



GOBIERNO DEL
ESTADO DE
CHIAPAS
2024 - 2030



UNIDAD DE
TRANSPARENCIA

SECRETARÍA DE EDUCACIÓN

GOBIERNO DE CHIAPAS
2024 - 2030

DOCUMENTO DE SEGURIDAD

PROTECCIÓN DE DATOS PERSONALES



**HUMANISMO QUE
TRANSFORMA**

GOBIERNO DE CHIAPAS
2024 - 2030

ÍNDICE

Introducción	1
Marco Normativo	2
Glosario	3
Obligatoriedad del documento de seguridad	8
Pasos para la elaboración del documento de seguridad	8
Sistema de gestión	11
Medidas y niveles de seguridad	12
De los sistemas de tratamiento y el inventario de datos personales	13
Inventario de datos	13
Funciones y obligaciones en el tratamiento de datos personales	14
Análisis de riesgo	16
Categoría de datos	17
Riesgo inherente a los datos personales	19

ÍNDICE

Formulario para el análisis de riesgo	19
Niveles de riesgo por unidad administrativa	21
Conclusión	22
La sensibilidad de los datos personales tratados	23
Las posibles consecuencias de una vulneración para los titulares	24
Las transferencias de datos personales	26
Las vulneraciones previas ocurridas en los sistemas de tratamiento	26
Recomendaciones de implementación	33
Plan de trabajo	33
Mecanismos de monitoreo y supervisión de protección de datos personales	34
Etapas de monitoreo	34
Etapas de supervisión	35

ÍNDICE

Mecanismos de actuación ante alertas y vulneraciones a la seguridad de los datos personales	36
Alertas seguridad de los datos personales	37
Vulneraciones de seguridad de los datos personales	38
Notificación de la vulneración a los particulares	41
Finalidades y objetivos	42
Instancia ejecutora y ámbito de aplicación	43
Etapas de las auditorías en materia de datos personales	43
Etapa de apertura	44
Etapa de revisión	45
Etapa conclusiva	46
Aprobación del documento de seguridad	50
ANEXOS: Catálogo completo de tratamientos	51

INTRODUCCIÓN

La información y los Datos Personales son activos que deben protegerse; en atención a esto, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas ha establecido las bases que regulan los procedimientos que garantizan el derecho a la protección de toda aquella información relativa a una persona física identificada o identificable en forma directa o indirecta.

Así mismo, debemos entender que, además de una situación de deber normativa, la gestión de la seguridad de la información en materia de datos personales es parte de un sistema de mejora continua, con implicaciones amplias y que busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información.

Partiendo de lo anterior y tomando en cuenta que la Secretaría de Educación es sujeto obligado en materia de protección de datos personales y considerando la probabilidad de los riesgos y vulneraciones que pudieran presentarse, y que resulte en una afectación a la privacidad y a la intimidad de los titulares de los datos que se recaban en los diversos procedimientos, y dando cumplimiento a los principios y deberes señalados en la normatividad aplicable, se elaboró el presente Documento de Seguridad para Sistemas de Datos Personales en congruencia de las disposiciones jurídicas vigentes, y los estándares internacionales, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal.

El Documento de Seguridad, brinda a la Secretaría de Educación homogeneidad en la organización de los procesos y sistemas, permite que el Comité de Transparencia, conjuntamente con la Unidad de Transparencia y los responsables de los tratamientos en las diversas Unidades Administrativas definan las medidas de seguridad administrativas, físicas y técnicas con que se deben contar, para implementar las mejoras en un plan de trabajo anual.

Así mismo, tiene como propósito controlar internamente el universo de datos personales, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas, así como los análisis de riesgo y brecha, las bitácoras de acceso, vulneraciones, el plan de trabajo anual y la implementación del plan de capacitación.

El presente documento de seguridad fue elaborado por la Unidad de Transparencia con la información aportada por cada una de las Unidades Administrativas que integran la secretaría y aprobado por el Comité de Transparencia.

MARCO NORMATIVO

Las bases jurídicas de los mecanismos de protección de datos personales y del presente documento se encuentran en:

- Constitución Política de los Estados Unidos Mexicanos artículos 6 y 16.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Lineamientos Generales de Protección de Datos Personales para el sector público.
- Constitución Política del Estado Libre y Soberano del Estado de Chiapas.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.
- Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas
- Ley Orgánica de la Administración Pública del Estado de Chiapas.
- Ley de Educación del Estado Libre y Soberano de Chiapas.
- Reglamento Interior de la Secretaría de Educación del Estado de Chiapas.

GLOSARIO

Autoridades Garantes Al Órgano Desconcentrado, jerárquicamente subordinado a la Secretaría Anticorrupción y Buen Gobierno y a los órganos encargados de la contraloría interna u homólogos o equivalentes de los poderes Legislativo y Judicial, así como de los organismos u órganos autónomos; el Instituto de Elecciones y Participación Ciudadana, por cuanto hace a los partidos políticos.

Aviso de privacidad Al documento puesto a disposición de la persona titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus Datos Personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Bases de datos Al conjunto ordenado de Datos Personales referentes a una persona 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 A la identificación y conservación de 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 estas. Durante dicho periodo, los Datos Personales no podrán ser objeto de tratamiento y, transcurrido este, se procederá a su cancelación en la base de datos que corresponda.

Comité de Transparencia A la Instancia a la que hace referencia el artículo 39 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

Cómputo en la nube Al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

Consentimiento La manifestación de la voluntad libre, específica e informada de la persona titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

Datos personales A cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos personales sensibles A los datos que se refieran a la esfera más íntima de su titular o cuya utilización indebida pueda dar lugar a discriminación o conlleve un riesgo grave para esta. De manera enunciativa más no limitativa, se consideran sensibles los Datos Personales que puedan revelar aspectos como origen étnico o racial, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Derechos ARCO A los derechos de acceso, rectificación, cancelación, oposición y Portabilidad al tratamiento de los Datos Personales.

Disociación El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

Documento de seguridad Al instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los Datos Personales que posee.

Evaluación de impacto en la protección de datos personales Al documento mediante el cual los Sujetos Obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de Datos Personales, valoran los impactos reales respecto de determinado tratamiento de Datos Personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de las personas titulares, así como los deberes de los responsables y las personas encargadas, previstos en las disposiciones jurídicas aplicables.

Fuentes de acceso público

Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución.

No se considerará fuente de acceso público cuando los datos personales contenidos en la misma sean obtenidos o tengan una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás normatividad que resulte aplicable.

LPDPPSOCH

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Ley General

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Medidas de Seguridad

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

Medidas de Seguridad administrativas

A las 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

Al conjunto de acciones y mecanismos para proteger el entorno físico de los Datos Personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
- d) Proveer a los equipos que contienen o almacenan Datos Personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

**Medidas de
seguridad técnicas**

Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

Persona encargada

A la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate Datos Personales a nombre y por cuenta del responsable.

Plataforma Nacional

A la Plataforma Nacional de Transparencia a la que hacen referencia la Ley General de Transparencia y Acceso a la Información Pública y la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

Remisión

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

Supresión

La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Sujetos Obligados

A cualquier autoridad, dependencia, entidad, órgano u organismo o equivalente de los poderes Ejecutivo, Legislativo y Judicial; organismos u órganos autónomos; partidos políticos y fideicomisos y fondos públicos, en el ámbito estatal y municipal.

Titular

La persona física a quien corresponden los datos personales.

Transferencia

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

Tratamiento

A 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, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de Datos Personales.

**Unidades
Administrativas**

Las áreas administrativas que integran a la Secretaría de Educación, previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento y ser responsables o encargadas de los Datos Personales.

**Unidad de
Transparencia**

A la instancia referida en el artículo 41 de la presente Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

OBLIGATORIEDAD DEL DOCUMENTO DE SEGURIDAD

El Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y tiene entre sus funciones el coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la Secretaría.

Atendiendo a los deberes que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, el documento de seguridad es aplicable para todas y cada una de las unidades administrativas de la Secretaría, por lo que todos los servidores públicos que en el ejercicio de sus atribuciones, administren y manejen bases de datos, en las que den tratamiento de datos personales a través de algún sistema, ya sea que se encuentren en soportes físicos o electrónicos, deberán realizar las acciones necesarias para cumplir con las obligaciones que establece el presente documento de seguridad, para lo cual deberán asignar los recursos materiales y humanos necesarios y prever lo que se requiera en sus programas de trabajo.

PASOS QUE SE SIGUIERON PARA LA ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD

Para identificar los sistemas de datos que se manejan en la Secretaría de Educación, se estableció un mecanismo de trabajo basado en la detección operativa desde cada una de las unidades administrativas generales, las cuales coordinaron la detección de los diversos sistemas en las direcciones, departamentos, oficinas y programas que están a su cargo; bajo este procedimiento se consultó a las unidades administrativas de la Secretaría de Educación para que informaran si cuentan con sistemas de datos personales, el objetivo y fundamento normativo de los mismos, que realizaran una descripción e identificación de la estructura de los sistemas de tratamientos de datos personales; así mismo se estableció un análisis de las medidas de seguridad que actualmente implementan y desarrollaran un análisis de riesgos y de brecha, que permitiera elaborar un plan de trabajo.

El ejercicio considero una estrategia trabajada con la estructura operativa y normativa; atentos a esto, se hizo llegar oficio a cada una de ellas con la finalidad de que nombrara al servidor público enlace de datos personales, y que será responsable de colaborar con cada una de las tareas establecidas, se procedió a revisar y conocer todas aquellas bases de datos en que se realiza tratamiento de datos; realizado el primer ejercicio identificativo general, fue necesario un análisis particular para cada uno de los tratamientos, acciones que se desarrollaron por medio de reuniones de trabajo grupales, asesorías presenciales individuales, capacitaciones virtuales, llamadas telefónicas y el uso de correo electrónico como medio para obtener información final; de esta forma se consolidó y reflejó la información de las diferentes áreas en ejercicio de sus atribuciones y funciones y se incluyeron todas aquellas que manejan bases de datos o que de alguna forma por normatividad supletoria dan tratamiento a datos de carácter personal con independencia de los soportes en que los concentren.

Mediante este procedimiento se determinó que las Unidades Administrativas que manejan y operan los sistemas de tratamientos que deberán observar el Programa de Protección de Datos Personales en la Secretaría de Educación son las siguientes:

- 1.** Oficina de la C. Secretaria de Educación
- 2.** COSICAMM
- 3.** Coordinación de Programas Especiales y Compensatorios
 - Programa Nacional de Ingles (PRONI)
 - PFSEE
 - PEMCH
 - INSUMOS
 - DESARROLLO SOCIAL
 - LIBROS DE TEXTO Y MATERIAL EDUCATIVO
 - AREA DE BECAS Y CONVOCATORIAS
 - VER BIEN PARA APRENDER MEJOR
- 4.** Coordinación General de Asuntos Jurídicos y Laborales
 - Dirección de Asuntos Federalizados
 - Dirección de Asuntos Estatales
- 5.** Dirección de Divulgación
- 6.** Igualdad de Género
- 7.** Unidad de Transparencia
- 8.** Dirección de Tecnologías Educativas y de la Información
- 9.** Direccion Técnica Educativa

- 10. Subsecretaría de Educación Estatal**
 - Dirección de Educación Básica
 - Primaria
 - Preescolar
 - Secundarias
 - Telesecundarias
 - Educación física
 - Educación indígena
 - Integración educativa
 - Dirección de Educación Media
 - Dirección de Educación Superior
 - Dirección de Fortalecimiento Educativo
- 11. Subsecretaría de Educación Federalizada**
 - Dirección de Educación Elemental
 - Dirección de Educación Primaria
 - Dirección de Educación Secundaria y Superior
 - Dirección de Educación Indígena
- 12. Subsecretaría de Planeación Educativa**
 - Oficina del Subsecretario
 - Dirección de Programación y Presupuesto
 - Dirección de Planeación Educativa
 - Dirección de Evaluación y Programas Institucionales
- 13. Coordinación General de Administración Estatal**
 - Oficina del Coordinador
 - Dirección de Administración de Personal
 - Dirección de Recursos Financieros
 - Dirección de Recursos Materiales y Adquisiciones
 - Dirección de Informática
 - Dirección de Auditorías
- 14. Coordinación General de Administración Federalizada**
 - Dirección de Administración de Personal
 - Dirección de Recursos Materiales y Adquisiciones
 - Dirección de Recursos Financieros
 - Dirección de Informática
 - Coordinación General de Auditorías
- 15. Dirección de Servicios Regionales**
- 16. Coordinación Estatal de Formación Continua de Maestros en Servicio**
- 17. FOVIMCHIS**

SISTEMA DE GESTIÓN

Los Lineamientos Generales de Protección de Datos Personales para el Sector Público, estipula que el sistema de gestión deberá permitir planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.

Y tiene como propósito controlar internamente el universo de datos personales que posee la Secretaría de Educación y forma parte de las políticas internas y de gestión del tratamiento de datos personales de la Secretaría, dentro de sus objetivos se encuentran los siguientes:

- I.** Establecer las acciones que se llevarán a cabo tendientes al establecimiento de medidas de seguridad para el tratamiento de datos personales en la Secretaría.
- II.** Definir las actividades que llevan a cabo las áreas administrativas para la implementación, monitoreo y buenas prácticas en el tratamiento y seguridad de los datos personales en la Secretaría, lo anterior mediante:
 - A.** El conocimiento del marco normativo y políticas aplicables en el tratamiento de datos personales.
 - B.** El establecimiento de la política interna de gestión y tratamiento de datos personales tomando en consideración: Atribuciones y obligaciones de las unidades administrativas; principios y deberes que rigen el tratamiento, transferencia, remisión, uso de cómputo en la nube, el ejercicio de derechos ARCOP, derecho de portabilidad, ciclo de vida, supresión, los procedimientos de orientación, atención de quejas y sanciones relacionadas con el tratamiento de datos personales.

