SECRETARÍA
DE SEGURIDAD Y
PROTECCIÓN CIUDADANA
GOBIERNO DE CHIAPAS

Tuxtla Gutiérrez, Chiapas, 16 de noviembre de 2023.

SECRETARIA DE SEGURIDAD Y PROTECCIÓN CIUDADANA DEL ESTADO DE CHIAPAS.

-Documento de seguridad-

Oficial de Datos Personales de la Secretaría

de Seguridad y Protección Ciudadana:

Lic. Diana Laura Figueroa Gallegos.

Tel. 6177020. Ext. 16024

C O N T E N I D O

3. Redacción del Documento de Seguridad

a) Contenido del Documento de Seguridad

b) Objetivos del Documento de Seguridad

c) Responsabilidades dentro del programa

d) Alcance del programa

e) Redacción del Sistema de gestión de Datos Personales

f) Inventario de tratamientos de datos personales

g) Redacción de Análisis de riesgo y de brecha

h) Análisis de la Información

-Gestión de vulneraciones.

i) Redacción de Medidas de Seguridad

-Control de Identificación y Autenticación de Usuarios.

-Procedimiento de Respaldo y Recuperación de Datos Personales.

-Plan de Contingencia

-Técnicas Utilizadas para la Supresión y Borrado Seguro de los Datos Personales

-Plan de Trabajo para la implementación de medidas de Seguridad

j) Monitoreo de las medidas de seguridad

k) Propuesta de capacitación en materia de protección de datos

Personales.

P R E S E N T A C I Ó N

El derecho a la protección de los datos personales es un derecho humano reconocido en la Constitución Política de los Estados Unidos Mexicanos en sus artículos 6, apartado A, fracción II y 16, párrafo segundo; su regulación específica para el sector público es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual fue publicada el 26 de enero de 2017 en el Diario Oficial de la Federación (DOF).

Ahora bien, de conformidad con los artículos 29 y 31 de la Ley General de Datos, esta Secretaría de Seguridad y Protección Ciudadana, debe observar en el tratamiento de los datos personales, entre otros, el principio de responsabilidad y el deber de seguridad. El deber de seguridad implica que esta Secretaría, establezca y mantenga las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales que trata, que permitan protegerlos contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Por su parte el principio de responsabilidad implica, la implementación de mecanismos y acciones para acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley de la mater

En el contexto del sistema de gestión, el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, determina que, como sujeto obligado el elaborar el denominado Documento de seguridad, en el cual la Secretaría deja constancia del propio sistema, incluido el plan de trabajo que permitirá fortalecer, en el corto, mediano y largo plazo la seguridad en el tratamiento de los datos personales.

O B J E T I V O

Establecer los principales elementos que integran las medidas de seguridad administrativas, físicas y técnicas que ha adoptado la Secretaria de Seguridad y Protección Ciudadana 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 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados 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 Áreas, Unidades, Direcciones y Subsecretarías que conforman esta Secretaría de Seguridad y Protección Ciudadana.

A N T E C E D E N T E S

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, busca garantizar el derecho de las personas a la protección de sus datos personales que estén en poder o posesión de todo ente público de los tres órdenes y niveles de gobierno, así como de los partidos políticos y otros sujetos obligados.

Para ello, establece que:

Artículo 48.- Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

Artículo 49.- El responsable deberá elaborar y aprobar un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo conforme a lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables en la materia. El documento de seguridad será de observancia obligatoria para los encargados y demás personas que realizan algún tipo de tratamiento de datos personales.

1. Elementos Conceptuales

A) ¿Qué son los datos personales?

Es toda la información concerniente a una persona física que permitirá identificarla. Se expresan de forma numérica, alfabética, alfa numérica, fotográfica, acústica o de cualquier otra manera. Los datos personales pueden ser:

De identificación: Nombre, edad, domicilio particular, sexo, RFC, CURP, etc.

Patrimoniales: Número de cuenta bancaria, saldos, propiedades, etc.

Sensibles: Refieren la esfera más íntima de su titular; revelan aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, creencias religiosas, filosóficas y morales, opiniones políticas, datos genéticos, datos biométricos y preferencia sexual.

Su utilización indebida puede dar origen a discriminación o representar un riesgo grave para la persona; lo que implica un mayor compromiso con su protección y uso.

B) Marco Legal

Artículo 16º de la Constitución Política de los Estados Unidos Mexicanos

"Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley…"

Derechos ARCO

•**Acceso=** El titular tendrá derecho de acceder a sus datos personales que obren en posesión del responsable, así como a conocer la información relacionada con las condiciones, generalidades y particularidades de su tratamiento. Artículo 60.

•**Rectificación=** El titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados. Artículo 61.

•**Cancelación=** El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión. Artículo 62.

