



GOBIERNO DEL
ESTADO DE
CHIAPAS
2024 - 2030



**SECRETARÍA
DE INFRAESTRUCTURA**
GOBIERNO DE CHIAPAS
2024 - 2030

DOCUMENTO DE SEGURIDAD

Tratamiento de datos personales en posesión de la
Secretaría de Infraestructura

Fecha de elaboración:

28 de septiembre

Contenido

Tabla de contenido

1.- Introducción.....	3
2.- Glosario de acrónimos, términos y conceptos.	6
3.- Objetivos y alcances del documento de seguridad de SEINFRA.	19
3.1 Objetivos Generales.	19
3.2 Objetivos Específicos.....	19
3.3 Alcance del documento de Seguridad.	20
4.- Sistema de gestión de seguridad de los datos personales en posesión de la Secretaría de Infraestructura. ..	21
5.- Inventario de datos y de los sistemas de tratamiento de datos personales de la Secretaría de Infraestructura.....	24
De Identificación:	28
Patrimoniales:	29
Sensibles:.....	29
Laborales:	29
Distribución de Datos Personales requeridos por las Áreas Responsables del Tratamiento	30
6.- Funciones y Obligaciones de las personas que tratan Datos Personales	30
7.- Prueba de Daño y Análisis de Riesgo y Brecha.	33
8.- Gestión de Vulneraciones y Plan de Contingencia	39
9.- Medidas de Seguridad Generales.	41
Plan de Trabajo para Medidas de Seguridad	41
Medidas Administrativas.....	41
Medidas Técnicas	41
Medidas Físicas	41
Mecanismos de Monitoreo y Programa de Capacitación	41
10.- Plan de trabajo.....	41
11.- Propuesta de Capacitación en Materia de Datos Personales.	43
ANEXO 1.....	¡Error! Marcador no definido.



GOBIERNO DEL
ESTADO DE
CHIAPAS
2024 - 2030



**SECRETARÍA
DE INFRAESTRUCTURA**
GOBIERNO DE CHIAPAS
2024 - 2030

1.- Introducción

En el sector público mexicano el derecho a la protección de los datos personales encuentra su antecedente en la expedición de la ya abrogada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental; considerando que los datos personales constituyen el principal activo de información objeto del presente documento, resulta necesario señalar que todos los elementos que lo integran conforman un **sistema interno para la gestión y el tratamiento de los datos personales en posesión de la Secretaría de Infraestructura**. La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, establecen un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos personales que se encuentren en posesión de los sujetos obligados.

A partir de la entrada en vigor de la LGPDPPSO, 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*.

El artículo 28 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, establece que las acciones relacionadas con las medidas de seguridad deberán estar debidamente documentadas e integradas en un sistema de gestión. Se entiende por sistema de gestión, al conjunto de elementos y actividades interrelacionados que permiten establecer, operar, monitorear, mantener y mejorar de manera continua, el tratamiento y la seguridad de los datos personales.

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.

El presente Documento de Seguridad tiene por objeto establecer el marco de referencia para el tratamiento de los datos personales que se realiza al interior de esta Secretaría de Infraestructura a través de los distintos órganos administrativos que integran su estructura orgánica, con la finalidad de mantener vigente y fortalecer la mejora continua de las medidas de protección de dichos datos, en términos de lo dispuesto por los artículos 25, 26, 27, 29, 30, y demás relativos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas

Así, la Secretaría de Infraestructura, comprometida con el cumplimiento de los principios y deberes que rigen el tratamiento de los datos personales, ha impulsado al interior de la institución las acciones necesarias para *prevenir la alteración, pérdida, transmisión, acceso, uso o tratamiento no autorizados de dichos datos*, mediante la *implementación de medidas de seguridad físicas, administrativas y técnicas*, orientadas a garantizar su *confidencialidad, integridad y disponibilidad* durante todo su ciclo de vida.

