

Documento de seguridad

en materia de tratamiento de datos personales en posesión de la
Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Chiapas

(Artículos 35 de la LGPDPPSO y 49 a 50 de la LPDPPSOCHIS)

Fecha de elaboración: 30 enero de 2023.

Fecha de última actualización: 20 de febrero de 2023.

Contenido

1.	Introducción	3
2.	Glosario de acrónimos, términos y conceptos	6
3.	Marco normativo	13
4.	Objetivo del documento de seguridad	14
5.	Responsabilidades	15
6.	Alcances del documento de seguridad	16
7.	Sistema de gestión de los datos personales	17
8.	Inventario de datos personales y de los sistemas de tratamiento o bases de datos personales	19
9.	Funciones y obligaciones de las personas que tratan datos personales	28
10.	Análisis de riesgos, análisis de brecha y plan de trabajo	46
11.	Mecanismos de monitoreo y revisión de las medidas de seguridad	55
12.	Programa general de capacitación	59
13.	Actualización del documento de seguridad	63

1. Introducción

El derecho a la protección de los datos personales en el sector público mexicano encuentra su antecedente en la expedición de la ya abrogada *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental* (LFTAIPG), publicada el 11 de junio de 2002 y que estuvo vigente hasta el 9 de mayo de 2016.

No obstante, las reformas constitucionales en materia de transparencia y protección de datos personales consagradas en los artículos 6 y 16 de la *Constitución Política de los Estados Unidos Mexicanos* (CPEUM) en 2009 y 2014, dieron lugar a la emisión de disposiciones legales secundarias con el propósito de regular y garantizar de forma específica el ejercicio de este derecho humano y fundamental de rango constitucional, el cual es un derecho autónomo e independiente del derecho de acceso a la información.

Fue así que el 1 de junio de 2009 se publicó en el Diario Oficial de la Federación el Decreto mediante el cual se adicionó un segundo párrafo al artículo 16 constitucional, mismo que dispone que toda persona tiene derecho al acceso, rectificación y cancelación de sus datos personales, así como a manifestar la oposición al tratamiento de los mismos, en los términos que fije la ley. Esta reforma propició la publicación de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* (LFPDPPP)¹ el 5 de julio de 2010, la cual prevé el marco de referencia para la protección de los datos personales en el sector privado.

Posteriormente y derivado de la reforma al artículo 6 constitucional de 2014, el 26 de enero de 2017 se publicó en el Diario Oficial de la Federación la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* (LGPDPSSO, en adelante)², misma que establece las bases y principios para garantizar el derecho que tiene toda persona física a la protección de sus datos personales en posesión de entes públicos de los tres niveles, ámbitos u órdenes de gobierno (federal, estatal y municipal) y define condiciones homogéneas que rigen el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales (derechos ARCOP, en adelante), mediante procedimientos sencillos y expeditos.

A fin de armonizar la legislación local en la materia con las disposiciones de la LGPDPSO, el 30 de agosto de 2017 se publicó en el Periódico Oficial del Estado la *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas* (LPDPSOCHIS, en adelante)³, la cual determina el marco de referencia para la protección de los datos personales en el sector público de esta entidad federativa -tanto a nivel estatal como municipal-, cuya autoridad local que debe garantizar el estricto cumplimiento u observancia de dicha Ley es el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas (ITAIPCH, en adelante), el cual es uno de los integrantes del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT).

A partir de la entrada en vigor de la LGPDPSO, todos los entes públicos -incluidos los partidos políticos-, adquieren el carácter de “responsables” y deben tratar los datos personales que poseen conforme a los principios rectores de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como implementar medidas de seguridad para proteger los datos personales en su poder y plasmarlas en un documento.

En ese contexto, los artículos 35 de la LGPDPSO y 49 a 50 de la LPDPSOCHIS establecen como obligación la elaboración de un documento de seguridad, que se define -según la fracción XIV del artículo 3 de la LGPDPSO y la fracción XIII del artículo 5 de la LPDPSOCHIS- 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.

¹ Consultable en: <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

² Consultable en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPSO.pdf>

³ Consultable en: https://www.congresochiapas.gob.mx/new/Info-Parlamentaria/LEY_0135.pdf

De conformidad con lo dispuesto en la LGPDPPSO, el documento deberá contener, al menos, la siguiente información:

- 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.

Con respecto a dicho contenido del documento de seguridad, el Diccionario de Protección de Datos Personales⁴, publicado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), refiere lo siguiente:

Inventario de datos personales y sistemas de tratamiento.

En la parte del inventario de los datos personales y los sistemas de tratamiento, el documento de seguridad debe contener un listado de todos los sistemas en los que se efectúe tratamiento de datos y una clasificación de todos los datos personales que se tratan.

En el mencionado diccionario, el doctor Uciel Fragoso Rodríguez también refiere que los sistemas de tratamiento consisten generalmente en todos los sistemas informáticos en los que se almacenan o procesan datos personales, tales como bases de datos, directorios, sistemas de recursos humanos y páginas web de registro, entre otros.

En relación con el resto del contenido del documento de seguridad, el doctor Fragoso Rodríguez puntualiza en dicho diccionario lo siguiente:

Funciones y obligaciones de las personas que traten datos personales.

Otra parte importante del documento de seguridad es la identificación de todas las personas que intervienen en el tratamiento de datos personales a lo largo de su ciclo de vida. El proceso de identificación se logra mediante el análisis de los procesos de negocio y los tipos de datos personales tratados como parte del flujo de información. El tratamiento que se les dé a los datos debe estar en concordancia con los roles y responsabilidades de las personas en su papel de responsable o encargado. La asignación no adecuada de privilegios puede producir que —por error o intencionalmente— se afecte la confidencialidad, integridad o disponibilidad de los datos personales.

Análisis de riesgos.

El análisis de riesgos en el documento de seguridad describe a detalle cómo se implementa el proceso en forma sistemática. Existen diversas metodologías o estándares en el mercado que pueden emplearse para su correcta implementación. Para el caso particular de datos personales, el INAI propone la metodología de análisis de riesgos MARBAA932⁵ que, para cada dato personal con un nivel de riesgo inherente asociado, se evalúan tres factores ligados a los propios datos: el volumen de los datos y su nivel de riesgo inherente (factor conocido como beneficio), el número de acceso a los datos (factor conocido como accesibilidad) y el entorno desde donde se acceden los datos (factor conocido como anonimidad).

⁴ Consultable en: http://inicio.inai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf

⁵ Consultable en: [http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP\(Junio2015\).pdf](http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf)

Independiente de la metodología utilizada, el proceso de análisis de riesgos inicia con la identificación del activo a proteger, que, en el caso de los datos personales, se identifican los tipos o categorías de los datos personales bajo estudio. La segunda fase en el proceso es identificar las amenazas que pudieran ocasionar algún daño a los datos. Las amenazas pueden ser internas o externas y pueden tener diferentes orígenes: fenómenos naturales, incidentes, infraestructura tecnológica o de origen humano.

Con la información recolectada se procede a construir escenarios de riesgo, los cuales describen situaciones que pueden pasar y que relacionan los componentes del riesgo: activo, amenazas y vulnerabilidades. Cada escenario de riesgo se evalúa estimando su probabilidad de ocurrencia y el impacto que pudiera tener en caso de que dicho escenario de riesgo se materialice.

Análisis de brecha.

El análisis de brecha es otro componente importante que debe contener el documento de seguridad. El análisis de riesgos permite llevar a cabo el análisis de brecha, el cual consiste en determinar la diferencia entre las medidas de seguridad existentes y las que faltan para reducir el riesgo hasta un nivel por abajo del establecido por la organización como nivel aceptable. Los análisis de riesgos y de brecha ayudan a seleccionar las medidas de seguridad aplicables a la protección de los datos personales.

Plan de trabajo y mecanismos de monitoreo y revisión de las medidas de seguridad.

Cada uno de los mecanismos de seguridad consiste en un control que puede ser del tipo tecnológico, administrativo o de procedimiento y su implementación debe realizarse definiendo un plan de trabajo. El plan de trabajo es parte medular del documento de seguridad y es donde se detallan las acciones tomadas para implementar las medidas de seguridad, además, se especifican los recursos del tipo económico, humano o de cualquier otra naturaleza. El plan de trabajo se puede controlar y documentar con alguna metodología existente de gestión de proyectos.

Programa general de capacitación.

Como parte final del documento de seguridad, se propone una sección en donde se establezca un programa general de capacitación que describa detalladamente los planes de capacitación para cada persona que intervenga en el tratamiento de datos personales a lo largo de su ciclo de vida. Los programas de capacitación deben ajustarse para los responsables y encargado del tratamiento de los datos según sus roles y responsabilidades asignadas.

Ahora bien, considerando el hecho de que la Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Chiapas (SESAECH, en adelante) es un organismo público descentralizado no sectorizado que tiene a su cargo, entre otras funciones, administrar los sistemas o plataformas informáticas con los que contará el Sistema Electrónico Estatal, tales como el Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal (S1) que implica un tratamiento intensivo y relevante de datos personales de las personas declarantes y terceras personas, en un sujeto obligado en materia de protección de datos personales y por ende responsable del tratamiento de los mismos, por lo que tiene la obligación de contar con su documento de seguridad.

En observancia a ese deber y obligación de cumplimiento inmediato que todos los sujetos obligados del estado de Chiapas debieron acatar a partir del 31 de agosto de 2017, a continuación se presenta el documento de seguridad de la SESAECH con los elementos informativos que establece la normatividad vigente, el cual da cuenta acerca de las medidas técnicas, físicas y administrativas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales en su poder y resulta de observancia general y obligatoria para todas las áreas o unidades administrativas y personas servidoras públicas a las que se alude.

2. Glosario de acrónimos, términos y conceptos

Para efectos del presente documento se entenderá por:

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.
Autentificar:	Acción de comprobar que la persona es quien dice ser.
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 de la Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Chiapas (SESAECH), que es puesto 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)
Clasificación:	Acto por el cual se determina fundada y motivadamente que la información que posee la SESAECH es de carácter reservada o confidencial.
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.
Cómputo en la nube:	Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informática, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.
Consentimiento:	Manifestación de la voluntad libre, específica 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 autenticación.
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 la SESAECH 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.
Información:	Todo aquel conjunto organizado de datos que generan, obtienen, 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.
Instituto o 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:	<p>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:</p> <ul style="list-style-type: none">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, yd) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.
Medidas de seguridad técnicas:	<p>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:</p> <ul style="list-style-type: none">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, yd) 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 las personas físicas, morales y sindicatos 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.
Secretaría Ejecutiva o SESAECH:	Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Chiapas.
Sistema(s) de tratamiento:	<p>Todo conjunto organizado de archivos, registros, ficheros, bases o bancos de datos personales en posesión de alguna de las áreas de la SESAECH, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso.</p> <p>Existen dos tipos de sistemas de tratamiento:</p> <p>Físicos: Conjunto ordenado de datos que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos.</p> <p>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.</p>
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.

3. Marco normativo

- Artículos 6, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM)⁶.
- Artículo 3 de la Constitución Política del Estado Libre y Soberano de Chiapas⁷.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)⁸.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS)⁹.
- Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (Lineamientos)¹⁰.

⁶ Consultable en: <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>

⁷ Consultable en: https://www.congresochiapas.gob.mx/new/Info-Parlamentaria/LEY_0002.pdf

⁸ Consultable en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>

⁹ Consultable en: https://www.congresochiapas.gob.mx/new/Info-Parlamentaria/LEY_0135.pdf

¹⁰ Consultables en: <https://itaipchiapas.org.mx/pdfs/marco-juridico/LINEAMIENTOS%20PARA%20PDP%20IAIP.pdf>

4. 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 de la SESAECH, como un medio para cumplir con las obligaciones que establecen las dos leyes antes mencionadas y los *Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas* (los Lineamientos, en adelante)¹¹ que emitió el Pleno del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas (ITAIPCH, en adelante), 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.

¹¹ Consultables en: <https://itaipchiapas.org.mx/pdfs/marco-juridico/LINEAMIENTOS%20PARA%20PDP%20IAIP.pdf>

5. Responsabilidades

Con fundamento en lo dispuesto en los artículos 83 de la LGPDPPSO y 113 de la LPDPPSOCHIS, los cuales establecen que el Comité de Transparencia es la máxima autoridad interna en materia de protección de datos personales y que tiene entre sus funciones las de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, a dicho órgano colegiado también le han sido conferidas las siguientes atribuciones:

- Elaborar, aprobar, coordinar y supervisar el programa de protección de datos personales (el programa, en adelante), en conjunto con las áreas que estime necesario involucrar o consultar;
- Proponer cambios y mejoras al programa, a partir de la experiencia de su implementación;
- Dar a conocer el programa al interior de la organización del responsable;
- Coordinar la implementación del programa en las áreas de la institución;
- Asesorar a las áreas en la implementación del programa, con el apoyo de la Unidad de Transparencia;
- Presentar un informe anual a la persona servidora pública que ejerza la titularidad del sujeto obligado, en el que se describan las acciones realizadas para cumplir con lo previsto en el programa.
- Supervisar la correcta implementación del programa;
- Elaborar, aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con las áreas que estime necesario involucrar o consultar, y
- Las demás que de manera expresa señale el propio programa.

La Unidad de Transparencia y el resto de las áreas de la SESAECH tendrán las funciones y responsabilidades que se describen más adelante en este documento.

Para que el objetivo planteado se logre 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 Secretario Técnico de la Secretaría Ejecutiva, a fin de que tome las medidas necesarias para que el mismo se observe en la SESAECH.

La intervención del Secretario Técnico tendrá la finalidad de impulsar la debida implementación del programa al interior de la Secretaría Ejecutiva, pero no podrá suplir ni afectar las funciones del Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la organización del responsable.

Asimismo, para que la implementación del programa tenga como resultado el cumplimiento integral de las obligaciones que establecen la LPDPPSOCHIS y los Lineamientos, el programa será de observancia obligatoria para todas las personas servidoras públicas adscritas a las áreas de la Secretaría Ejecutiva que traten datos personales en el ejercicio de sus atribuciones, facultades o funciones.

Las áreas deberán realizar las acciones necesarias para cumplir con las obligaciones que establece el programa, para lo cual deberán asignar los recursos humanos, materiales y financieros necesarios, así como prever lo que se requiera en sus respectivos programas de trabajo.

Para ello, resulta fundamental que el programa se conozca al interior de la SESAECH, por lo que el Comité de Transparencia se encargará de difundirlo ampliamente entre el personal de la Secretaría Ejecutiva.

6. Alcances del documento de seguridad

El documento de seguridad aplica a todas las áreas de la Secretaría Ejecutiva que realicen o efectúen tratamientos de datos personales en ejercicio de sus atribuciones, facultades o funciones, los cuales estarán bajo su estricta responsabilidad, tanto en los espacios físicos como en los medios electrónicos en los que los resguarden, operen y administren, en observancia a los principios, deberes y obligaciones que prevén la LGPDPPSO y la LPDPPSOCHIS, así como los Lineamientos.

Quedan exceptuados de la aplicación del programa los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que hacen referencia el Título Quinto de la *Ley General de Transparencia y Acceso a la Información Pública* (LGTAIP, en adelante)¹² y el Título Sexto de la *Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas* (LTAIPCHIS, en adelante)¹³.

Las áreas que forman parte de la SESAECH y que deberán observar el programa, son las siguientes:

1. Secretaría Técnica;
2. Unidad de Apoyo Administrativo;
3. Coordinación de Archivos;
4. Unidad de Transparencia;
5. Dirección Jurídica;
6. Dirección de Vinculación y Políticas Públicas, y
7. Dirección de Sistemas Electrónicos y Plataforma Digital.