•**Oposición**= El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando exista una causa legítima y su situación específica así lo requiera o sus datos sean objeto de un sistema automatizado con efectos jurídicos.

C) El deber de seguridad

Artículo 45° de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados de Chiapas, establece que el deber de seguridad implica la implementación de Medidas de seguridad de carácter administrativo, físico y técnico cuya finalidad es protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

1.- Medidas de seguridad físicas

Son Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

a) Prevenir que el acceso no autorizado;

b) Prevenir el daño a las instalaciones;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico

d) proveer a los equipos un mantenimiento eficaz que asegure su disponibilidad

e integridad.

2. 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.

a) Prevenir que el acceso a las bases de datos o a la información

b) Generar un esquema de privilegios

c) Revisar la configuración de seguridad

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento;

e) Medidas de seguridad administrativas

f) Políticas y Procedimientos

g) La identificación y clasificación de la información

h) Sensibilización y capacitación del personal

i) Documentos necesarios para la seguridad de la información

3. Medidas de seguridad administrativas

Son el conjunto de Políticas y Procedimientos para garantizar la protección de datos personales mediante la implementación de acciones relacionadas con:

a. La identificación y clasificación de la información

b. Sensibilización y capacitación del personal

c. Documentos necesarios para la seguridad de la información

<u>D) Sistema de Gestión</u>

Se entenderá por sistema de gestión al conjunto de acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión, integrado por un conjunto de elementos y actividades interrelacionadas para

- Establecer
- Implementar

• Operar

• Monitorear

• Revisar

• Mantener y

• Mejorar el tratamiento y seguridad de los datos personales.

Artículo 48° de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas. Documenta y contiene las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales.

ELEMENTOS DE BASE PARA EL SISTEMA DE GESTIÓN

•Actuar

•Planificar

•Verificar

•Hacer

2.- Desarrollo de la política de gestión

Como parte del desarrollo de la política de gestión de datos personales, se identificarán las obligaciones que se deberán cumplir en los tratamientos, según el ciclo de vida de los datos personales, desde su obtención, durante el uso y hasta su eliminación una vez que ha sido concluido el tratamiento para el que fueron otorgados. –OBTENCIÓN –USO –ELIMINACION.

A) DOCUMENTO DE SEGURIDAD

Artículo 49° de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas. El responsable deberá elaborar y aprobar un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo conforme a lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables

en la materia. Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee. El documento de seguridad será de observancia obligatoria para los encargados y demás personas que realizan algún tipo de tratamiento de datos personales.

B) LA CONSTRUCCIÓN DEL DOCUMENTO DE SEGURIDAD

•Identificación de tratamientos y datos personales

•El inventario de datos personales y de los sistemas de tratamiento

•Análisis de riesgo y de brecha

•Desarrollo de procedimientos y mecanismos para la conservación y supresión de datos personales

•Programa de revisión y monitoreo de la efectividad del programa

•Programa de capacitación y actualización

C) IDENTIFICACIÓN DE DATOS PERSONALES Y TRATAMIENTOS

Operaciones llevadas a cabo durante el ciclo de vida de los datos personales, desde el momento de su obtención, pasando por su explotación o aprovechamiento, hasta su supresión o eliminación.

Se identifican los datos personales utilizados en cada tratamiento, en el cual se incluye:

• Sujeto obligado o institución

• Unidad Administrativa

• Departamento

• Tratamiento o proceso

• funcionarios que tratan datos personales (nombre y función)

• Datos personales que utiliza, considerando tipo de datos (identificativos, patrimoniales, sensibles)

IDENTIFICACIÓN DE DATOS PERSONALES Y TRATAMIENTOS

La persona oficial de datos personales compartirá esta cédula entre todas las áreas del Sujeto Obligado, para que identifiquen si trabajan con datos personales, cuales son estos datos y su categoría (Identificativos, patrimoniales y/o sensibles), el nombre del tratamiento o proceso en que los ocupa (tramite que realizamos para atender a los ciudadanos en una gestión o solicitud de un servicio) y las personas funcionarias que tienen acceso a estos datos.

Es necesario llenar esta cédula por cada tratamiento que se realice en la institución.