Para tal efecto, y en términos de lo dispuesto por el artículo 29 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, que establece la obligación de los responsables de elaborar su Documento de Seguridad como parte de un proceso de mejora continua, SEINFRA ha llevado a cabo diversas acciones orientadas a su creación.

Entre dichas acciones destacan la elaboración de los inventarios de datos personales, la revisión y fortalecimiento de las medidas de seguridad implementadas para su tratamiento, así como la realización de análisis de riesgos y de brecha, con el propósito de monitorear la eficacia de las medidas adoptadas, identificar posibles vulnerabilidades y mitigar los riesgos asociados al tratamiento de datos personales.

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.



GOBIERNO DEL
ESTADO DE
CHIAPAS
2024 - 2030



**SECRETARÍA
DE INFRAESTRUCTURA**
GOBIERNO DE CHIAPAS
2024 - 2030

Asimismo, se ha impulsado un proceso permanente de sensibilización institucional sobre la importancia de adoptar medidas preventivas y correctivas en la materia, tomando como referencia los resultados obtenidos de la revisión de los sistemas de datos personales, así como los esquemas de autorregulación y capacitación del personal, con el fin de fortalecer la protección de la información bajo resguardo de Secretaría de Infraestructura.



2.- Glosario de acrónimos, términos y conceptos.

Con respecto a dicho contenido del documento de seguridad, el Diccionario de Protección de Datos Personales, 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 MARBAA932 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).

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**

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.

Autenticar

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 de Infraestructura (SEINFRA), 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 SEINFRA es de carácter reservada o confidencial.
Comité de Transparencia:	Instancia prevista en los artículos 39 y 40 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y regulada, en materia de protección de datos personales, por los artículos 77 y 78 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 77 y 78 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados 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 SEINFRA 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.
TPCH:	Transparencia para el Pueblo 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 a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.
Medidas de seguridad físicas:	Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información. b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información; c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.
Medidas de seguridad técnicas:	Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con el hardware y el software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.



Oficial de Protección de Datos Personales:	Persona servidora pública especialista en protección de datos personales, adscrita a la Unidad de Transparencia, con suficiente jerarquía para implementar las disposiciones normativas en la materia al interior del sujeto obligado. Cabe precisar que la designación del Oficial de Protección de Datos Personales se encuentra prevista en una norma facultativa o potestativa, no imperativa, lo cual única y exclusivamente aplica tratándose de responsables que en el ejercicio de sus funciones sustantivas llevan a cabo tratamientos relevantes o intensivos, por lo que no es obligatorio ni necesario que todos los sujetos obligados cuenten con dicho Oficial, es opcional. La SEINFRA no cuenta con esta figura en la actualidad.
Plataforma Nacional o PNT:	La Plataforma Nacional de Transparencia a que hace referencia el artículo 46 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.
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

Remisión:

Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.



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



Sistema(s) de tratamiento:	Todo conjunto organizado de archivos, registros, ficheros, bases o bancos de datos personales en posesión de alguna de las áreas de la SEINFRA, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Existen dos tipos de sistemas de tratamiento: Físicos: Conjunto ordenado de datos que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos. Automatizados: Conjunto ordenado de datos que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.
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 o 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 prevista en el artículo 41 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y regulada, en materia de protección de datos personales, por el artículo 79 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.



GOBIERNO DEL
ESTADO DE
CHIAPAS
2024 - 2030



**SECRETARÍA
DE INFRAESTRUCTURA**
GOBIERNO DE CHIAPAS
2024 - 2030

3.- Objetivos y alcances del documento de seguridad de SEINFRA.

3.1 *Objetivos Generales.*

El presente documento tiene por objeto ofrecer el marco de trabajo necesario para la protección de los datos personales en posesión de la SEINFRA, 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, 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.

