



ESTADO DE CHIAPAS

**INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACION
Y PROTECCION DE DATOS PERSONALES DEL ESTADO DE CHIAPAS**
Organismo constitucional autónomo, integrante del Sistema Nacional de
Transparencia, Acceso a la Información Pública y Protección de Datos Personales
“2023. Año de Francisco Villa, el Revolucionario del Pueblo”



Dirección de Capacitación y Promoción de la Transparencia

Tuxtla Gutiérrez, Chiapas. 9 de febrero de 2023

MTRA. GETSEMANÍ MORENO MARTÍNEZ
Instituto de la Juventud del Estado de Chiapas
Presente

Una vez recibido y analizado el Documento de Seguridad de la institución a su cargo, hemos encontrado que contiene las medidas de seguridad de carácter físico, técnico y administrativo necesarias, conforme a lo señalado el Artículo 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y los lineamientos correspondientes. A partir de lo anterior, por acuerdo tomado en la Tercera Sesión Ordinaria de Pleno de 2023, se emite

DICTAMEN FAVORABLE

Reconociendo el compromiso manifiesto con el cumplimiento de la Ley e invitándole a continuar promoviendo la protección de los datos personales mediante la implementación de acciones que garanticen a la ciudadanía que su información personal se encontrará libre de vulneraciones durante el desarrollo de los procesos propios de las funciones que atañen a la institución.

ATENTAMENTE



ROSARIO GUADALUPE CHÁVEZ MOGUEL
Directora de Capacitación y Promoción de la Transparencia



INSTITUTO
DE LA JUVENTUD
GOBIERNO DE CHIAPAS

Documento de Seguridad de Datos Personales

Instituto de la Juventud del Estado de Chiapas



Índice

1. Presentación.....	3
2. Objetivo y alcance del documento.	5
3. Sistema de gestión de los datos personales en posesión del IJECH.	6
4. Inventario de Datos Personales del IJECH.....	9
5. Análisis de riesgos y de brecha.....	16
6. Medidas de seguridad generales.	18
6.1 Monitoreo de las medidas de seguridad.....	19
7. Propuesta de capacitación en materia de datos personales.	20
8. Funciones y responsabilidades del tratamiento de datos personales.	22
9. Programa de trabajo para la implementación de medidas de seguridad.....	28

1. Presentación.

La Constitución Política de los Estados Unidos Mexicanos en los artículos 6 y 16 incorpora el derecho de toda persona a la protección de sus datos personales, así como al acceso, rectificación, cancelación y oposición en los términos que determina la ley.

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), establece un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentren en posesión de los sujetos obligados, entre los que figura el Instituto de la Juventud del Estado de Chiapas (IJECH), como órgano administrativo desconcentrado del Poder Ejecutivo del Estado de Chiapas.

De ahí que el presente **Documento de Seguridad** tiene como propósito establecer el marco de referencia del tratamiento de los datos personales que se llevan a cabo al interior del IJECH por las diversas unidades administrativas que conforman su estructura orgánica, por las diversas unidades administrativas que conforman su estructura orgánica. Todo lo anterior, con base en el Artículo 45 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

En ese sentido, el IJECH ha identificado los procesos que en el ámbito de su competencia involucran el tratamiento de datos personales, a efecto de mantener la seguridad de los mismos durante el ciclo de vida de la información, indicando la forma en la que se trata, las medidas de seguridad adoptadas y las áreas responsables de su protección, así como las finalidades del tratamiento de acuerdo a sus respectivos ámbitos de funciones.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, es necesario señalar que todos y cada uno de los elementos que lo integran, constituyen un sistema interno para la gestión y tratamiento de los datos personales en posesión del IJECH, entendiéndose por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales.

Esto implica el planteamiento de acciones conducentes para evitar la alteración, pérdida, transmisión y acceso no autorizados a los datos, mediante la implementación de medidas físicas, administrativas y técnicas, tendentes a garantizar la seguridad e integralidad de los mismos, así como su seguimiento y supervisión continua. De ahí, que dicho Sistema permita disponer de información relacionada con las medidas de seguridad, el análisis general de las amenazas y posibles vulnerabilidades, así como los mecanismos o acciones a implementar para mitigarlas.

Dicho lo anterior, el presente documento se integra a partir la gestión de actividades coordinadas para controlar y verificar que el tratamiento de los datos personales sea acorde con los principios que rigen su protección, pues para el IJECH la política de seguridad en esta materia constituye un compromiso con el cumplimiento de las disposiciones previstas tanto en la citada LPDPPSOCHIS, como en los Lineamientos Generales de Protección de Datos Personales para el Sector Público por parte de todos los involucrados.

Finalmente, ante la necesidad de mantener actualizado el documento de seguridad se ha de procurar la mejora continua, además, se ha procedido a la actualización de los elementos que integran el documento de seguridad; las medidas de seguridad adoptadas en su tratamiento, el análisis de riesgo y brecha, que permiten dar seguimiento a las medidas adoptadas, identificar las posibles vulneraciones y aminorar los riesgos. Todo lo anterior, acompañado del desarrollo del programa de capacitación que permita comprender la importancia de adoptar medidas para la prevención de las vulneraciones a los datos personales.

2. Objetivo y alcance del documento.

Establecer los principales elementos que integran las medidas de seguridad administrativas, físicas y técnicas necesarias para la protección de los datos personales en posesión del Instituto de la Juventud del Estado de Chiapas, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales; así como determinar las posibles vulnerabilidades, amenazas y riesgos de los que pueden ser objeto en un plano general los diversos sistemas de información y procesos en los se tratan datos personales por las diversas unidades administrativas, conforme a lo establecido en la LPDPPSOCHIS y a los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

El alcance de este documento se relaciona con la identificación de sistemas de información o procesos administrados por parte de las Unidades Administrativas que conforman las áreas de este Sujeto Obligado IJECH, de acuerdo a su reglamento interno, a saber: Dirección General, Delegación Administrativa, Unidad de Transparencia, Área Jurídica, Dirección de Proyectos Creativos Juveniles y Dirección de Orientación e Inclusión, en los que de acuerdo con su ámbito de funciones llevan a cabo el uso y tratamiento de datos personales, mismos que se encuentran bajo su estricta responsabilidad tanto en los medios electrónicos como en los espacios físicos en que se administran, operan y resguardan dichos datos personales.

