



GOBIERNO DEL
ESTADO DE
CHIAPAS
2024 - 2030



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

Glosario de acrónimos , términos y conceptos.

Fecha de elaboración:

28 de septiembre



GOBIERNO DEL
ESTADO DE
CHIAPAS
2024 - 2030



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

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 Frago 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 Frago 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.
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 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.