3.2 *Objetivos Específicos*

- Elaborar, aprobar, coordinar y supervisar el programa de protección de datos personales 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



GOBIERNO DEL
ESTADO DE
CHIAPAS
2024 - 2030



**SECRETARÍA
DE INFRAESTRUCTURA**
GOBIERNO DE CHIAPAS
2024 - 2030

Las demás que de manera expresa señale el propio programa.

3.3 Alcance del documento de Seguridad.

El documento de seguridad aplica a todas las áreas de la Secretaría de Infraestructura 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.

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

- 1.Coordinación de Administración y Finanzas;
- 2.Unidad de Informática;
- 3.Subsecretaría de Planeación y Programación;
- 4.Unidad de Transparencia;
- 5.Unidad de Asuntos Jurídicos;
6. Subsecretaría de Desarrollo Urbano y Proyectos;
- 7.Coordinación de Delegaciones;
- 8.Subsecretaría de Obras Públicas;
9. Unidad de Servicios Técnicos

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

4.- Sistema de gestión de seguridad de los datos personales en posesión de la Secretaría de Infraestructura.

El sistema de gestión es el medio por el cual la Secretaría Infraestructura 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, 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 LGPDPSO 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 SEINFRA 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 su responsabilidad, considerando lo establecido en la fracción III de los artículos 27 de la LGPDPSO y 27 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.

Es así que a través del desarrollo de un instrumento homogéneo y estandarizado, se llevó a cabo el levantamiento de inventario de datos, con el propósito de identificar, entre otros aspectos, la categoría y tipo de datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, el nombre, cargo y adscripción de los servidores públicos que tienen acceso a los datos personales, además de si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican; y la vía útil de los datos personales, en ese mismo sentido, el inventario ha contribuido desde el punto operativo a considerar el ciclo de vida de los datos personales, de forma tal que los servidores públicos que intervienen en el tratamiento conocen que, una vez cumplida la finalidad para la cual los datos fueron recabados, estos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción,

lo que cobra especial relevancia en el marco del proceso de baja documental que las áreas realizan conforme a las disposiciones que regulan la gestión documental al interior de la Institución.

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 esta Secretaría.



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, aun cuando no haya existido un daño real, mediante la identificación de la ineficiencia de los controles de acceso físico y electrónicos y el inadecuado establecimiento de los esquemas de privilegios, sumado al poco conocimiento de procesos y responsabilidades en materia de protección de datos personales, además de la falta de definición de perfiles y roles y de seguimiento y monitoreo a los medios de seguridad y la inexistencia de mecanismos para garantizar la confidencialidad por parte del personal.

Las amenazas que se busca prevenir pueden ser de los siguientes tipos:

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

El riesgo que puede presentarse en caso de que las amenazas señaladas 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 SEINFRA.

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.

5.- Inventario de datos y de los sistemas de tratamiento de datos personales de la Secretaría de Infraestructura.

De acuerdo con la fracción I del artículo 29 de la LGPDPPSO y la fracción I del artículo 29 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 SEINFRA.

Por inventario de datos personales se entenderá el control documentado que se llevará de los tratamientos que realizan las áreas de la Secretaría de Infraestructura, realizado con orden y precisión.

A partir de lo anterior, la SEINFRA elaboró los inventarios de los distintos tratamientos de datos personales que realizan o efectúan sus áreas que conforman la estructura orgánica de la Secretaría de Infraestructura, identificando los elementos informativos del inventario a que se refieren los artículos 27, fracción III, y 29, fracción I, de la LPDPPSOCHIS, así como las disposiciones aplicables de los Lineamientos, considerando 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 Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas contenidos en el apartado siguiente:



Órgano Administrativo	Proceso o Tratamiento	Número de Inventarios	Finalidad
1.- Coordinación de Administración y Finanzas	1.- Sistema de registro de asistencia mediante huella. 2.- Integración de expediente de personal 3.- Alta de Personal 4.- Actualización de datos patrimoniales 5.- Tramita el pago de proveedores y contratistas 6.- Envío de documentación del área de contabilidad para viáticos. 7.- Contrato de bienes o servicios 8.- Obtención de Carta de Autorización formato proporcionado por los proveedores	8	1.-Control de asistencia 2.- Alta de Personal y resguardo de documentación 3.- Nómina de pago de personal 4.-Declaración Patrimonial en Declara-Chiapas. 5.- Pago a proveedores y contratistas por Obra pública y proveedores 6.- Pago de viáticos 7.- La información obtenida tiene como finalidad presentar los fundamentos legales y acreditación jurídica de proveedores para poder generar la contratación de bienes o servicios. 8.- La información obtenida tiene como finalidad presentar los datos bancarios para poder generar el proceso de pago de los bienes o servicios contratados



2.- Unidad de Informática	1.- Llenado de datos en la Plataforma de la Secretaría de Anticorrupción y Buen Gobierno	1	1.- Generar certificado de firma electrónica para Declaración Patrimonial.
3.- Subsecretaría y Planeación y Programación	1.- Solicitud de obra de Energía eléctrica. 2.-Solicitud de vialidades 3.- Solicitud de Infraestructura Urbana	3	1, 2 y 3.- Para su revisión técnica e integración de la cédula de Información Técnica (CIT) 1,2 y 3.- Gestionar internamente los expedientes para su programación.
4.- Unidad de Transparencia	1.- Solicitudes de Información Pública. 2.- Solicitudes de ejercicio de Derechos ARCOP. 3.-Sistema de registro de asistencia a capacitaciones.	3	1.- Identificación de la persona solicitante 2.-Identificación de la persona solicitante. 3.-Pase de lista e identificación de los participantes.
5.- Unidad de Asuntos Jurídicos	1.- Elaboración y gestión de Contratos y Convenios de colaboración. 2.-Procesos administrativos del personal adscrito a la SEINFRA.	2	1.- Para acreditar la identidad de la persona al validar su personalidad jurídica. 2.-Para acreditar la identidad de la persona al validar su personalidad jurídica.
6.- Coordinación de Delegaciones	1.- Atención a audiencias y asesorías.	1	1.- Identificación de los participantes.



7.- Subsecretaría de Obras Públicas	1.- Servidor local institucional de obra y supervisión.	1	1.- Identificación de los contratistas participantes para verificar el cumplimiento de los contratos de obra.
8.-Subsecretaría de Desarrollo Urbano y Proyectos	1.- Atención a audiencias y lista de asistencia 2.-Elaboración de Proyectos arquitectónico 3.-Estudios preliminares y cálculos estructurales. 4. Expedientes técnicos de infraestructura de salud. 5.-Expedientes técnicos de electrificación. 6.- Expediente técnico de obra pública. 7.- Integración de expediente en materia de ordenamiento territorial.	7	1.- Pase de lista e identificación de los participantes. 2 y 3.- integrar el expediente técnico de obra pública con Estudios Preliminares-Proyectos Arquitectónico- Proyecto Estructural- Proyecto de Instalaciones- Presupuesto de Obra, para su aceptación de propuesta en el proceso de contratación y ejecución de obra. 4, 5 y 6.- Integración y consulta de expediente técnico para elaboración de presupuesto de obra pública, de acuerdo al tabulador vigente. 7.-Promover la formulación de instrumentos de ordenamiento territorial y desarrollo urbano, para la planeación y regulación del uso de suelo.



9.-Unidad de Servicios Técnicos	1.- Convocatorias para adjudicación de obra o por licitación o invitación.	3	1.-Recabar y disponer de información precisa y verídica sobre la situación técnica y financiera de las empresas contratistas.
	2.- Registro formal de las empresas que asisten a las convocatorias.		2.- Para acreditar la identidad de la persona al validar su personalidad jurídica en la elaboración del acta que contiene firma de los asistentes y determinar la relación contractual entre las partes para la ejecución de la obra pública.
	3.- Captura en el sistema COMPRANET		3.-Se recaban datos para ajustar la oferta técnica para integración de expediente unitario de obra para presentar las propuestas al Comité de Obra Pública para el fallo en el proceso de Licitación e Invitación.