La Unidad de Transparencia integra este documento de seguridad con base en la información generada por las siete áreas antes señaladas que conforman la Secretaría Ejecutiva.

¹² Consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP_200521.pdf

¹³ Consultable en: https://www.congresochiapas.gob.mx/new/Info-Parlamentaria/LEY_0084.pdf

7. Sistema de gestión de los datos personales

El sistema de gestión es el medio por el cual la Secretaría Ejecutiva garantiza el tratamiento de los datos personales que 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.

Por lo anterior, se inició un proceso de organización y planeación de los medios para la protección de datos, tomando como punto de partida la identificación de los procesos y tareas en las que, dadas sus atribuciones, las distintas áreas de la SESAECH realizan o efectúan tratamientos de datos personales. Para tal fin, se elaboró un formulario que facilitó a cada área la identificación de los 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, logrando con ello el levantamiento del inventario de datos que forma parte del presente documento de seguridad, tratando de identificar 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.

Además, el inventario 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 de la Secretaría Ejecutiva.



Una vez integrados los inventarios de tratamientos y de datos, se estableció la metodología para el análisis de riesgos, con la intención de que se identificaran el valor de los datos y su ciclo de vida, así como el valor de exposición y las posibles consecuencias para las personas titulares de los datos por el uso indebido o posible vulneración y las condiciones de riesgo a los que podrían encontrarse expuestos dichos datos por medidas de seguridad poco confiables. Lo anterior, permitió identificar la brecha entre las medidas de seguridad existentes y las medidas de seguridad faltantes para que garanticen la seguridad de los datos en posesión, tanto administrativas, como físicas y técnicas.

A partir de esta identificación de posibles vulneraciones es factible prevenir posibles debilidades en la seguridad de los datos y las áreas de oportunidad, aún 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 exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada comprometiendo su confidencialidad, disponibilidad e integridad; y en este sentido, las medidas de seguridad por parte de cada dirección están orientadas justamente a proteger los datos personales. En el marco del sistema de gestión y política de seguridad institucional, se procurará:

- Que los datos personales sean tratados conforme a lo establecido en la normatividad vigente.
- Identificar a las personas servidoras públicas responsables del tratamiento de los datos personales.
- Que los tratamientos de datos personales estén sujetos al principio de consentimiento siempre que la Ley lo permita.
- Responder al principio de información a 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 de la SESAECH.

Buscando el logro de lo anterior y tomando como punto de partida la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que, de acuerdo con otras experiencias y mejores prácticas tomadas como referencia, se encaminan a la mejora continua por parte de las personas involucradas en el tratamiento de los datos personales.

En la búsqueda de lograr 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.

8. 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 en un diagnóstico realizado por cada una de 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 de éstos.

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.

A partir de lo anterior, la SESAECH elaboró los inventarios de los distintos tratamientos de datos personales que realizan o efectúan sus áreas, identificando la mayor parte de los elementos informativos que prevén los artículos 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 dichos Lineamientos. Dichos inventarios forman parte integral del presente documento y se encuentran contenidos en el **Anexo No. 1**.

La siguiente tabla muestra un resumen de esos inventarios contenidos en el **Anexo No. 1**, elaborados por las áreas:

Número de participante	Área, unidad administrativa u órgano administrativo	Número de inventarios	Sistemas de tratamiento o bases de datos personales
1	Secretaría Técnica	2	1. Registro de visitas. 2. Agenda telefónica.
2	Unidad de Apoyo Administrativo	9	1. Contratación de personal. 2. Expediente único de personal. 3. Cuestionario médico. 4. Consentimiento de seguro de vida. 5. Control de asistencia. 6. Nómina de pago de personal. 7. Hoja de trayectoria laboral. 8. Expediente de prestadores del servicio social y prácticas profesionales. 9. Procedimientos de contrataciones o compras públicas y proveedores.
3	Coordinación de Archivos	1	1. Registro de documentos recibidos.
4	Unidad de Transparencia	4	1. Solicitudes de acceso a la información dirigidas a la SESAECH. 2. Solicitudes de datos personales o para el ejercicio de los derechos ARCOP dirigidas a la SESAECH. 3. Recursos de revisión en materia de acceso a la información que en su caso sean presentados, promovidos o interpuestos ante la Unidad de Transparencia de la SESAECH. 4. Recursos de revisión en materia de datos personales que en su caso sean presentados, promovidos o interpuestos ante la Unidad de Transparencia de la SESAECH.
5	Dirección Jurídica	2	1. Instrumentos jurídicos consensuales. 2. Registro de asistencia a las sesiones del Sistema Anticorrupción del Estado de Chiapas (SAECH).
6	Dirección de Vinculación y Políticas Públicas	5	1. Consulta en línea (encuesta anticorrupción), a través de la plataforma SurveyMonkey. 2. Diagnóstico a órganos internos de control (OICs) y unidades de transparencia (UTs) municipales, a través de la plataforma SurveyMonkey. 3. Encuesta a comunidades indígenas y poco comunicadas. 4. Listas de asistencia de los conversatorios regionales. 5. Listas de asistencia de los talleres para priorizar acciones en el combate y control de la corrupción en la Política Estatal Anticorrupción (PEA).

7	Dirección de Sistemas Electrónicos y Plataforma Digital	22	<ol style="list-style-type: none"> 1. Instrumento diagnóstico de la situación de los sistemas electrónicos existentes que contiene la Información a que hace referencia el artículo 47 de la Ley del Sistema Anticorrupción del Estado de Chiapas. 2. Sistema Declaramun PI. 3. Registro de participantes de la reunión de trabajo denominada “Mecanismo para la Recepción de las Declaraciones Patrimoniales Municipales”. 4. Sistema DeclaraFácil PI Portable. 5. Registro de participantes de la reunión de trabajo denominada “Mecanismo para la Obtención de las Versiones Públicas de las Declaraciones Patrimoniales y de Intereses a través del Sistema Declaramun PI”. 6. Lista de asistencia de la Dirección de Sistemas Electrónicos y Plataforma Digital. 7. Gestión de la generación de la Firma Electrónica Avanzada (FEA). 8. Registro de participantes del “Taller de Acciones Conjuntas contra la Corrupción 2021, SAECH – Ayuntamientos”. 9. Sistema de Votación Electrónico. 10. Directorio de funcionarios municipales. 11. Formulario de contacto del sitio de internet institucional. 12. Formulario de contacto del Sistema Electrónico Estatal (SEE). 13. Registro de participantes de la capacitación denominada “Tecnologías Anticorrupción: Conecta SAECH, Declaramun PI y DeclaraFácil PI Portable”. 14. Sistema Conecta SAECH. 15. Sistema Contrata SP. 16. Sistema Sancionados SP. 17. Sistema Sancionados P. 18. Registro de participantes de la capacitación denominada “Generalidades del Sistema Anticorrupción del Estado de Chiapas”. 19. Registro de participantes de la capacitación del Sistema DeclaraFácil PI Portable. 20. Sistema DeclaraFácil PI Portable VP. 21. Centro de Capacitación en Línea de la SESA ECH. 22. Gestor de enlaces.
Total:		45	

Como resultado del proceso de análisis realizado, se logró identificar entonces que son las siguientes áreas de la SESAECH las que efectúan tratamientos de datos personales en ejercicio de sus atribuciones, facultades o funciones:

- Secretaría Técnica;
- Unidad de Apoyo Administrativo;
- Coordinación de Archivos;
- Unidad de Transparencia;
- Dirección Jurídica;
- Dirección de Vinculación y Políticas Públicas, y
- Dirección de Sistemas Electrónicos y Plataforma Digital.

Tales tratamientos se realizan en absoluto apego a las atribuciones, facultades y funciones que prevén las disposiciones aplicables de la *Ley del Sistema Anticorrupción del Estado de Chiapas*¹⁴ y del *Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Chiapas*¹⁵, así como del *Manual de Organización de la Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Chiapas*¹⁶ y el dictamen No. SH/CGRH/DEO/174/2020¹⁷, las cuales son ejecutadas por las áreas a las que les han sido conferidas y permiten el desarrollo de los procesos que éstas realizan para el cumplimiento de dichas atribuciones, facultades y funciones.

Asimismo, como resultado de ese proceso de análisis también se identificaron los diferentes tipos de los datos personales sometidos a tratamiento, los cuales corresponden a las siguientes seis **categorías**:

De identificación o identificativos

- Nombre(s) y/o apellido(s) (paterno y/o materno), sexo, nacionalidad, año y lugar de nacimiento, edad, características físicas, firma autógrafa o electrónica, Clave Única de Registro de Población (CURP), Registro Federal de Contribuyentes (RFC), domicilio particular, número telefónico personal de teléfono fijo o móvil, cuenta de correo electrónico personal, datos personales contenidos en documentos para acreditar la identidad de una persona física, como los contenidos en identificaciones oficiales (credencial para votar, cédula profesional, título profesional, pasaporte, cartilla militar, licencia de conducir, documento migratorio, etc.), etc.

Académicos

- Formación académica, escolaridad o educación; documento obtenido; número de cédula profesional; etc.

Laborales

- Experiencia o antecedentes laborales; puesto o empleo, cargo o comisión; denominación o razón social del ente público o de la empresa, sociedad o asociación; área de adscripción; datos sindicales; domicilio oficial o institucional; número telefónico oficial o institucional; cuenta de correo oficial o institucional; fecha de ingreso al empleo; fecha de egreso; etc.

Patrimoniales

- Número de cuenta bancaria, CLABE interbancaria, bienes inmuebles, vehículos, bienes muebles, adeudos o pasivos, número de crédito, préstamo o comodato por terceros, ingresos netos propios, de la pareja y de los dependientes económicos, etc.

Biométricos

- Rostro, huella digital o dactilar y firma autógrafa (para reconocimiento de la firma).

Sensibles

- Origen étnico o racial (pertenencia a un pueblo originario o comunidad indígena), lengua indígena o de algún pueblo originario, datos de salud (enfermedades o padecimientos), discapacidades, tipo de sangre, circunstancias socioeconómicas, religión, etc.

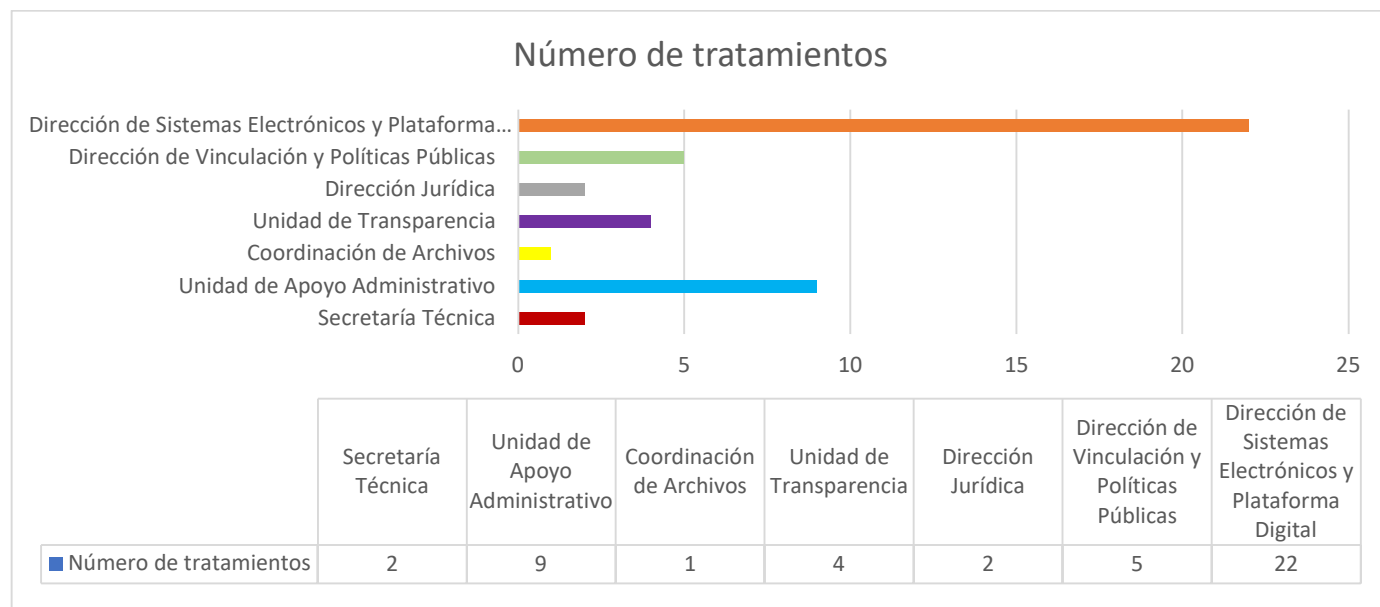
¹⁴ Consultable en: https://www.congresochiapas.gob.mx/new/Info-Parlamentaria/LEY_0128.pdf

¹⁵ Consultable en: <https://sesaech.gob.mx/views/docs/normatividad/normatividad-interna-estatutos/estatuto-organico-de-la-secretaria-ejecutiva-del-sistema-anticorrupcion-del-estado-de-chiapas.pdf>

¹⁶ Consultable en: <https://sesaech.gob.mx/views/docs/normatividad/normatividad-interna-manuales/manual-de-organizacion-de-la-sesaech.pdf>

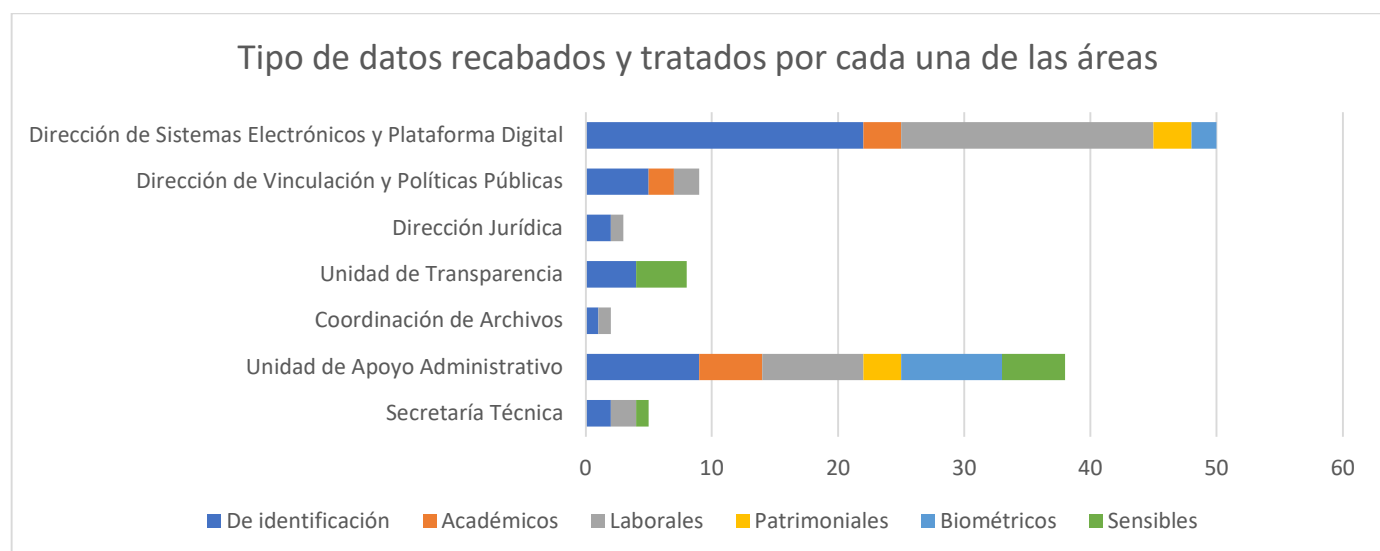
¹⁷ Consultable en: <https://sesaech.gob.mx/assets/documentos/transparencia/obligacionestransparencia/funciones.pdf>

Dichos datos son tratados en 45 procesos, de los cuales dos corresponden a la Secretaría Técnica, nueve a la Unidad de Apoyo Administrativo, uno a la Coordinación de Archivos, cuatro a la Unidad de Transparencia, dos a la Dirección Jurídica, cinco a la Dirección de Vinculación y Políticas Públicas y veintidós a la Dirección de Sistemas Electrónicos y Plataforma Digital.