IDENTIFICACIÓN DE TRATAMIENTO

Sujeto obligado: Secretaría de Seguridad y Protección Ciudadana

Unidad Administrativa (dirección o área) Área de Recursos Materiales y Servicios Generales

Departamento Sección de Facturación

Tratamiento o proceso Registro de Facturas en el Sistema Balance

IDENTIFICACIÓN DE FUNCIONARIOS

Anotar en la tabla los nombres de las personas funcionarias que tratan datos personales (nombre y función):

No	Nombre de la persona funcionaria	Función que desempeña
1	-Ricardo Manuel Ignacio Rodríguez González	Jefe de la Sección de Facturación

IDENTIFICACIÓN DE DATOS PERSONALES

Identificar en la tabla los datos personales (identificativos, patrimoniales y/o sensibles) que usa, señalándolos con una X en la casilla “SI”

D) INVENTARIO DE DATOS PERSONALES Y TRATAMIENTOS

El Artículo 47° fracción III de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del estado de Chiapas. Establece la necesidad de elaborar un inventario de los datos personales y/o sistemas de tratamiento; que consiste en un documento en el que daremos cuenta de:

•Tratamientos de datos personales que se realizan

•Unidad administrativa a cargo de estos procesos

Donde se determinará, de acuerdo con el ciclo de vida de los datos personales lo siguiente:

• ¿Cómo se obtienen los datos personales?

• ¿Qué tipo de datos personales se tratan? ¿Son sensibles?

• ¿Dónde se almacenan y realiza el tratamiento de los datos personales?

• ¿Para qué finalidades se utilizan los datos personales?

• ¿Quién tiene acceso a la base de datos o archivos (sistemas de tratamiento)?

•¿a quién se comunican los datos personales al interior del sujeto obligado?

• ¿Intervienen encargados en el tratamiento de los datos personales?

•¿Cuál es el instrumento mediante el cual se formaliza su intervención?

• ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?

• ¿Se difunden los datos personales?

2. - INVENTARIO DE DATOS PERSONALES Y TRATAMIENTOS

<u>E) ANÁLISIS DE RIESGO DE LOS DATOS PERSONALES</u>

Artículo 5 fracción IV de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas. señala que hay que realizar un análisis de riesgo

de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, hardware, software, personal del responsable, entre otros. Para ello hay que considerar lo siguiente:

I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;

II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;

III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;

IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida;

V. El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las amenazas y vulnerabilidades existentes para los datos personales y los recursos o activos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal o cualquier otro recurso humano o material, entre otros;

VI. La sensibilidad de los datos personales tratados;

VII. El desarrollo tecnológico;

VIII. Las transferencias de datos personales que se realicen;

IX. El número de titulares;

X. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y

XI. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Las medidas de seguridad que deberán adoptarse por el responsable deben tomar como referencia el nivel de riesgo que presenta cada tratamiento de datos personales. Para ello,

es necesario calcular los factores de riesgo por tipo de dato, por número de usuarios por tipo de acceso, y por entorno desde el cual se realizan los tratamientos de los datos personales**.**

TIPO DE DATO	RIESGO INHERENTE	NIVEL DE RIESGO
Datos identificativos	Bajo	1
Datos laborales, patrimoniales, procedimientos administrativos	Medio	2
Datos de tránsito y movimientos migratorios; de salud, biométricos	Alto	3
Datos sensibles	Muy alto	4.5

El nivel de riesgo por tipo de dato en relación con el número de titulares, servirá para determinar los controles que se deben considerar para su protección. Es necesario tomar en cuenta también el volumen de titulares con los que trabajamos, teniendo en cuenta que a mayor número de titulares, mayor será el riesgo por tipo de dato. Es decir, el riesgo inherente más el volumen de titulares, da como resultado el nivel de riesgo por tipo de dato.

	NUMERO DE TITULARES			
TIPO DE DATO	>100	>1000	>10000	>10000
Datos identificativos	4	4	5	5
Datos laborales, patrimoniales, procedimientos administrativos	1	2	3	3
Datos de tránsito y	1	1	2	2

movimientos migratorios; de salud, biométricos				
Datos sensibles	1	1	1	1

Cada área de esta Secretaria de Seguridad y Protección Ciudadana identificará el nivel de riesgo en que se encuentran los datos personales a partir de: El tipo de dato, el volumen, el número de accesos y el entorno en el que se almacena Se realiza el análisis por tratamiento seleccionando el número correspondiente de acuerdo con el manejo que se hace de los datos personales en todos los tratamientos, se suman todos los valores seleccionados y se dividen entre 4 para obtener el riesgo inherente de cada tratamiento.

Posteriormente, se integrarán todos los análisis por tratamiento, para realizar un cuadro en el que se señale por unidad administrativa, área o dirección, las medidas de seguridad implementadas, las medidas de seguridad faltantes y el riesgo inherente en que se encuentran los datos personales. Se sumarán todos los valores de riesgo inherente y se dividirán entre el número de tratamientos que realiza el área o dirección en cuestión, el resultado será el riesgo inherente de cada dirección.

La combinación de los cuatro factores analizados da como resultado el nivel de riesgo latente de cada tratamiento de datos personales, lo cual contribuye a identificar el nivel de medidas de seguridad que deben implementarse en cada caso.