MEDIDAS Y NIVELES DE SEGURIDAD

De acuerdo con lo señalado en la Normatividad Estatal se indica la obligación de adoptar las medidas que se estime necesarias para brindar garantía en la protección y resguardo de los sistemas y bases de datos personales, siendo esencial su establecimiento e implementación y proteger la información que se recaba; en este sentido las medidas de seguridad de los datos personales deberán ser el conjunto de acciones, actividades, controles o mecanismos que permiten protegerlos contra su daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, garantizando con ello su confidencialidad, integridad y disponibilidad. Las medidas de seguridad pueden clasificarse en administrativas, físicas y técnicas:

1. Medidas de seguridad administrativas: A las 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

2. Medidas de seguridad físicas: Al 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.

3. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

De las medidas anteriores se establecen tres niveles de seguridad:

- **Básico:** Medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas y bases de datos personales.
- **Medio:** Implica la adopción de medidas de seguridad cuya aplicación corresponde a bases o sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.
- **Alto:** Son las medidas de seguridad aplicables a bases o sistemas de datos concernientes a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad pública, prevención, investigación y persecución de delitos.

DE LOS SISTEMAS DE TRATAMIENTO Y EL INVENTARIO DE DATOS PERSONALES

Tomando en consideración lo señalado por el artículo 27 fracción III de la LPDPPSOCH y con la información proporcionada por cada una de las unidades administrativas, se obtuvo el inventario de los sistemas de tratamiento, al respecto fue necesario contar con un diagnóstico de cada uno de los procesos que involucran tratamiento de datos personales, tomando en consideración los elementos señalados en los Lineamientos Generales de Protección de Datos Personales para el Sector Público

Como parte del proceso, la Unidad de Transparencia realizó en coordinación con las áreas competentes, la revisión y homologación de los inventarios y se documentó la existencia de 323 tratamientos de datos personales, los cuales se encuentran debidamente integrados en los formatos digitales y archivos de la Secretaría.

INVENTARIO DE DATOS

De acuerdo con el artículo 27, fracción III, de la LGPDPPSO, 27, fracción III, de la LPDPPSOCH, se establece como una de las actividades que conectan con el establecimiento y mantenimiento de las medidas de seguridad de los datos personales, realizar un inventario de datos personales. Para ello el artículo 58, de los Lineamientos Generales, señala que el inventario deberá elaborarse con información básica de cada tratamiento de datos personales; la Secretaría de Educación elaboró este inventario partiendo de los elementos esenciales y se documentaron y soportaron en medios electrónicos y considerando, al menos, los elementos siguientes:

- I.** El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
- II.** Las finalidades de cada tratamiento de datos personales;
- III.** El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;
- IV.** El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
- V.** La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;
- VI.** En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable; y,
- VII.** En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

FUNCIONES Y OBLIGACIONES EN EL TRATAMIENTO DE DATOS PERSONALES

El artículo 26 y 27, de la LPDPPSOCH, señalan que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, se deberán definir las funciones y obligaciones del personal involucrado en su tratamiento.

Para esto el artículo 57, de los Lineamientos Generales, determina que los responsables deberán establecer y documentar roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales.

En cumplimiento de lo anterior, previa identificación de las competencias, se solicitó, que las unidades administrativas:

Identificarán los tratamientos que se realizan con datos personales.

Ordenar los tratamientos en cuanto a la forma de que se generan, ya sea manuales o mediante sistemas electrónicos.

Relacionar los tratamientos con el servidor público a su cargo, identificando el proceso desde el ejecutor hasta el responsable.

Presentar de cada servidor público, las funciones que realiza de acuerdo a su normatividad, especificando sus funciones en el tratamiento.

Todo lo anterior se registró y soporto mediante las bitácoras de responsables y usuarios de los sistemas de datos personales, las cuales se integraron a los archivos físicos y electrónicos de la secretaría.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.

Se testa el apartado número 6, 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 o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 3, fracción IX, y 7, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

ANÁLISIS DE RIESGO

El presente análisis identifica el riesgo inherente a los datos personales en el tratamiento que reciben por parte de la Secretaría de Educación del Estado de Chiapas, al ejercer sus atribuciones, de manera que pueda ser controlado por la institución para satisfacer el derecho humano a la autodeterminación informativa.

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

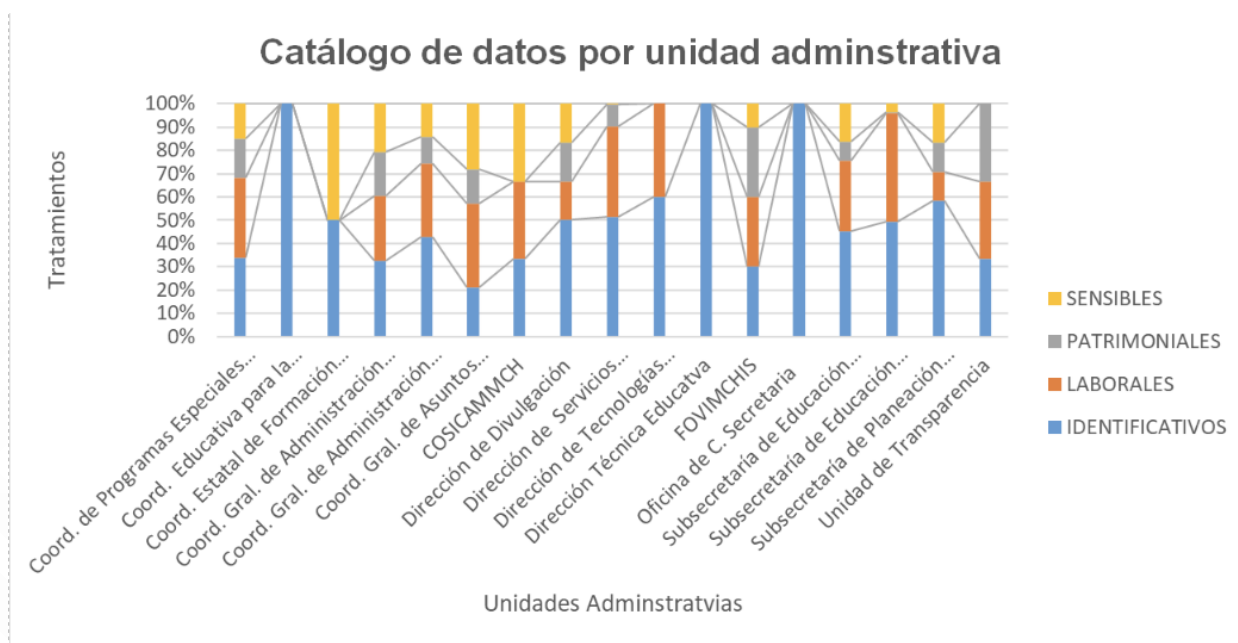
En la Secretaría de Educación del Estado de Chiapas se identificaron **323 tratamientos** donde se manejan datos personales de las 17 unidades administrativas que la conforman, como se visualiza en la siguiente tabla.

NO	AREA	TRATAMIENTOS	10	SUBSECRETARIA DE EDUCACION ESTATAL	89	DIRECCIÓN DE EVALUACIÓN Y PROGRAMAS INSTITUCIONALES	2		
1	OFICINA DE LA C. SECRETARIA DE EDUCACIÓN	1		DIRECCIÓN DE EDUCACIÓN BÁSICA	36	13	COORDINACIÓN GENERAL DE ADMINISTRACIÓN ESTATAL	54	
2	COSICAMM	4		PRIMARIA					
3	COORDINACIÓN DE PROGRAMAS ESPECIALES Y COMPENSATORIOS	19		PREESCOLAR					
	PROGRAMA NACIONAL DE INGLES	2		SECUNDARIAS					
	PFSEE	3		TELESECUNDARIAS					
	PEMCH	3		EDUCACION FISICA					
	INSUMOS	3		EDUCACION INDIGENA					
	DESARROLLO SOCIAL	4		INTEGRACION EDUCATIVA					
	LIBROS DE TEXTO	1		DIRECCIÓN DE EDUCACIÓN MEDIA	15				
	VER BIEN PARA APRENDER MEJOR	1		DIRECCIÓN DE EDUCACIÓN SUPERIOR	24				
	AREA DE BECAS	2		DIRECCIÓN DE FORTALECIMIENTO EDUCATIVO	14				
4	COORDINACIÓN GENERAL DE ASUNTOS JURÍDICOS Y LABORALES	31	11	SUBSECRETARIA DE EDUCACIÓN FEDERALIZADA	39	14	COORDINACIÓN GENERAL DE ADMINISTRACIÓN FEDERALIZADA	21	
	DIRECCIÓN DE ASUNTOS FEDERALIZADOS	17		DIRECCIÓN DE EDUCACIÓN ELEMENTAL					
	DIRECCIÓN DE ASUNTOS ESTATALES	14		DIRECCIÓN DE EDUCACIÓN PRIMARIA					
				DIRECCIÓN DE EDUCACIÓN SECUNDARIA Y SUPERIOR (FEDERAL)					
				DIRECCIÓN DE EDUCACIÓN INDIGENA					
5	DIRECCIÓN DE DIVULGACIÓN	3	12	SUBSECRETARÍA DE PLANEACIÓN EDUCATIVA	25	15	DIRECCIÓN DE SERVICIOS REGIONALES	27	
6	IGUALDAD DE GÉNERO	1		OFICINA DEL SUBSECRETARIO	2				
7	UNIDAD DE TRANSPARENCIA	3		DIRECCIÓN DE PROGRAMACIÓN Y PRESUPUESTO	13				
8	DIRECCIÓN DE TECNOLOGÍAS EDUCATIVAS Y DE LA INFORMACIÓN	3		DIRECCIÓN DE PLANEACIÓN EDUCATIVA	8				
9	DIRECCION TECNICA EDUCATIVA	1				6	FOVIMCHIS	1	
						TOTAL			323

CATEGORIA DE DATOS

Para analizar los riesgos de los datos personales que son objetos de tratamiento se aplicó un instrumento para, primeramente, clasificar los datos utilizados, a partir de la categorización existente en la ley; las cuatro categorías de datos que maneja la Secretaría de Educación son:

- **Datos identificativos, académicos:** que se describen la información por la que se identifica a una persona y/o permiten su contacto y los académicos que cuentan la trayectoria académica de la persona, como lo son: currículum vitae, títulos profesionales, cédula profesional, nombre de persona física, acta de nacimiento, año de nacimiento o edad, correo electrónico, credencial de elector, CURP, RFC, datos personales contenidos en documento para acreditar personalidad del representante, datos personales contenidos en la identificación oficial presentada por la persona física, domicilio, firma, fotografía, huella digital, nacionalidad, sexo, teléfono fijo o celular
- **Datos laborales:** que describen la situación laboral de la persona como: antecedentes laborales, constancia del servicio activo, constancia de situación fiscal, datos sindicales, nivel educativo, ocupación, talón de cheques, clave nominal, clave presupuestal, lugar de adscripción, número de empleado, categoría, copia de comisión y/o nombramiento, constancia de no inhabilitación.
- **Datos patrimoniales, biométricos, menores de edad, beneficiarios:** que comprenden la información que se encuentran vinculados al patrimonio de una persona como: circunstancias socioeconómicas, descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil, entre otros), discapacidad, estado de cuenta bancaria, clave interbancaria, huella dactilar, constancia de no propiedad.
- **Datos sensibles:** que consideran la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleva un riesgo grave para éste como: creencias religiosas, filosóficas o morales, datos sobre procedimientos judiciales o seguidos en forma de juicio, estado de interdicción o incapacidad legal, información migratoria, lengua indígena, opiniones políticas, origen étnico o racial, pasaporte, pertenencia a pueblo indígena, vida sexual.



De lo anterior podemos concluir que de las 17 unidades administrativas todas manejan datos identificativos, 13 unidades utilizan la segunda categoría de datos laborales, 11 manejan la tercera categoría de datos patrimoniales y 12 unidades manipulan datos sensibles en sus procesos. También podemos observar todas las unidades administrativas maneja varios tipos de categorías, ya que, el análisis que se hizo fue en base a tratamientos y no por unidad administrativa.

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

Para el desarrollo del análisis, se recuperaron cuatro tipos de amenazas sustentados en la Ley:

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

RIESGO INHERENTE A LOS DATOS PERSONALES

1. El riesgo inherente a los datos personales tratados.

Las medidas de seguridad que deberán adoptarse por el responsable deben tomar como referencia el nivel de riesgo latente de cada tratamiento de datos personales. Para la determinación del riesgo latente es necesario calcular los factores de riesgo por tipo de dato, por entorno, por tipo de acceso, y por volumen de titulares en la base de datos. Además, a cada tipo de riesgo se le agregaron 4 categorías y a cada una de ellas un nivel de riesgo inherente bajo, medio, alto y muy alto, según sea el caso de cada procedimiento; todo este cálculo se hizo a través de un cuestionario aplicado a las 17 unidades administrativas, como se ve en el siguiente ejemplo.

FORMULARIO PARA EL ANÁLISIS DE RIESGO

Unidad Administrativa:

Dirección:

Dpto. o Programa:

Proceso:

Finalidad:

1.1 Riesgo por tipo de datos (catálogo de datos).

1	Datos identificativos	bajo
2	Datos laborales	medio
3	Datos patrimoniales, biométricos, menores de edad, beneficiarios.	alto
4	Datos sensibles, circunstancias socioeconómicas, información migratoria, procedimientos judiciales, etc.	muy alto

1.1 Riesgo por entorno (donde se resguardan los datos).

1	Físico (archiveros de la unidad)	bajo
2	Equipo de computo	medio
3	Red	alto
4	Nube / intranet, Dropbox, google drive, etc.)	muy alto

1.1 Riesgo por número de accesos a la base de datos (en un periodo de 24 horas).

1	1 a 5 veces	bajo
2	6 a 10 veces	medio
3	11 a 20 veces	alto
4	Más de 20 veces	muy alto

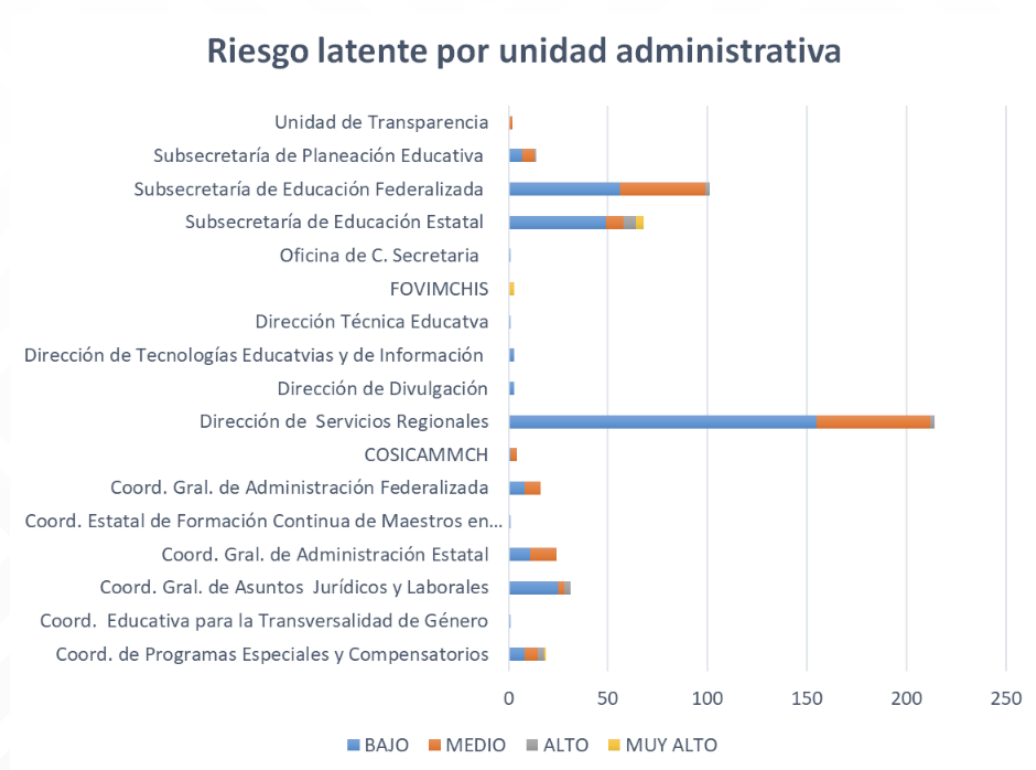
1.1 Riesgo por número de titulares en la base de datos.