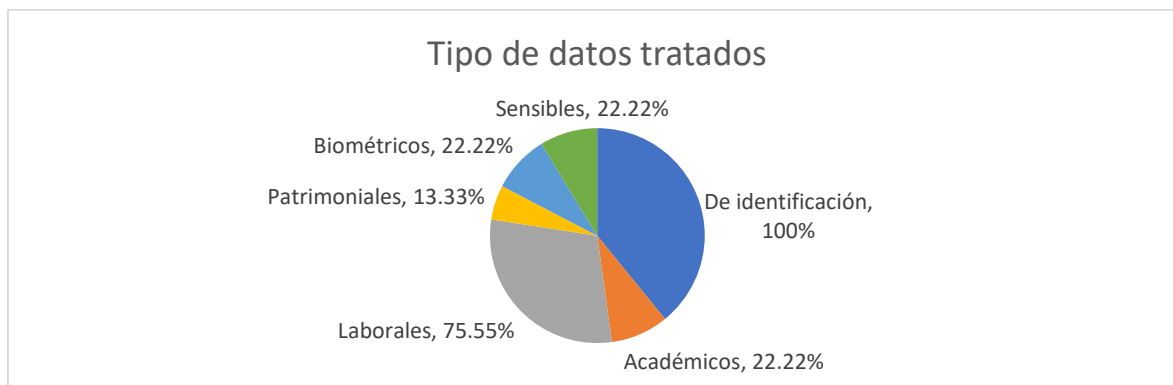


Como se puede apreciar en la gráfica anterior, el área con mayor número de procesos es Dirección de Sistemas Electrónicos y Plataforma Digital con 22 tratamientos, mientras que la Coordinación de Archivos es la que menos procesos desarrolla al ser un solo tratamiento el que realiza o efectúa.

En relación con los datos tratados, todas las áreas recaban datos de identificación, mientras que solamente dos áreas tratan datos biométricos, tal como se presenta en la siguiente gráfica:



En este sentido, se identificó también que, en relación con los procesos en los que se tratan datos, en el 100 por ciento se tratan datos de identificación, en el 22.22 por ciento se tratan datos académicos, en el 75.55 por ciento se tratan datos laborales, en el 13.33 por ciento se tratan datos patrimoniales, en el 22.22 por ciento se tratan datos biométricos y en el 22.22 por ciento se tratan datos sensibles; como se muestra a continuación:



A partir de lo anterior, podemos identificar que la categoría de los datos personales con mayor número de áreas y tratamientos es la de carácter identificativo, en segundo término los que incluyen datos laborales y en tercer lugar los relacionados con datos sensibles. Asimismo, hay que señalar que se identificaron ocho procesos en los que se realiza el tratamiento de datos biométricos, como se muestra en la gráfica que aparece en la página siguiente.

La Dirección de Sistemas Electrónicos y Plataforma Digital es el área que desarrolla el mayor número de procesos en los que intervienen tratamientos de datos personales, dada la naturaleza de las atribuciones, facultades o funciones que ejerce, dado que a las dos jefaturas de departamento que la integran les compete tratar los datos personales que se recaban con motivo de la puesta en operación de los seis sistemas que conforman al Sistema Electrónico Estatal de Chiapas (SEE), el cual se encuentra previsto en el artículo 47 de la *Ley del Sistema Anticorrupción del Estado de Chiapas*; siendo éstos los siguientes:

1. Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal (S1 o sistema 1);
2. Sistema de los servidores públicos que intervengan en procedimientos de contrataciones públicas (S2 o sistema 2);
3. Sistema de servidores públicos y particulares sancionados (S3 o sistema 3);
4. Sistema de información y comunicación del Sistema Anticorrupción del Estado de Chiapas y del Sistema Estatal de Fiscalización (S4 o sistema 4);
5. Sistema de denuncias públicas de faltas administrativas y hechos de corrupción (S5 o sistema 5), y
6. Sistema de información pública de contrataciones (S6 o sistema 6).

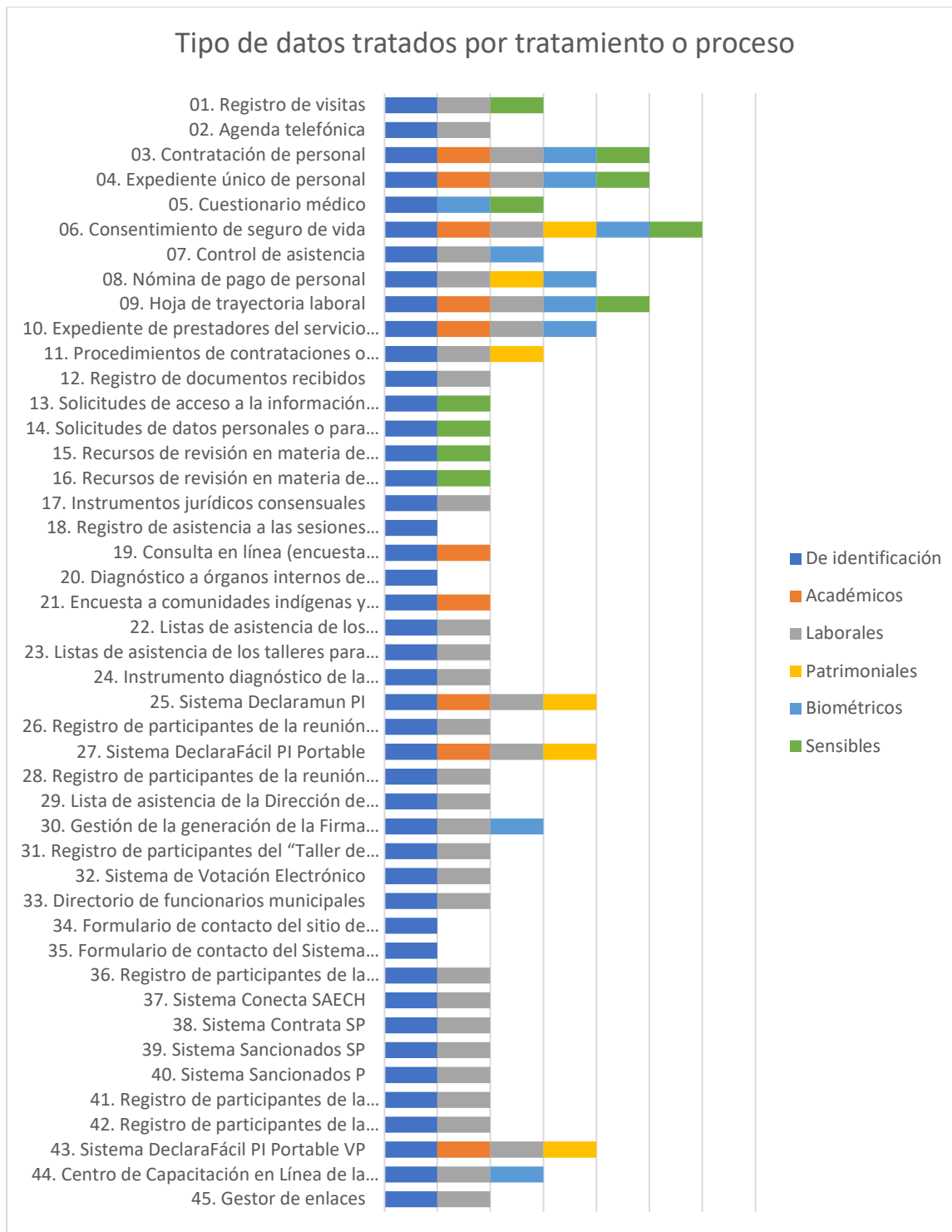
Al respecto, cabe destacar que en cumplimiento a lo dispuesto en los artículos 74 de la LGPDPPSO y 103 de la LPDPPSOCHIS, hasta la fecha de elaboración de este documento de seguridad ha sido elaborada y dictaminada la *Evaluación de Impacto en la Protección de Datos Personales del Sistema de Evolución Patrimonial, de Declaración de Intereses y Constancia de Presentación de Declaración Fiscal (S1) del Sistema Electrónico Estatal de Chiapas (SEE)*, cuya versión pública se encuentra públicamente disponible para su consulta en cualquiera de las siguientes direcciones electrónicas del portal institucional de internet de la SESAECH:

<https://sesaech.gob.mx/datos-personales/evaluaciones-de-impacto>

y/o

<https://sesaech.gob.mx/sistema-electronico-estatal/evaluaciones-de-impacto>

Asimismo, cabe mencionar que la *Evaluación de Impacto en la Protección de Datos Personales del Sistema de Servidores Públicos y Particulares Sancionados (S3) del Sistema Electrónico Estatal de Chiapas (SEE)* actualmente se encuentra en proceso de dictaminación.



Por otra parte, se identificó que cada área tiene un medio propio para recabar u obtener los datos personales que trata, los cuales preponderantemente son de manera personal con la presencia física de la persona titular de los datos personales, por correo electrónico y a través de sistemas electrónicos, así como que cada área también se encarga de desarrollar estrategias para la protección de los datos personales que posee, mediante la aplicación de diversas medidas de seguridad.

Es por ello que el inventario de datos personales y de los sistemas de tratamiento o bases de datos personales de la Secretaría Ejecutiva, a partir de los hallazgos identificados en su elaboración, 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.

En este mismo sentido, ayuda a trazar las rutas para la capacitación en materia protección de datos hacia las personas servidoras públicas adscritas a la SESAECH, como una vía de fortalecimiento en la operación de los procesos en que se tratan los datos, en la búsqueda de sensibilizar y preparar a los responsables y encargados de los mismos para que los tratamientos se realicen de conformidad con los estándares nacionales e internacionales en la materia.

En apego a lo anterior, el inventario de datos personales y de los sistemas de tratamiento o bases de datos personales de la Secretaría Ejecutiva 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 del ámbito local del estado de Chiapas.

Finalmente y de conformidad con lo dispuesto en las dieciséis fracciones del artículo 50 de la LPDPPSOCHIS, resulta necesario señalar que cada uno de los sistemas de tratamiento o bases de datos personales que conforman el inventario contiene la siguiente información:

- I. El nombre de los sistemas de tratamiento o bases de datos personales.
- II. El nombre, cargo y adscripción del administrador de cada sistema de tratamiento o base de datos personales.
- III. Las funciones y obligaciones de las personas que traten datos personales.

Al respecto, cabe precisar que las funciones del administrador y usuario responsable que se consideran son las estrictamente concernientes al tratamiento de los datos personales o la finalidad para la cual fueron recabados.

De igual manera, las obligaciones que consideran son exclusivamente las tienen que ver con el tratamiento de los datos personales.

- IV. El inventario de los datos personales tratados.
- V. La estructura y descripción de los sistemas de tratamiento 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.
- 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.

MUY IMPORTANTE: 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 de la SESAECH, ubicada en Boulevard Andrés Serra Rojas 1090, piso 16 de la Torre Chiapas, Colonia El Retiro o Paso Limón, C.P. 29045, Tuxtla Gutiérrez, Chiapas, México, o 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 cualquiera de las cuentas oficiales transparencia@sesaech.gob.mx y/o sesaech@transparencia.chiapas.gob.mx; o bien, mediante cualquier otro medio que al efecto establezcan o aprueben el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (CONAIP-SNT) o el Pleno del ITAIPCH, conforme a lo establecido en el Título Tercero de la LGPDPSO 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 LGPDPSO 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 de la propia Secretaría Ejecutiva, 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 de la propia SESAECH; o bien, consultarlo en los documentos que despliegan las direcciones electrónicas <https://ln.sesaech.gob.mx/formato-solicitud-derechos-arcop> y <https://ln.sesaech.gob.mx/manual-solicitudes-derechos-arcop>, así como en la URL <https://sesaech.gob.mx/datos-personales/derechos-arco>

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.

9. 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**.

De acuerdo con 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:

Funciones y obligaciones.

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.

De conformidad con lo anterior, las **funciones y obligaciones del personal de la SESAECH que trata datos personales** se han identificado en dos niveles:

1. A **nivel macro**, a través del **Programa de Protección de Datos Personales** de este sujeto obligado, en el cual se describen todas las obligaciones que establecen la LGPDPPSO y la LPDPPSOCHIS, las cuales se asocian con el área responsable de su cumplimiento, y
2. A **nivel de persona servidora pública**, a través de los **inventarios** que se desarrollaron por cada uno de los tratamientos, en los cuales se identificó el personal que realiza el tratamiento, el área a la que está adscrito y la finalidad de dicho tratamiento.

A continuación, se muestra un ejemplo de cómo se identifican las **funciones y obligaciones a nivel marco**, por cada una de las obligaciones que establecen la LGPDPPSO y la LPDPPSOCHIS:

Obligaciones	Actividades para su cumplimiento	Áreas o unidades administrativas responsables del cumplimiento	Medios que facilitan la acreditación del cumplimiento
Sujetar el tratamiento de los datos personales a las atribuciones, facultades y funciones que la normatividad confiera al sujeto obligado, así como con estricto apego y cumplimiento a lo establecido en dicha normatividad y el derecho positivo, respetando los derechos de las personas titulares.	Identificar el marco normativo (leyes, reglamentos, lineamientos, etc., con sus respectivos títulos, capítulos, artículos, párrafos, fracciones e incisos) que faculta a tratar los datos personales para cada una de las finalidades, así como aquél que regula el tratamiento respectivo.	Todas las que tratan datos personales.	Marco normativo respectivo.

Por su parte, el **inventario de datos personales y de los sistemas de tratamiento o bases de datos personales (Anexo No. 1)** contiene las siguientes columnas, en las cuales se identifican las funciones del personal que interviene en el tratamiento de los datos personales:

Personas servidoras públicas que tienen acceso a la base de datos (15)	Área, unidad u órgano administrativo de adscripción (16)	Finalidad del acceso (17)
Señalar los puestos o cargos de las personas servidoras públicas que tienen acceso a la base de datos del tratamiento correspondiente. Nota: Uno por fila.	Indicar la denominación del área, unidad u órgano administrativo al que está adscrita la persona servidora pública que tiene acceso a la base de datos del tratamiento correspondiente.	Señalar con qué fines o finalidades tienen acceso las personas servidoras públicas antes identificadas. Nota: Uno por fila, según corresponda.

Cabe señalar que la **cadena de rendición de cuentas** del personal se define en el análisis de riesgo respectivo.

Asimismo, el **Comité de Transparencia** es la instancia responsable de dar a conocer al personal de la SESAECH el Programa de Protección de Datos Personales, que se basa en un sistema de gestión, a fin de que las personas servidoras públicas conozcan sus funciones para el cumplimiento de dicho sistema y las consecuencias de su incumplimiento.