En este sentido, la Unidad de Transparencia integra el presente documento de seguridad con base en la información generada por las citadas unidades administrativas acorde al ámbito de sus funciones y, de conformidad con las disposiciones aplicables.

3. Sistema de gestión de los datos personales en posesión de la ASF.

Para el tratamiento de los datos personales que lleva a cabo el IJECH a través de su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable a los mismos, se realiza el establecimiento de políticas y métodos orientados a salvaguardar su confidencialidad, integridad y disponibilidad, conforme a los preceptos previstos por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

En tal virtud, el IJECH inició su proceso de planificación de los esquemas de protección de datos mediante la identificación de todos y cada uno de los procesos y tareas en los que, de acuerdo con el ámbito de funciones de las distintas áreas que conforman la institución, se involucra el tratamiento de datos personales. Para ello, se dispuso de un formato que permitió a las diversas unidades administrativas realizar el levantamiento de inventarios de los datos personales que se encuentran bajo su responsabilidad, considerando los elementos mínimos que establece el artículo 47, fracción II de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y el diverso 58 de los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas.

Es así que a través del desarrollo de un instrumento homogéneo y estandarizado, se llevó a cabo el levantamiento del inventario de datos, con el propósito de identificar, entre otros aspectos, la categoría y tipo de datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, y el nombre, cargo y adscripción de los servidores públicos que tienen acceso al tratamiento, además de si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

En ese mismo sentido, el inventario ha contribuido desde el punto operativo a considerar el ciclo de vida de los datos personales, de forma tal que los servidores públicos que intervienen en el tratamiento conocen que, una vez concluida la finalidad de los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, lo que cobra especial relevancia en el marco del proceso de baja documental que las áreas realizan conforme a las disposiciones que regulan la gestión documental al interior del IJECH.

De igual forma, una vez integrados los inventarios de tratamientos y datos, se dispuso de la metodología para el análisis de riesgos, con la intención de que se identificaran el valor de los datos de acuerdo a su categoría y su ciclo de vida, así como el valor de exposición, las posibles consecuencias para los titulares por el uso indebido y/o posible vulneración y las condiciones de riesgo a los que podrían encontrarse

expuestos por medidas de seguridad poco confiables. Lo anterior, permitió identificar la brecha entre las medidas de seguridad existentes y las medidas de seguridad faltantes para que garanticen la seguridad de los datos, tanto administrativas, como físicas y técnica.

Con base en dicho análisis de riesgo, además de promover el reconocimiento de las medidas de seguridad administrativas, entendidas como el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información; físicas, que corresponden a las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento y, técnicas que se valen de la tecnología para proteger el entorno digital de la información, también se han registrado nuevas medidas de seguridad que deberán desarrollarse para fortalecer algunos de los controles que actualmente son implementados; es decir, el análisis de brecha a partir del cual será posible mitigar los riesgos a los que están expuestos los datos tratados.

Considerando que la identificación de vulnerabilidades tiene por objeto prevenir posibles dificultades en la seguridad de los datos bajo un enfoque proactivo; es decir, identificar áreas de oportunidad en materia de seguridad de datos personales sin que éstas constituyan un daño efectivo, es que se listan, de manera enunciativa más no limitativa, algunos tipos de amenazas, que pueden ser intencionales o no, a las que podría enfrentarse este sujeto obligado y sus activos de información.

TIPOS DE AMENAZAS
<ul style="list-style-type: none">• Robo, extravío o copia no autorizada.• Uso, acceso o tratamiento no autorizado.• Daño, alteración o modificación no autorizado.• Pérdida o destrucción no autorizada.• Otras.

El riesgo que de manera general puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada con el fin de comprometer su confidencialidad, disponibilidad e integridad, por lo que las medidas de seguridad por parte de las áreas comisionadas están orientadas a proteger los datos personales.

A partir de la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que de acuerdo a la experiencia y mejores prácticas son monitoreadas para lograr la mejora continua por parte de todos los involucrados en el tratamiento. Como parte del sistema de gestión y política de seguridad institucional, se enmarcan las reglas generales siguientes:

- Tratar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley General;
- Sujetar el tratamiento de los datos personales al principio de consentimiento, salvo las excepciones previstas por la Ley;

- Informar a los titulares del tratamiento de los datos y sus finalidades;
- Procurar que los datos personales tratados sean correctos y estén actualizados;
- Suprimir los datos personales cuando hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron;
- Tratar los datos personales estrictamente para propósitos legales o legítimos de la ASF;
- Limitar el tratamiento de los datos personales al cumplimiento de las finalidades;
- No obtener datos personales a través de medios fraudulentos;
- Respetar la expectativa razonable de privacidad del titular;
- Tratar estrictamente los datos personales necesarios, adecuados y relevantes en relación con las finalidades;
- Velar por el cumplimiento de los principios;
- Establecer y mantener medidas de seguridad;
- Guardar la confidencialidad de los datos personales;
- Identificar el flujo y ciclo de vida de los datos personales;
- Mantener actualizado el inventario de datos personales o de las categorías que maneja la ASF;
- Respetar los derechos de los titulares en relación con su datos personales;
- Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales, y;
- Identificar a los servidores públicos de la ASF responsables del tratamiento de los datos personales.