Una vez que se calcula el nivel de riesgo latente por cada tratamiento de datos personales, es posible realizar estrategias para identificar los modelos de medidas de seguridad que deben aplicarse a cada uno de ellos.

Realizar un análisis de riesgos por cada tratamiento ayudará a identificar las medidas de seguridad que deben ser implementadas para la protección de los datos personales. Posteriormente, se realiza un comparativo con aquellas que son implementadas por las áreas, obteniendo con ello un análisis de brecha, a través del cual se construirán los planes de trabajo, mecanismos de monitoreo y revisión de medidas de seguridad y programas de capacitación necesario.

F) ANALÍSIS DE BRECHA

El Artículo 5° fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas. Establece que es necesario realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable. El análisis de brecha consiste en identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados. Este análisis es de naturaleza diagnóstica y contribuye a conocer las áreas de oportunidad por cada tratamiento.

Implica que se logre realizar un comparativo entre las medidas implementadas por las áreas y las que tendría que implementar; con esta información podrá desarrollarse:

• Los planes de trabajo

• Mecanismos de monitoreo y revisión de medidas de seguridad

• Programas de capacitación necesarios, por ejemplo, si se recomienda implementar al tratamiento "A" un conjunto de medidas "C", y el área responsable de dicho tratamiento informa que de ese conjunto de medidas hacen falta implementar algunas, la identificación de lo que hace falta implementar se conoce como brecha.

Para su realización, se tomará en cuenta lo siguiente:

• Las medidas de seguridad existente y efectiva;

• Las medidas de seguridad faltantes, y

• La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

3.- REDACCIÓN DEL DOCUMENTO DE SEGURIDAD

CONTENIDO DEL DOCUMENTO DE SEGURIDAD

Objetivos del documento de seguridad

Responsabilidades

Alcance del documento de seguridad

Redacción del Sistema de Gestión de los datos personales

Inventario de tratamientos y datos personales

Redacción de Análisis de riesgo y brecha

Análisis de la información

Redacción de Medidas de seguridad

Monitoreo de medidas de seguridad

Propuesta de capacitación en materia de datos personales

1.- OBJETIVOS DEL DOCUMENTO DE SEGURIDAD

El presente programa tiene como objetivos los siguientes:

1.- Proveer el marco de trabajo necesario para la protección de los datos personales en posesión de la Secretaría de Seguridad y Protección Ciudadana.

2. Cumplir con las obligaciones que establece, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y los Lineamientos Generales, así como la normatividad que derive de los mismos.

3. Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua.

4. Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que el programa se haya implementado de manera integral en la organización, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos.

2.- RESPONSABILIDADES DENTRO DEL PROGRAMA

Con fundamento en lo dispuesto por los artículos 113 y 114, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones en relación con este programa:

I. Aprobar, supervisar y evaluar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la presente Ley y demás disposiciones que resulten aplicables en la materia.

II. Coordinar, realizar y supervisar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en las que resulten aplicables en la materia, en coordinación con el oficial de protección de datos personales, en su caso.

III. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.

IV. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se declare improcedente, por cualquier causa, el ejercicio de alguno de los derechos ARCO.

V. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se declare improcedente, por cualquier causa, el ejercicio de alguno de los derechos ARCO.

VI. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad

VII. Coordinar el seguimiento y cumplimiento de las resoluciones emitidas por el Instituto.

VIII. Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales.

Anualmente se presentará un informe, en las primeras dos semanas del mes de marzo de cada año y referirá al año inmediato anterior.

Algunos de los elementos que pueden incluirse en el informe son:

• Estadística e información general sobre el cumplimiento de las obligaciones señaladas en el Programa de Protección de Datos Personales por parte de las unidades administrativas.

• Acciones realizadas por el Comité de Transparencia y la Unidad de Transparencia para cumplir con las obligaciones específicas que establece el Programa de Protección de Datos Personales.

• Los resultados de las revisiones y auditorias.

La intervención de la Secretaría de Seguridad y protección Ciudadana tendrá la finalidad única de impulsar la debida implementación del Programa al interior del sujeto obligado, pero no podrá suplir ni afectar las funciones que otorgan los artículos 113 y 114 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas al Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la institución.

Asimismo, para que la implementación del programa tenga como resultado el cumplimiento integral de las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y los Lineamientos correspondientes, el programa será de observancia obligatoria para todos los servidores públicos del sujeto obligado que en el ejercicio de sus funciones traten datos personales. Para que los objetivos planteados en la primera sección se logren con éxito, el Programa requiere del apoyo e impulso directo del más alto nivel de la institución.

En ese sentido, el Programa se deberá hacer del conocimiento de la Secretaría de Seguridad y Protección Ciudadana, a fin de que tome las medidas necesarias para que el mismo se observe en la Secretaría de Seguridad y Protección Ciudadana.