Adicionalmente, conviene señalar que las funciones y obligaciones del personal que trata datos personales se encuentran definidas en la legislación y normatividad que rige el actuar de la SESAECH, por lo cual, para efectos del presente documento de seguridad, el marco normativo de referencia se encuentra establecido en la *Ley del Sistema Anticorrupción del Estado de Chiapas* y en la *Ley de Entidades Paraestatales del Estado de Chiapas*, así como en el *Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Chiapas* y en el dictamen No. SH/CGRH/DEO/174/2020, emitido por la Dirección de Estructuras Orgánicas de la Coordinación General de Recursos Humanos de la Secretaría de Hacienda del Gobierno del Estado de Chiapas, lo mismo que en el *Manual de Organización de la Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Chiapas*.

Como resultado de la identificación de los procesos en los que se tratan datos personales, relacionado en el inventario de datos personales y de los sistemas de tratamiento o bases de datos personales de la Secretaría Ejecutiva, resulta importante tomar en consideración las atribuciones, facultades y funciones que el Estatuto Orgánico, el dictamen No. SH/CGRH/DEO/174/2020 y el manual de organización le confieren a las personas servidoras públicas adscritas a las áreas que realizan o efectúan tratamientos, a fin de observar el principio de legalidad, por lo que a continuación se ilustran las funciones y obligaciones de quienes tratan datos personales:

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
Secretaría Técnica	Analista técnico especializado	<ul style="list-style-type: none"> • Capturar la información para la elaboración de los informes generales y especiales que realiza el Secretario Técnico, en representación del organismo a las autoridades competentes. • Revisar e integrar la información de la inspección realizada a las áreas respecto del cumplimiento de los planes y programas del organismo. • Organizar la información para la elaboración del presupuesto de egresos anual de la Secretaría Ejecutiva conforme a los lineamientos emitidos.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
		<ul style="list-style-type: none"> • Apoyar en la elaboración del informe anual de actividades de la Secretaría Ejecutiva para presentarlo al Órgano de Gobierno. • Capturar el marco teórico y las directrices para la implementación, desarrollo y operación del Sistema Estatal Anticorrupción determinados ante el Comité Coordinador. • Apoyar en la certificación y/o difusión de los acuerdos que se tomen en el Comité Coordinador y en el Órgano de Gobierno que así se determine. • Apoyar en la evaluación de las políticas integrales y el informe correspondiente. • Capturar y elaborar propuestas de acuerdos, así como informes del sistema estatal anticorrupción, para su revisión y aprobación. • Apoyar y recabar la información para la elaboración del organigrama, el Estatuto Orgánico y los manuales administrativos de organización y procedimientos. • Apoyar en la elaboración del presupuesto anual y los estados financieros en función de los planes y programas anuales de operación.
Secretaría Técnica	Auxiliar Administrativo	<ul style="list-style-type: none"> • Elaborar los informes generales y especiales que el Secretario Técnico le indique. • Solicitar información de los planes y programas que ejecutarán los órganos administrativos para su archivo de consulta para el Secretario Técnico. • Recabar información para la elaboración del presupuesto anual de egresos de la Secretaría Ejecutiva. • Realizar las órdenes del día para las sesiones en donde participe el Secretario Técnico. • Recabar información para la elaboración del informe anual de actividades de la Secretaría Ejecutiva.
Unidad de Apoyo Administrativo	Jefe del Área de Recursos Humanos y Materiales	<ul style="list-style-type: none"> • Elaborar y tramitar los movimientos nominales de altas, bajas, promociones, licencias y cambios de adscripción del personal de la Secretaría Ejecutiva. • Tramitar ante el instituto de seguridad social al que corresponda el trabajador, altas, bajas y modificaciones salariales. • Supervisar y controlar el registro de asistencia, permisos, incapacidades, días de descanso y periodos vacacionales del personal adscrito a la Secretaría Ejecutiva, que sea acorde a los lineamientos normativos. • Capturar quincenalmente la nómina de pagos salariales del personal adscrito a la Secretaría Ejecutiva.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
		<ul style="list-style-type: none"> • Elaborar proyectos de manuales administrativos y movimientos de estructura orgánica y plantilla de plazas. • Realizar los procesos de contratación y admisión de prestadores de servicio social y becarios. • Elaborar las credenciales de identificación y nombramientos del personal adscrito a la Secretaría Ejecutiva. • Elaborar el presupuesto de egresos anual correspondiente al capítulo 1000 servicios personales. • Aplicar las políticas, normas y procedimientos que en materia de recursos materiales correspondan. • Elaborar el programa anual de adquisiciones, arrendamientos y servicios, así como efectuar adquisiciones de recursos materiales y servicios en apego a los procedimientos establecidos en la Ley de Adquisiciones, Arrendamientos de Bienes Muebles y Contratación de Servicios para el Estado de Chiapas. • Controlar el registro de entrada y salida de material de almacén, así como su inventario del patrimonio de la Secretaría Ejecutiva. • Atender los requerimientos de materiales que soliciten los órganos administrativos de la Secretaría Ejecutiva. • Formular y resguardar los contratos que en materia de recursos materiales que celebre la Secretaría Ejecutiva. • Realizar trámites de pagos de compras y servicios de los órganos administrativos de la Secretaría Ejecutiva. • Elaborar el programa de capacitación de protección civil de la Secretaría Ejecutiva, así como el programa de mantenimiento correctivo y preventivo de los bienes muebles e inmuebles.
Unidad de Apoyo Administrativo	Auxiliar Administrativo del Área de Recursos Humanos y Materiales	<ul style="list-style-type: none"> • Llevar el control de asistencia del personal y elaborar reportes quincenalmente para aplicar los descuentos disciplinarios. • Llevar el control de incidencias por licencias, vacaciones y permisos. • Elaborar cálculos nominales de percepciones y deducciones salariales. • Realizar los registros de bienes muebles de las áreas de la Secretaría Ejecutiva para su control en el inventario. • Controlar las entradas y salidas de material y equipos de almacén.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
		<ul style="list-style-type: none"> Realizar trámites de cotización, compras y contratación de servicios de los órganos administrativos de la Secretaría Ejecutiva. Realizar las altas y bajas del mobiliario y equipo de oficina. Realizar los registros del personal en las actividades de capacitación. Recibir el suministro de materiales y distribuirlo a las áreas solicitantes.
Unidad de Apoyo Administrativo	Jefe del Área de Recursos Financieros	<ul style="list-style-type: none"> Aplicar las políticas normas y procedimientos que en materia de control de recursos financieros y presupuestales establezcan las instancias normativas. Vigilar que la documentación comprobatoria y probatoria del gasto se integre de acuerdo con la normatividad vigente, cumpliendo con los requisitos fiscales y administrativos establecidos por las instancias correspondientes. Elaborar cheques y/o transferencias bancarias para el pago de sueldos y salarios, así como de bienes y servicios contratados. Registrar en el Sistema Integral de Administración Hacendaria Estatal (SIAHE) los eventos presupuestarios, mediante cédulas del gasto y documentos múltiples de todas las erogaciones presupuestales de acuerdo a la normatividad. Registrar en el Sistema Integral de Administración Hacendaria Estatal (SIAHE) los eventos económicos y financieros para elaborar mensualmente los estados financieros y presupuestales, así como el pre-cierre y cierre del ejercicio, de acuerdo a la normatividad contable y presupuestal. Realizar semestralmente la Cuenta de la Hacienda Pública Estatal, en la parte cuantitativa (contable-presupuestal), así como la cuenta pública anual. Realizar los registros contables del ejercicio del gasto y conciliaciones bancarias.
Unidad de Apoyo Administrativo	Auxiliar Administrativo del Área de Recursos Financieros	<ul style="list-style-type: none"> Recibir y tramitar la suficiencia presupuestal de las solicitudes de material y contratación de servicios que requieran las áreas de la Secretaría Ejecutiva. Recibir e integrar la documentación para el pago de suministros y contratación de servicios. Realizar los registros de gasto en el Sistema de Administración Hacendaria del Estado (SIAHE), así como realizar los reintegros. Realizar el registro de las ministraciones presupuestales. Resguardar la documentación probatoria y comprobatoria del gasto.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
Coordinación de Archivos	Coordinador de Archivos	<ul style="list-style-type: none"> • Elaborar, con la colaboración de los responsables de los archivos de trámite, de concentración y en su caso histórico, los instrumentos de control y consulta archivística previstos en la ley y en sus disposiciones reglamentarias, así como en la normativa que derive de ellos. • Elaborar criterios específicos y recomendaciones en materia de organización y conservación de archivos, cuando la especialidad del sujeto obligado así lo requiera. • Elaborar y someter a consideración del titular del sujeto obligado o a quien éste designe, el Programa Anual de Desarrollo Archivístico (PADA). • Coordinar los procesos de valoración y disposición documental que realicen las áreas. • Coordinar las actividades destinadas a la modernización y automatización de los procesos archivísticos y a la gestión de documentos electrónicos de las áreas. • Brindar asesoría técnica para la operación de los archivos. • Elaborar programas de capacitación en gestión documental y administración de archivos. • Coordinar con las áreas las políticas de acceso y la conservación de los archivos. • Coordinar la operación de los archivos de trámite, concentración y, en su caso, histórico, de acuerdo con la normatividad aplicable. • Autorizar la transferencia de los archivos cuando un área del sujeto obligado sea sometida a procesos de fusión, escisión, extinción o cambio de adscripción; o cualquier modificación de conformidad con las disposiciones legales aplicables. • Formular las políticas, manuales e instrumentos archivísticos. • Desarrollar medidas y acciones permanentes para el resguardo y conservación de documentos y expedientes clasificados, y aquellos que sean parte de los sistemas de datos personales, en coordinación y concertación con los responsables de las unidades de archivo. • Vigilar la correcta aplicación de los instrumentos de control y consulta archivística para la protección de la información confidencial o reservada. • Aprobar, en coordinación con el Grupo Interdisciplinario, los instrumentos de control y consulta archivística; así como las bajas documentales y transferencias secundarias.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
		<ul style="list-style-type: none"> • Las que establezcan las demás disposiciones jurídicas aplicables o sean acordadas por el Consejo Nacional o el Consejo Estatal de Archivos. • Vigilar el cumplimiento de las disposiciones administrativas, en materia de integración, protección, custodia, resguardo y conservación de la documentación y/o expedientes de la Secretaría Ejecutiva, del Órgano de Gobierno, del Comité Coordinador y de la Comisión Ejecutiva. • Implementar acciones para la integración, protección, custodia, resguardo y conservación de la documentación y/o expedientes de la Secretaría Ejecutiva, del Órgano de Gobierno, del Comité Coordinador y de la Comisión Ejecutiva, de conformidad con la legislación aplicable. • Coordinar que la integración y operación del sistema institucional de archivos de la Secretaría Ejecutiva, se realice conforme a las disposiciones jurídicas, criterios, herramientas y procesos de gestión documental emitidos en la materia. • Establecer los criterios de clasificación y catalogación de los documentos resguardados en los archivos. • Controlar las consultas al archivo de concentración de la Secretaría Ejecutiva. • Autorizar que las consultas de expedientes que las partes en litigio soliciten se proporcionen previa acreditación de su personalidad jurídica para facilitar el acceso y el derecho legítimo a la consulta del expediente relativo a su caso. • Coordinar la actualización del Sistema Institucional de Archivos y la normativa adyacente en la materia. • Resguardar, registrar, clasificar y conservar los expedientes y documentos procedentes de los órganos administrativos, con el objeto de que éstos se conserven íntegros y disponibles para permitir y facilitar un acceso expedito a la información contenida en los mismos y para contribuir con los objetivos generales de la Secretaría Ejecutiva. • Dar a conocer los lineamientos en materia archivística, así como capacitar al personal de la Secretaría Ejecutiva.
Unidad de Transparencia	Jefe de la Unidad de Transparencia	<p>En materia de transparencia y acceso a la información:</p> <ul style="list-style-type: none"> • Recabar y difundir la información a que se refiere el Título Quinto de la Ley General de Transparencia y Acceso a la Información Pública y el Título Sexto de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, así como propiciar que las áreas la actualicen periódicamente, conforme la normatividad aplicable.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
		<ul style="list-style-type: none"> • Recibir y tramitar las solicitudes de acceso a la información que se presenten y darles seguimiento hasta la resolución que de fin a las mismas. • Auxiliar a los particulares en la elaboración de solicitudes de acceso a la información que se presenten y, en su caso, orientarlos sobre los sujetos obligados competentes conforme a la normatividad aplicable. • Realizar los trámites internos necesarios para la atención de las solicitudes de acceso a la información que se presenten. • Efectuar notificaciones a las personas solicitantes. • Proponer al Comité de Transparencia los procedimientos internos que aseguren la mayor eficiencia de la gestión en cualesquiera de las solicitudes que sean presentadas, conforme a la normatividad aplicable. • Proponer personal habilitado que sea necesario para recibir y dar trámite a las solicitudes de acceso a la información. • Llevar un registro de las solicitudes, sus respuestas y resultados, así como los costos de reproducción y gastos de envío. • Derivado de solicitudes de acceso a la información, verificar que la información solicitada no se encuentre clasificada. • Promover e implementar políticas de transparencia proactiva procurando su accesibilidad. • Fomentar la transparencia y accesibilidad al interior del sujeto obligado. • Hacer del conocimiento de la instancia competente la probable responsabilidad por el incumplimiento de las obligaciones previstas en la ley y en las demás disposiciones aplicables. • Administrar el Portal de Transparencia de la Secretaría Ejecutiva. • Las que resulten de la Ley General de Transparencia y Acceso a la Información Pública, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y demás normatividad aplicable. <p>En materia de protección de datos personales en posesión de sujetos obligados:</p> <ul style="list-style-type: none"> • Auxiliar y orientar a la persona titular que lo requiera con relación al ejercicio del derecho a la protección de los datos personales. • Gestionar las solicitudes para el ejercicio de los derechos ARCOP.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
		<ul style="list-style-type: none"> • Establecer mecanismos para asegurar que los datos personales sólo se entreguen a su titular o su representante debidamente acreditados. • Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables. • Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCOP. • Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCOP. • Asesorar a las áreas adscritas al responsable en materia de protección de datos personales. • Dar atención y seguimiento a los acuerdos emitidos por el Comité de Transparencia.
Unidad de Transparencia	Auxiliar Administrativo	<ul style="list-style-type: none"> • Realizar la difusión de las obligaciones de transparencia a los órganos administrativos de la Secretaría Ejecutiva. • Registrar las solicitudes de acceso a la información y dar seguimiento y control hasta la resolución de las mismas. • Apoyar a los particulares en la elaboración de solicitudes de acceso a la información. • Realizar el registro de solicitudes mediante el procedimiento establecido que permita obtener eficiencia en la gestión. • Realizar investigaciones documentales de temas relacionados con las políticas, programas y acciones vinculadas con la transparencia. • Transcribir documentos relacionados con los asuntos de la Unidad de Transparencia. • Registrar los avisos de privacidad.
Dirección Jurídica	Director Jurídico	<ul style="list-style-type: none"> • Representar legalmente a la Secretaría Ejecutiva, en el ámbito de su competencia, ante toda clase de autoridades judiciales, administrativas, del trabajo, militares, fiscales y del fuero federal, estatal o municipal; así como ante sociedades, asociaciones, y particulares, en los procedimientos de cualquier índole, con las atribuciones generales y especiales de un mandato para pleitos y cobranzas. • Formular la documentación previa a las sesiones del Órgano de Gobierno y del Comité Coordinador; así como realizar el seguimiento de los acuerdos, de conformidad con la normatividad aplicable.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
		<ul style="list-style-type: none"> • Implementar acciones para la recepción y atención de denuncias por faltas administrativas y hechos de corrupción, con base a lo que establezca el Comité Coordinador y la legislación aplicable. • Vigilar el cumplimiento de las disposiciones jurídicas, en las acciones de las áreas que conforman a la Secretaría Ejecutiva. • Expedir constancias y certificar documentos oficiales que obren en los archivos de la Secretaría Ejecutiva. • Participar en la celebración y suscripción de contratos, convenios, acuerdos y demás actos jurídicos relacionados con los asuntos competencia de la Secretaría Ejecutiva. • Proponer al Secretario Técnico proyectos de elaboración o actualización del Estatuto Orgánico de la Secretaría Ejecutiva. • Proponer al Secretario Técnico los proyectos de iniciativas leyes, decretos, acuerdos, reglamentos y demás disposiciones jurídicas, en materia de anticorrupción competencia de la Secretaría Ejecutiva. • Presentar al Secretario Técnico las sanciones laborales a que se haga acreedor el personal adscrito a la Secretaría Ejecutiva, conforme a la legislación aplicable. • Vigilar que la compilación y difusión de las leyes, reglamentos, decretos, acuerdos, y demás normas jurídicas relacionadas con las atribuciones de la Secretaría Ejecutiva, se efectúe de acuerdo con los tiempos establecidos. • Proporcionar asesoría jurídica al Secretario Técnico y a los titulares de las áreas que integran a la Secretaría Ejecutiva. • Habilitar al personal para que realice notificaciones de oficios, acuerdos y resoluciones de los procedimientos jurídicos, competencia de la Secretaría Ejecutiva. • Proponer al Secretario Técnico las resoluciones y sanciones de los procedimientos administrativos y laborales a que se haga acreedor el personal adscrito a la Secretaría Ejecutiva, así como substanciar los mismos, conforme a la legislación aplicable. • Formular denuncias y querellas ante la institución del Ministerio Público competente, respecto de hechos que pudieran constituir delitos en los que la Secretaría Ejecutiva tenga el carácter de ofendida o se encuentre legitimada para hacerlo; de conformidad con la legislación aplicable, previo acuerdo y aprobación del Secretario Técnico.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
		<ul style="list-style-type: none"> • Coordinar la elaboración de los proyectos de leyes, decretos, reglamentos, circulares y demás disposiciones jurídicas en las materias que sean competencia de la Secretaría Ejecutiva y que se apeguen a las disposiciones legales aplicables. • Participar en la elaboración de los informes que tengan que rendir el Consejo de Participación Ciudadana y la Secretaría Ejecutiva, en el ámbito de su competencia. • Difundir los criterios jurídicos que emitan los tribunales como resultado de sus determinaciones que pudieran impactar en el desarrollo de las funciones de la Secretaría Ejecutiva o en el Sistema Anticorrupción. • Presentar las denuncias penales que procedan como resultado de las irregularidades detectadas, en los términos de lo dispuesto por la Ley del Sistema Anticorrupción del Estado, así como coadyuvar con la autoridad. • Ejecutar sanciones administrativas y penales que se deriven de la omisión en la entrega de información, así como la entrega de documentación e información presuntamente apócrifa y la simulación de actos en que incurran los servidores públicos, así como cualquier entidad, persona física o moral, pública o privada, fideicomiso, mandato o fondo, o cualquier otra figura jurídica, que reciban o ejerzan recursos públicos cuando así se lo soliciten. • Someter a consideración del Secretario Técnico los acuerdos de reformas y adiciones a la normatividad aplicable. • Recibir las quejas y denuncias por hechos de corrupción para su análisis correspondiente en términos de la legislación en materia de responsabilidades administrativas y del Sistema Anticorrupción. • Proponer reglas y procedimientos mediante los cuales se recibirán las peticiones, solicitudes y denuncias fundadas y motivadas por la sociedad civil. • Elaborar y certificar los acuerdos que se tomen en el Comité Coordinador y en el Órgano de Gobierno. • Realizar estudios especializados en materias de prevención, detección y disuasión de hechos de corrupción y de faltas administrativas, fiscalización y control de recursos públicos por acuerdo del Comité Coordinador.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
		<ul style="list-style-type: none"> • Representar a la Secretaría Ejecutiva ante las autoridades federales y locales, tribunales y demás personas físicas y morales; ejercer las acciones judiciales, civiles, penales y contencioso-administrativas en los juicios en los que la Secretaría Ejecutiva sea parte. • Elaborar propuestas de recomendaciones públicas no vinculantes y darles el seguimiento correspondiente, a efecto de garantizar la adopción de medidas dirigidas al fortalecimiento institucional para la prevención de faltas administrativas y hechos de corrupción, así como para mejorar el desempeño del control interno.
Dirección Jurídica	Jefe del Departamento de Asuntos Jurídicos, Normatividad y Seguimiento de Acuerdos	<ul style="list-style-type: none"> • Elaborar los proyectos de estudios de leyes, decretos, reglamentos, circulares y demás disposiciones jurídicas en las materias que sean competencia de la Secretaría Ejecutiva y que éstos se apeguen a las disposiciones legales y normativas aplicables. • Elaborar los informes técnicos y jurídicos solicitados a la Dirección Jurídica. • Elaborar denuncias penales que procedan como resultado de las irregularidades detectadas, en los términos de lo dispuesto por la Ley del Sistema Anticorrupción del Estado, la legislación penal y demás normativa aplicable. • Ejecutar sanciones administrativas y penales que se deriven de la omisión en la entrega de información en que incurran los servidores públicos, entidad, persona física o moral, pública o privada, fideicomiso, mandato o fondo, o cualquier otra figura jurídica, que reciban o ejerzan recursos públicos, a los que se les solicite información en los términos de la Ley del Sistema Anticorrupción del Estado. • Elaborar reglas y procedimientos para la recepción de peticiones, solicitudes y denuncias que la sociedad civil pretenda hacer llegar a la Auditoría Superior del Estado. • Elaborar los acuerdos que se determinen en el Comité Coordinador y Órgano de Gobierno y de los instrumentos jurídicos. • Representar a la Secretaría Ejecutiva ante las autoridades federales y locales, tribunales y demás personas físicas y morales. • Elaborar los proyectos para contestar demandas, presentar pruebas y alegatos y actuar en defensa de los intereses jurídicos de la propia Secretaría Ejecutiva, dando el debido seguimiento a los procesos y juicios en que actúe.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
Dirección Jurídica	Auxiliar Administrativo del Departamento de Asuntos Jurídicos, Normatividad y Seguimiento de Acuerdos	<ul style="list-style-type: none"> • Elaborar propuestas de estudios de leyes, decretos, reglamentos y circulares jurídicas. • Recibir y transcribir denuncias penales de incumplimiento de los servidores públicos en materia de anticorrupción. • Realizar proyectos de sanciones de servidores públicos en materia de anticorrupción. • Elaborar reglas y procedimientos de recepción de solicitudes de denuncias de anticorrupción. • Transcribir acuerdos jurídicos de los órdenes de gobierno. • Dar seguimiento a las acciones judiciales, civiles, penales y contenciosas que se hayan promovido. • Transcribir demandas en materia de anticorrupción. • Realizar los informes periódicos a las instancias normativas internas y externas y gestiones administrativas. • Ordenar los archivos físicos y digitales que tengan que ver con los asuntos del departamento.
Dirección de Vinculación y Políticas Públicas	Director de Vinculación y Políticas Públicas	<ul style="list-style-type: none"> • Preparar en el ámbito de su competencia, los anteproyectos de la política pública estatal en materia de anticorrupción, encaminadas a la prevención, detección y disuasión de hechos de corrupción y de faltas administrativas, para su presentación al Secretario Técnico, de conformidad con la normatividad aplicable. • Preparar en el ámbito de su competencia, las metodologías, indicadores y políticas integrales en materia de anticorrupción, de conformidad con la normatividad aplicable. • Instrumentar propuestas de evaluaciones a la política estatal de anticorrupción y demás políticas integrales; así como realizar dichas evaluaciones una vez aprobadas por el Comité Coordinador. • Implementar acciones para la realización de estudios especializados en materias de prevención, detección y disuasión de hechos de corrupción y de faltas administrativas y de fiscalización y control de recursos públicos, de conformidad con la normatividad aplicable. • Implementar acciones para la elaboración de los anteproyectos de informes del Sistema para su revisión y observación por parte de la Comisión Ejecutiva y remitirlos para aprobación del Comité Coordinador. • Proponer al Secretario Técnico, mecanismos de vinculación con instituciones de los tres órdenes de gobierno para generar acciones conjuntas de impacto social en materia de prevención, detección y erradicación de hechos de corrupción.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
		<ul style="list-style-type: none"> • Implementar estrategias de difusión y comunicación, para dar a conocer al público en general, las acciones a realizar y las realizadas por la Secretaría Ejecutiva, en materia de anticorrupción, así como de los objetivos del Sistema Estatal. • Coordinar la cobertura y difusión en los diferentes medios de comunicación, de los eventos realizados por la Secretaría Ejecutiva, en materia de anticorrupción. • Las demás atribuciones que, en el ámbito de su competencia, le sean encomendadas por el Secretario Técnico, así como las que le confieran las disposiciones legales, administrativas y reglamentarias aplicables.
Dirección de Vinculación y Políticas Públicas	Jefe del Departamento de Diseño, Seguimiento y Evaluación de Políticas Públicas	<ul style="list-style-type: none"> • Elaborar el anteproyecto de la política estatal en materia anticorrupción. • Realizar las evaluaciones correspondientes a la política estatal y demás políticas integrales aprobadas por el Comité Coordinador. • Elaborar las solicitudes de información a los entes públicos respecto del cumplimiento de la política estatal anticorrupción. • Realizar estudios especializados en materia de prevención, detección y disuasión de hechos de corrupción y de faltas administrativas. • Dar seguimiento a los procesos de evaluación generada en temas de anticorrupción para conocimiento del Órgano de Gobierno de la Secretaría Ejecutiva. • Proponer mecanismos, bases y principios para la coordinación con las autoridades de fiscalización, control y de prevención y disuasión de faltas administrativas y hechos de corrupción. • Elaborar los informes requeridos por el Secretario Técnico en materia de políticas públicas.
Dirección de Vinculación y Políticas Públicas	Auxiliar Administrativo del Departamento de Diseño, Seguimiento y Evaluación de Políticas Públicas	<ul style="list-style-type: none"> • Realizar investigaciones sobre las políticas públicas de anticorrupción para ser promovidas por las autoridades superiores en la Secretaría Ejecutiva. • Realizar metodologías para evaluar las políticas públicas de anticorrupción. • Dar seguimiento al cumplimiento de las políticas públicas implementadas de anticorrupción. • Integrar la base de datos de las instituciones que tengan afinidad y relación con la Secretaría Ejecutiva. • Realizar los informes periódicos a las instancias normativas internas y externas y gestiones administrativas.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
Dirección de Sistemas Electrónicos y Plataforma Digital	Director de Sistemas Electrónicos y Plataforma Digital	<ul style="list-style-type: none"> • Implementar el Sistema Electrónico Estatal (SEE) y los sistemas de información que de éste emanen, para contar con información necesaria en materia de anticorrupción y retroalimentar la Plataforma Digital Nacional (PDN), de conformidad con la normatividad aplicable. • Vigilar el cumplimiento de las disposiciones en materia de tecnologías de la información y comunicaciones, en las acciones de los órganos administrativos que conforman a la Secretaría Ejecutiva. • Proponer al Secretario Técnico proyectos de tecnologías de información y comunicaciones para contribuir en la calidad de los servicios que proporciona la Secretaría Ejecutiva. • Contribuir en la remisión y otorgamiento de información vía electrónica con los órganos administrativos que conforman a la Secretaría Ejecutiva. • Proporcionar asesoría, capacitación y asistencia técnica, en materia de tecnologías de la información y comunicaciones, al personal adscrito a los órganos administrativos que integran a la Secretaría Ejecutiva. • Proponer al Secretario Técnico, la normatividad y los programas de desarrollo de sistemas para contribuir en la calidad de los servicios que proporciona la Secretaría Ejecutiva. • Establecer coordinación con las instancias normativas y participar en los comités, consejos y comisiones integrados para mejora de los servicios electrónicos, tecnologías de la información y comunicaciones. • Vigilar que la administración y operación de equipos y sistemas instalados en los órganos administrativos que integran a la Secretaría Ejecutiva sea de acuerdo con la normatividad establecida. • Diseñar y establecer las normas, proyectos y políticas en materia de tecnologías de información y comunicación de la Secretaría Ejecutiva. • Gestionar la implementación y mantenimiento de los sistemas de información ante el Instituto de Ciencia, Tecnología e Innovación del Estado de Chiapas. • Asesorar a los órganos administrativos de la Secretaría Ejecutiva para el adecuado uso y aprovechamiento de los bienes y servicios en materia de tecnologías de información y el acceso a los mismos.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
		<ul style="list-style-type: none"> • Supervisar que el mantenimiento de las redes e infraestructura informática de la Secretaría Ejecutiva se realice oportunamente. • Implementar medidas de control y evaluación para el cumplimiento de las políticas de seguridad en materia de sistemas, tecnologías de información, comunicación y de infraestructura física. • Actualizar los sistemas correspondientes y supervisar el adecuado funcionamiento de los portales electrónicos de la Secretaría Ejecutiva. • Presentar para su autorización los estudios y/o dictámenes de viabilidad técnica y operativa de los requerimientos de contratación de servicios, adquisición o arrendamiento de bienes en materia de redes, tecnologías de información y comunicación al Secretario Técnico. • Administrar la red informática, hardware, software y sistemas de comunicación utilizados dentro de la Secretaría Ejecutiva. • Establecer, en coordinación con el Instituto de Ciencia, Tecnología e Innovación del Estado de Chiapas, un Sistema Electrónico Estatal para que las autoridades competentes tengan acceso. • Generar los mecanismos digitales para que cada responsable en su esfera de competencia pueda dar la retroalimentación a la Plataforma Digital Nacional a que se refiere la Ley General del Sistema Nacional Anticorrupción. • Generar un mecanismo digital para llevar un registro voluntario de las organizaciones de la sociedad civil que deseen colaborar de manera coordinada con el Consejo de Participación Ciudadana para establecer una red. • Diseñar las herramientas para las evaluaciones y estudios realizados a los sistemas de información. • Implementar y administrar los sistemas necesarios para que la Secretaría Ejecutiva cumpla con sus fines, en coordinación con el Instituto de Ciencia, Tecnología e Innovación del Estado de Chiapas. • Supervisar el mantenimiento preventivo y correctivo de los bienes informáticos y de comunicación con los que cuenta la Secretaría Ejecutiva. • Administrar y controlar el inventario de licencias y otros bienes informáticos. • Las demás atribuciones que, en el ámbito de su competencia, le sean encomendadas por el Secretario Técnico, así como las que le confieran las disposiciones legales, administrativas y reglamentarias aplicables.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
Dirección de Sistemas Electrónicos y Plataforma Digital	Jefe del Departamento de Plataforma Digital	<ul style="list-style-type: none"> • Desarrollar sistemas que integren y conecten los diversos sistemas estatales, municipales y federales, en coordinación con el Instituto de Ciencia, Tecnología e Innovación del Estado de Chiapas. • Elaborar mecanismos digitales para el desarrollo de las actividades de las diversas áreas de la Secretaría Ejecutiva cuando así se requiera para dar cumplimiento a las atribuciones referidas en la Ley del Sistema Anticorrupción del Estado de Chiapas. • Elaborar mecanismos digitales para llevar registros de las organizaciones de la sociedad civil para establecer una red de participación ciudadana. • Ejecutar las herramientas digitales para la integración y publicación de las evaluaciones y estudios realizados a los sistemas. • Administrar y asegurar el funcionamiento de los sistemas de evolución patrimonial y de declaración de intereses, de servidores públicos y particulares sancionados, de información pública de contrataciones, de información y comunicación y demás que en el marco de operación del Sistema Electrónico Estatal o de la Plataforma Digital Nacional sean necesarios.
Dirección de Sistemas Electrónicos y Plataforma Digital	Jefe del Departamento de Soporte y Sistemas Electrónicos	<ul style="list-style-type: none"> • Elaborar lineamientos para el adecuado uso y aplicación de los recursos informáticos y de comunicaciones de la Secretaría Ejecutiva. • Supervisar la operatividad de los sistemas de información que requieran las diferentes áreas que conforman la Secretaría Ejecutiva. • Impartir cursos de capacitación para la operación de los sistemas de información al personal de la Secretaría Ejecutiva, así como al personal de las dependencias y entidades de la administración pública estatal en temas anticorrupción. • Desarrollar un programa de mantenimiento preventivo y correctivo de los bienes informáticos con los que cuenta la Secretaría Ejecutiva. • Administrar y controlar el inventario de licencias y otros bienes informáticos. • Elaborar proyectos de mejora continua en materia de tecnologías de información y comunicación. • Realizar el seguimiento al uso correcto de las cuentas de correo electrónico asignadas a los servidores públicos de la Secretaría Ejecutiva. • Controlar el uso de la red de telefonía gubernamental, asignación de equipos de comunicación, bienes informáticos, acceso y asignación de cuentas de red de datos al interior de la Secretaría Ejecutiva.