Con base en lo anterior, el IJECH determina las pautas de acción del personal encargado de tratamiento de datos personales con miras a generar su correcto resguardo, buscando en todo momento actuar en apego a las directrices de la LPDPPSOCHIS y los Lineamientos de la materia, siempre en consideración de la salvaguarda del derecho a la privacidad y protección de datos de las personas.

4. Inventario de Datos Personales del IJECH

Para cumplir con los objetivos y obligaciones que prevé la LPDPPSOCHIS, particularmente en materia de seguridad y, como parte del Sistema de Gestión de Seguridad de Datos Personales del IJECH, se realizó una actualización dentro las unidades administrativas que conforman su estructura orgánica, para identificar los procesos en los que actualmente se lleva a cabo tratamiento de datos personales; obteniendo con ello el denominado Inventario de Datos Personales del IJECH.

Por inventario de tratamiento de datos, se entiende el control documentado del conjunto de operaciones que realizan las áreas que integran el Instituto de la Juventud del Estado de Chiapas con motivo de los datos que se recaban de las personas, a través de procedimientos automatizados o físicos, que van desde su obtención, registro, organización, conservación, utilización, cesión, difusión, interconexión, hasta la rectificación, cancelación y oposición, con motivo de la atención del ejercicio de éstos derechos en el ámbito de sus atribuciones.

En tal virtud, en coordinación con las áreas y derivado del proceso de actualización de información, se advirtió que, en general 5 de las 6 unidades administrativas que conforman la estructura orgánica de este sujeto obligado, llevan a cabo el tratamiento de datos personales.

- Unidad de Transparencia
- Área jurídica
- Delegación Administrativa
- Dirección de Proyectos Creativos Juveniles
- Dirección de Orientación e Inclusión

Como resultado de dicha actualización, se advirtió que en las 5 unidades administrativas en la que se tratan datos, a través una o varias de las áreas que las conforman, dicho tratamiento atiende a las operaciones o procesos que realizan con motivo del ejercicio de sus facultades.

Debe indicarse que de conformidad con el decreto de creación del Instituto de la Juventud de fecha 08 de diciembre de 2018, publicado en el periódico oficial mediante publicación 3333-A-2018, el IJECH tiene por objeto, principalmente, planear, desarrollar, fomentar y coordinar las políticas públicas en materia de juventud, así como impulsar la inclusión de la juventud en los programas y acciones de Gobierno, para fomentar su desarrollo y detonar su crecimiento en los ámbitos social, económico, político y cultural, en condiciones de equidad y solidaridad, coordinándose para ello, con las demás Dependencias y Entidades, para el cumplimiento de sus fines artículo.

Es decir, al ser un ente de naturaleza pública con autonomía técnica y de gestión, el IJECH lleva a cabo diversos procesos dentro de las unidades administrativas que lo integran, cuyas actividades involucran tratamientos de datos debido a la actividades, programas y convocatorias que realiza.



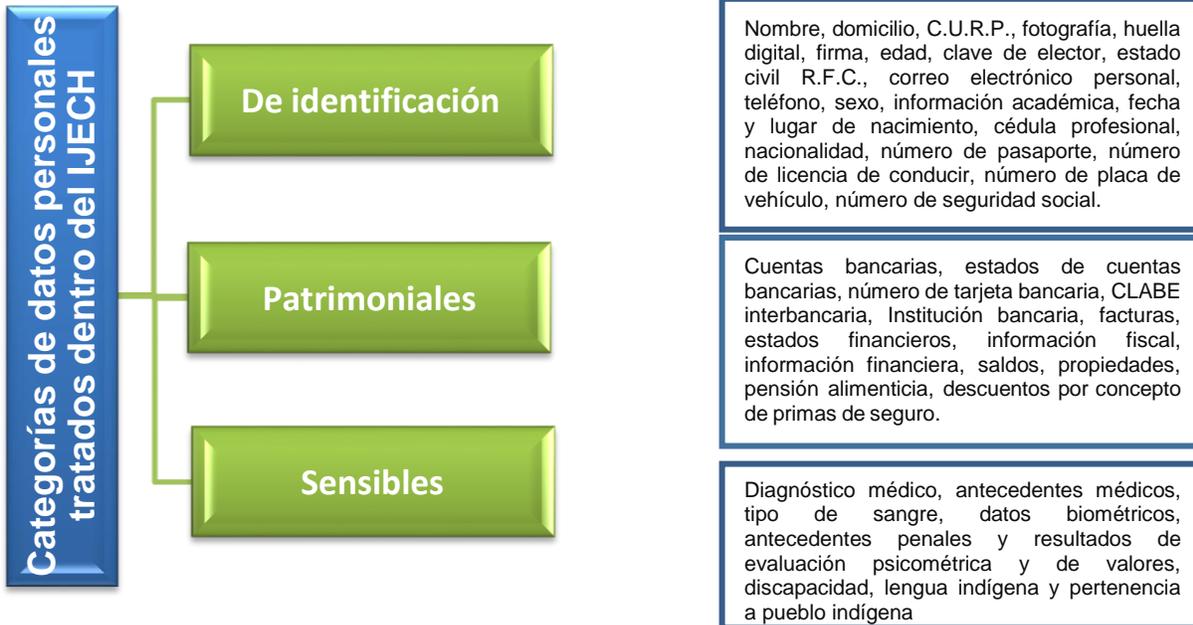
Sin embargo, también determina operaciones de naturaleza jurídica y administrativa que no derivan, necesariamente, del proceso de atención de la población juvenil, pero que sí permiten generar las condiciones para un desarrollo óptimo de sus atribuciones. Ejemplo de ello son las actividades de carácter administrativo derivadas de recursos humanos, materiales y financieros, los procesos de capacitación, así como el cumplimiento a las obligaciones en materia de transparencia, dada su calidad de sujeto obligado en materia de datos personales.