3.- ALCANCE DEL PROGRAMA

El presente programa aplicará a todas las unidades administrativas que realicen tratamiento de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que éstas efectúen en ejercicio de sus atribuciones.

Se cubrirán todos los principios, deberes y obligaciones de la **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas**.

Artículo 12°. - En todo tratamiento de datos personales, el responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad,

Artículo 13°. - El responsable deberá tratar los datos personales en su posesión con estricto apego y cumplimiento de lo dispuesto por la presente Ley, la legislación mexicana que resulte aplicable y, en su caso, el derecho internacional, respetando los derechos y libertades del titular: debiendo para tales efectos sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

Artículo 14°.- Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, explícitas, lícitas y legítimas, relacionadas con las atribuciones expresas que la normatividad aplicable le confiera.

Para efectos de la presente Ley, se entenderá que las finalidades son:

L.-Concretas: Cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que sea posible la existencia de finalidades genéricas que puedan confundir al titular.

ll.- Explicitas: Cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad, y;

III. Licitas y legítimas: Cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones expresas del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable.

Las Unidades Administrativas involucradas son:

•Subsecretaria de Servicios Estratégicos de Seguridad.

•Subsecretaria de Sanciones Penales y Medidas de Seguridad.

•Dirección de Tránsito del Estado.

•Dirección de la Policía Fuerza Ciudadana.

•Unidad de Apoyo Jurídico.

•Unidad de Tecnologías de la Información.

•Unidad de Protección y Promoción Derechos Humanos y Atención a Víctimas.

•Área de Comunicación Social y Divulgación.

•Área de Revisión Jurídica y Auditorias.

•Área de Recursos Materiales.

•Área de Recursos Financieros.

•Área de Recursos Humanos.

4. REDACCIÓN DEL SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES

El tratamiento de datos personales que realicen las unidades administrativas deberá cumplir con los principios, deberes y obligaciones que prevé la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, para lo cual este programa establecerá el marco de trabajo mínimo que se deberá seguir para alcanzar dicho objetivo. Para ello, se identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las unidades administrativas, de acuerdo con lo que establece la Ley de la materia y los Lineamientos Generales, y según el ciclo de vida de los datos personales. Asimismo, el sujeto obligado procurará la adopción de mejores prácticas para la protección de datos personales, en aquellos tratamientos que así lo permitan y según el nivel de madurez que exista.

CICLO DE VIDA DE LOS DATOS PERSONALES

Registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso. Manejo, aprovechamiento, divulgación, transferencia y disposición.

En cumplimiento del deber de confidencialidad, esta Secretaria de Seguridad y Protección Ciudadana, ha implementado mecanismos que garantizan la confidencialidad en las diferentes fases del tratamiento de los datos personales. Entre otras, podemos contar con: La integración de cláusulas en los contratos de los encargados (cuando sea el caso) y el personal, que comprometen a la confidencialidad de los datos personales.

5.- INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

Para el debido cumplimiento de las obligaciones que se establecen en este documento, fue necesario que cada una de las unidades administrativas realizara un diagnóstico de los tratamientos de datos personales que llevan a cabo. El diagnóstico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en la Secretaría de Seguridad y Protección Ciudadano Por "inventario de tratamientos de datos personales" se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas de esta Secretaría, realizado con orden y precisión.

A continuación, se presenta la información respecto a los tratamientos que realiza cada Unidad Administrativa.

NOMBRE DE LA UNIDAD ADMINISTRATIVA	TRATAMIENTO
Subsecretaria de Servicios Estratégicos de Seguridad.	-Movimientos de personal (altas y bajas). -Solicitudes de Información pública.
Subsecretaria de Sanciones Penales y Medidas de Seguridad.	-Plantilla y Expedientes del Personal. -Realización de traslados de Personas Privadas de su Libertad y Excarcelaciones Judiciales de imputados. -Registro de procesados y sentenciados.
Dirección de Tránsito del Estado.	

Dirección de la Policía Fuerza Ciudadana	-Movimiento de personal (alta y baja). -Incorporación de documentación a los expedientes del personal al archivo. -Medidas de protección de violencia de género.
Unidad de Apoyo Jurídico.	-Gestión de requerimientos jurisdiccionales y administrativos. - Procedimiento Disciplinario Adversarial.
Unidad de Tecnologías de la Información.	-Investigación y Atención a Delitos Cibernéticos. -Sistema de Atención de Denuncia 089, Ciudadano Vigilante, Sistema de Atención Telefónica 01800 y Denunci@Net.
Unidad de Protección y Promoción Derechos Humanos y Atención a Víctimas.	-Quejas. -Recomendaciones. -Medidas precautorias.
Área de Comunicación Social y Divulgación.	-Cubrir eventos.
Área de Revisión Jurídica y Auditorias	-Auditorias -Serape
Área de Recursos Financieros.	-Elaboración de pago de viáticos.
Área de Recursos Humanos.	- Resguardo de archivo - programación de exámenes -Evaluaciones -Promociones. -Movimientos altas y bajas. -Pago. - incapacidades médicas. -Pensión y jubilación -Gastos Fúnebres.