Asimismo, durante el proceso de sistematización se observó que los datos personales cuyo tratamiento se lleva a cabo en los 28 procesos identificados, corresponden a las siguientes 4 categorías, y analizadas mediante tablas de tratamiento **(ANEXO1)**:

De Identificación:

Nombre, Domicilio, CURP, Fotografía, Huella Dactilar, Número de Seguridad Social, Firma, Edad, Clave de Elector, Estado Civil, RFC, Correo Electrónico, No. de Teléfono Personal, Sexo, Información Académica, Fecha y



GOBIERNO DEL
ESTADO DE
CHIAPAS
2024 - 2030



**SECRETARÍA
DE INFRAESTRUCTURA**
GOBIERNO DE CHIAPAS
2024 - 2030

Lugar de Nacimiento, Grado de Estudios Máximo, Nombre del tercero interesado y Domicilio del Tercero Interesado.

Patrimoniales:

Cuentas Bancarias, CLABE Interbancaria, Institución Bancaria, plaza y sucursal y Tipo de Cuenta.

Sensibles:

Alergias, Enfermedades Crónicas, Estado Físico, Estado Mental, Tipo de Sangre, Afiliaciones Políticas, Discapacidad, Historia Clínica, Resultados de Evaluación Psicométrica y de Valores, Creencias Religiosas.

Laborales:

Área de Adscripción, Cargo, Correo electrónico institucional, Teléfono Institucional, Domicilio laboral, Nombre del Representante Legal y categoría.

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

Como resultado de la implementación de los inventarios de datos personales, se identificaron los órganos administrativos que, en el ejercicio de sus atribuciones, llevan a cabo tratamientos que implican la recopilación y el manejo de un mayor volumen de datos personales, por lo que requieren la aplicación de medidas de seguridad acordes con el nivel de riesgo asociado a dichos tratamientos