En este sentido, fue posible identificar que en el ejercicio sus atribuciones, **38 procesos** en cuyo cauce se actualiza algún tratamiento de datos personales, por lo que mediante un ejercicio de sistematización, se pudo colegir que dichas actividades pueden ser categorizadas en los siguientes rubros:

Unidad Administrativa	Proceso o Tratamiento
Unidad de Transparencia	<ul style="list-style-type: none">• Atención a solicitudes de ejercicio de derechos ARCO.• Sustanciación de recursos de revisión en materia de transparencia• Atención a solicitudes de acceso a la información• Integración y actualización del comité de Transparencia• Actualización de las Obligaciones de Transparencia• Seguimiento de denuncias por incumplimiento de las Obligaciones de Transparencia• Reporte de solicitudes de acceso a la información recibidas• Elaboración de memorándums y oficios
Área Jurídica	<ul style="list-style-type: none">• Juicios Laborales• Presentación de denuncias penales• Procedimientos de amparo.• Elaboración de Contratos• Elaboración de Convenios• Nombramientos• Elaboración de actas en auxilio de las diferentes unidades administrativas• Elaboración de memorándums y oficios• Sistema Institucional de Archivo
Delegación Administrativa	<ul style="list-style-type: none">• Proceso de seguimiento de auditorías• Movimientos nominales de altas, bajas, validación de perfil y promociones de personal• Seguros de vida.• Trámites ante el IMSS• Expediente único de personal.• Proceso de entrega-Recepción• Padrón de Proveedores• Registro de entradas y salidas de personas a las instalaciones del IJECH.

	<ul style="list-style-type: none"> • Nómina de Personal. • Elaboración de memorándums y oficios • Registro de Movimientos ante Suite Integral de Administración del Patrimonio del Estado
Dirección de Proyectos Creativos Juveniles	<ul style="list-style-type: none"> • Convocatorias • Programas • Capacitaciones • Elaboración de memorándums y oficios • Invitaciones
Dirección de Orientación de Inclusión	<ul style="list-style-type: none"> • Campañas y capacitaciones en materia de salud, educación, derechos humanos y medio ambiente • Coordinación de Comités Municipales de Atención a las Juventud • Coordinación de Comités Distritales de Atención a las Juventud • Elaboración de memorándums y oficios • Invitaciones

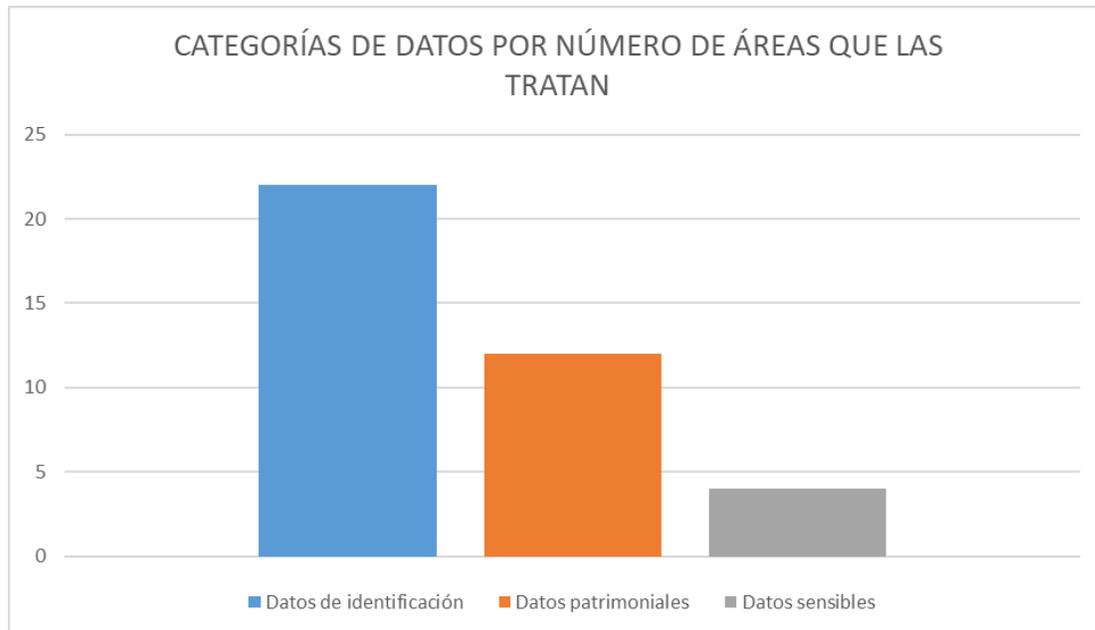
Asimismo, durante el proceso de sistematización se observó que los datos personales cuyo tratamiento se lleva a cabo en los 65 procesos identificados, corresponden a las siguientes 3 categorías:



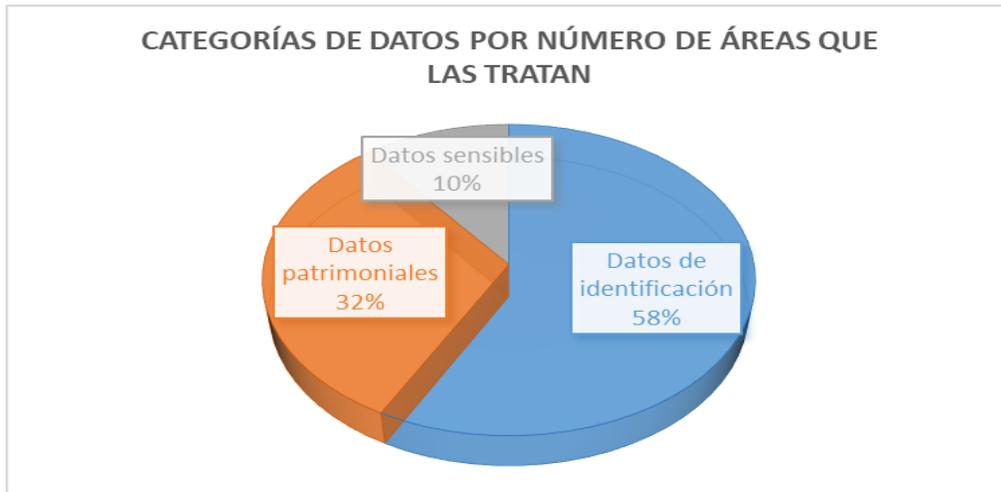
A partir de lo anterior, el Inventario de Datos Personales del Instituto de la Juventud del Estado de Chiapas posibilitó la identificación de hallazgos en relación con el tratamiento de datos personales, aportando los elementos que permiten focalizar las áreas con mayor incidencia en el tratamiento de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