	-Seguro de vida. -Constancias. -Jubilaciones.
Área de Recursos Materiales.	-Procesos Licitatorios. -Registro de Facturas en el Sistema Balance.

Por otra parte, en lo que se refiere a los medios para la obtención de los datos, es preciso señalar que esto se lleva a cabo por los siguientes:

•Ficha técnica

• Base de datos

• Directamente del titular

• De manera personal, con la presencia física del titular de los datos personales o su representante, en su caso.

• Por escrito presentado directamente en las oficinas del sujeto obligado

• De una fuente de acceso público; entre otras.

Entre estos, se recaban 13 datos identificativos, 4 datos patrimoniales y 7 datos sensibles. Para su uso, se requiere, en el caso de todos los datos no se requiere consentimiento.

Datos Personales IDENTIFICATIVOS	**Datos Personales PATRIMONIALES**	**Datos Personales SENSIBLES**
NOMBRE	DATOS CONTENIDOS EN DECLARACIONES PATRIMONIALES	DATOS DE SALUD
CURP	PROPIEDADES Y BIENES INMUEBLES	CIRCUNSTANCIAS SOCIECONOMICAS
RFC	SALDOS DE CUENTA BANCARIA	DATOS SOBRE PROCEDIMIENTOS

		JUDICIALES O SEGUIDOS EN FORMA DE JUICIO
AÑO DE NACIMIENTO O EDAD	DESCUENTOS PERSONALES	DISCAPACIDAD
DOMICILIO		LENGUA INDIGENA
FIRMA		ORIGEN ETNICO O RACIAL
ANTECEDENTES LABORALES		PERTENENCIA A PUEBLO INDIGENA
CORREO ELECTRONICO		
DATOS DE IDENTIFICACIÓN		
OCUPACION		
NACIONALIDAD		
TELEFONO FIJO O CELULAR		
DATOS PERSONALES CONTENIDOS EN LA IDENTIFICACION OFICIAL PRESENTADA POR LA PERSONA FISICA		

Cada área realiza el tratamiento con una finalidad definida por sus funciones, tal como se señala en los inventarios realizados para cada tratamiento, correspondiente a cada una de las áreas involucradas para tal efecto.

FUNCIONES Y RESPONSABILIDADES EN EL TRATAMIENTO DE DATOS PERSONALES

Los funcionarios que, dadas sus atribuciones, en cada área involucrada en esta Secretaría, que tienen acceso a los datos son:

NOMBRE DE LA UNIDAD ADMINISTRATIVA	**PERSONAS QUE TIENEN ACCESO A LOS DATOS PERSONALES**

Subsecretaria de Servicios Estratégicos de Seguridad.	-Rosalba Guadalupe Hernández Gutiérrez -Edgar Bueno Huesca
Subsecretaria de Sanciones Penales y Medidas de Seguridad.	-Julio Cesar Méndez Hernández -Teresa de Jesús Tóala Tóala -Karla Rubí Barrios Martínez -Maclovio Tóala López -Deasy Anabel Maldonado de los Santos
Dirección de Tránsito del Estado.	
Dirección de la Policía Fuerza Ciudadana	-Gabriela del rocío Ramírez molina -catalina Pérez Pérez -Ana Karen nanga Velasco
Unidad de Apoyo Jurídico.	-Verónica Campos Escobar -Yareni Liset Roblero Herrera -Blanca Lilia López Hernández - Sandra Isabel Pozo Gómez -Zurisadai Espinoza Morales - Selene Ivonne Ugarte Espinoza -Azariel Gómez Morales -Lucinda Pérez Pérez -Emmanuel Adamian Juárez López
Unidad de Tecnologías de la Información.	-Carlos Alberto Ocaña Pérez -María Asunción Córdova Blassi -Floriberto Patricio Vázquez -Julieta del Carmen Avendaño Flores -María Candelaria Pérez Roldan -Eneri del Carmen Velasco Vázquez -Alicia Marina Madariaga
Unidad de Protección y Promoción Derechos Humanos y Atención a Víctimas.	-César Artemio Del Valle Ruiz