1	Menos de 100	bajo
2	Menos de 1000	medio
3	Menos de 10,000	alto
4	Más de 10,000	muy alto

NIVEL DE RIESGO: bajo – medio – alto- muy alto.

Tomando en cuenta que cada unidad administrativa, maneja diferentes números de tratamientos, en la siguiente gráfica podemos ver que una misma unidad puede manejar diferentes niveles de riesgo, pero siempre tiende a mediar uno o dos estos.

NIVELES DE RIESGO POR UNIDAD ADMINISTRATIVA



El nivel de riesgo de la Secretaría de Educación oscila entre el nivel bajo y medio.

De todas las unidades solo 3 operan con nivel de riesgo muy alto, FOVIMCHIS, la Subsecretaría de Educación Estatal en tres de sus tratamientos y Coord. de Programas Especiales y Compensatorios en un proceso;

En el nivel de riesgo alto contamos con seis unidades, con 17 tratamientos en total, Subsecretaría de Educación Estatal (6), Coord. de Programas Especiales y Compensatorios (3), Coord. Gral. de Asuntos Jurídicos y Laborales (3), Dirección de Servicios Regionales (2), Subsecretaría de Educación Federalizada (2), Subsecretaría de Planeación Educativa (1),

Con nivel de riesgo medio tenemos a diez unidades administrativas Coordinación de Programas Especiales y Compensatorios, Coordinación General de Administración Estatal, Coordinación General de Administración Federalizada, Coordinación General de Asuntos Jurídicos y Laborales, COSICAMMCH, Dirección de Servicios Regionales, Subsecretaría de Educación Estatal, Subsecretaría de Educación Federalizada, Subsecretaría de Planeación Educativa, Unidad de Transparencia.

Con nivel de riesgo bajo a quince unidades; Coordinación de Programas Especiales y Compensatorios, Igualdad de Género, Coordinación Estatal de Formación Continua de Maestros en Servicio, Coordinación General de Administración Estatal, Coordinación General de Administración Federalizada, Coordinación General de Asuntos Jurídicos y Laborales, COSICAMMCH, Dirección de Divulgación, Oficina de C. Secretaria, Dirección de Servicios Regionales, Dirección de Tecnologías Educativas y de Información, Dirección Técnica Educativa, Subsecretaría de Educación Estatal, Subsecretaría de Educación Federalizada, Subsecretaría de Planeación Educativa.

CONCLUSIÓN

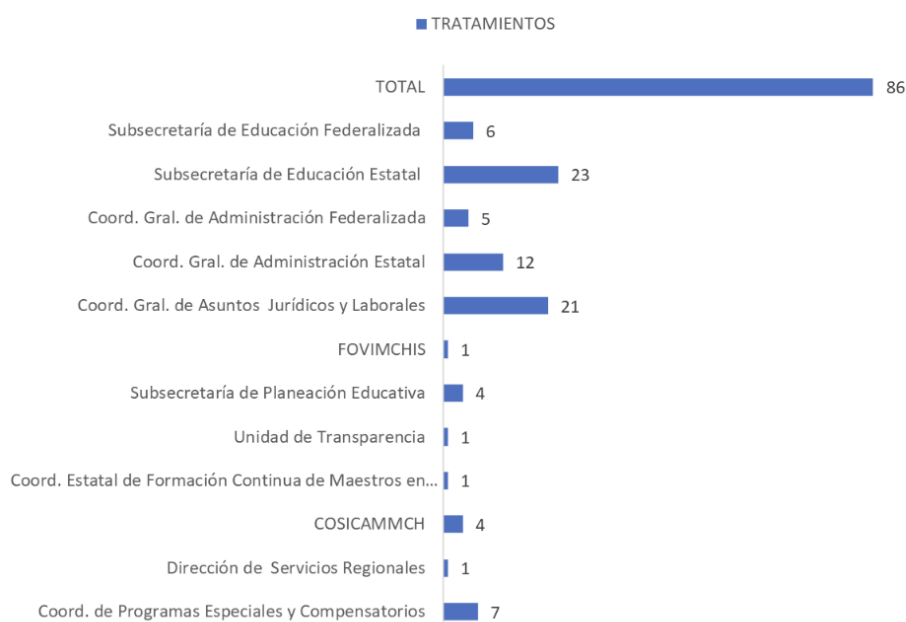
Concluimos que el riesgo general de la Secretaría de Educación oscila entre el nivel bajo y medio, ya que la gran mayoría de las unidades administrativas con excepción de dos manejan un nivel bajo en sus tratamientos y solo tres unidades presentan un nivel alto, lo cual corresponde a 6 de los 319 procesos con los que cuenta la Secretaría.

También cabe destacar que cada una de las unidades administrativas pueden manejar varios niveles de riesgo, ya que, el análisis fue en base a tratamientos y no por unidad administrativa.

LA SENSIBILIDAD DE LOS DATOS PERSONALES TRATADOS

Además del riesgo inherente, existen otros tipos de riesgo a considerar como lo es, la sensibilidad de los datos. Si bien, la mayoría de la información que se maneja en la Secretaría de Educación es de carácter identificativo, académico y laboral, también algunas unidades administrativas manejan datos personales sensibles como lo son:

Datos sensibles por unidad administrativa

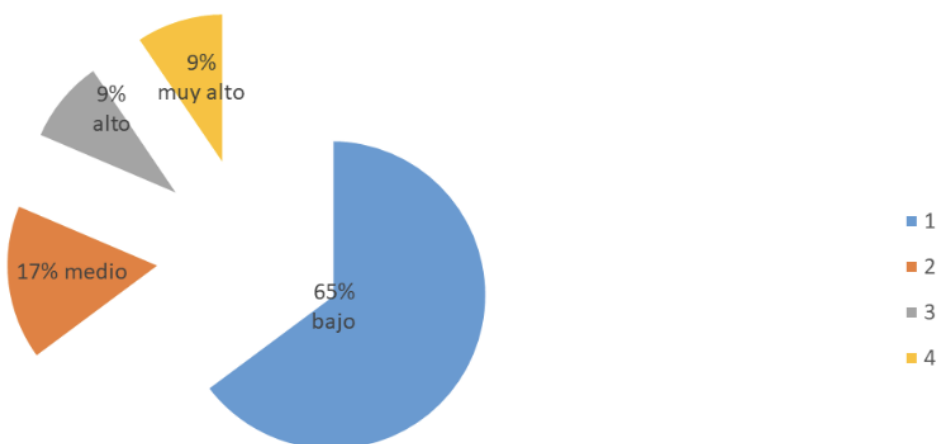


De los 323 tratamientos de datos personales que maneja la Secretaría, en 86 de estos se manejan datos sensibles, lo que equivale a un 26.95 % correspondiente a doce unidades administrativas.

LAS POSIBLES CONSECUENCIAS DE UNA VULNERACIÓN PARA LOS TITULARES

Para medir el presente nivel de riesgo y darnos cuenta de su alcance, se hizo un aproximado de la información en base al número total de titulares que existen en la base de datos según la cifra de tratamientos que maneja cada unidad administrativa. Considerando en número 1 como menos de 100, 2 menos de 1000, 3 menos de 10,000 y 4 más de 10,000 como podemos observar en la siguiente gráfica.

Porcentaje de titulares por unidades administrativas



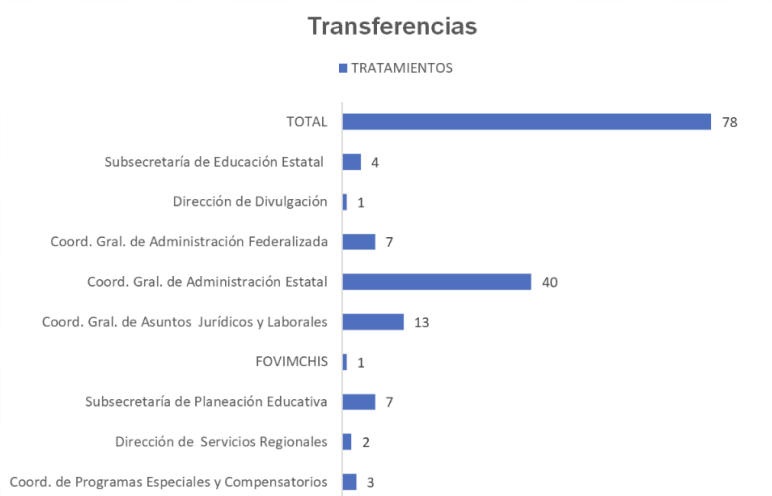
El 65 % de los tratamientos de datos personales que se manejan en la Secretaría de Educación, cuentan con menos de 100 titulares, el 17% de los procesos refieren a una base de datos de menos de 1,000 titulares, el 9% de los trámites operan con una base de menos de 10,000 titulares y solo el 9% de los procedimientos que se manejan cuentan con una base de datos de más de 10,000 titulares.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DE GESTIÓN Y PLAN DE CONTINGENCIA.

Se testa el apartado número 7, 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 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.

LAS TRASFERENCIAS DE DATOS PERSONALES

Otro de los riesgos al manejar datos personales es cuando debemos transferir datos a otra dependencia diferente a la Secretaría de Educación. En base a la información que se recabo, tenemos que 9 unidades administrativas manejan transferencias; dando un total de 78 tratamientos, Coord. Gral. de Administración Estatal (40), Coord. Gral. de Asuntos Jurídicos y Laborales (13), Coord. Gral. de Administración Federalizada (7), Subsecretaría de Planeación Educativa (7), Subsecretaría de Educación Estatal (4), Coord. de Programas Especiales y Compensatorios (3), Dirección de Servicios Regionales (2), Dirección de Divulgación (1), FOVIMCHIS (1); pero debemos dejar en claro que todas las transferencias que se realizan en la Secretaría no necesitan el consentimiento por escrito del titular ya que se encuentran como excepciones previstas en la Ley General.



LAS VULNERACIONES PREVIAS OCURRIDAS EN LOS SISTEMAS DE TRATAMIENTO

La Secretaría de Educación ha sido escenario en repetidas ocasiones de vandalismo por parte de diferentes grupos manifestantes, por lo que se proporciona una tabla con los incidentes de los últimos 5 años, 2018, 2019, 2020, 2021, 2022, que nos reporta la Coordinación de protección civil de dicha institución.

AÑO	MES		REPORTE DE INCIDENCIA
2018	marzo y noviembre		Actos de vandalismo, afectando en el interior del inmueble
2019	enero y febrero		Actos de vandalismo, afectando en el interior del inmueble
2020	septiembre		Actos de vandalismo, afectando en el exterior e interior del inmueble
2021	junio		Actos de vandalismo, interrumpiendo actividades.
2022	marzo		Actos de vandalismo, afectando en el interior del inmueble, cristales rotos, archivos quemados, paredes pintadas con grafitis.

I. Análisis de Brecha

De acuerdo al artículo 26 de la Ley de Datos personales del Estado de Chiapas donde menciona que las medidas de seguridad adoptadas deberán considerar: El riesgo inherente a los datos personales tratados, la sensibilidad de los datos personales tratados, el desarrollo tecnológico, las posibles consecuencias de una vulneración para los titulares, las transferencias de datos personales que se realicen, el número de titulares, y las vulneraciones previas ocurridas en los sistemas de tratamiento; riesgos que ya fueron valuados en el análisis de riesgo, ahora nos abocaremos a la implementación de medidas de seguridad que nos permitan reducir el nivel de riesgo posible en la Secretaría de Educación.

Para detectar las medidas de seguridad administrativas, físicas y técnicas se consensó por medio de un cuestionario a las 17 unidades administrativas, las cuales contestaron de acuerdo al número de procedimientos que reportaron previamente y donde manejan datos personales.

El cuestionario contó con 32 preguntas, donde 10 corresponden a medidas de seguridad administrativas, 8 a medidas de seguridad físicas y 12 a medidas de seguridad técnicas, por medio de este análisis se calculó si las medidas de seguridad son efectivas, no efectivas o faltantes en las diferentes unidades administrativas.

Las medidas de seguridad administrativas se refieren a las 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, formación y capacitación del personal, en materia de protección de datos personales.

De las 10 preguntas de medidas de seguridad administrativas que se consensaron en las 17 unidades, quedando fuera de este análisis dos unidades; los resultados arrojaron la siguiente información: cinco medidas de seguridad salieron efectivas, o por arriba del 50 %, las cuales son de mayor a menor porcentaje:

- ✓ ¿Llevas registro de la información que manejas y la clasificas? 82%,
- ✓ ¿Pones atención en no dejar a la vista información personal en el escritorio, impresoras, escáneres y copiadoras? 81%,
- ✓ ¿Se informa al personal sobre sus deberes mínimos de seguridad y protección de datos? 66 %,
- ✓ ¿Tomas precauciones con los procedimientos de reutilización? 60%.
- ✓ ¿Se fomenta la cultura de la seguridad de la información? 60%.