Sobre el particular, se identificó que por lo que hace al tratamiento de **datos de identificación**, en las 5 unidades administrativas aludidas se llevan a cabo tratamientos de datos de esta naturaleza; por lo que hace a los **patrimoniales** en **3 de ellas** se realiza tratamiento de éstos, y por los que hace a los **sensibles**, únicamente en **3** unidad administrativa trata este tipo de datos.

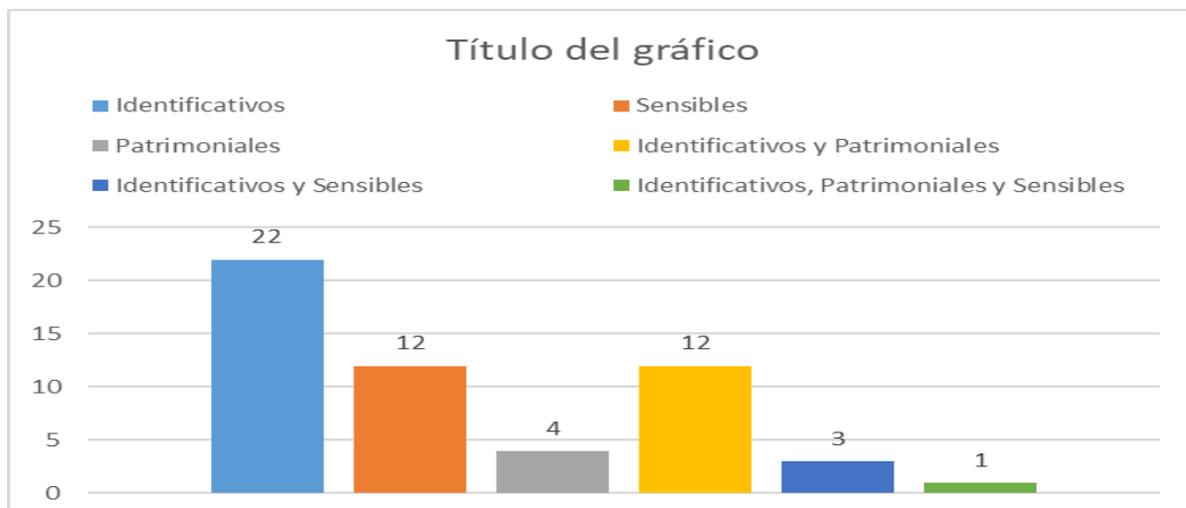


Por otro lado, en relación con los **38 procesos** en los que se tratan datos, se identificó que, por lo que hace a los identificativos, en **57.89% de ellos** se realiza algún tipo de tratamiento; por lo que hace a los **patrimoniales**, en el **31.57%** se llevan a cabo tratamientos de éstos, y respecto de los datos **sensibles**, únicamente en el **10.52%** interviene algún tipo de tratamiento relacionado con dicha categoría de datos; como se muestra a continuación:



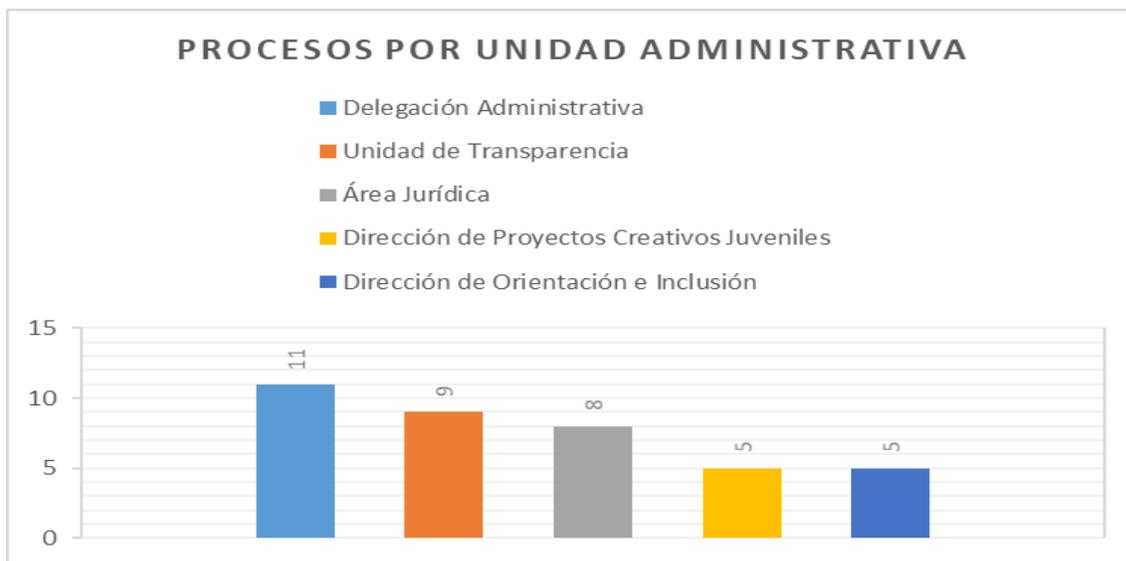
Lo anterior permite advertir que la categoría de datos personales con mayor número de áreas y procesos **son los de carácter identificativos**, seguidos por los patrimoniales y, en casos muy específicos, los datos de naturaleza sensible. Sin embargo, es preciso indicar que se detectaron procesos en los que se realiza tratamiento de datos tanto identificativos y patrimoniales, otros con identificativos y sensibles, y también de identificativos, patrimoniales y sensibles en un mismo proceso.