Área de Comunicación Social y Divulgación.	-Gerardo Rodrigo Ruíz Corzo -Elías Durantes Clemente
Área de Revisión Jurídica y Auditorias	-Ariel Ocaña Caballero - Martin Víctor Escobar
Área de Recursos Financieros.	-Iris Elvira Chiñas González -Verónica Chacón Gamboa -Rodrigo Hernández Ruiz
Área de Recursos Humanos.	-Francisco Humberto trinidad Marín -limbano González moreno -Luis enrique Lázaro Gómez -Beatriz López bautista -María de Lourdes Jiménez molina -Amanda melba Ruiz Mendoza -Ariana Pérez orantes
Área de Recursos Materiales.	-Eduardo Martin Morgado Sinta -José Joaquín Ramos Montesinos -Pedro Alberto Rojas Molina -Marcos Mendoza Escobar -Deysi Yakareni Pérez Vázquez -Jacob Lehi Martínez Hernández

Como parte del proceso, cabe hacer mención que se transfieren datos personales a las diversas instituciones siempre y cuando exista un requerimiento formal y cumpla con la motivación y fundamentación requerida para tal efecto, por parte de la institución solicitante; y se difunden a otras áreas para recabar información correspondiente de la misma.

CANTIDAD DE PROCESOS Y PERSONAS QUE UTILIZAN DATOS PERSONALES

Estos datos son utilizados en **38 tratamientos**, correspondientes a las unidades administrativas involucradas al respecto, en los cuales se utilizan datos personales

patrimoniales y sensibles. Datos los cuales se encuentran descritos de forma particular en las gráficas antes descritas.

Donde se puede apreciar, la unidad administrativa con mayor número de tratamientos es el área de Recursos Humanos, mientras que el área de Comunicación Social y Divulgación y el área de Recursos Financieros, son las que menos tratamientos desarrollan, al ser solamente uno en cada área.

-BITACORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Cada unidad administrativa de esta Dependencia, deberá llevar una bitácora de las vulneraciones a la seguridad, en la que se describa, la fecha en la que ocurrió, el motivo de ésta y las acciones.

Por lo que, la Bitácora de Vulneraciones, misma que se adjunta a continuación, atiende en sus términos lo establecido en el artículo 53.- de la LGPDPPSO:

El responsable deberá llevar una bitácora de las vulneraciones a la seguridad ocurridas en la que se describa:

I. La fecha en la que ocurrió.

II. El motivo de la vulneración de seguridad, y

III. Las acciones correctivas implementadas de forma inmediata y definitiva.

UNIDAD ADMINISTRATIVA:	
FECHA DE LA VULNERACIÒN OCURRIDA:	
RUBRO	INFORMACION
Motivos (posibles o identificados) de la vulneración:	
Acciones correctivas realizadas por el área de forma inmediata y definitiva:	
Nombre y firma del responsable de los Datos Personales	

6.- REDACCIÓN DE ANÁLISIS DE RIESGOS Y DE BRECHA

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

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

Con base en la Ley de la materia, la valoración de los riesgos de los datos personales forma parte de los elementos mínimos que debe contener el instrumento que describe y da cuenta, en lo general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas, en este caso, por la Secretaría de Seguridad y Protección Ciudadana, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de ese tipo de datos bajo su posesión. Aunado a lo anterior, el análisis de riesgos de los datos personales tratados debe contemplar los siguientes aspectos:

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.

El riesgo inherente, la sensibilidad, las posibles consecuencias de vulneración para los titulares, las transferencias y vulneraciones previas ocurridas sobre los datos personales, así como el número de titulares de éstos y el riesgo por su valor potencial, además del desarrollo tecnológico.

7.- ANÁLISIS DE LA INFORMACIÓN

Se tiene que la Secretaría de Seguridad y Protección Ciudadana cuenta con 12 unidades administrativas en las que se da tratamiento de datos personales mediante 38 tratamientos como se visualiza a continuación:

NOMBRE DE LA UNIDAD ADMINISTRATIVA	**TRATAMIENTOS**
Subsecretaria de Servicios Estratégicos de Seguridad.	2

Subsecretaria de Sanciones Penales y Medidas de Seguridad.	3
Dirección de Tránsito del Estado.	5
Dirección de la Policía Fuerza Ciudadana	3
Unidad de Apoyo Jurídico.	2
Unidad de Tecnologías de la Información.	2
Unidad de Protección y Promoción Derechos Humanos y Atención a Víctimas.	3
Área de Comunicación Social y Divulgación.	1
Área de Revisión Jurídica y Auditorias	2
Área de Recursos Financieros.	1
Área de Recursos Humanos.	12
Área de Recursos Materiales.	2

Bajo esta premisa, para analizar los riegos de los datos personales que son objeto de tratamiento en esta Secretaría de Seguridad y Protección Ciudadana, se aplicó un instrumento para, primeramente, clasificar los datos 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.