Por otro lado, cinco de las diez medidas de seguridad administrativas resultaron faltantes, y a este porcentaje, se sumó el porcentaje de no efectividad, ya que, al tener medidas de seguridad, pero no ser efectivas, sería como si no se tuvieran. Las medidas seguridad faltantes y no efectivas son las siguientes de mayor a menor porcentaje:

- ¿Se asegura la protección de datos personales en subcontrataciones? $63\% + 3\% = 66$
- ¿Se tienen procedimientos para actuar ante vulneraciones a la seguridad de los datos personales? $60\% + 4\% = 64\%$
- ¿Fijas periodos de retención y destrucción de información? $61\% + 2\% = 63\%$
- ¿Tienes mecanismos para eliminar de manera segura la información? $57\% + 5\% = 62\%$
- ¿Realizas respaldos periódicos de los datos personales? $49\% + 4\% = 53\%$.

Por lo que se concluye que, en cuanto a medidas de seguridad administrativas nos encontramos en un nivel bajo o de inmadurez, donde debemos implementar mecanismos y prácticas que regulen la protección de datos personales en esta área.

- a) Cada unidad administrativa a través de su enlace de archivo deberá manejar el control, almacenamiento y clasificación de la información de acuerdo al Sistema Institucional de Archivos.
- b) Es importante que todo el personal que maneja datos personales se encuentre capacitado y conozca los deberes mínimos de seguridad en materia de protección de datos. Es por ello que el enlace de datos personales de cada unidad administrativa deberá asistir a todos los cursos y capacitaciones que la unidad de transparencia ofrezca, para que este a su vez baje la información que se le brinde a los sub enlaces y a todo el personal que trabaje con datos personales, fomentando así una cultura de protección de datos entre los servidores públicos. Cada año la unidad de transparencia brindará cursos y capacitaciones en esta materia y cada unidad administrativa podrá solicitar a la unidad de transparencia a través de un oficio, capacitaciones al personal que lo requiera.
- c) Cada unidad administrativa deberá implementar políticas de protección de datos en cuanto a la conservación, destrucción y eliminación de la información de manera segura. Así como fijar periodos internos para respaldar la información que se maneja.
- d) Cláusulas de confidencialidad en los contratos de personal docente y administrativo, así como cartas responsivas de confidencialidad por área, programa, departamento, dirección u oficina donde el personal maneje datos personales.
- e) Crear una bitácora de vulneraciones donde se pueda llevar un control por unidad administrativa, y donde esta contenga de acuerdo a la ley, fecha, naturaleza de la vulneración o incidente, datos personales contenidos, acciones correctivas implementadas de forma inmediata y definida.

-
-
-
-
-

Bitácora de Vulneraciones			
Unidad Administrativa:			
Fecha del incidente o vulneración.	Incidente o Vulneración.	Datos personales involucrados.	Acciones correctivas.

- f) Identificar los mecanismos de tratamiento seguro de la información en los procesos de los archivos de trámite, considerando las diferentes etapas y especialmente cuando se realicen procedimientos internos por uso, reutilización, corrección o equivocación.
- g) Pedir el apoyo en informática para establecer periodos y prácticas recurrentes para el respaldo de la información.

Las medidas de seguridad físicas, son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

De las 8 preguntas de medidas de seguridad físicas que se consensaron en las 17 unidades administrativas, quedando fuera de este análisis dos unidades, los resultados arrojaron la siguiente información: cinco medidas de seguridad salieron efectivas, o por arriba del 50 %, las cuales son de mayor a menor porcentaje.

- ✓ ¿cuidas el movimiento de información en entornos de trabajo físicos? 76%
- ✓ ¿mantienes en movimiento sólo copias de la información, no el elemento original? 61%.
- ✓ ¿tienes medidas de seguridad que protejan el área donde trabajas? 58%
- ✓ ¿cuentas con protección, cerraduras y candados para garantizar el resguardo de tus documentos? 56%
- ✓ ¿existe un control de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico? 54%

Así mismo, 3 de las medidas de seguridad físicas resultaron faltantes y a este porcentaje se le agrego el de no efectivas, ya que, al tenerlas, pero no ser efectivas, quedarían en el rango de faltantes, las cuales son de mayor a menor porcentaje:

- ¿usas mensajería certificada? 80%
- ¿mantienes registros del personal con acceso al entorno de trabajo? $54\% + 4\% = 58\%$
- ¿tienes medidas de seguridad para evitar el robo? $45\% + 10\% = 55\%$

Respecto a medidas de seguridad físicas, podemos concluir que, aunque la estadística arroja mayor nivel de porcentaje en cuanto a efectividad se refiere, el porcentaje de faltante y no efectividades es muy alto de igual manera. Por lo que se deben reforzar las medidas de seguridad físicas esenciales e implementar nuevas medidas que nos permitan resguardar de manera segura los documentos y equipos que contengan datos personales.

RECOMENDACIONES DE IMPLEMENTACIÓN

- a) Identificar las áreas, donde se imprimen documentos en una misma máquina para borrar la información que se manda a imprimir, así mismo desarrollar políticas que ayuden a prevenir el robo, extravío en el movimiento de la información.
- b) Detectar las medidas físicas esenciales de seguridad en las diferentes áreas de las unidades administrativas como llaves, cerraduras, candados en puertas, archiveros para un resguardo seguro de los documentos.
- c) Establecer mecanismos de control que nos permitan mantener un control sobre la salida de información a través de documentos físicos, lap tops u otros equipos de cómputos, unidades de almacenamiento electrónico etc.
- d) ¿Qué se entiende como mensajería certificada?

Las medidas de seguridad técnicas, son el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software, para proteger el entorno digital de los datos de personales y recursos involucrados en su tratamiento.

De las 12 preguntas sobre medidas de seguridad técnicas que se consensaron, siete de ellas resultaron efectivas, las cuales son de mayor a menor porcentaje las siguientes:

- ✓ bloqueo y cierre de sesiones 74%
- ✓ ¿tienes un equipo de cómputo institucional para realizar el trabajo? 68%
- ✓ uso de contraseñas y/o cifrado y ¿cuidas el movimiento de información en entornos de trabajo digitales? 67%
- ✓ ¿tienes seguridad de la información enviada y recibida? 65%
- ✓ uso de conexiones seguras 62%
- ✓ administrar usuarios y accesos 59%

Por otro lado, 5 medidas de seguridad técnicas resultaron faltantes y no efectivas, las cuales son de mayor a menor porcentaje:

- ¿revisas periódicamente el software instalado en el equipo de cómputo? $58\% + 7\% = 65\%$
- ¿revisas la configuración de seguridad del equipo de cómputo? $56\% + 3\% = 59\%$
- ¿tienes medidas de seguridad para navegar en entornos digitales? $50\% + 7\% = 57\%$
- ¿realizas actualizaciones al equipo de cómputo? $41\% + 13\% = 54\%$
- reglas de navegación segura $48\% + 4\% = 52\%$

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL 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 del análisis de brecha, en él se establecen las acciones específicas que el sujeto obligado implementará para corregir deficiencias, fortalecer controlar 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.

De lo anterior podemos deducir que las medidas de seguridad técnicas efectivas son mayoría versus faltantes y no efectivas. Considerando que como segunda opción de almacenamiento de datos que las unidades administrativas utilizan para resguardo de los datos personales se encuentra en equipos de cómputo, es de importancia implementar nuevos y mejores mecanismos de seguridad que nos permitan reducir los riesgos en esta esfera.

RECOMENDACIONES DE IMPLEMENTACIÓN

- a) Las sesiones, documentos o programas que abran deben cerrarse cada vez que se terminan de consultar.
- b) Usar conexiones seguras de internet.
- c) Cambio de contraseñas cada vez que se cambia el personal que tiene acceso a la información.
- d) Pedir al área de informática que se revise mínimo una vez al año (los primeros tres meses de cada año) el software y la configuración de seguridad de los equipos de cómputos de la Secretaría.

PLAN DE TRABAJO

El Documento de Seguridad se perfila como una radiografía institucional en materia de protección de datos personales; con él podemos determinar sus fortalezas, pendientes y las áreas de oportunidad, a la vez, es un insumo determinante para la toma de decisiones de cada una de las Unidades Administrativas y sus sistemas de datos.

De las particularidades que revela dicho instrumento, es posible obtener información sobre necesidades específicas para el diseño de planes de trabajo; así como la implementación y factibilidad de mecanismos de monitoreo y revisión de medidas de seguridad, que también integran el Documento de Seguridad.

En este sentido el Comité de Transparencia instruye a la Unidad de Transparencia para que una vez aprobado el presente Documento, elabore un plan de trabajo, tomando en consideración los elementos encontrados en los análisis y se desarrolle como una herramienta que complemente e instrumente el documento de seguridad y que tendrá como objetivo fundamental:

Eliminar las brechas a través de la implementación de medidas de seguridad.
Consolidar y preservar los niveles de protección de los datos personales a través de mecanismos de monitoreo y revisión.

Así mismo se determina que las actividades encaminadas al cumplimiento de dichos objetivos se realizarán y coordinarán por la Unidad de Transparencia, tomando en consideración el modelo operativo y directivo utilizado para la formulación del documento de seguridad.

MECANISMOS DE MONITOREO Y SUPERVISIÓN DE PROTECCIÓN DE DATOS PERSONALES

El artículo 33, fracción VII, de la Ley General, establece que se deberán monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Al respecto, la Unidad de Transparencia será el área administrativa encargada de ejecutar el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, el cual se integrará por las etapas de monitoreo y supervisión.

La etapa de monitoreo consistirá en el requerimiento por parte de la Unidad de Transparencia del Reporte de Seguridad de Datos Personales, el cual deberá ser desahogado por las instancias que, en el ámbito de sus atribuciones, sean las encargadas de los sistemas de tratamiento de datos personales.

La etapa de supervisión consistirá en el análisis por parte de la Unidad de Transparencia del Reporte de Seguridad de Datos Personales, al cual corresponderá un Dictamen de Seguridad de Datos Personales en el que se plasmen las recomendaciones o requerimientos que se consideren pertinentes.

ETAPA DE MONITOREO

Se realizará tomando como punto de partida lo informado por cada instancia ante la Unidad de Transparencia en la integración del Documento de Seguridad, lo cual abarcó, entre otros aspectos, lo siguiente:

- 1.** Datos personales que se obtienen o reciben en cada tratamiento.
- 2.** Motivos y fundamento legal por los cuales se recaban o reciben los datos personales.
- 3.** Tecnologías empleadas para el tratamiento.
- 4.** Medidas de control implementadas, incluyendo su objetivo, la forma en que se instrumentan y el responsable de su ejecución.
- 5.** Identificación de controles preventivos
- 6.** Identificación de controles correctivos.

La Unidad de Transparencia requerirá a cada instancia, por cada uno de los tratamientos que realiza, la elaboración del Reporte de Seguridad de Datos Personales, en el que deberán precisarse los elementos siguientes:

- 1.** Acciones desarrolladas para la ejecución de las medidas de control existentes.
- 2.** Manifestación de si existe alguna actualización o modificación respecto de las medidas de seguridad y controles implementados en el tratamiento de datos personales que realice. De ser así, deberán incluir una explicación de tal actualización o modificación.
- 3.** Indicar de manera clara la actualización de los aspectos siguientes:
 - La incorporación de nuevos activos en el tratamiento que realiza, como podrían ser una actualización o modificación en el hardware o software del sistema utilizado, personal de nuevo ingreso a cargo del tratamiento o cualquier otro recurso humano o material que tenga impacto en el tratamiento de los datos personales.
 - El surgimiento de nuevas amenazas en el tratamiento de los datos.
 - La posibilidad de que las nuevas amenazas actualicen una vulnerabilidad en el tratamiento de datos respectivo
 - Casos en los que una amenaza haya sufrido alguna modificación que derive en el incremento del impacto que tendría su materialización en la seguridad de los datos personales.

El requerimiento a cada instancia del Reporte de Seguridad de Datos Personales se realizará de acuerdo a la calendarización que presente la Unidad de Transparencia y aprobado por el Comité de Transparencia.

ETAPA DE SUPERVISIÓN

La Unidad de Transparencia analizará los reportes de seguridad de datos personales remitidos por las instancias, verificando especialmente lo siguiente:

- 1.** La idoneidad y efectividad de las medidas de seguridad y control respecto del tratamiento.
- 2.** La suficiencia de controles preventivos y correctivos.
- 3.** La gestión interna de nuevas amenazas, vulnerabilidades e incrementos en el impacto de probables daños.
- 4.** Avances generados conforme a lo establecido en el Plan de Trabajo.
- 5.** El cumplimiento de políticas, planes, procesos y procedimientos en materia de seguridad de datos personales.

Posterior a su examinación, se elaborará un Dictamen de Seguridad en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad. Lo que será notificado a las instancias, puntualizando las cuestiones que se estimen de atención prioritaria, señalando la forma en que las recomendaciones y/o requerimientos habrán de ser desahogados, destacando el plazo en que deberán remitirse las evidencias de su cumplimiento a la Unidad de Transparencia.

Si de las recomendaciones concluidas puede derivarse una estrategia que maximice la seguridad de los datos personales, la Unidad de Transparencia la integrará en el Plan de Trabajo, con el objeto de que sean atendibles por aquellas instancias que les puedan resultar aplicables.

Asimismo, de advertir una modificación sustancial a determinado tratamiento que derive en un cambio en su nivel de riesgo o una estrategia que maximice la seguridad de los datos personales que pueda ser aplicable a diversas instancias, la Unidad de Transparencia deberá analizar la necesidad de actualizar el Documento de Seguridad, en términos de lo establecido para esos efectos.

MECANISMOS DE ACTUACIÓN ANTE ALERTAS Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

La Ley General, dispone que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales. En ese sentido, el artículo 63, fracción VII, de los Lineamientos Generales, entre otras disposiciones estipula que, para evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, se deberán monitorear las vulneraciones de seguridad ocurridas.

En este documento se definen los mecanismos que las unidades administrativas deberán operar ante el surgimiento de una alerta o vulneración en las medidas de seguridad de los datos personales.