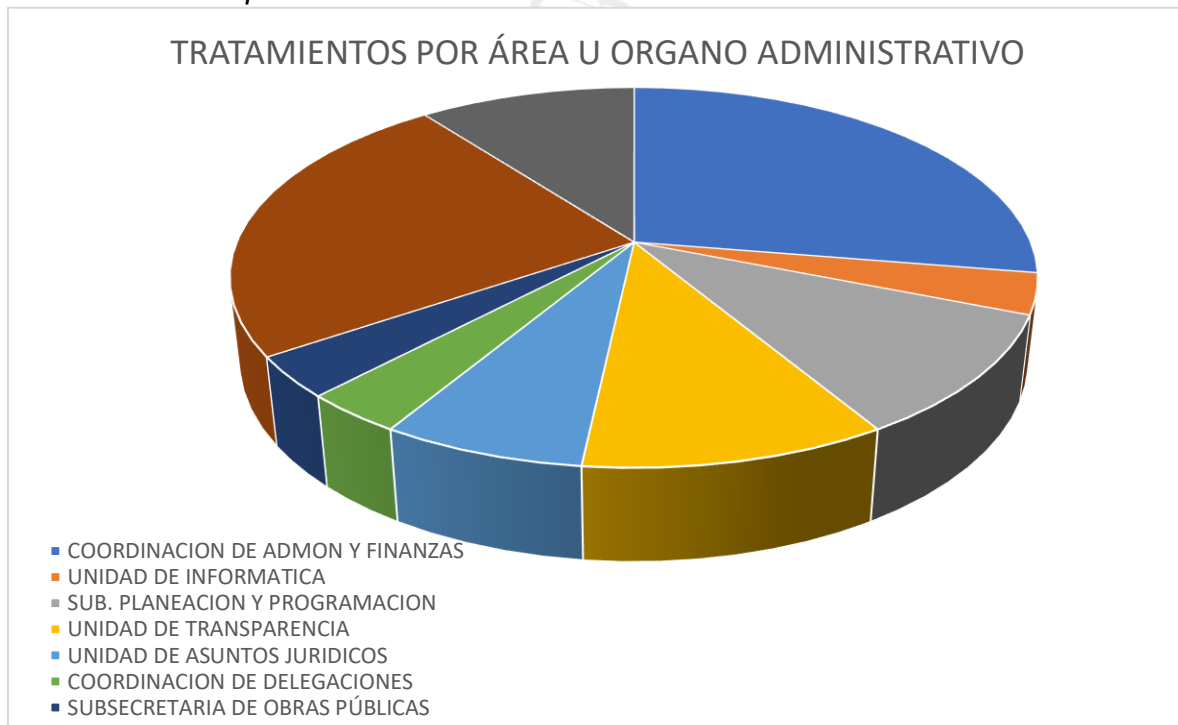


GOBIERNO DEL
ESTADO DE
CHIAPAS
2024 - 2030



**SECRETARÍA
DE INFRAESTRUCTURA**
GOBIERNO DE CHIAPAS
2024 - 2030

Distribución de Datos Personales requeridos *por las Áreas Responsables del Tratamiento*



6.- Funciones y Obligaciones de las personas que tratan Datos Personales

La fracción II de los artículos 27 de la LGPDPPSO y 27 de la LPDPPSOCHIS establece como una de las actividades para implementar y mantener las medidas de seguridad la definición de las funciones y obligaciones del personal 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.

Funciones y obligaciones.

De conformidad con lo anterior, las funciones y obligaciones del personal de la SEINFRA 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:

Órgano Administrativo	Proceso o tratamiento	Nombre o cargo del Servidor Público que tratan datos personales
1.- Coordinación de Administración y Finanzas	1.- Sistema de registro de asistencia mediante huella.	Departamento de Personal y Métodos / C.P. David Espinosa Osorio
	2.- Integración de expediente de personal	
	3.- Alta de Personal	Departamento de Nóminas y Prestaciones Laborales/ Lic. Rosalinda Velázquez Cuesta
	4.- Actualización de datos patrimoniales	
	5.- Tramita el pago de proveedores y contratistas	
	6.- Envío de documentación del área de contabilidad para viáticos.	Dirección de Recursos Materiales y Servicios / Lic. Francisco Javier Vera Morales
	7.- Contrato de bienes y servicios	
	8.- Obtención de Carta de Autorización formato proporcionado por los proveedores	Dirección de Presupuesto y Contabilidad/ C.P. Guadalupe Gómez Chandoquí
2.- Unidad de Informática	1.- Llenado de datos en la Plataforma de la Secretaría de Anticorrupción y Buen Gobierno	Jefe de Unidad de Informática/ L.S.C. Jorge Arturo Morales Herrera
3.- Subsecretaría y Planeación y Programación	1.- Solicitud de obra de Energía eléctrica.	
	2.- solicitud de vialidades	Subsecretaría de Planeación y Programación
	3.- Solicitud de Infraestructura Urbana	Arq. Hermilo Bedrán Ruíz