Área de adscripción	Cargo de la persona que trata datos personales	Funciones
		<ul style="list-style-type: none"> • Respalda la información de las bases de datos que se encuentre en los servidores de la Secretaría Ejecutiva. Elaborar estudios y/o dictámenes de viabilidad técnica y operativa de los requerimientos de los órganos administrativos de la Secretaría Ejecutiva en materia de tecnologías de información y comunicación.

Obligaciones comunes de todas las personas que tratan datos personales

- Observar en todo momento los principios rectores de la protección de datos personales (calidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad y responsabilidad), así como los deberes que los rigen (confidencialidad y seguridad), en cualquier tratamiento que efectúen.
- Proteger los datos personales que tengan en posesión.
- Tratar los datos personales cuando sea exclusivamente necesario.
- Vigilar y supervisar el correcto resguardo de los datos personales que tengan en posesión.

10. Análisis de riesgos, análisis de brecha y plan de trabajo

Las fracciones 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 de un **plan de trabajo**, en los siguientes términos:

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. [...]
- IV. *Realizar un análisis de riesgos 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. [...]

De acuerdo con las fracciones III, IV y V del artículo 35 de la LGPDPPSO y las fracciones IX, X y XVII del artículo 50 de la LPDPPSOCHIS, los análisis de riesgos y de brecha, así como el plan de trabajo, forman parte de **este documento**, como un medio para identificar las medidas de seguridad implementadas y, en relación con ello, las amenazas de vulneración en que se encuentran los datos personales.

Por su parte, los artículos 55, 56 y 57 de los Lineamientos establecen lo siguiente:

Análisis de riesgo. (SIC)

Artículo 55.- *Para dar cumplimiento al artículo 47, fracción IV, de la Ley Estatal, el responsable deberá realizar un análisis de riesgo de los datos personales tratados considerando lo siguiente: (SIC)*

- I. *Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;*
- II. *El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;*
- III. *El valor y exposición de los activos involucrados en el tratamiento de los datos personales;*
- IV. *Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y*
- V. *Los factores previstos en el artículo 47 de la Ley Estatal. (SIC)*

Análisis de brecha.

Artículo 56.- *Con relación al artículo 47, fracción V, de la Ley Estatal, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:*

- I. *Las medidas de seguridad existentes y efectivas;*
- II. *Las medidas de seguridad faltantes, y*
- III. *La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.*

Plan de trabajo.

Artículo 57.- De conformidad con lo dispuesto en el artículo 47, fracción VI, de la Ley Estatal, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Por su parte, los artículos 32 de la LGPDPPSO y 46 de la LPDPPSOCHIS, disponen lo siguiente:

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.*

El análisis de riesgos tiene por objeto identificar el **riesgo inherente** a los datos personales en el tratamiento al que son sometidos en el ejercicio de las atribuciones, facultades y funciones que le han sido conferidas a la SESAECH, con respeto a la integridad de las personas titulares de los mismos, de manera que pueda ser controlado por la institución para satisfacer el derecho humano a la autodeterminación informativa.

La normatividad considera que determinar el riesgo inherente a los datos personales tratados es un deber de los sujetos obligados en la adopción de **medidas de seguridad**, para lo que deben realizar un análisis que considere las **amenazas y vulnerabilidades** para los datos, así como los recursos involucrados en el tratamiento de estos.

Con base en las disposiciones aplicables, la valoración de los riesgos de los datos personales forma parte de los elementos mínimos que debe contener este documento que describe y da cuenta, en lo general, sobre las medidas de seguridad **técnicas, físicas y administrativas** adoptadas, en este caso, por la Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Chiapas, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de ese tipo de datos que están bajo su posesión.

La evaluación de riesgos de los datos personales forma parte de la serie de elementos que integran el presente documento, cuyo propósito es garantizar la **confidencialidad, integridad y disponibilidad** de los datos personales en posesión de este organismo público descentralizado no sectorizado de la administración pública estatal.

A partir de lo expuesto, el análisis de riesgos se lleva a cabo a partir de cuatro fuentes de información:

1. Análisis de riesgos de la **infraestructura tecnológica y recursos de software y hardware**;
2. Análisis de riesgos de **hábitos de seguridad del personal** de la Secretaría Ejecutiva;
3. Análisis de riesgos a partir de los **inventarios de tratamientos** de datos personales, y
4. Análisis de riesgos vinculado con el **cumplimiento de obligaciones** normativas en materia de protección de datos personales en posesión de sujetos obligados.

Los dos primeros análisis se realizan de manera general y aplican transversalmente, ya que el primero refiere a los distintos sistemas o medios en los que se llevan a cabo los diversos tratamientos que realiza el responsable, por lo que los riesgos y controles que se determinen aplican de manera directa a estos medios o sistemas; mientras que el segundo versa sobre los hábitos de seguridad del personal, de manera general y no asociados a un tratamiento en lo particular.

Por su parte, los análisis 3 y 4 se realizan, de manera específica, asociados a cada uno de los tratamientos, y tomando en cuenta sus particularidades.

Los **elementos requeridos** en la fracción IV de los artículos 33 de la LGPDPPSO y 47 de la LPDPPSOCHIS, así como en el artículo 55 de los Lineamientos, se atienden de la siguiente forma:

Elemento requerido	Fundamento	Fuente	Observaciones
Tomar en cuenta amenazas y vulnerabilidades existentes.	Fracción IV de los artículos 33 de la LGPDPPSO y 47 de la LPDPPSOCHIS.	<ul style="list-style-type: none"> Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware; Análisis de riesgos de hábitos de seguridad del personal de la SESAECH; Análisis de riesgos a partir de los inventarios de tratamientos de datos personales, y Análisis de riesgos vinculado con el cumplimiento de obligaciones normativas en materia de protección de datos personales en posesión de sujetos obligados. 	
Tomar en cuenta los recursos involucrados.	Fracción IV de los artículos 33 de la LGPDPPSO y 47 de la LPDPPSOCHIS.	<ul style="list-style-type: none"> Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware, y Análisis de riesgos a partir de los inventarios de tratamientos de datos personales. 	En los inventarios de datos personales y de los sistemas de tratamiento o bases de datos personales se identificaron los medios de almacenamiento y obtención de los datos personales.
Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.	Fracción I del artículo 55 de los Lineamientos.	<ul style="list-style-type: none"> Análisis de riesgos vinculado con el cumplimiento de obligaciones normativas en materia de protección de datos personales en posesión de sujetos obligados. 	El Código de Conducta de la SESAECH ¹⁸ prevé como compromiso de trabajo el manejo apropiado de la información, observando las disposiciones específicas en materia de transparencia y acceso a la información y de protección de datos personales en posesión de sujetos obligados.

¹⁸ Consultable en: <https://sesaech.gob.mx/views/docs/comite-de-etica/normatividad/codigo-de-conducta-de-la-secretaria-ejecutiva-del-sistema-anticorrupcion-del-estado-de-chiapas-2022.pdf>

Elemento requerido	Fundamento	Fuente	Observaciones
El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.	Fracción II del artículo 55 de los Lineamientos.	<ul style="list-style-type: none"> Análisis de riesgos a partir de los inventarios de tratamientos de datos personales. 	En los inventarios de datos personales y de los sistemas de tratamiento o bases de datos personales se identificaron el tipo de datos tratados.
El valor y exposición de los activos involucrados en el tratamiento de los datos personales.	Fracción III del artículo 55 de los Lineamientos.	<ul style="list-style-type: none"> Análisis de riesgos de hábitos de seguridad del personal de la SESAECH. 	
Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.	Fracción IV del artículo 55 de los Lineamientos.	<ul style="list-style-type: none"> Ponderación de riesgos. 	En la ponderación que se hizo al realizar el análisis de riesgos se tomaron en cuenta las posibles consecuencias de una vulneración para las personas titulares de los datos personales, a fin de priorizar y determinar del tratamiento del riesgo.
El riesgo inherente a los datos personales sometidos a tratamiento.	Fracción I de los artículos 32 de la LGPDPPSO y 46 de la LPDPPSOCHIS.	<ul style="list-style-type: none"> Análisis de riesgos a partir de los inventarios de tratamientos de datos personales. 	En los inventarios de datos personales y de los sistemas de tratamiento o bases de datos personales se identificaron el tipo de datos tratados y las finalidades del tratamiento, lo que es considerado al momento de determinar los riesgos.
La sensibilidad de los datos personales sometidos a tratamiento.	Fracción II de los artículos 32 de la LGPDPPSO y 46 de la LPDPPSOCHIS.	<ul style="list-style-type: none"> Análisis de riesgos a partir de los inventarios de tratamientos de datos personales. 	En los inventarios de datos personales y de los sistemas de tratamiento o bases de datos personales se identificaron el tipo de datos tratados y las finalidades del tratamiento, lo que es considerado al momento de determinar los riesgos.
El desarrollo tecnológico.	Fracción III de los artículos 32 de la LGPDPPSO y 46 de la LPDPPSOCHIS.	<ul style="list-style-type: none"> Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware. 	En un análisis que posteriormente realizará la Dirección de Sistemas Electrónicos y Plataforma Digital se considerará el desarrollo tecnológico.
Las posibles consecuencias de una vulneración para las personas titulares de los datos personales.	Fracción IV de los artículos 32 de la LGPDPPSO y 46 de la LPDPPSOCHIS.	<ul style="list-style-type: none"> Ponderación de riesgos. 	Se tomaron en cuenta las posibles consecuencias de una vulneración.

Elemento requerido	Fundamento	Fuente	Observaciones
Las transferencias de datos personales que se realicen o efectúen.	Fracción V de los artículos 32 de la LGPDPPSO y 46 de la LPDPPSOCHIS.	<ul style="list-style-type: none"> Análisis de riesgos a partir de los inventarios de tratamientos de datos personales. 	En los inventarios de datos personales y de los sistemas de tratamiento o bases de datos personales se identificaron las transferencias, lo que es considerado al momento de determinar riesgos y medidas de seguridad.
El número de personas titulares de los datos personales.	Fracción VI de los artículos 32 de la LGPDPPSO y 46 de la LPDPPSOCHIS.	<ul style="list-style-type: none"> Ponderación de riesgos. 	Al elaborar las evaluaciones de impacto en la protección de datos personales del S1 y el S3 del SEE, se tomó en consideración el número de personas titulares de los datos personales para la priorización y determinación del tratamiento del riesgo.
Las vulneraciones previas ocurridas en los sistemas de tratamiento.	Fracción VII de los artículos 32 de la LGPDPPSO y 46 de la LPDPPSOCHIS.	<ul style="list-style-type: none"> Reportes de vulneraciones al Comité de Transparencia. 	Se asume la obligación de notificar al Comité de Transparencia las vulneraciones ocurridas para prever medidas de seguridad y actualizar el documento de seguridad.
El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales sometidos a tratamiento para una tercera persona no autorizada para su posesión.	Fracción VIII del artículo 32 de la LGPDPPSO.	<ul style="list-style-type: none"> Ponderación de riesgos. 	Se deberá tomar en cuenta 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, a fin de priorizar y determinar el tratamiento del riesgo.

Aunado a lo anterior y conforme a lo establecido en el artículo 55 de los Lineamientos, el análisis de riesgos de los datos personales tratados también debe contemplar los siguientes aspectos para garantizar la observancia de lo que expresamente dispone la fracción IV de los artículos 33 de la LGPDPPSO y 47 de la LPDPPSOCHIS:

- Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.
- El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida.
- El valor y exposición de los activos involucrados en el tratamiento de los datos personales.
- Las consecuencias negativas para las personas titulares de los datos personales, que puedan derivar en una vulneración de seguridad.
- El riesgo inherente, la sensibilidad, las posibles consecuencias de vulneración para las personas titulares, las transferencias y vulneraciones previas ocurridas sobre los datos personales, así como el número de titulares de éstos y el riesgo por su valor potencial, además del desarrollo tecnológico.

Bajo esta premisa, para analizar los riesgos de los datos personales que son objeto de tratamiento por la Secretaría Ejecutiva, se aplicó un instrumento para, primeramente, clasificar los datos utilizados, a partir de la categorización existente en la normatividad vigente:

1. **De identificación**, que se refieren a información por la que se identifica a una persona y/o permiten su contacto, como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes (RFC), la Clave Única de Registro de Población (CURP) o la edad.
2. **Patrimoniales**, que comprenden la información que se encuentran vinculados al patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.
3. **Sensibles**, que consideran la información concerniente a la esfera más íntima de la persona titular de los datos o que su uso puede dar origen a discriminación o conllevar un riesgo grave para ésta, como, por ejemplo, el origen étnico o racial, el estado de salud física y/o mental presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

Al respecto y como ya se señaló previamente en este documento, se identificó que en la SESAECH se trabaja sobre todo con datos identificativos o de identificación.

En un segundo momento, para la determinación del riesgo sobre esa tipología de datos personales se valoró la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación (**ciclo de vida**), en correspondencia con la cantidad de datos involucrados, se materialice uno o más factores que pueden causar un daño a la persona titular de los datos (**amenazas**).

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.

A partir de lo anterior, se consideró 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 de la Secretaría Ejecutiva 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.

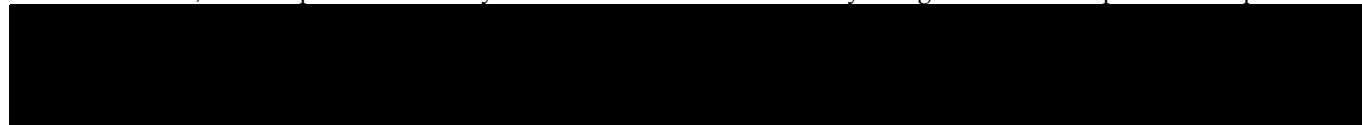
Forma parte integral de este documento de seguridad el **Anexo No. 2** que da cuenta de la realización del análisis de riesgos y el análisis de brecha.