A efecto de ejemplificar lo anterior, a continuación, se muestra el número de procesos por categoría de datos en las operaciones que llevan a cabo las unidades administrativas que conforman la estructura orgánica del Instituto de la Juventud del Estado de Chiapas:



A partir de lo anterior, también se puede advertir que la unidad administrativa con más número de procesos en los que se tratan datos personales es la Delegación Administrativa con **11**, seguida por la Unidad de Transparencia con **9**; el Área Jurídica con **8** y las Direcciones de Proyectos Creativos Juveniles y Orientación e Inclusión con **5** procesos cada una.

A continuación, se presenta de manera gráfica la distribución de procesos en los que se tratan datos personales, en relación con las unidades administrativas que los ejecutan:



Como se puede observar, la Delegación Administrativa posee el mayor número de operaciones en las que intervienen tratamientos de datos personales, dada la naturaleza de sus funciones, toda vez que entre las áreas que la integran se encuentran aquellas con atribuciones para administrar los recursos humanos, materiales y financieros de la institución, por lo que el hallazgo en sí mismo representa un insumo imprescindible para el cumplimiento de sus funciones. Por tal motivo, las áreas de atención, oportunidad y verificación en materia de protección de datos deben contar con un enfoque de importancia en el desarrollo de las actividades de esta unidad administrativa.

Debe destacarse que, si bien la Delegación Administrativa es la unidad administrativa con más operaciones en las que converge el tratamiento de datos, también lo es que todas las demás, en menor medida, cuentan con áreas en las que se implementa algún tipo de proceso con tratamiento de datos, con una diferencia de tan solo 2 procesos con la Unidad de Transparencia, por lo que la política de protección debe ser entendida como una acción de frecuencia generalizada.

El inventario de datos personales del Instituto de la Juventud del Estado de Chiapas, se integra como un elemento del sistema de gestión de datos personales, en base a los hallazgos identificados en su actualización que junto con las medidas de seguridad representa un instrumento útil para la implementación de las medidas necesarias en materia de protección de datos personales. Asimismo, ayuda a planear capacitaciones focalizada en materia protección de datos hacia los funcionarios del IJECH, teniendo como objetivo prepararlos y sensibilizarlos para los escenarios donde se realicen el tratamiento de datos personales, conformidad con los estándares nacionales e internacionales en la materia.

En tal virtud se consolida el inventario de datos personales del Instituto de la Juventud del Estado de Chiapas como un elemento de la política implementada para la observancia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, aportando con ello certeza a la ciudadanía sobre cuál son y cuál es el destino de los datos recabados por éste sujeto obligado.

5. Análisis de riesgos y de brecha.

El análisis de riesgo y de brecha es parte del documento de seguridad, de acuerdo con el artículo 50 de la LPDPPSOCHIS, es una forma de identificar las medidas de seguridad implementadas y, con respecto a ello, las amenazas de vulneración en que se encuentran los datos personales.

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

La valoración de los riesgos de los datos personales forma parte de los elementos que integran el documento de seguridad, cuyo propósito es garantizar la confidencialidad, integridad y disponibilidad de los datos personales en posesión del IJECH.

Por otra parte, para el análisis de riesgo se tomó en cuenta lo establecido en los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas, que en su artículo 55, define que para el cumplimiento al artículo 47 fracción IV de la Ley Estatal, el responsable deberá realizar un análisis de riesgo de los datos personales tratados considerando lo siguiente:

- Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.
- El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.
- El valor y exposición de los activos involucrados en el tratamiento de los datos personales.
- Las consecuencias negativas para los titulares de los datos personales, que puedan derivar en una vulneración de seguridad ocurrida; y
- Los factores previstos en el artículo 47 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas

Bajo esta premisa, la seguridad de los datos personales que son objeto de tratamiento por parte del IJECH, implica conocer y entender los riesgos a los que se encuentran expuestos en los diversos procesos que realizan las áreas, lo que permitiría solucionarlos de manera adecuada y oportuna.

Para analizar los riesgos de los datos personales que son objeto de tratamiento por el IJECH, se aplicó un instrumento para que, a partir de considerar su objeto y atribuciones constitucionales, clasificar los datos en utilizados a partir de la categorización existente en la ley:

- 1) De **identificación o contacto**, que se refieren a información por la que se identifica a una persona y/o permiten su contacto como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población o la edad.
- 2) **Patrimoniales**, que comprenden la información que se encuentran vinculados al

patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.

- 3) **Sensibles**, que consideran la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleva un riesgo grave para éste como, por ejemplo, el origen étnico, el estado de salud presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

Para la determinación del riesgo sobre esa tipología de datos personales se valora la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación (ciclo de vida), en correspondencia con una diversidad de activos 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.

A partir de lo anterior, se consideró una probabilidad baja, media o alta de que la amenaza suceda en las distintas etapas de vida y tipo de datos personales. Además, se tomó en cuenta la consecuencia desfavorable que podría sufrir el titular en caso de vulneración, la cual que puede ser leve, moderada o grave.

La identificación y valoración del riesgo en cada proceso en que se tratan datos personales por las unidades administrativas del IJECH se basaron en una escala del 0 al 3, representándose de la forma siguiente:

Tipo de Datos	Riesgo Inherente	Nivel de Riesgo
Datos identificativos	Bajo	1
Datos patrimoniales	Medio	2
Datos Sensibles	Alto	3

6. Medidas de seguridad generales.

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

a) Medidas administrativas.