GOBIERNO DEL
ESTADO DE
CHIAPAS
2024 - 2030



**SECRETARÍA
DE INFRAESTRUCTURA**
GOBIERNO DE CHIAPAS
2024 - 2030

4.- Unidad de Transparencia	1.- Solicitudes de Información Pública. 2.- Solicitudes de ejercicio de Derechos ARCOP. 3.- Sistema de registro de asistencia a capacitaciones.	Responsable de la Unidad de Transparencia / Lic. Jonathan de Jesús Molina Orozco
5.- Unidad de Asuntos Jurídicos	1.- Elaboración y gestión de Contratos y Convenios de colaboración. 2.- Procesos administrativos del personal adscrito a la SEINFRA.	Jefe de la Unidad de Asuntos Jurídicos / Lic. Jonathan de Jesús Molina Orozco Jefe del Área de Asuntos Administrativos / Lic. Octavio Solís Jiménez
6.- Coordinación de Delegaciones	1.- Atención a audiencias y asesorías.	Coordinación de Delegaciones / Ing. Hugo Adrián de la Cruz Vázquez
7.- Subsecretaría de Obras Públicas	1.- Servidor local institucional de obra y supervisión.	Subsecretario de Obras Públicas / Ing. Cicerón Arguello Kanter.
8.- Subsecretaría de Desarrollo Urbano y Proyectos	1.- Atención a audiencias y lista de asistencia 2.- Elaboración de Proyectos arquitectónico 3.- Estudios preliminares y cálculos estructurales. 4. Expedientes técnicos de infraestructura de salud. 5.- Expedientes técnicos de electrificación.	Subsecretario de Desarrollo Urbano y Proyectos / Mtro. Marco Antonio Constantino Vera Directora de Proyectos / Arq. Violeta Aurora González Gerardo Jefe de Departamento de Presupuestos de la Obra Pública / Ing. Gustavo Enrique Cristiani Gordillo Jefa de Departamento de Regulación de Uso de Suelo / Arq. Liliana Gómez Bustamante



	6.- Expediente técnico de obra pública. 7.- Integración de expediente en materia de ordenamiento territorial.	Jefa de Departamento de Estudios y Programas de Desarrollo Urbano/ Arq. Karla María García Rodríguez Jefe de Departamento de Cálculo Estructural e Instalaciones/ Ing. David Alvarado Jiménez Directora de Ingeniería de Costos/ Arq. María del Carmen Torres Rincón Jefe de Departamento de Cuantificación de Obra Pública/ Ing. Isidro Martínez Martínez
9.-Unidad de Servicios Técnicos	1.- Convocatorias para adjudicación de obra o por licitación o invitación. 2.- Registro formal de las empresas que asisten a las convocatorias. 3.- Captura en el sistema COMPRANET	Jefa de la Unidad de Servicios Técnicos/ C.P. Ofelia Núñez Cabrera. Jefe del Área de Contrato y Archivo Único/ Lic. Sergio Lorenzo López Córdova Jefa del Área de Normatividad y Convocatoria/ L.A.E. Ibrahim Díaz Cortez

7.- Análisis de Riesgos y Análisis de Brecha.

Los artículos 28, fracciones IV, V y VI, y 29 fracciones III, IV y V de la LPDPPSOCHIS establecen respectivamente, la obligación de seguridad la realización de los análisis de riesgos y de brecha, y elaborar el plan de trabajo, así como su incorporación al Documento de Seguridad 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:

- 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;

De acuerdo con las fracciones III, IV y V del artículo 29 de la LGPDPPSO y las fracciones III, IV y V del artículo 29 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.

En ese contexto cada área administrativa realizó su Análisis de Riesgo y Brecha:

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



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

aplicaciones o en el sistema



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

2.- Unidad de
Informática

de contraseñas debiles.



**3.- Subsecretaría y
Planeación y
Programación**

**4.- Unidad de
Transparencia**

**5.- Unidad de
Asuntos Jurídicos**

**6.- Coordinación
de Delegaciones**

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

3.- Comparar
archivos sin control



**7.- Subsecretaría
de Obras Públicas**

**8.-Subsecretaria
de Desarrollo
Urbano y
Proyectos**

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

**9.-Unidad de
Servicios Técnicos**



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

8.- Gestión de Vulneraciones y Plan de Contingencia

Se testa el apartado número 8, que contiene la Gestión de Vulneraciones y Plan de contingencia, toda vez que contiene información sensible sobre la forma en que el sujeto obligado previene, detecta, contiene, responde y recupera la operación ante incidentes de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3 fracción IX, y 6 párrafo primero, de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

todo con datos identificativos o de identificación.