ALERTAS SEGURIDAD DE LOS DATOS PERSONALES.

El mecanismo persigue los objetivos siguientes:

- Registrar las amenazas que configuren alertas de seguridad.
- Analizar las alertas de seguridad registradas con la finalidad de definir estrategias para la prevención de una vulneración de seguridad.
- Integrar las estrategias de prevención en el Plan de Trabajo a efecto de que, en los casos conducentes, se implementen como medidas adicionales de seguridad.

Es importante destacar, que resultará indispensable identificar que efectivamente los hechos constituyan una alerta a la seguridad de los datos personales, para lo cual, las instancias deberán verificar la materialización de los supuestos siguientes:

Que exista una amenaza que, de haberse concretado, hubiera producido sus efectos en el tratamiento de los datos personales.

Que dichos efectos, de haberse materializado, hubieran representado un daño en las bases de datos, el hardware, software, archivos o documentos electrónicos o en papel, o en cualquier de los activos de importancia.

En caso de advertir una alerta de seguridad se deberá proceder conforme al mecanismo siguiente:

Verificada la existencia de una alerta de seguridad, la instancia deberá emitir un Reporte de Alerta de Seguridad, en el cual se deberá considerar, como mínimo, los aspectos siguientes:

Detección.

Nombre, cargo y adscripción del servidor público que detectó la amenaza.

Fecha, hora y lugar en que se detectó, así como una descripción detallada de cómo fue descubierta.

Tratamiento o sistema en que ocurrió.

Nombre, cargo y adscripción del servidor público responsable del tratamiento o sistema.

Datos personales involucrados en la amenaza.

Al tercer día hábil siguiente a la detección de la alerta, el reporte deberá ser remitido a la Unidad de Transparencia, la cual procederá a su registro y análisis y deberá valorar los siguientes aspectos:

El impacto que tiene la alerta en la seguridad de los datos personales.

Observaciones en materia de seguridad que la instancia debe observar en el futuro desarrollo del tratamiento.

Medidas de seguridad adicionales que se estime conducente implementar.

Si resulta posible determinar una estrategia de prevención con instancias en las que la alerta de seguridad pueda desencadenarse.

Si del análisis de la alerta de seguridad la Unidad de Transparencia advierte la posibilidad de generar una estrategia de prevención, procederá a su integración en el Plan de Trabajo.

VULNERACIONES DE SEGURIDAD DE LOS DATOS PERSONALES

Resulta indispensable que los responsables del sistema de tratamiento identifiquen que efectivamente los hechos ocurridos constituyen una vulneración a la seguridad de los datos personales, deberán verificar la materialización de los supuestos siguientes:

- Que exista una afectación concreta en el tratamiento de los datos personales que haya generado conjunta o separadamente lo siguiente:
 - 1.** La pérdida o destrucción no autorizada.
 - 2.** El robo, extravío o copia no autorizada.
 - 3.** El uso, acceso o tratamiento no autorizado.
 - 4.** El daño, la alteración o modificación no autorizada.
- Que la afectación implique un daño a las bases de datos, al personal, el hardware, software, archivos o documentos electrónicos o en papel, o en cualquiera.

Si alguno de los puntos anteriores no se actualiza, no se considerará una vulneración de los tratamientos o sistemas de datos personales, razón por la cual no será necesario la ejecución del proceso descrito en este apartado, y deberá procederse, en su caso, en los términos previstos para una alerta de seguridad.

Ante una vulneración en la seguridad de los datos personales, se establecen las obligaciones siguientes:

Analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales a efecto de evitar que la vulneración se repita.

Informar sin dilación alguna al titular y a través de la Unidad de Transparencia a Transparencia para el Pueblo de Chiapas, las vulneraciones que afecten de forma significativa derechos patrimoniales o morales, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

El cumplimiento de las citadas obligaciones se realizará de la forma siguiente:

Análisis de las causas por las cuales se presentó la vulneración y de las acciones preventivas y correctivas correspondientes.

Una vez que se detecte la vulneración, los responsables del tratamiento de que se trate, deberán elaborar un Informe de Causas y Acciones de la Vulneración y deberá remitirlo a la Unidad de Transparencia a más tardar el segundo día hábil siguiente a la fecha en que se detecte.

Para la emisión del informe deberá considerar, como mínimo, el desarrollo de los aspectos siguientes:

Información general de la vulneración.

Nombre, cargo y adscripción del servidor público que detectó la vulneración.

Fecha, hora y lugar en que se detectó la vulneración.

Tratamiento o sistema que fue vulnerado.

Nombre, cargo y adscripción del servidor público responsable del tratamiento o sistema.

Datos personales involucrados en la vulneración.

Descripción detallada de la forma en que se detectó la vulneración.

Así mismo deberá realizar una investigación que permita identificar el nivel de impacto y afectación, con la finalidad de determinar si existe una afectación significativa, de que tipo se considera y que permita proceder de inmediato a informar a los titulares y a Transparencia para el Pueblo de Chiapas.

Justificar si la vulneración pudo ser prevenida, es decir, si hubiera sido posible eliminar las causas del riesgo que fue materializado, detallando las herramientas, medios, procedimientos y el personal con que se cuente que efectivamente hubiera podido llevar a cabo tal prevención.

Si la vulneración no pudo ser prevenida, describir de manera detallada la herramienta, medida o procedimiento con la que se estaría en oportunidad de prevenir futuras vulneraciones del mismo tipo.

Analizar las medidas que, de acuerdo con la magnitud de la vulneración ocurrida, permitan el restablecimiento del tratamiento o sistema de datos personales.

Analizar las medidas correctivas que permitan evitar la reincidencia de las acciones que propiciaron la vulneración

Recomendaciones para el titular afectado.

Medio puesto a través del cual pueda obtenerse mayor información respecto de la vulneración.

Datos de contacto de los servidores públicos designados para la gestión de la vulneración.

Cualquier información y/o documentación que se considere conveniente.

La Unidad de Transparencia analizará de forma exhaustiva las particularidades de la vulneración y realizará lo siguiente:

Identificará si en el Informe de Causas y Acciones de una Vulneración, la instancia respectiva consideró que la afectación sufrida causaba un daño significativo en detrimento de los titulares de los datos personales afectados.

Supervisará las acciones implementadas por la instancia para restituir la seguridad del tratamiento de los datos personales y en caso de que el responsable haya considerado que la afectación causada es significativa, dentro de las 72 horas siguientes a la confirmación de la ocurrencia de la vulneración, la Unidad de Transparencia realizará un informe dirigido a Transparencia para el Pueblo de Chiapas donde considere los aspectos siguientes.

- La hora y fecha de la identificación de la vulneración.
- La hora y fecha del inicio de la investigación sobre la vulneración.
- La naturaleza de la vulneración ocurrida.
- La descripción detallada de las circunstancias en torno a la vulneración ocurrida.
- Las categorías y número aproximado de titulares afectados.
- Los sistemas de tratamiento y datos personales comprometidos.
- Las acciones correctivas realizadas de forma inmediata.
- La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida.
- Las recomendaciones dirigidas al titular.
- El medio puesto a disposición del titular para que pueda obtener más información al respecto.
- El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar más información.
- Cualquier otra información y documentación que se considere conveniente hacer del conocimiento.

NOTIFICACIÓN DE LA VULNERACIÓN A LOS PARTICULARES

De haberse considerado la actualización de una afectación significativa al titular o titulares de los datos personales, los responsables deberán realizar un informe que considere los aspectos siguientes:

- La naturaleza de la vulneración.
- Los datos personales comprometidos.
- Las recomendaciones al titular acerca de las medidas que este pueda adoptar para proteger sus intereses.
- Las acciones correctivas realizadas de forma inmediata.
- Los medios donde puede obtener más información al respecto.
- La descripción de las circunstancias generales en torno a la vulneración ocurrida, que le ayuden a entender el impacto de la vulneración.
- Cualquier otra información y documentación que se considere conveniente para apoyar a los titulares de los datos personales afectados.

Lo anterior deberá notificarse por los responsables al particular o los particulares afectados dentro de las 72 horas siguientes a la detección de la vulneración.

Dicha notificación, deberá efectuarse a través del medio que resulte idóneo y de fácil acceso, considerando la forma en que se obtuvieron los datos personales, el perfil que guarda el titular y la forma en que se mantiene contacto con él y en ninguno de los casos, deberá generarle costo alguno.

Entre los mecanismos que se deben adoptar para cumplir con el principio de responsabilidad el artículo 30, fracción IV, de la Ley General de Datos Personales en Posesión de Sujetos Obligados, establece que se deberá mantener un sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de datos personales.

Así mismo el artículo 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, dispone que además del monitoreo y supervisión periódica de las medidas de seguridad, se deberá contar con un programa de auditoría para revisar la eficacia y eficiencia del sistema de gestión.

Con la finalidad de comprobar el cumplimiento de las políticas de protección de datos personales, así como para monitorear y revisar la eficacia y eficiencia del sistema de gestión, se presenta el Mecanismo de Auditoría en Materia de Datos Personales.

FINALIDADES Y OBJETIVOS

Las auditorías en materia de datos personales tendrán las finalidades siguientes:

Determinar que los tratamientos de datos personales se encuentren apegados a la normativa aplicable. Supervisar la adopción y cumplimiento de las políticas, procedimientos y mecanismos determinados en el Sistema de Gestión y el Documento de Seguridad.

Verificar la eficiencia de las medidas de seguridad físicas, administrativas y técnicas instauradas.

Validar el avance de los objetivos planteados en el Plan de Trabajo.

Prevenir la materialización de vulneraciones a la seguridad de los datos personales.

Promover la implementación de mejoras en el tratamiento de los datos personales, que permitan elevar su grado de protección.

Es importante referir que el alcance que tendrán las auditorías practicadas se concentrará exclusivamente en el análisis de la forma en que cada instancia, en el ámbito de su competencia, implementa las políticas que les resulten aplicables en materia de datos personales, así como la evaluación del estado de seguridad en que se encuentran los datos personales bajo su tratamiento; lo anterior, con la finalidad de implementar mejoras que de manera progresiva permitan perfeccionar el manejo y protección de los datos personales.

INSTANCIA EJECUTORA Y ÁMBITO DE APLICACIÓN

La Unidad de Transparencia debe establecer un sistema de supervisión de vigilancia para comprobar el cumplimiento de las políticas en materia de datos personales. Consecuentemente, el Programa de Auditoría en materia de Datos Personales será ejecutado por la Unidad de Transparencia.

Por lo que se refiere al ámbito de aplicación, se indica que las unidades administrativas que en ejercicio de sus funciones realicen el tratamiento de datos personales, serán los sujetos auditables materia del programa, de modo que se encuentran obligadas a coadyuvar activamente con la Unidad de Transparencia para el desarrollo de las auditorías respectivas.

ETAPAS DE LAS AUDITORÍAS EN MATERIA DE DATOS PERSONALES

Las auditorías en materia de protección de datos personales estarán conformadas por las etapas de apertura, revisión y conclusiones.

La etapa de apertura tendrá la finalidad de definir el personal de la instancia auditada ante el cual la Unidad de Transparencia substanciará la auditoría, así como los tratamientos de datos personales que serán auditados, el tipo de revisión que ameritará (documental, presencial o virtual), y los requerimientos específicos necesarios para su realización.

En la etapa de revisión se realizará el escrutinio de la forma en que la Unidad Administrativa acredita el cumplimiento de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como los deberes de seguridad y confidencialidad, de conformidad con lo previsto en la normativa aplicable.

En la etapa conclusiva, la Unidad de Transparencia puntualizará a la instancia auditada las consideraciones efectuadas, abundará en los puntos de mejora y las cuestiones que se estimen de atención prioritaria y señalará la forma en que las observaciones y requerimientos deberán ser cumplimentados, destacando el plazo en que deberán remitir las evidencias correspondientes.

ETAPA DE APERTURA

Notificación de auditoría

De conformidad con el calendario de auditorías en materia de datos personales, la Unidad de Transparencia comunicará por oficio a la instancia correspondiente, lo siguiente:

- I.** La fecha en que dará inicio la auditoría, la cual deberá realizarse con un mínimo de 5 días hábiles entre la notificación del oficio y su celebración.
- II.** La necesidad de que la unidad administrativa auditada designe al personal con el que la Unidad de Transparencia substanciará la auditoría.
- III.** La convocatoria a una reunión previa al inicio de la auditoría, entre el personal de la Secretaría de Protección de Datos Personales y el personal designado por la instancia auditada.

Reunión previa

En el día señalado para la reunión previa, se informarán los tratamientos de datos personales que serán auditados, el tipo de revisión que ameritará (documental, presencial, virtual o mixta), así como los requerimientos específicos necesarios para la realización de la propia auditoría.

Efectuada la reunión previa, se elaborará una minuta en la que se precisará el desarrollo de la propia reunión, la cual deberá ser signada por los involucrados.

Acuerdo de inicio

En el día estipulado para el comienzo de la auditoría, se emitirá un acuerdo de inicio en el que deberá asentar lo siguiente:

- I.** El día en que comenzará y finalizará la auditoría.
- II.** El servidor público designado por la Unidad de Transparencia para sustanciar la auditoría.
- III.** El servidor público designado por la instancia auditada para sustanciar la auditoría.
- IV.** Identificación del tratamiento o tratamientos de datos personales materia de la auditoría.
- V.** El tipo de revisión que amerite el tratamiento (documental, presencial, virtual o mixta).
- VI.** La documentación, sistema o espacio físico que deberá estar plenamente disponible para ser examinado.
- VII.** Los datos de contacto de la Unidad de Transparencia ante los cuales podrán solventarse dudas relacionadas con el desarrollo de la auditoría.

El acuerdo de inicio deberá ser notificado y deberá obrar en el expediente que para esos efectos integre la Unidad de Transparencia.

ETAPA DE REVISIÓN

Esta etapa corresponde el escrutinio de la forma en que se acredita el cumplimiento de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como los deberes de seguridad y confidencialidad.