1. Adopción de un esquema de capacitación permanente en materia de la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados del Estado de Chiapas, impartido a quienes colaboran en este sujeto obligado Instituto de la Juventud del Estado de Chiapas.
2. Implementación de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.
3. Aplicación de estrategias de seguridad para el resguardo de los expedientes, con observancia de criterios vinculados con el sistema de gestión documental.
4. Suscripción de una carta responsiva por parte de los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.
5. Previsión de reportes de incidencias, mediante la elaboración e implementación de los formularios correspondientes.

b) Medidas técnicas.

1. Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas, prestarlas o registradas a la vista de otras personas.
2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.
3. Notificar de manera inmediata a la Dirección General de Sistemas o el área administrativa correspondiente, los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero.
4. Utilizar el correo electrónico para fines relacionados con las actividades laborales, evitando remitir datos personales.
5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.

6. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.

6.1 Monitoreo de las medidas de seguridad.

La supervisión de las medidas de seguridad técnicas y físicas es un elemento importante para la mejora continua, pues permite definir nuevos controles de monitoreo y seguimiento de éstas. Entre las medidas de supervisión y monitoreo se encuentran las siguientes:

1. Revisión y actualización permanente de las contraseñas utilizadas para resguardar los datos personales en equipos de cómputo.
2. Revisar de manera permanente el cumplimiento de protocolos implementados para la protección de los datos personales.
3. Vigilar que el ingreso de personas sea a través de los accesos correspondientes, plenamente identificados.

7. Propuesta de capacitación en materia de datos personales.

La aplicación del programa de protección de datos personales dentro del Instituto de la Juventud, requiere como un factor esencial, la formación y sensibilización de las personas que ahí laboran, de tal forma que pueda garantizarse la actualización y mejora continua del inventario de datos personales, la observancia de la normatividad y Ley, por lo que se propone un programa de capacitación en el tema de protección de datos personales que favorezca la profundización en el conocimiento del tema por parte de quienes intervienen en el tratamiento de datos personales. A manera de propuesta, se han considerado los siguientes temas:

Así, entre los elementos de los que resulta necesario profundizar se encuentran los siguientes:

- I) Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.
 - ✓ Antecedentes.
 - ✓ Principios.
 - ✓ Alcances.
 - ✓ Objetivo.
 - ✓ Implicaciones.
- II) Obligaciones en la observancia de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.
 - ✓ Deberes.
 - ✓ Medidas de Seguridad
 - ✓ Procedimientos y sanciones/ Derechos ARCO (acceso, rectificación, cancelación y oposición)
 - ✓ Medios de defensa
- III) El programa de protección de datos personales.
 - ✓ Sistema de datos Personales.

- ✓ Inventario y base de datos.
- ✓ Medidas de seguridad.
- ✓ Análisis de brecha y riesgo.
- ✓ Funciones y obligaciones.

IV) El principio de información: Avisos de Privacidad en el marco del programa de protección de datos personales.

- ✓ Contenido: integral, simplificado.
- ✓ Consentimiento.
- ✓ Deber de información.
- ✓ Finalidades del tratamiento de los datos.

8. Funciones y responsabilidades del tratamiento de datos personales.

A raíz de los procesos determinados en el Inventario de Datos Personales, por las áreas que integran las unidades administrativas que realizan tratamiento de éstos dentro del Instituto de la Juventud del Estado de Chiapas, resultó necesario asociar dichas actividades con las facultades que el Reglamento Interior otorga a los servidores públicos responsables de dicho tratamiento, a efecto de generar certeza y dar cumplimiento al principio de legalidad que debe atender todo servidor público.

En tal virtud, a continuación se precisan las funciones otorgadas por el ordenamiento jurídico a los servidores públicos que llevan a cabo tratamiento de datos personales dentro de las unidades administrativas que conforman la estructura orgánica de este ente de Fiscalización Superior:

Unidad Administrativa	Cargo del personal responsable del tratamiento de los datos ³	Funciones relacionadas con el tratamiento de datos.	Obligaciones
Unidad de Transparencia	Responsable de la Unidad de Transparencia.	<p>Artículo 17.- El titular de la Unidad de Transparencia, tiene las atribuciones y funciones conferidas en el artículo 70 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y demás disposiciones legales aplicables.</p>	<p>Garantizar el acceso a la información pública, así como mantener actualizada la información del portal de transparencia del Instituto. Atendiendo las solicitudes de acceso a la información.</p>



<p>Área Jurídica</p>	<p>Jefa del área Jurídica</p>	<p>Artículo 18.- El titular del Área Jurídica, tendrá las atribuciones siguientes</p> <p>I. Representar legalmente al Instituto en el ámbito de su competencia, ante toda clase de autoridades judiciales, administrativas, del trabajo, militares, fiscales y del fuero Federal, Estatal 40 miércoles 11 de agosto de 2021 Periódico Oficial No. 179 o Municipal; así como ante sociedades, asociaciones y particulares en los procedimientos de cualquier índole, con las atribuciones generales y especiales de un mandato para pleitos y cobranzas. La representación a que se refiere esta fracción, comprende el desahogo de todo tipo de pruebas, promoción de incidentes, rendición de informes, presentación de recursos o medios de impugnación en acciones o controversias, lo cual constituye una representación amplísima.</p> <p>IV. Vigilar que las sanciones laborales a que se hagan acreedores los servidores públicos adscritos al Instituto, se apliquen conforme a la legislación correspondiente.</p> <p>V. Formular contratos, convenios, acuerdos y demás documentos jurídicos y administrativos relacionados con los asuntos competencia del Instituto.</p> <p>XI. Habilitar al personal a su cargo para que realice</p>	<p>Representación legal del sujeto obligado Instituto de la Juventud, con carácter de mandatario judicial, así como el trámite y la resolución de los asuntos que sean de su competencia. Así como aplicar métodos y técnicas archivísticas que garanticen la organización, conservación, disponibilidad, integridad y localización expedita, de los documentos del archivo dependiente del Instituto</p>
-----------------------------	-------------------------------	--	---