Análisis de la información

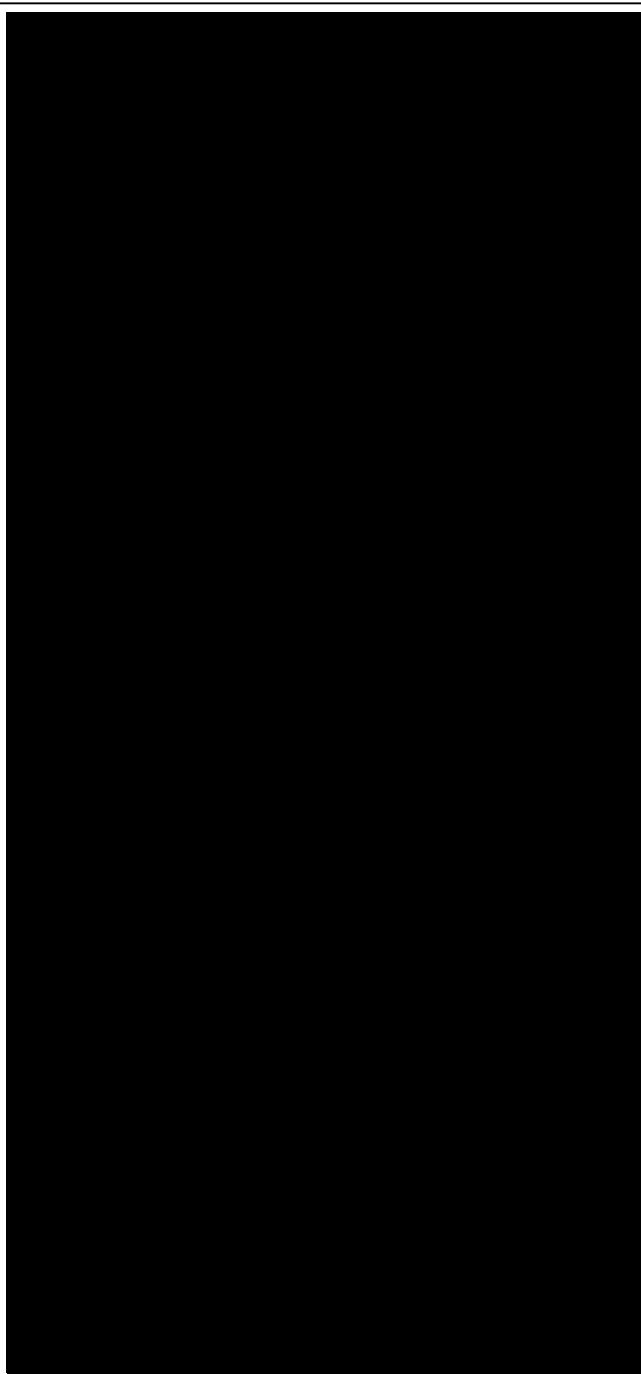
Como resultado de la realización de los análisis de riesgos y de brecha, se identificó que la Secretaría Ejecutiva cuenta con siete áreas en las que tienen lugar tratamientos de datos personales para el desarrollo de 45 procesos, como se ilustra a continuación:

Secretaría Técnica	• 2 tratamientos.
Unidad de Apoyo Administrativo	• 9 tratamientos.
Coordinación de Archivos	• 1 tratamiento.
Unidad de Transparencia	• 4 tratamientos.
Dirección Jurídica	• 2 tratamientos.
Dirección de Vinculación y Políticas Públicas	• 5 tratamientos.
Dirección de Sistemas Electrónicos y Plataforma Digital	• 22 tratamientos.

En ese contexto, el área que observa mayor estado de vulnerabilidad y riesgo de los datos personales que trata es



Nivel de riesgo inherente



La etapa del ciclo de vida en la que los datos personales se encuentran más vulnerables es la correspondiente al

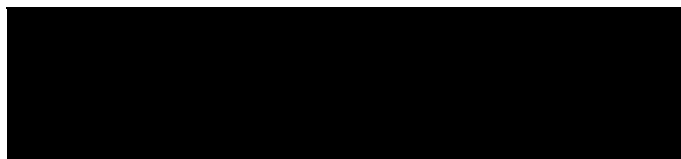


Boulevard Andrés Serra Rojas 1090,
Piso 16 de la Torre Chiapas,
Colonia El Retiro o Paso Limón,
C.P. 29045 Tuxtla Gutiérrez, Chiapas.

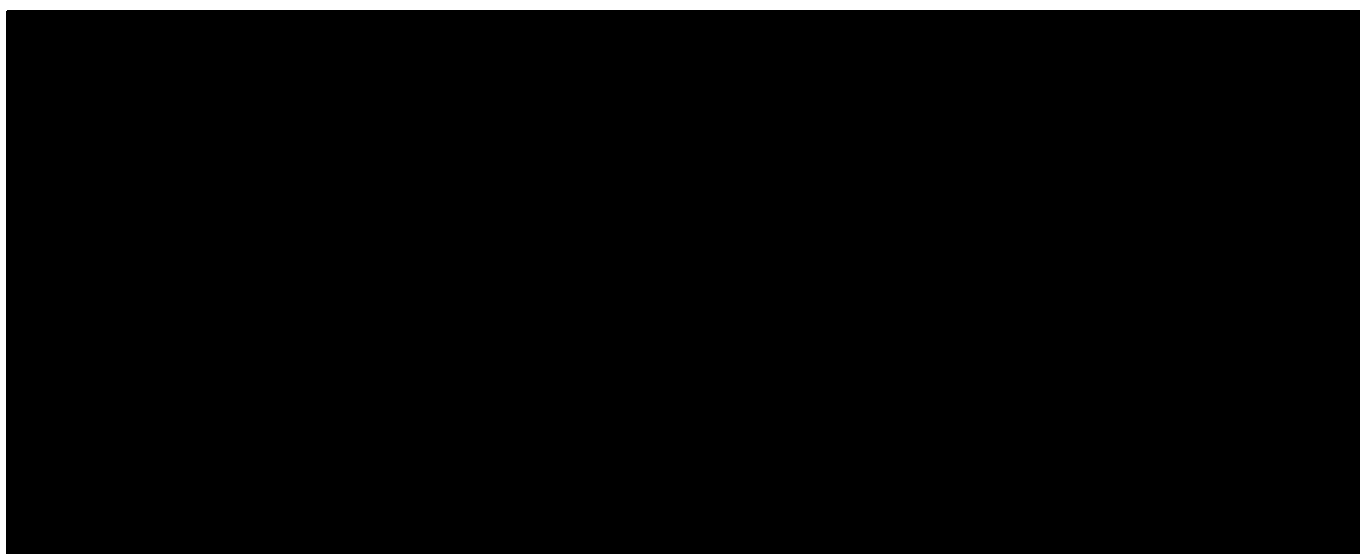
9616912373, opción 3, ext. 69226
transparencia@sesaech.gob.mx

Chiapas sin
Corrupción

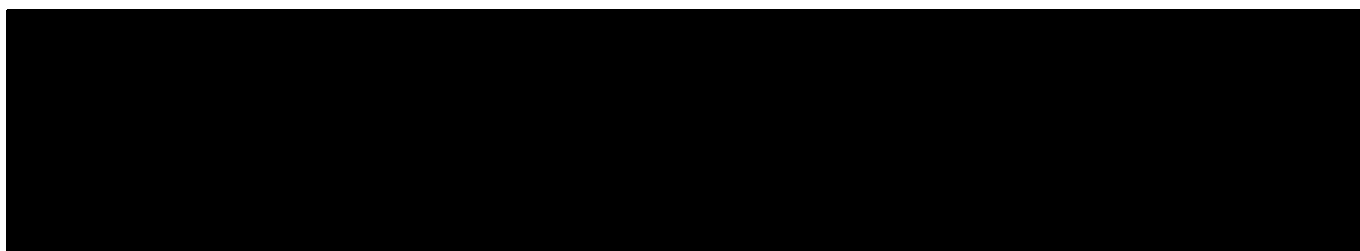
Las amenazas a las que se ven expuestos los datos personales en posesión de la Secretaría Ejecutiva son básicamente:



Nivel de amenaza



Plan de trabajo



por lo que la elaboración de esas evaluaciones de impacto en la protección de datos personales será considerada como el **plan de trabajo** del presente documento de seguridad a corto plazo, a reserva de lo que determine el organismo garante local del estado de Chiapas cuando emita su opinión técnica acerca de las consultas que realice este sujeto obligado del ámbito estatal con fundamento en lo dispuesto en el artículo 12 de las *Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales*¹⁹, expedidas por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (CONAIP-SNT) y publicadas en el Diario Oficial de la Federación (DOF) el 23 de enero de 2018.

¹⁹ Consultables en: http://www.dof.gob.mx/nota_detalle.php?codigo=5511113&fecha=23/01/2018

11. 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 la SESAECH.

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

Medidas de seguridad

Las **medidas generales de seguridad administrativas, físicas y técnicas** con las que actualmente cuenta la Secretaría Ejecutiva para mantener la confidencialidad e integridad de la información, así como para proteger los datos personales contra daño, pérdida, destrucción o alteración, así como evitar su uso, acceso o tratamiento no autorizado, e impedir la divulgación no autorizada de los mismos, son las siguientes:

a) Medidas administrativas



b) Medidas físicas

c) Medidas técnicas

Mecanismos de monitoreo

La supervisión de las medidas de seguridad es un elemento importante para la mejora continua, pues permite definir nuevos controles de monitoreo y seguimiento de éstas, de acuerdo con las necesidades de la Secretaría Ejecutiva.

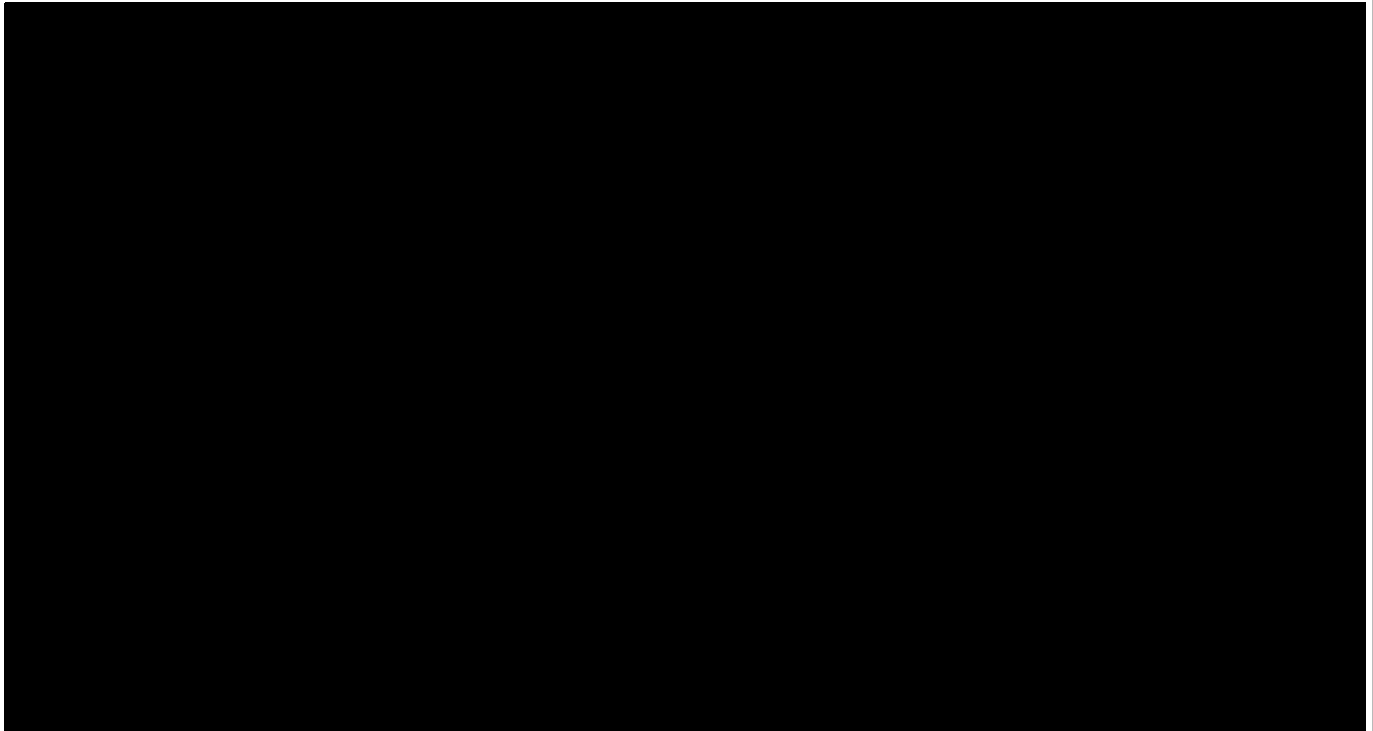
Para los tratamientos de datos personales que realiza la SESA ECH, se han definido los siguientes tipos de monitoreo:

- 1) **Revisión del cumplimiento de las políticas internas de la Secretaría Ejecutiva, relacionadas con el tratamiento de datos personales.** Tiene el objetivo de asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en concordancia con lo establecido en la LGPDPPSO, en la LPDPPSOCHIS, en los Lineamientos y en el resto de la normatividad vigente que resulte aplicable.

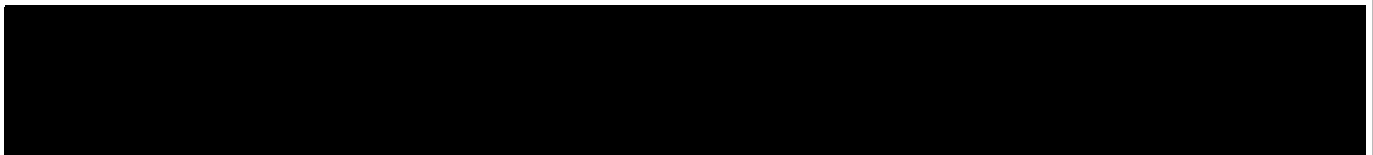
Para ello, cuando se identifique algún cambio en los instrumentos antes mencionados, se deberán realizar las siguientes actividades:

- a. Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.
- b. Revisar y, en su caso, actualizar los avisos de privacidad, así como las funciones y obligaciones del personal y los inventarios de datos personales y de los sistemas de tratamiento, según corresponda.
- c. Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar el análisis de riesgos, el análisis de brecha y el plan de trabajo.
- d. Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

- 2) **Revisión del riesgo.** Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para lo cual se implementarán los siguientes monitoreos:



- 3) **Otros mecanismos adicionales** a los anteriormente señalados:



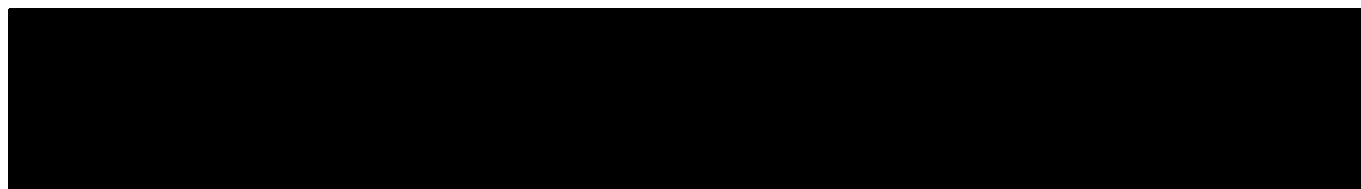
A continuación, se describen los mecanismos de monitoreo y revisión de este sujeto obligado del ámbito estatal:

Elemento por revisar	Fundamento	Acciones
Los activos que se incluyan en la gestión de riesgos.	Fracción I del artículo 58 de los Lineamientos.	
Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.	Fracción II del artículo 58 de los Lineamientos.	
Las nuevas amenazas que podrían estar activas dentro y fuera de la organización y que no han sido valoradas.	Fracción III del artículo 58 de los Lineamientos.	