Examinación

En el marco de lo estipulado en el acuerdo de inicio, se procederá a la revisión del tratamiento o tratamientos de datos personales, a efecto de corroborar que se encuentren apegados a los principios y deberes siguientes:

- A.** Principio de licitud: el tratamiento de datos personales deberá tener sustento o estar relacionado con las facultades o atribuciones que la normatividad aplicable confiera a la unidad administrativa auditada.
- B.** Principio de finalidad: el tratamiento de datos personales deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable le confiera a la instancia auditada.
- C.** Principio de lealtad: que los datos personales no se hayan obtenido a través de medios engañosos o fraudulentos.
- D.** Principio de consentimiento: cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la Ley General, se deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales.
- E.** Principio de calidad: que se haya adoptado las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.
- F.** Principio de proporcionalidad: que sólo se haya tratado los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad para la cual fueron recabados.
- G.** Principio de información: que se haya informado al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales.
- H.** Principio de responsabilidad: que se hayan adoptado las políticas y mecanismos necesarios para asegurar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la normatividad.
- I.** Deber de seguridad: que se haya establecido y mantenido medidas de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión.
- J.** Deber de confidencialidad: Deberá demostrar la existencia de controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos.

Documento de conclusiones

Se elaborará el documento de conclusiones, en el cual se asentará la información que derive de la examinación realizada, debiendo exponer lo siguiente:

- I. La estimación de cumplimiento correspondiente a cada principio y deber.
- II. Consideraciones que se estimen relevantes en cuanto al tratamiento de los datos personales.
- III. Recomendaciones en materia de seguridad de los datos personales.
- IV. Observaciones y requerimientos que deban ser atendidos ante una deficiencia, desviación o mejora necesaria en el tratamiento de los datos personales, especificando el plazo en que las instancias deberán remitir las evidencias a la Unidad de transparencia.

Conclusiones generales de la auditoría

ETAPA CONCLUSIVA

Reunión final

La Unidad de Transparencia convocará a una reunión final, con el objetivo de hacer entrega del documento de conclusiones.

En dicha reunión se explicarán a detalle las consideraciones efectuadas, se abundará en los puntos de mejora y las cuestiones que se estimen de atención prioritaria y se puntualizará el plazo y la forma en que las observaciones y requerimientos deberán ser cumplimentados, destacando el plazo en que deberán remitir las evidencias correspondientes.

Efectuada la reunión final, se elaborará una minuta en la que se concentrarán las conclusiones alcanzadas, la cual deberá ser firmada por los involucrados.

Cumplimiento de observaciones y requerimientos

Dentro del plazo otorgado en el documento de conclusiones, se deberá remitir a la Unidad de Transparencia las evidencias del cumplimiento de las observaciones y requerimientos que le hubieran sido realizados.

Las evidencias serán examinadas a efecto de dilucidar si cumplen con los extremos determinados y con ello, se atendió la deficiencia, desviación o mejora en el tratamiento de los datos personales.

Si de su examen se corrobora que han sido adecuadamente cumplidas las observaciones y requerimientos, se procederá al cierre de la auditoría.

Por el contrario, de concluir que existen extremos no cumplidos total o parcialmente, se realizará un único requerimiento adicional, reiterando la forma en que la instancia auditada debe demostrar su acatamiento. Si a pesar de ello persiste el incumplimiento, se hará constar la persistencia de la deficiencia o desviación y procederá al cierre de la auditoría.

Informe de cierre de la auditoría

Teniendo a la vista la documentación generada en las etapas de la auditoría, la minuta de la reunión final y las evidencias que deriven del cumplimiento de observaciones y requerimientos, se elaborará un informe final con el cual se dará por concluida la auditoría.

Si del informe efectuado se advierte un incumplimiento a las observaciones y requerimientos efectuados, se dará cuenta al Comité de Transparencia a efecto de que tome conocimiento de la deficiencia o desviación en el tratamiento respectivo y proceda de acuerdo con sus facultades.

La programación de las auditorías se realizará a través de una selección de instancias basada en criterios aplicados al panorama general que guarda el tratamiento de los datos personales, de manera que, las auditorías a practicar se programarán analizando dicho panorama a la luz de criterios de selección específicos.

Panorama general

Del Inventario de Datos Personales y Sistemas, se tomará en consideración lo siguiente:

- El número de Unidades administrativas involucradas en el tratamiento de datos personales.
- El número de tratamientos que cada unidad realiza, así como el resultado global de tal estadística.
- Los tratamientos se clasificarán en las categorías siguientes:
 - Datos de carácter identificativo.
 - Características personales.
 - Circunstancias sociales.
 - Datos académicos y profesionales.
 - Detalles del empleo.
 - Información comercial.
 - Datos económicos.
 - Financieros y de seguro.
 - Instancias que operen uno o varios tratamientos que conlleven datos personales sensibles.

Criterios de selección

Ante el panorama general expuesto, los criterios de selección serán los siguientes:

- I. Tratamientos con un número considerable de riesgos.
- II. Tratamientos que, de ser objeto de una vulneración, tengan como consecuencia un impacto mayor al titular de los datos personales.

III. Tratamientos prioritarios, especiales o estratégicos, que serán aquellos que conlleven un alto valor potencial cuantitativo y cualitativo para una tercera persona no autorizada para su posesión.

IV. Unidades Administrativas cuyas funciones impliquen un alto número de tratamientos.

V. Instancias cuyas funciones impliquen el tratamiento de datos sensibles.

En su análisis se considerarán los factores siguientes:

- El riesgo inherente a cada dato personal de acuerdo a su categoría.
- La sensibilidad del dato personal.
- El desarrollo tecnológico del sistema que opera el tratamiento.
- Posible impacto y consecuencias de la vulneración del dato personal.
- Número de titulares.
- Vulneraciones previas ocurridas en el sistema de datos.
- Valor y exposición de los activos involucrados con el tratamiento.

Programación de Auditorías

Una vez realizada la selección de las instancias bajo los criterios expuestos, la Unidad de Transparencia ponderará la cronología que deberá seguir la calendarización de las auditorías, lo cual deberá hacerse del conocimiento del Comité de Transparencia para su aprobación.

Programa de capacitación

El responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.

En ese sentido, a propuesta de la Unidad de Transparencia, el Comité deberá aprobar anualmente el programa de capacitación de datos personales, mismo que deberá contener mínimamente los siguientes temas.

Sistema de gestión de datos Personales, Promover el Sistema de gestión de datos personales de la Secretaría.

- ¿Qué son los datos personales?
- Base normativa.
- Marco normativo aplicable a la Secretaría de Educación.
- Principios Datos Personales.
- Deberes Datos Personales.

- Observancia general para la Secretaría de Educación.
- Transferencias y remisión.
- Computó en la nube.
- Derechos Arcop.
- Portabilidad.
- Ciclo de Vida.
- Orientación y quejas.

Documento de Seguridad, dar a conocer a todos los servidores públicos de la Secretaría de Educación el documento de seguridad, para implementar las medidas de seguridad y formatearía que las unidades administrativas tendrán que incorporar para la protección en materia de datos personales.

- ¿Qué es y para qué sirve?
- Normatividad.
- Inventario de Datos Personales.
- Análisis de Riesgo.
- Análisis de Brecha.
- Plan de Trabajo.
- Mecanismos de Monitoreo.
- Programa de Capacitación.
- Sanciones.

Proveer conocimientos básicos en materia de protección de datos personales a los servidores públicos de la Secretaría de Educación.

- Avisos de Privacidad
- ¿Qué es un aviso de privacidad?
- Elementos que lo conforman.
- Uso y disponibilidad.
- Cambios y actualización.

El artículo 30 de la Ley General de Datos y el 30, de la LPDPPSOCH establecen la obligación de la actualización del documento de seguridad cuando ocurra lo siguiente:

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

En ese sentido, cuando se actualice alguno de los supuestos antes citados, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia, con el objeto de que este determine si considera procedente la actualización del presente documento de seguridad.

Todos los sistemas de tratamiento que integran el documento de seguridad deben mantenerse actualizados; sin embargo, se entenderá que las modificaciones implican la necesidad de actualizar el documento de seguridad cuando al adecuarse el nivel de riesgo reportado las medidas de seguridad resulte insuficientes.

Por lo anterior, con el propósito de mantener una mejora continua en el Documento de Seguridad se realizará la revisión y de ser necesaria la actualización en forma anual, tomando en consideración la fecha de su aprobación.

APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

El presente Documento de Seguridad fue sometido al análisis y aprobación del Comité de Transparencia de la Secretaría de Educación del Estado de Chiapas, con fundamento en lo dispuesto por los artículos 77 y 78, fracciones I y V, de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas, en la Ciudad de Tuxtla Gutiérrez, el mes de septiembre de 2026.

CATÁLOGO DE TRATAMIENTOS ESTATAL / FEDERAL

AVISOS DE PRIVACIDAD INTEGRAL

Nº P.	Área	Núm. de proceso	Folio de formato
1	Oficina de la c. Secretaria de Educación	1	
1.1	Recepción de solicitudes dirigidas a la Secretaría	1.1	API-OS-OP-001
2	COSICAMMCH	4	
2.1	Proceso de admisión en educación básica y proceso de admisión en educación media superior	2.1	API-COSICAMMCH-001
2.2	Proceso de promoción a horas adicionales en educación básica / proceso de promoción a funciones directivas o de supervisión en educación básica / proceso de promoción a cargos con función directiva o de supervisión en educación media superior (preparatorias estatales)	2.2	API-COSICAMMCH-002
2.3	Proceso de promoción horizontal por niveles con incentivos en educación básica	2.3	API-COSICAMMCH-003
2.4	Proceso de reconocimiento a funciones de asesoría técnica en educación básica / proceso de reconocimiento a funciones de tutoría en educación básica / proceso para otorgar el reconocimiento de beca comisión en educación. Básica / proceso a la práctica educativa	2.4	API-COSICAMMCH-004
3	Coordinación de programas especiales y compensatorios	19	
3.1	PRONI	2	
3.1.1	Contratación de servicio de asesores externos especializados		API-COPEYCO-001
3.1.2	Constitución de comités de contraloría social del programa nacional de inglés		API-COPEYCO-002
3.2	PFSEE		
3.2.1	Acciones académicas para agentes educativos en temas de discapacidad y aptitudes sobresalientes	3	API-COPEYCO-003
3.2.2	Acciones de atención complementaria para estudiantes con discapacidad y / o con aptitudes sobresalientes		API-COPEYCO-004
3.2.3	Equipamiento específico en beneficio de estudiantes con discapacidad y/o con aptitudes sobresalientes		API-COPEYCO-005
3.3	PEMCH	3	
3.2.1	Altas de personal académico y administrativo del capítulo 4000 (ayuda especiales a voluntarios que participan en diversos programas especiales de educación)		API-COPEYCO-006
3.2.2	Expedientes, altas y bajas del sistema saech y sinacem de los niños, niñas y adolescentes migrantes y docentes voluntarios.		API-COPEYCO-007
3.2.3	Recepción y entrega de material didáctico		API-COPEYCO-008

Nº P.	Área	Núm. de proceso	Folio de formato
3.4	Insumos	3	
3.4.1	Entrega de útiles escolares a escuelas de educación básica		API-COPEYCO-009
3.4.2	Entrega de pantallas digitales a escuelas de educación básica		API-COPEYCO-010
3.4.3	Contratación de personal del capítulo 3000 del programa insumos		API-COPEYCO-011
3.5	Desarrollo social	4	
3.5.1	Constitución de comités de contraloría social		API-COPEYCO-012
3.5.2	Instalación de los consejos de participación escolar y municipales en la educación		API-COPEYCO-013
3.5.3	Integración y operación de las asociaciones de madres y padres de familia (amapaf) en las escuelas de educación		API-COPEYCO-014
3.5.4	Protocolo local para erradicar el acoso escolar, la violencia sexual y el maltrato en las escuelas de educación básica en el estado de chiapas.		API-COPEYCO-019
3.6	Área de becas y convocatorias	2	
3.6.1	Constitución de comités de contraloría social		API-COPEYCO-015
3.6.2	Convocatorias		API-COPEYCO-016
3.7	Ver bien, para aprender mejor	1	
3.7.1	Brindar atención optométrica gratuita y dotar de anteojos de alta calidad a niños y niñas y adolescentes de primarias, secundarias y telesecundarias públicas.		API-COPEYCO-017
3.8	Libros de texto	1	
3.8.1	Selección de libros gratuitos de secundaria y telesecundaria		API-COPEYCO-018
4	Coordinación general de asuntos jurídicos y laborales	31	
4.1	Dirección de asuntos federalizados	17	
4.1.1	Validar los requisitos de solicitud de corrección de certificados y enviarlos al área de certificación del edificio de planeación educativa		API-CGAJL-DAF-001
4.1.2	Que el solicitante acredite tener parentesco con el extinto (a) trabajador (a)		API-CGAJL-DAF-002
4.1.3	Proyectar las determinaciones, mediante las cuales se resuelven la procedencia de los ceses y bajas laborales de los trabajadores federalizados de la secretaria de educación		API-CGAJL-DAF-003
4.1.4	Responder las demandas de amparos, ante los juzgados de distrito de amparos		API-CGAJL-DAF-004

Nº P.	Área	Núm. de proceso	Folio de formato
4.1.5	Amparos laborales		API-CGAJL-DAF-005
4.1.6	Ejecución de sanciones administrativas a los servidores públicos impuestas por la dirección de responsabilidades de la Secretaría de la honestidad y función pública		API-CGAJL-DAF-006
4.1.7	Notificación de oficios de requerimientos, emitidos por la dirección de evolución patrimonial, conflicto de interés y ética de la secretaría de la honestidad y función pública		API-CGAJL-DAF-007
4.1.8	Formular querellas o denuncias penales		API-CGAJL-DAF-008
4.1.9	Regularización de los bienes inmuebles		API-CGAJL-DAF-009
4.1.10	Contestación de demandas laborales		API-CGAJL-DAF-010
4.1.11	Gestionar las orientaciones entre la comisión nacional de los derechos humanos (cndh), la comisión estatal de los derechos humanos (cedh) y los diferentes niveles educativos del subsistema federalizado de la secretaría de educación		API-CGAJL-DAF-011
4.1.12	Gestionar las quejas recibidas entre comisión nacional de los derechos humanos (cndh), la comisión estatal de los derechos humanos (cedh) y los diferentes niveles educativos del del subsistema federalizado de la Secretaría de Educación		API-CGAJL-DAF-012
4.1.13	Gestionar las recomendaciones recibidas entre comisión nacional de los derechos humanos (cndh), la comisión estatal de los derechos humanos (cedh) y los diferentes niveles educativos del subsistema federalizado de la Secretaría de Educación		API-CGAJL-DAF-013
4.1.14	Tramitar ante los diversos niveles educativos y coordinaciones el cumplimiento de las resoluciones emitidas por el juzgado especializado en materia burocrática, dictados a través de laudos		API-CGAJL-DAF-014
4.1.15	Desarrollo del juicio, desahogo de pruebas y resolución definitiva		API-CGAJL-DAF-015
4.1.16	Procedimiento administrativo (se recibe denuncia, se investiga, se realizan diligencias y se resuelven)		API-CGAJL-DAF-016
4.1.17	Validación y autorización de licencias con goce y sin goce de sueldos		API-CGAJL-DAF-017
4.2	Dirección de asuntos estatales	14	
4.2.1	Asistir en representación del titular de la secretaría de educación a las audiencias de diferentes dependencias que requieran como terceros interesados		API-CGAJL-DAE-018
4.2.2	Atender peticiones, impugnaciones, opiniones jurídicas, canalizaciones a niveles educativos y áreas administrativas, así como radicar, sustanciar y resolver procedimientos administrativos internos disciplinarios al personal docente y / o administrativo, que incurran en irregularidades en el desempeño de sus funciones, con base en el reglamento de las condiciones generales de trabajo del personal de la secretaría de educación		API-CGAJL-DAE-019
4.2.3	Área de dictámenes prejubilatorios, corrección de nombres, apellidos y género		API-CGAJL-DAE-020

