desprende que las amenazas a las que se exponen los datos personales fueron consideradas de acuerdo a los análisis de riesgos vinculados con el cumplimiento de obligaciones normativas en materia de protección de datos y por el inventario de tratamientos de datos personales.

Para el desarrollo del análisis, se consideraron los siguientes cuatro tipos de amenazas previstas en la legislación:

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

Considerando una probabilidad baja, media o alta de que la amenaza suceda en las distintas etapas de vida y tipos o categorías de datos personales. Además, se tomó en cuenta la consecuencia desfavorable que podría sufrir la persona titular de los datos en caso de vulneración, la cual que puede ser leve, moderada o grave.

En cuanto a la valoración del riesgo por el tipo de dato en cada proceso en el que las áreas del ICOSORP tratan datos personales, aplicando la metodología indicada por el organismo garante y especializado del estado, se utilizó una escala del 1 al 3, representándose de la siguiente forma:

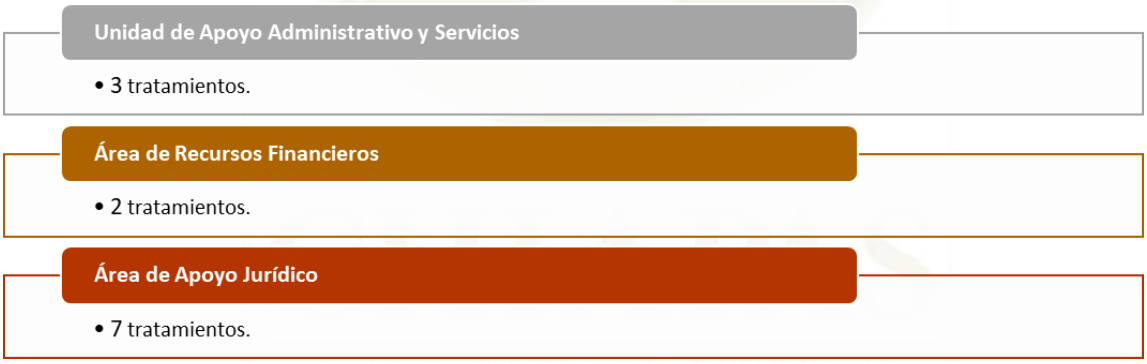
Tipo de dato	Riesgo inherente	Nivel de riesgo
Datos identificativos	Bajo	1
Datos laborales, patrimoniales y de procedimientos administrativos	Medio	2
Datos sensibles	Alto	3

Esto es, se tomó en consideración la probabilidad baja, media o alta de que la amenaza suceda en las distintas etapas de vida de los datos personales. Así, se consideró también la consecuencia desfavorable leve, moderada o grave que a la persona titular provoca en caso de que la amenaza ocurra (impacto).

Una vez determinados los riesgos y las medidas de seguridad necesarias para mitigarlos, se realizó el análisis de brecha, que consistió en identificar cuáles son las medidas técnicas, físicas y administrativas que hace falta implementar a partir de aquéllas definidas como necesarias.

Análisis de la información

Como resultado de la realización de los análisis de riesgos y de brecha, se identificó que el ICOSORP cuenta con tres unidades administrativas en las que tienen lugar tratamientos de datos personales para el desarrollo de 07 procesos, como se ilustra a continuación:



Plan de trabajo

De acuerdo a lo establecido en el artículo 33, fracción VI de la LGPDPPSO y referente al análisis de brecha, es importante generar las acciones que permitan la seguridad de la información, así como de su localización, para resolver de manera eficaz el acceso, rectificación, corrección u oposición de las personas titulares de la información; por lo que a continuación se presentan las actividades que este Instituto realizará:

- ✓ Reuniones de trabajo con las unidades administrativas para identificar nuevas amenazas o riesgos de perdida de información, para que, a su vez, se identifiquen alternativas de solución en los tres ámbitos que señala la ley de la materia, administrativo, físico y técnico.
- ✓ Fortalecer los mecanismos de control de seguridad de la información en las unidades administrativas para evitar posibles vulneraciones.

Mecanismos de monitoreo y revisión de las medidas de seguridad

La fracción VII de los artículos 33 de la LGPDPPSO y 47 de la LPDPPSOCHIS establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

De acuerdo con la fracción VI del artículo 35 de la LGPDPPSO y la fracción XVIII del artículo 50 de la LPDPPSOCHIS, los mecanismos de monitoreo y revisión forman parte del documento de seguridad.

Al respecto, el artículo 58 de los Lineamientos prevé lo siguiente:

Monitoreo y supervisión periódica de las medidas de seguridad implementadas.

> *Artículo 58.- Con relación al artículo 47, fracción VII, de la Ley Estatal, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.*

Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:

I. Los activos que se incluyan en la gestión de riesgos;

II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;

III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;

IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;

V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y

VII. Los incidentes y vulneraciones de seguridad ocurridas.

De lo anterior es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer, a través de un ciclo de mejor continua, la protección de los datos personales que resguarda el ICOSORP

A continuación, se describen las medidas de seguridad y se desarrollan las acciones de monitoreo y supervisión periódica:

[redacted]

Se testa el área que observa mayor estado de vulnerabilidad y riesgo de los datos personales que trata, con fundamento en lo dispuesto en las fracciones V y VII de los artículos 113 de la *Ley General de Transparencia y Acceso a la Información Pública* (LGTAIP) y 136 de la *Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas* (LTAIPCHIS), así como los numerales vigésimo tercero y vigésimo sexto de los *Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas*.

Programa General de Capacitación

Continuando con el programa general de capacitación, este Instituto aplicará el programa de protección de datos personales mediante la capacitación de las personas servidoras públicas a través de los cursos que el órgano garante oferta así como los que se difunden e invitan el INAI, considerando para ello los temas siguientes:

- ✓ Uso del Sistema de Portales de Obligaciones de Transparencia (SIPOT) de la Plataforma Nacional de Transparencia.
- ✓ Ejercicio de los Derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad de los Datos Personales y Medios de Impugnación.
- ✓ Gobierno Abierto y Transparencia Proactiva.
- ✓ Sistema de Gestión de Seguridad de Datos Personales en el Sector Público.

Por lo anterior y así convenir a los intereses de protección, uso, aplicación y manejo de información de datos personales, se realizarán las invitaciones para que asistan a las capacitaciones tanto presencial como de manera virtual a las personas responsables autorizadas para el uso de datos personales, el oficial de datos personales, personal de la unidad de transparencia, responsables del cumplimiento de las obligaciones en materia de transparencia, titulares de las unidades administrativas, enlace de transparencia e integrantes del comité de transparencia del ICOSORP.

Actualización del documento de seguridad

Los artículos 36 de la LGPDPPSO y 51 de la LPDPPSOCHIS establecen la obligación de actualizar el documento de seguridad cuando ocurran los siguientes eventos:

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

En ese sentido, el Comité de Transparencia deberá estar atento a la actualización de alguno de los supuestos antes citados, para, en su caso, actualizar el presente documento de seguridad.

***Unidad de Transparencia del Instituto de Comunicación Social y Relaciones Públicas del Estado de Chiapas*.**

***Correo**: icosorp@transparencia.chiapas.gob.mx*

***Portal Institucional**: https://icosorp.chiapas.gob.mx/site/*