Elemento por revisar	Fundamento	• Acciones
Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.	Fracción V del artículo 58 de los Lineamientos.	
El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.	Fracción VI del artículo 58 de los Lineamientos.	
Los incidentes y vulneraciones de seguridad ocurridas.	Fracción VII del artículo 58 de los Lineamientos.	

Mecanismos de supervisión, revisión o auditoría

Además del monitoreo continuo de las medidas de seguridad, se requiere realizar una supervisión periódica de tales medidas a través de revisiones o auditorías, las cuales pueden ser internas (desarrolladas por la propia SESAECH) o externas (realizando una contratación o a través de un convenio con un tercero).



12. Programa general de capacitación

Con relación al programa de capacitación, la fracción VIII de los artículos 33 de la LGPDPPSO y 47 de la LPDPPSOCHIS señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá 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.

De acuerdo con la fracción VII del artículo 35 de la LGPDPPSO y la fracción XIX del artículo 50 de la LPDPPSOCHIS, el programa de capacitación forma parte del **documento de seguridad**.

Artículo 35.- De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

VII. El programa general de capacitación.

Artículo 50.- El documento de seguridad deberá contener, al menos, lo siguiente:

XIX. El programa general de capacitación.

Por su parte, el artículo 59 de los Lineamientos dispone lo siguiente:

Capacitación.

Artículo 59.- Para el cumplimiento de lo previsto en el artículo 47, fracción VIII, de la Ley Estatal, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.

En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:

- I. Los requerimientos y actualizaciones del sistema de gestión;*
- II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;*
- III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales,*
y
- IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.*

Asimismo, los artículos 44, fracciones V y VI, de la LGTAIP y 66, fracciones V y VI, de la LTAIPCHIS, así como los artículos 84, fracción VII, de la LGPDPPSO y 114, fracciones I y VIII, de la LPDPPSOCHIS, establecen lo siguiente:

Artículo 44.- Cada Comité de Transparencia tendrá las siguientes funciones:

VIII. Promover la capacitación y actualización de los servidores públicos o integrantes adscritos a la Unidad de Transparencia.

IX. Establecer programas de capacitación en materia de transparencia, acceso a la información, accesibilidad y protección de datos personales para todos los servidores públicos o integrantes del sujeto obligado.

Artículo 66.- Son atribuciones y funciones de los comités de transparencia:

- V. Promover la capacitación y actualización de los servidores públicos o integrantes adscritos a las áreas.
- VI. **Establecer programas de capacitación en materia de transparencia, acceso a la información, accesibilidad y protección de datos personales para el personal del sujeto obligado.**

Artículo 84.- Para los efectos de la presente Ley y sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que le resulte aplicable, el Comité de Transparencia tendrá las siguientes funciones:

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

Artículo 114.- Para los efectos de la presente Ley y sin perjuicio de otras atribuciones que le sean conferidas en la ley de transparencia y demás normatividad que resulte aplicable, el Comité de Transparencia tendrá las siguientes funciones:

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

[Énfasis añadido]

Por ese motivo, en su tercera sesión ordinaria del año 2022, celebrada el 11 de marzo de 2022, el Comité de Transparencia de la Secretaría Ejecutiva aprobó el siguiente “Programa interno de capacitación en transparencia, acceso a la información, protección de datos personales y temas relacionados del ejercicio 2022”:

PROGRAMA INTERNO DE CAPACITACIÓN EN TRANSPARENCIA, ACCESO A LA INFORMACIÓN, PROTECCIÓN DE DATOS PERSONALES Y TEMAS RELACIONADOS					2022	
Entidad federativa	Chiapas	Tuxtla Gutiérrez	Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Chiapas (SESAACH)	Funcionario público al que pertenece	Personal que presta servicios en esta entidad	
Objetivo del programa de capacitación	Impartir cursos de capacitación para cumplir las disposiciones legales en materia de transparencia, acceso a la información y protección de datos personales en posibilitar de sujetos obligados, así como para sensibilizar a los y las beneficiarios de las acciones de capacitación respecto de las consecuencias del incumplimiento de la ley de transparencia.			Fecha de inicio del programa de capacitación	Fecha de término del programa de capacitación	
Perfil del participante a capacitar	Ingeniero del Comité de Transparencia	Si	Si	Si	Si	
	Personal administrativo	Si	Si	Si	Si	
ACCIONES DE CAPACITACIÓN Y PARTICIPANTES PROGRAMADOS A CAPACITAR EN EL 2022						
Acciones de capacitación programadas para el ejercicio 2022 programadas para el ejercicio 2022	Número de acciones programadas a impartir		Número de acciones programadas a impartir			
	Presencial		Presencial		Presencial	
Tema 1: Actualización de la Ley General de Transparencia y Acceso a la Información Pública	1	1	1	1	1	1
Tema 2: Actualización de la Ley General de Transparencia y Acceso a la Información Pública	1	1	1	1	1	1
Tema 3: Procedimiento de impugnación de resoluciones administrativas	1	1	1	1	1	1
Tema 4: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	1	1	1	1	1	1
Tema 5: Tratamiento de datos personales y normas de protección de datos personales	1	1	1	1	1	1
Total	5	5	5	5	5	5

Al respecto, cabe señalar que dicho programa fue documentado en el formato establecido por la *RED Nacional por una Cultura de la Transparencia* que integran o conforman las áreas de capacitación de los 33 organismos garantes del país con la finalidad de unificar, estandarizar u homologar criterios, entre ellas la Dirección General de Capacitación del organismo garante nacional y la Dirección de Capacitación y Promoción de la Transparencia del organismo garante local del estado de Chiapas; el cual fue materializado en los siguientes términos en lo que única y exclusivamente respecta a la materia de protección de datos personales en posesión de sujetos obligados:

Curso	Modalidad	Dirigido a	Lugar	Fecha o periodo para tomar el curso	Fecha límite para entrega de constancia a la UT
4. <i>Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO).</i>	Virtual o en línea.	Todo el personal, las 29 personas servidoras públicas adscritas a la Secretaría Ejecutiva.	https://cevinai-snt.inai.org.mx	Del 1 de julio al 30 de septiembre de 2022.	30 de septiembre de 2022.
5. <i>Tratamiento de datos biométricos y manejo de incidentes de seguridad de datos personales.</i>	Virtual o en línea.	Todo el personal, las 29 personas servidoras públicas adscritas a la Secretaría Ejecutiva.	https://cevinai-snt.inai.org.mx	Del 1 de octubre al 31 de diciembre de 2022.	31 de diciembre de 2022.

Como se puede apreciar, adicionalmente a los cursos impartidos de forma presencial y virtual por la Unidad de Transparencia de la SESAECH o por la Dirección de Capacitación y Promoción de la Transparencia del ITAIPCH, se previó que las personas servidoras públicas beneficiarias de las acciones de capacitación tomaran los cursos en línea que también ofrecen el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT) y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) a través del Centro Virtual de Formación de dicho instituto (CEVINAI), a fin de garantizar un mayor nivel de especialización en las prácticas y conocimientos técnicos de las personas servidoras públicas resguardantes de la información que poseen sus áreas de adscripción, así como responsables del resguardo y tratamiento de los datos personales en posesión de la Secretaría Ejecutiva, lo cual acreditaron mediante la entrega de las siguientes constancias:



Para efectos del ejercicio 2023, el Comité de Transparencia aprobó el siguiente programa interno de capacitación en su segunda sesión ordinaria de dicha anualidad, celebrada el viernes 10 de febrero de 2023:

PROGRAMA INTERNO DE CAPACITACIÓN EN TRANSPARENCIA, ACCESO A LA INFORMACIÓN, PROTECCIÓN DE DATOS PERSONALES Y TEMAS RELACIONADOS					2023			
Entidad federativa:	Chiapas	Sujeto obligado:	Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Chiapas (SESAECH)	Familia o sector al que pertenece:	Poder Ejecutivo, organismo público descentralizado no sectorizado.			
Objetivo del programa de capacitación:	Impartir cursos de capacitación para cumplir las disposiciones legales en materia de transparencia, acceso a la información y protección de datos personales en posesión de sujetos obligados, así como para sensibilizar a las y los beneficiarios de las acciones de capacitación respecto de las consecuencias del incumplimiento de dichas disposiciones.			Fecha de envío del programa al ITAIPCH:	Sujeta a la fecha en que lo apruebe el Comité de Transparencia.			
Perfiles prioritarios a capacitar:	Integrantes del Comité de Transparencia	X	Oficial de Protección de Datos Personales (en caso de que exista)		Enlaces de transparencia de las áreas	X		
	Personal adscrito a la Unidad de Transparencia	X	Titulares de las áreas	X	Áreas priorizadas por el sujeto obligado	X		
ACCIONES DE CAPACITACIÓN Y PARTICIPANTES PROGRAMADOS A CAPACITAR EN EL 2023								
Acciones de capacitación programadas para el ejercicio 2023 (presencial y/o en línea a través del CEVNAI)	Meta estimada de cursos a impartir		Número estimado de participantes a capacitar		Número de cursos programados a impartir por semestre			
					1er. semestre 2023		2do. semestre 2023	
	Presencial	En línea	Presencial	En línea	Presencial	En línea	Presencial	En línea
Tema 1) Guía instructiva para el uso del Sistema de Portales de Obligaciones de Transparencia (SIPOT) de la Plataforma Nacional de Transparencia (PNT).		1		29		1		
Tema 2) Ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad de los datos personales y medios de impugnación.	1		7		1			
Tema 3) Gobierno abierto y transparencia proactiva.		1		29				1
Tema 4) Sistema de gestión de seguridad de datos personales en el sector público.		1		29				1
Total:	1	3	7	87	1	1	0	2

El programa se concretará en los siguientes términos en lo que respecta a la materia de protección de datos personales:

Curso	Modalidad	Dirigido a	Lugar	Fecha o periodo para tomar el curso	Fecha límite para entrega de constancia a la UT
2. Ejercicio de los derechos ARCOP y medios de impugnación.	Presencial.	Enlaces de transparencia de las áreas (7 personas).	Sala Oval o Sala Circular de la Secretaría Ejecutiva	Miércoles 17 de mayo de 2023, de las 11:00 a las 15:00 horas	No aplica.
4. Sistema de gestión de seguridad de datos personales en el sector público.	Virtual o en línea.	Todo el personal (29 personas).	https://cevifaipublica.inai.org.mx	Del 1 de octubre al 29 de diciembre de 2023.	29 de diciembre de 2023.

Al igual que lo hizo en el 2022, la Unidad de Transparencia difundirá ampliamente el nuevo programa interno de capacitación y actualización para las personas servidoras públicas adscritas a esta entidad paraestatal, a efecto de que el personal de la Secretaría Ejecutiva se capacite acerca de la protección de los datos personales en posesión de sujetos obligados, con la finalidad de que las personas servidoras públicas titulares de las áreas y quienes tratan datos personales adquieran los conocimientos técnicos necesarios que les permitan cumplir las disposiciones legales que regulan la materia en el sector público, de tal forma que puedan garantizarse la actualización y mejora continua del inventario de datos personales y de los sistemas de tratamiento o bases de datos personales, así como de los análisis de riesgos y de brecha, al igual que el plan de trabajo, las medidas de seguridad y los mecanismos de monitoreo y revisión de tales medidas, que en su conjunto forman parte integral del presente documento de seguridad, por lo que cada año se propondrá un programa de capacitación que fortalezca las capacidades técnicas de quienes están directa o indirectamente involucrados en la elaboración y actualización de este documento.

13. 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.

Leyenda informativa en colofón que rige a todo el documento sometido a versión pública

Denominación del área o unidad administrativa del cual es titular quien clasifica la información testada:

Unidad de Transparencia.

Identificación del documento del que se elabora la versión pública:

Documento de seguridad en materia de tratamiento de datos personales en posesión de la Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Chiapas (artículos 35 de la LGDPPSO y 49 a 50 de la LPDPPSOCHIS).

Partes o secciones clasificadas, así como las páginas que la conforman:

Apartado	Subapartado	Partes o secciones clasificadas	Página(s)
Análisis de riesgos, análisis de brecha y plan de trabajo	Análisis de riesgos	Observaciones respecto de dos elementos requeridos en la fracción IV de los artículos 33 de la <i>Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados</i> (LGDPPSO) y 47 de la <i>Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas</i> (LPDPPSOCHIS), siendo éstos los siguientes:	
		<ul style="list-style-type: none"> Las amenazas y vulnerabilidades existentes. 	48 (cuarenta y ocho)
		<ul style="list-style-type: none"> El valor y exposición de los activos involucrados en el tratamiento de los datos personales. 	49 (cuarenta y nueve)
		<ul style="list-style-type: none"> El área que observa mayor estado de vulnerabilidad y riesgo de los datos personales que trata. 	52 (cincuenta y dos)
		<ul style="list-style-type: none"> El nivel de riesgo inherente de cada una de las áreas. 	53 (cincuenta y tres)
		<ul style="list-style-type: none"> Las etapas del ciclo de vida en las que los datos personales se encuentran más vulnerables. 	53 (cincuenta y tres)

Apartado	Subapartado	Partes o secciones clasificadas	Página(s)
Análisis de riesgos, análisis de brecha y plan de trabajo	Análisis de riesgos	• Las amenazas a las que se ven expuestos los datos personales.	54 (cincuenta y cuatro)
		• El nivel de amenaza.	54 (cincuenta y cuatro)
	Análisis de brecha	• El análisis de brecha.	Segunda hoja del anexo 2
	Plan de trabajo	• Los tres primeros renglones del párrafo relativo al plan de trabajo.	54 (cincuenta y cuatro)
Mecanismos de monitoreo y revisión de las medidas de seguridad	Medidas de seguridad	• Las medidas administrativas.	55 (cincuenta y cinco)
		• Las medidas físicas.	56 (cincuenta y seis)
		• Las medidas técnicas.	56 (cincuenta y seis)
	Mecanismos de monitoreo	• Los monitoreos que se implementarán en la revisión del riesgo.	57 (cincuenta y siete)
		• Los mecanismos adicionales a los monitoreos que se implementarán en la revisión del riesgo.	57 (cincuenta y siete)
		• Las acciones de los mecanismos de monitoreo y revisión.	57 (cincuenta y siete) y 58 (cincuenta y ocho)
	Mecanismos de supervisión, revisión o auditoría	• Datos sobre los mecanismos de revisión o auditoría.	58 (cincuenta y ocho)

Fundamento que sustenta la clasificación:

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*, emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Razones o circunstancias que motivaron la clasificación:

Difundir o brindar el acceso a las partes o secciones que fueron clasificadas y testadas (párrafos, renglones, líneas, palabras y números o cifras), comprometería la seguridad de los datos personales de personas físicas y podría menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.

Nombre y firma de la persona servidora pública titular del área que clasifica la información:

C. Carlos Gabriel Téllez Girón Gómez



Fecha y número del acta de la sesión de Comité de Transparencia en la que se confirmó o aprobó la versión pública y confirmó la clasificación de la información testada: martes 21 de febrero de 2023, mediante acta número SESA ECH/CT/001-EXT/2023 y resolución número SESA ECH/CT/RES/002/2023.