Nº P.	Área	Núm. de proceso	Folio de formato
4.2.4	Interposición en calidad de apoderado legal de la secretaría de educación de querellas y denuncias ante la fiscalía del Ministerio público correspondiente		API-CGAJL-DAE-021
4.2.5	Enlace ante la comisión estatal de los derechos humanos, coadyuvar en la atención de quejas, orientaciones jurídicas, propuestas conciliatorias, medidas precautorias y recomendaciones emitidas por la comisión estatal y/o nacional de los derechos humanos		API-CGAJL-DAE-022
4.2.6	Realizar resolutivos derivados de las actas administrativas iniciadas por los distintos órganos administrativos de la Subsecretaría de Educación Estatal / resoluciones de reconsideraciones derivadas de las mismas / resoluciones de resguardos de plazas y su reincorporación		API-CGAJL-DAE-023
4.2.7	Promover demandas y recursos en materia de amparo laboral directo e indirecto		API-CGAJL-DAE-024
4.2.8	Contestar demandas, planillas de liquidación que provienen de los juzgados especializados en materia burocrática del poder judicial del estado		API-CGAJL-DAE-025
4.2.9	Análisis, revisión, opiniones jurídicas y validación de los instrumentos jurídicos de los órganos administrativos de la Secretaría de Educación que lo soliciten		API-CGAJL-DAE-026
4.2.10	Integrar los expedientes del personal administrativo de la coordinación		API-CGAJL-DAE-027
4.2.11	Escanear los expedientes y control de la base datos		API-CGAJL-DAE-028
4.2.12	Realizar los procesos de sanciones en tiempo y forma a las personas servidoras públicas, derivadas de los procedimientos administrativos emitidos por la secretaría de honestidad y función pública / dar cumplimiento a los requerimientos de las distintas autoridades		API-CGAJL-DAE-029
4.2.13	Contestar informes previos y justificados de los juicios de amparo en los que la titular, subsecretario de educación estatal, coordinador general de asuntos jurídicos y laborales, director de asuntos estatales y jefe del departamento de trámites jurídicos y administrativos son autoridades responsables. Así como interponer recursos de revisión en los asuntos en la que la resolución no sea favorable		API-CGAJL-DAE-030
4.2.14	Brindar asesoría en la regularización de los bienes inmuebles ocupados por las escuelas de la subsecretaría de Educación Estatal.		API-CGAJL-DAE-031
5	Dirección de divulgación	3	
5.1	Cobertura de evento		API-DD-DVE-001
5.2	Pensiones premio Chiapas		API-DD-DVE-002
5.3	Buzón escolar		API-DD-DVE-003
6	Coordinación educativa para la transversalidad de género	1	
6.1	Capacitación, cursos, talleres de sensibilización preventivos para las niñas, niños y adolescentes, docentes y administrativos		API-CETG-001
7	Unidad de transparencia	3	
7.1	Solicitud de derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales (arco)		API-UT-001
7.2	Solicitud de información pública		API-UT-002
7.3	Lista de asistencia, capacitaciones, cursos y talleres		API-UT-003

Nº P.	Área	Núm. de proceso	Folio de formato
8	Dirección de tecnologías educativas y de la información	3	
8.1	Mantenimiento red EDUSAT y equipos de cómputo		API-DTEI-001
8.2	Certificación de firmas electrónicas		API-DTEI-002
8.3	Cursos y capacitación		API-DTEI-003
9	Dirección técnica educativa	1	
9.1	Registro de participantes a cursos de capacitación o reuniones de trabajo		API-DTE-001
10	Subsecretaría de educación estatal	88	
10.1	Dirección de educación básica (PRE, P, S, TS, EF, EI, IE)	35	
10.1.1	Contratación docente de nuevo ingreso o interino		API-SBEE-001
10.1.2	Elaboración de constancias		API-SBEE-002
10.1.3	Jubilación		API-SBEE-003
10.1.4	Radicación de sueldos		API-SBEE-004
10.1.5	Construir programa de mejora continua		API-SBEE-005
10.1.6	Elaboración y expedición de certificados de estudios para alumnos y exalumnos del nivel correspondiente		API-SBEE-006
10.1.7	Expedición de duplicado de certificado de estudios		API-SBEE-007
10.1.8	Verificación de datos académicos del nivel educativo (primaria y secundaria)		API-SBEE-008
10.1.9	Apoyos educativos (telesecundaria)		API-SBEE-009
10.1.10	Bajas		API-SBEE-010
10.1.11	Integrar plantillas del personal		API-SBEE-011
10.1.12	Corrección de datos		API-SBEE-012
10.1.13	Licencias con goce de sueldo o sin goce de sueldo		API-SBEE-013
10.1.14	Pago de titulación, maestría o doctorado		API-SBEE-014
10.1.15	Reanudación de labores		API-SBEE-015
10.1.16	Promoción horizontal o vertical		API-SBEE-016
10.1.17	Alta por reconsideración de cese o reinstalación		API-SBEE-017
10.1.18	Suspensión de sueldos por proceso administrativo o penal		API-SBEE-018
10.1.19	Brindar seguimiento a los programas compensatorios		API-SBEE-019
10.1.20	Contribuir al seguimiento de auditorías		API-SBEE-020
10.1.21	Atender asuntos por faltas administrativas o jurídicas		API-SBEE-021
10.1.22	Recepción de la correspondencia diversa		API-SBEE-022
10.1.23	Descuentos, centralización, retención de sueldos		API-SBEE-023
10.1.24	Verificar el cumplimiento del acuerdo para la incorporación de escuelas particulares		API-SBEE-024
10.1.25	Seguimiento a los requerimientos por falta de declaración patrimonial		API-SBEE-025

Nº P.	Área	Núm. de proceso	Folio de formato
10.1.26	Diseñar estrategias para guiar la evaluación diagnóstica		API-SBEE-026
10.1.27	Atención a las solicitudes de la comisión nacional de derechos humanos		API-SBEE-027
10.1.28	Altas y bajas de becarios del departamento de educación indígena		API-SBEE-028
10.1.29	Control de asistencia (entrada y salida) del personal del departamento de educación indígena		API-SBEE-029
10.1.30	Directorio del personal administrativo del departamento de educación indígena		API-SBEE-030
10.1.31	Formación y capacitación técnico pedagógica a becarios del departamento de educación indígena		API-SBEE-031
10.1.32	Movimientos de becarios del departamento de educación indígena		API-SBEE-032
10.1.33	Pago de becas a becarios del departamento de educación indígena		API-SBEE-033
10.1.34	Pago de viáticos del departamento de educación indígena		API-SBEE-034
10.1.35	Reagrupación de becarios del departamento de educación indígena		API-SBEE-035
10.2	Dirección de educación media	15	
10.2.1	Asesoría y apoyo jurídico		API-SBEE-036
10.2.2	Control del personal adscrito a la dirección de educación media		API-SBEE-037
10.2.3	Gestión de viáticos		API-SBEE-038
10.2.4	Movimientos nominales personal docente y administrativo de educación terminal y telebachillerato		API-SBEE-039
10.2.5	Compactación y descargas académicas		API-SBEE-040
10.2.6	Gestiones administrativas		API-SBEE-041
10.2.7	SUPERVISIÓN A ESCUELAS PREPARATORIAS (pendiente)		API-SBEE-042
10.2.8	Movimientos nominales del personal administrativo preparatorias		API-SBEE-043
10.2.9	Movimientos nominales del personal docente preparatorias		API-SBEE-044
10.2.10	Vinculación de actividades		API-SBEE-045
10.2.11	Becas de educación media		API-SBEE-046
10.2.12	Certificación de documentos escolares de escuelas preparatorias, bivalentes y terminales		API-SBEE-047
10.2.13	Sistema de control escolar		API-SBEE-048
10.2.14	Validación del historial académico (kardex)		API-SBEE-049
10.2.15	Programa atención de planteles públicos de educación media superior con estudiantes con discapacidad		API-SBEE-088
10.3	Dirección de educación superior	24	
10.3.1	Actas de examen y titulación		API-SBEE-050
10.3.2	Asignación de matrículas de ingreso		API-SBEE-051

Nº P.	Área	Núm. de proceso	Folio de formato
10.3.3	Becas		API-SBEE-052
10.3.4	Certificado de grado		API-SBEE-053
10.3.5	Contratos de docentes que imparten cursos y asesorías		API-SBEE-054
10.3.6	Movimiento nominales de continuidad		API-SBEE-055
10.3.7	Trámites de titulación proyecto chol		API-SBEE-056
10.3.8	Apoyos económicos a directivos		API-SBEE-057
10.3.9	Asignación temporal		API-SBEE-058
10.3.10	Bajas por defunción o renuncia		API-SBEE-059
10.3.11	Compactación docente		API-SBEE-060
10.3.12	Corrección de datos (curp, rfc, homonimia, nombre)		API-SBEE-061
10.3.13	Días económicos no disfrutados		API-SBEE-062
10.3.14	Jubilación		API-SBEE-064
10.3.15	Movimientos nominales para altas de interinos, docentes y/o administrativos		API-SBEE-063
10.3.16	Permisos por casos médicos		API-SBEE-065
10.3.17	Promociones de administrativos		API-SBEE-066
10.3.18	Recategorización de los docentes		API-SBEE-067
10.3.19	Revisión y validación de plantilla docente		API-SBEE-068
10.3.20	Licencias y/o prórrogas con goce y sin goce de sueldos		API-SBEE-069
10.3.21	Programa edinen		API-SBEE-070
10.3.22	Examen de ceneval		API-SBEE-071
10.3.23	Becas exoneración de pagos superior		API-SBEE-072
10.3.24	Programa oportunidades para todos		API-SBEE-073
10.4	Dirección de fortalecimiento educativo	14	
10.4.1	Expedición de certificados de educación primaria y secundaria para adultos		API-SBEE-074
10.4.2	Expedición de duplicado de certificado de educación primaria y secundaria para adultos		API-SBEE-075
10.4.3	Expedición de oficio de exoneración de pago (becas) para estudiar en centros de capacitación para el trabajo		API-SBEE-076
10.4.4	Expedientes de centros de capacitación para el trabajo y centros de educación primaria y secundaria para adultos		API-SBEE-077
10.4.5	Inscripción de alumnos de centros de educación primaria y secundaria para adultos		API-SBEE-078
10.4.6	Expedición de certificados de terminación de estudios de egresados de los centros de capacitación para el trabajo incorporados a la secretaría de educación		API-SBEE-079
10.4.7	Expedición de duplicados de certificados de egresados de centros de capacitación para el trabajo		API-SBEE-080

Nº P.	Área	Núm. de proceso	Folio de formato
10.4.8	Inscripción de alumnos de centros de capacitación para el trabajo		API-SBEE-081
10.4.9	Legalización de diplomas de egresados de centros educativos de capacitación para el trabajo		API-SBEE-082
10.4.10	Actualización de expedientes del personal de estructura de la dirección de fortalecimiento educativo		API-SBEE-083
10.4.11	Elaboración de comisión y formatos de viáticos del personal de estructura de la dirección		API-SBEE-084
10.4.12	Mantener actualizados los resguardos de inventarios del personal de estructura de la dirección		API-SBEE-085
10.4.13	Reporte quincenal de incidencias y lista de asistencia del personal de estructura de la dirección de fortalecimiento educativo		API-SBEE-086
10.4.14	Validación de certificados y diplomas de estudios de egresados de los centros de capacitación para el trabajo incorporados a la Secretaría de Educación		API-SBEE-087
11	Subsecretaría de educación federalizada (ee,ep, es, ets, sf y ei)	39	
11.1	Activación de quinquenios		API-SBSEF-001
11.2	Actualización de grado académico		API-SBSEF-002
11.3	Alta definitiva docentes		API-SBSEF-003
11.4	Alta por cambio o permuta de estado		API-SBSEF-004
11.5	Atención a las solicitudes de la comisión nacional de derechos humanos		API-SBSEF-005
11.6	Auditorías		API-SBSEF-006
11.7	Búsqueda de personal por faltas de declaración patrimonial		API-SBSEF-007
11.8	Cambio de actividad		API-SBSEF-008
11.9	Certificación		API-SBSEF-009
11.10	Certificación de firmas electrónicas		API-SBSEF-010
11.11	Combustible		API-SBSEF-011
11.12	Contratación de docentes nuevo ingreso		API-SBSEF-012
11.13	Contratación de interinos		API-SBSEF-013
11.14	Corrección de datos		API-SBSEF-014
11.15	Elaboración de bajas		API-SBSEF-015
11.16	Elaboración de constancias		API-SBSEF-016
11.17	Expedición de diplomas y cartas de pasantes		API-SBSEF-017
11.18	Jubilación		API-SBSEF-018
11.19	Licencia de paternidad		API-SBSEF-019
11.20	Licencia por beca comisión		API-SBSEF-020
11.21	Licencia / prorroga de beca comisión		API-SBSEF-021
11.22	Licencias por gravidez		API-SBSEF-022
11.23	Licencias y o prorrogas sin goce de sueldo		API-SBSEF-023
11.24	Licencias y/o prorrogas con goce de sueldo por acuerdo presidencial 754		API-SBSEF-024
11.25	Nómina de proyecto alternativas de educación preescolar rural y proyecto orientación a padres de familia		API-SBSEF-025
11.26	PLADSE		API-SBSEF-026