		<p>notificaciones de oficios, acuerdos y resoluciones de los procedimientos jurídicos competencia del Instituto.</p> <p>XII. Substanciar los procedimientos administrativos a los que se encuentren sujetos los servidores públicos del Instituto, de conformidad con la normatividad aplicable.</p> <p>XIII. Formular denuncias y querellas ante la institución del Ministerio Público competente, respecto de los hechos que pudieran constituir delitos en los que el Instituto tenga el carácter de ofendido o se encuentre legitimado para hacerlo, de conformidad con la legislación aplicable, previo acuerdo y aprobación del Director General.</p>	
		<p>Artículo 19.- El titular de la Delegación Administrativa tiene las atribuciones siguientes:</p> <p>I. Vigilar el cumplimiento de las disposiciones administrativas, en materia de recursos humanos, financieros y materiales, a cargo del Instituto.</p> <p>II. Emitir documentos administrativos para el suministro y control de los recursos humanos, financieros y materiales del Instituto.</p>	



<p>Delegación Administrativa</p>	<p>Delegada Administrativa</p>	<p>IV. Conocer y resolver los asuntos de carácter administrativo y laboral, relacionados con la administración de los recursos humanos, financieros y materiales del Instituto.</p> <p>V. Otorgar las identificaciones oficiales del personal adscrito al Instituto.</p> <p>XII. Generar los movimientos nominales del personal adscrito al Instituto, para su trámite ante la instancia normativa correspondiente.</p> <p>XV. Generar la información presupuestal, financiera y contable del Instituto, en las formas y términos establecidos por las instancias normativas correspondientes.</p> <p>XVIII. Vigilar en el ámbito de su competencia, que las adquisiciones, abasto, conservación, mantenimiento y reparación de bienes muebles e inmuebles, se apeguen a la normatividad establecida.</p> <p>XXX. Vigilar que la administración y operación de equipos y sistemas, instalados en los Órganos Administrativos que integran el Instituto, sea de acuerdo con la normatividad establecida.</p>	<p>Implementación de las medidas administrativas, técnicas y físicas que permitan asegurar el debido tratamiento de los datos personales recabados con motivo del ejercicio de sus funciones; destacando el aseguramiento de los registros en que obran los mismos y el acceso restringido con personal.</p>
---	--------------------------------	---	--



Dirección de Proyectos Creativos Juveniles	Director de Proyectos Creativos Juveniles	<p>Artículo 22.- El Titular de la Dirección de Proyectos Creativos Juveniles, tiene las atribuciones siguientes:</p> <p>I. Elaborar en el ámbito de su competencia, los programas y proyectos de emprendimiento, recreación, arte, cultura, trabajo e innovación en beneficio de la juventud en el Estado.</p> <p>II. Coordinar con el Poder Legislativo del Estado el Parlamento de la Juventud Chiapaneca y fomentar su difusión.</p> <p>V. Promover en las instancias correspondientes la atención de las demandas y necesidades, relacionadas con la salud, empleo, educación, capacitación, seguridad, justicia, cultura y recreación de la juventud en el Estado.</p> <p>VIII. Coordinar la participación de las asociaciones juveniles en el desarrollo de proyectos que mejoren la calidad y cobertura de la Política</p>	<p>Mantener el resguardo de los datos personales recabados con motivo de la implementación de convocatorias, acciones y programas de acuerdo a sus facultades y atribuciones; privilegiando en todo momento el acceso a los registros únicamente a personal previamente autorizado; particularmente mediante la implementación de medidas de seguridad físicas y técnicas.</p>



		<p>Estatutal de la Juventud en el Estado.</p>	
<p>Dirección de Orientación e Inclusión</p>	<p>Director de Orientación e Inclusión</p>	<p>Artículo 22.- El Titular de la Dirección de Proyectos Creativos Juveniles, tiene las atribuciones siguientes:</p> <p>II. Coordinar la instalación y funcionamiento del Comité Directivo del Sistema Estatal de Atención a la Juventud en el Estado así como la integración de los Comités Municipales de Atención a la Juventud, de conformidad con la normatividad establecida en la materia.</p> <p>III. Coordinar la formulación y el seguimiento del Plan Estatal de Atención a la Juventud, de conformidad con la legislación aplicable.</p> <p>IV. Implementar el Sistema de Difusión, Información e Investigación que permita el intercambio de conocimientos y experiencias sobre las realidades juveniles en el Estado.</p> <p>VIII. Promover la inclusión de la juventud en las políticas públicas que desarrollen los diferentes Organismos de la Administración Pública</p>	<p>Mantener el resguardo de los datos personales recabados con motivo de la implementación de convocatorias, acciones y programas de acuerdo a sus facultades y atribuciones; privilegiando en todo momento el acceso a los registros únicamente a personal previamente autorizado; particularmente mediante la implementación de medidas de seguridad físicas y técnicas.</p>

		Estatal.	
--	--	----------	--

9. Programa de trabajo para la implementación de medidas de seguridad.

Conforme al análisis de brecha, existen algunas medidas de seguridad que se requiere implementar, por lo que a continuación se presentan las actividades generales que se planea realizar:

- Celebración de reuniones de trabajo con unidades administrativas a efecto identificar alternativas de solución técnicas, físicas y administrativas a desarrollar en el mediano y largo plazo.
- Promover un sistema de gestión y administración de datos personales que permita centralizar mediante la identificación de datos por categorías, asociando los diversos tratamientos y procesos a las políticas de seguridad que resultan aplicables a cada caso, conforme a los estándares y mejores prácticas en la materia.
- Implementar mecanismos de divulgación y conocimiento de las políticas generales de seguridad y, verificar de manera continua su cumplimiento.
- Fortalecer los mecanismos de control de documentos e información en las distintas unidades administrativas, a efecto de evitar posibles vulneraciones.