Se testa el apartado número 8, que contiene la Gestión de Vulneraciones y Plan de contingencia, toda vez que contiene información sensible sobre la forma en que el sujeto obligado previene , detecta , contiene, responde y recupera la operación ante incidentes de seguridad, de conformidad en los dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3 fracción IX, y 6 párrafo primero, de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

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.

9.- Medidas de Seguridad Generales.

Plan de Trabajo para Medidas de Seguridad

Para mitigar los riesgos identificados, se ejecutarán de manera inmediata las siguientes medidas:

Medidas Administrativas

- Firmar cartas de confidencialidad con todos los servidores públicos adscritos a las Direcciones.

Medidas Técnicas

- Restringir los accesos en red mediante perfiles de usuario protegidos con contraseñas robustas (mínimo 12 caracteres, alfanuméricas).
- Prohibir la transferencia de expedientes técnicos que contengan datos personales a través de memorias USB o correos electrónicos personales (@gmail, @outlook, etc.).

Medidas Físicas

- Custodiar el archivo de concentración de las Direcciones

Mecanismos de Monitoreo y Programa de Capacitación

- **Vigilancia y revisión:** el director y jefes de Departamento realizarán revisiones semestrales aleatorias en los archivos físicos y digitales del área de obras.
- **Programa de Capacitación:** Todo el personal administrativo y de supervisión deberá tomar el curso anual "La protección de datos personales en los procesos de contratación y ejecución de Obra" y "Guía para la elaboración de Documentos de Seguridad y Tratamiento de Datos Personales en los procesos"

10.- Plan de trabajo.

Se testa el apartado número 9, que contiene el Plan de Trabajo, en virtud de ser un instrumento de gestión que deriva del análisis de riesgo y brecha, en el que se establecen las acciones específicas que el sujeto obligado implementará para corregir deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de datos personales, de conformidad con lo dispuesto en los Artículos 103 fracción III, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo trigésimo octavo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.



GOBIERNO DEL
ESTADO DE
CHIAPAS
2024 - 2030



**SECRETARÍA
DE INFRAESTRUCTURA**
GOBIERNO DE CHIAPAS
2024 - 2030

Se testa el apartado número 9, que contiene el Plan de Trabajo, en virtud de ser un instrumento de gestión que deriva del análisis de riesgo y brecha, en el que se establecen las acciones específicas que el sujeto obligado implementará para corregir deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de datos personales, de conformidad con lo dispuesto en los Artículos 103 fracción III, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo trigésimo octavo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Se testa el apartado número 9, que contiene el Plan de Trabajo, en virtud de ser un instrumento de gestión que deriva del análisis de riesgo y brecha, en el que se establecen las acciones específicas que el sujeto obligado implementará para corregir deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de datos personales, de conformidad con lo dispuesto en los Artículos 103 fracción III, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo trigésimo octavo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

11.- Propuesta de Capacitación en Materia de Datos Personales.

La Unidad de Transparencia difundirá ampliamente el nuevo programa interno de capacitación y actualización para las personas servidoras públicas adscritas a esta Secretaría de Infraestructura, a efecto de que el personal de la Secretaría de Infraestructura 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.

PROGRAMA INTERNO DE CAPACITACIÓN EN TRANSPARENCIA, ACCESO A LA INFORMACIÓN, PROTECCIÓN DE DATOS PERSONALES Y TEMAS RELACIONADOS					2026
Entidad federativa:	Chiapas	Sujeto obligado:	Secretaría de Infraestructura	Sector al que pertenece:	Poder Ejecutivo
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			Fecha de envío del programa:	Sujeta a la fecha en que lo apruebe el Comité de Transparencia.



	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.					
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 prioritizadas por el sujeto obligado	X