N° P.	Área	Núm. de proceso	Folio de formato
11.27	Plantillas de personal		API-SBSEF-027
11.28	Programa de estímulo al desempeño al personal docente de educación superior		API-SBSEF-028
11.29	Promoción horizontal		API-SBSEF-029
11.30	Promoción vertical		API-SBSEF-030
11.31	Recepción de correspondencia		API-SBSEF-031
11.32	Recepción de inasistencias		API-SBSEF-032
11.33	Recepción de licencias médicas		API-SBSEF-033
11.34	Reconsideración de cese y reinstalación		API-SBSEF-034
11.35	Suspensión temporal		API-SBSEF-035
11.36	Técnico pedagógico		API-SBSEF-036
11.37	Trámite administrativo jurídico		API-SBSEF-037
11.38	Transferencia de plaza (reubicación)		API-SBSEF-038
11.39	Viáticos		API-SBSEF-039
12	Subsecretaría de planeación educativa	25	
12.1	Oficina del subsecretario	2	
12.1.1	Actualización de plantilla de personal administrativo oficina del c. Subsecretario		API-SUBPE-001
12.1.2	Elaboración de contratos y nóminas oficina del c. Subsecretario		API-SUBPE-002
12.2	Dirección de programación y presupuesto	13	
12.2.1	Recepción de solicitudes para proyecto auto equipamiento		API-SUBPE-003
12.2.2	Recepción de cédulas de infraestructura		API-SUBPE-004
12.2.3	Recepción de solicitudes para el proyecto del programa nacional de mantenimiento de los espacios educativos (PRONAMEE).		API-SUBPE-005
12.2.4	Actualización de plantilla de personal administrativo de la dirección de programación y presupuesto		API-SUBPE-006
12.2.5	Lista de asistencia departamento de programación de espacios educativos		API-SUBPE-007
12.2.6	Propuesta de inversión anual		API-SUBPE-008
12.2.7	Validación de expedientes técnicos		API-SUBPE-009
12.2.8	Análisis de plantillas docentes y administrativas		API-SUBPE-010
12.2.9	Compactación y regularización de personal docente en educación media y superior		API-SUBPE-011
12.2.10	Gestión para pago de laudos		API-SUBPE-012
12.2.11	Regularización y compactación de horas y/o plazas docentes		API-SUBPE-013
12.2.12	Amparos y quejas de derechos humanos		API-SUBPE-014
12.2.13	Lista de asistencia del departamento de programación y presupuesto federalizado		API-SUBPE-015
12.3	Dirección de planeación educativa	8	
12.3.1	Alta, cambio de atributos o baja de un centro de trabajo educativo		API-SUBPE-016
12.3.2	Incorporación de escuelas particulares		API-SUBPE-017
12.3.3	Búsqueda de información de antecedentes escolares de nivel básico		API-SUBPE-018
12.3.4	Certificación de copias de estudios de educación superior		API-SUBPE-019
12.3.5	Expedición de duplicados de educación básica		API-SUBPE-020
12.3.6	Solicitud de firmas electrónicas avanzadas estatales		API-SUBPE-021
12.3.7	Validación de autenticidad de certificados de educación básica		API-SUBPE-022

Nº P.	Área	Núm. de proceso	Folio de formato
12.3.8	Revalidación de estudios realizados en el extranjero y equivalencias de todos los niveles para que el alumno continúe sus estudios		API-SUBPE-023
12.4	Dirección de evaluación de programas institucionales	2	
12.4.1	Actualización de plantilla de personal administrativo de la dirección de evaluación de programas institucionales		API-SUBPE-024
12.4.2	Trámite de viáticos		API-SUBPE-025
13	Coordinación general de administración estatal	54	
13.1	Oficina del coordinador	1	
13.1.1	Recepción de quejas y denuncias ante el comité de ética		API-CGAE-001
13.2	Dirección de administración de personal (estatal)	40	
13.2.1	Solicitar cálculo de reintegro al departamento de personal docente y administrativo		API-CGAE-002
13.2.2	Solicitar documentos a los niveles educativos		API-CGAE-003
13.2.3	Solicitar expedientes personales al departamento de archivo		API-CGAE-004
13.2.4	Solicitar nóminas al departamento de pagos		API-CGAE-005
13.2.5	Atención de solicitud para constancias de servicio del personal docente y administrativo		API-CGAE-006
13.2.6	Certificación de documentos		API-CGAE-007
13.2.7	Control y seguimientos de pagos a docentes por años de servicio y jubilación, 15 de mayo (día del maestro)		API-CGAE-008
13.2.8	Recepción de documentos que integran el expediente laboral del trabajador		API-CGAE-009
13.2.9	Recepción de documentos que envían las diferentes áreas administrativas del subsistema estatal		API-CGAE-010
13.2.10	Recepción de pólizas de seguro de vida		API-CGAE-011
13.2.11	Recepción de solicitudes de nombramientos		API-CGAE-012
13.2.12	Atención a trámites de nivel básica		API-CGAE-013
13.2.13	Atención de trámites correspondientes al nivel medio, superior y la estructura del edificio.		API-CGAE-014
13.2.14	Control de la información sobre cheques emitidos y analítico de cheques cancelados		API-CGAE-015
13.2.15	Control de los pagos emitidos para la recaudación de tuxtla Gutiérrez		API-CGAE-016
13.2.16	Control de pagos radicados		API-CGAE-017
13.2.17	Pago de pensión alimenticia y captura de cheques cancelados		API-CGAE-018
13.2.18	Pago y control de pagos por conceptos de interinos y complementarias en oficinas centrales		API-CGAE-019
13.2.19	Reprocesos y reexpedición de cheques		API-CGAE-020
13.2.20	Resolución de auditorías y atención a trámites de pensión alimenticia		API-CGAE-021
13.2.21	Revisión y validación de documentación generada por el departamento de pagos.		API-CGAE-022
13.2.22	Alta de nómina electrónica		API-CGAE-023
13.2.23	Altas (nuevo ingreso normales, incrementos, reinstalación e interinato)		API-CGAE-024
13.2.24	Altas y bajas del personal administrativo ante el imss		API-CGAE-025
13.2.25	Bajas (renuncia, jubilación o pensión, acta administrativa, destitución o inhabilitación y defunción)		API-CGAE-026
13.2.26	Captura de los movimientos nominales (altas, bajas, reanudaciones, intercambios de plazas, promociones, titulación / Maestría, licencias, suspensiones, radicaciones, incremento y decremento de horas)		API-CGAE-027

Nº P.	Área	Núm. de proceso	Folio de formato
13.2.27	Comisión administrativa por asignación temporal		API-CGAE-028
13.2.28	Compactación de plazas		API-CGAE-029
13.2.29	Declaración patrimonial		API-CGAE-030
13.2.30	Evaluación de personal		API-CGAE-031
13.2.31	Licencia con y sin goce de sueldo		API-CGAE-032
13.2.32	Modificaciones generales		API-CGAE-033
13.2.33	Reanudaciones de pagos		API-CGAE-034
13.2.34	Suspensión de sueldo		API-CGAE-035
13.2.35	Titulación, licenciatura, maestría y doctorado		API-CGAE-036
13.2.36	Informes de asuntos estatales y órganos administrativos		API-CGAE-037
13.2.37	Raditaciones de sueldo		API-CGAE-038
13.2.38	Gestión para la aplicación de pensión alimenticia ordenada por una autoridad judicial		API-CGAE-039
13.2.39	Trámite para el pago de seguro de vida institucional a los beneficiarios del personal docente y administrativo que no contaban con cobertura		API-CGAE-040
13.2.40	Trámite para iniciar el proceso licitatorio del seguro de vida institucional		API-CGAE-041
13.3	Dirección de recursos financieros (estatal)	4	
13.3.1	Pago del capítulo 4000		API-CGAE-042
13.3.2	Solicitud de pago a proveedores de bienes y servicios		API-CGAE-043
13.3.3	Solicitud de pago por servicios básicos (agua, luz, teléfono, internet y arrendamiento)		API-CGAE-044
13.3.4	Solicitudes de pago por viáticos (normal y reembolso)		API-CGAE-045
13.4	Dirección de recursos materiales y adquisiciones (estatal)	7	
13.4.1	Alta en sistema de mobiliario		API-CGAE-046
13.4.2	Entrega de bienes muebles		API-CGAE-047
13.4.3	Entrega de insumos		API-CGAE-048
13.4.4	Recepción de insumos		API-CGAE-049
13.4.5	Adquisición de bienes y/o servicios por licitación o adjudicación directa con recurso federal y estatal		API-CGAE-050
13.4.6	Adquisición de bienes y/o servicios por licitación o adjudicación directa con recurso federal y estatal		API-CGAE-051
13.4.7	Seguro escolar		API-CGAE-052
13.5	Dirección de informática (estatal)	1	
13.5.1	Recepción y entrega de bienes informáticos por servicio de mantenimiento correctivo		API-CGAE-053
13.6	Dirección de auditorías	1	
13.6.1	Control y seguimiento de auditoría		API-CGAE-054
14	Coordinación general de administración federalizada	21	
14.1	Dirección de administración de personal (federal)	4	
14.1.1	Pago de sueldos y prestaciones al personal docente y administrativo del subsistema federalizado		API-CGAF-001
14.1.2	Validación de la nómina		API-CGAF-002
14.1.3	Servicios al personal docente y administrativo del subsistema federalizado		API-CGAF-003
14.1.4	Movimientos nóminales		API-CGAF-004

Nº P.	Área	Núm. de proceso	Folio de formato
14.2	Dirección de materiales y adquisiciones (federal)	5	
14.2.1	Procesos licitatorios		API-CGAF-005
14.2.2	Aseguramiento en caso de siniestro de la plantilla vehicular		API-CGAF-006
14.2.3	Hoja de no adeudo de activo fijo		API-CGAF-007
14.2.4	Contratos de arrendamientos y servicios		API-CGAF-008
14.2.5	Reembolso de gastos médicos escolares		API-CGAF-009
14.3	Dirección de recursos financieros (federal)	10	
14.3.1	Registro presupuestal de gastos de operación y de servicios personales		API-CGAF-010
14.3.2	Pago de nómina de programas (personal temporal)		API-CGAF-011
14.3.3	Pago de cheques		API-CGAF-012
14.3.4	Captura e impresión de cheques		API-CGAF-013
14.3.5	Pago de impuestos		API-CGAF-014
14.3.6	Pago de marcha		API-CGAF-015
14.3.7	Pagos por transferencias bancarias		API-CGAF-016
14.3.8	Registros contables		API-CGAF-017
14.3.9	Viáticos		API-CGAF-018
14.3.10	Elaboración de contratos del personal eventual		API-CGAF-019
14.4	Dirección de informática (federal)	1	
14.4.1	Almacenamiento y procesamiento de datos para sistemas, trámites y servicios digitales		API-CGAF-020
14.5	Coordinación general de auditorías (federal)	1	
14.5.1	Atención de solicitud de información para la realización, seguimiento y / o procedimientos administrativos de las auditorías realizadas por los entes fiscalizadores		API-CGAF-021
15	Dirección de servicios regionales	27	
15.1	Actas de madres y padres de familia (AMAPAF)		API-DSR-001
15.2	Becas de exoneración de pago del nivel superior		API-DSR-002
15.3	Distribución y comprobación de la entrega de útiles escolares, kits de limpieza, libros de texto y material educativo		API-DSR-003
15.4	Administración de correo electrónico oficial		API-DSR-004
15.5	Expedición de firmas electrónicas		API-DSR-005
15.6	Gestionar el alta o la renovación para ser agentes certificadores de firma electrónica avanzada		API-DSR-006
15.7	Recepción, realización de los pagos (ordinaria, extraordinaria, plazas regularizadas, pensión, becas, estímulo de años de servicio), retención o cancelación, integración y comprobación de los mismos		API-DSR-007
15.8	Constancias de servicio		API-DSR-008
15.9	Plantilla PLADSE		API-DSR-009
15.10	Plantilla bimestral de personal		API-DSR-010
15.11	Día de las madres		API-DSR-011
15.12	Recepción y envío de las solicitudes de apoyos culturales (trámite de lentes y ortopédicos) del personal federalizado		API-DSR-012
15.13	Recepción y envío de cédulas de evaluación del desempeño del servidor público del mes		API-DSR-013
15.14	Diplomas y medallas del personal docente y administrativo		API-DSR-014

Nº P.	Área	Núm. de proceso	Folio de formato
15.15	Gestionar las licencias médicas de los trabajadores de la subsecretaría de educación federalizada		API-DSR-015
15.16	Credenciales de subsecretaría de educación federalizada		API-DSR-016
15.17	Reporte de inasistencia del personal docente y de la subsecretaría de educación federalizada		API-DSR-017
15.18	Gastos de operación		API-DSR-018
15.19	Alternativas		API-DSR-019
15.20	Micro planeación		API-DSR-020
15.21	Tramitar y elaborar viáticos para el personal de la dirección de servicios regionales		API-DSR-021
15.22	Elaboración y pago de cheques a personal comisionado la delegación, becarios y proveedores del proyecto Administración Regional		API-DSR-022
15.23	Elaborar e integrar los viáticos, pasajes del personal comisionado de la delegación para su respectiva comprobación		API-DSR-023
15.24	Gestión de solicitudes de certificaciones de estudios (duplicado) de educación básica federalizada		API-DSR-024
15.25	Distribuir y comprobar la documentación de entrega de mobiliario escolar de las escuelas beneficiadas de educación básica federalizada		API-DSR-025
15.26	Validación de la alta o traslado, baja y corrección de datos, de los alumnos del nivel de educación básica en el sistema SAECH		API-DSR-026
15.27	Regularizaciones a alumnos de nivel secundaria		API-DSR-027
14	Coordinación estatal de formación continua de maestros en servicio	1	
16.1	Atención otorgada a figuras educativas de educación básica		API-CEFCMS-001
17	FOVIMCHIS	1	
17.1	Otorgar créditos para enganche, escrituración o accesorios		API-CEFCMS-001
	Total	322	