De los anteriores, se identificó que se trabaja con Datos de Identificación, datos patrimoniales, y datos sensibles.

Esto es, se tomó en cuenta la probabilidad baja, media o alta de que la amenaza suceda en las distintas etapas de vida de los datos personales. Así, se consideró la consecuencia desfavorable leve, moderada o grave que al titular provoca en caso de que la amenaza ocurra (impacto).

La identificación y valoración del riesgo en cada proceso en que se tratan datos personales por las unidades administrativas de la Secretaría de Seguridad y Protección Ciudadana, se basaron en una escala del 0 al 3, representándose de la forma siguiente por cada unidad administrativa involucrada:

ANÁLISIS DE BRECHA Y RIESGO

UNIDAD DE APOYO JURÍDICO

Análisis de Brecha		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
Gestión de requerimientos jurisdiccionales y administrativos	Escritorio Computadoras con contraseña	Archivero con llave
Procedimiento Disciplinario Adversarial	Escritorio Computadoras con contraseña	Ninguna

Análisis de riesgo					
Tratamiento	**Tipo de dato**	**Volumen**	**Accesos**	**Entorno**	**Promedio de riesgo inherente**
Gestión de requerimientos jurisdiccionales y administrativos	1	1	2	2	1.5
Procedimiento Disciplinario Adversarial	1	1	2	2	1.5
Promedio total					1.5

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

Análisis de Brecha		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
Investigación y Atención a Delitos Cibernéticos	Esquema de privilegios Computadoras con contraseña Oficinas restringidas	Ninguna
Sistema de Atención de Denuncia 089, Ciudadano Vigilante, Sistema de Atención Telefónica 01800 y Denunci@Net,	Esquema de privilegios Computadoras con contraseña Oficinas restringidas	Ninguna

Análisis de riesgo					
Tratamiento	**Tipo de dato**	**Volumen**	**Accesos**	**Entorno**	**Promedio de riesgo inherente**

Investigación y Atención a Delitos Cibernéticos	4	1	1	4	2.5
Sistema de Atención de Denuncia 089, Ciudadano Vigilante, Sistema de Atención Telefónica 01800 y Denunci@Net,	4	1	1	4	2.5
Promedio total					5

SUBSECRETARÍA DE SERVICIOS ESTRATEGICOS DE SEGURIDAD

Análisis de Brecha		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
Movimientos de altas y bajas	Escritorio Computadoras con contraseña	Archiveros con llave
Solicitudes de información pública	Escritorio Computadoras con contraseña	Archiveros con llave

Análisis de riesgo					
Tratamiento	**Tipo de dato**	**Volumen**	**Accesos**	**Entorno**	**Promedio de riesgo inherente**

Movimientos de altas y bajas	1	1	2	2	1.5
Solicitudes de información pública	1	1	2	2	1.5
Promedio total					1.5

SUBSECRETARIA DE EJECUCIÓN DE SANCIONES PENALES Y MEDIDAS DE SEGURIDAD.

Análisis de Brecha		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
Plantilla y Expedientes del Personal	Archivero Computadoras	Llave en los archiveros
Registro de Procesados y Sentenciados: · Captura de datos de los ppl's por centro penitenciario. · Consulta de información jurídica de ppl's. · Externaciones de ppl's por mandamiento judicial.	Computadoras con contraseña Contraseñas por usuario SITE (Servidor de nodos o red) Computadoras con contraseña Servidor con contraseña	Archiveros con llave Llave en el SITE Cámaras de video vigilancia
Realización de traslados de Personas Privadas de su Libertad y Excarcelaciones Judiciales de imputados	Archivero Computadoras con diferentes usuarios con contraseña segura	Esquema de privilegios de acceso (permisos a usuarios) Espacios con llave

Análisis de riesgo

Tratamiento	Tipo de dato	Volumen	Accesos	Entorno	Promedio de riesgo inherente
Plantilla y Expedientes del Personal	4	4	4	4	4
Registro de Procesados y Sentenciados:	11	4	13	8	9
Realización de traslados de Personas Privadas de su Libertad y Excarcelaciones Judiciales de imputados	4	1	1	2	2
Promedio total					3.7

ÁREA DE REVISIÓN JURÍDICA, SEGUIMIENTO Y ENLACE DE AUDITORIAS

Análisis de Brecha		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
Auditorias	Escritorio Computadoras con contraseña	Archiveros con llave
SERAPE	Escritorio Computadoras con contraseña	Archiveros con llave

Análisis de riesgo

Tratamiento	Tipo de dato	Volumen	Accesos	Entorno	Promedio de riesgo inherente
Auditorias	1	1	2	2	1.5
Serape	1	1	2	2	1.5
Promedio total					1.5

COMUNICACIÓN SOCIAL Y DIVULGACIÓN

Análisis de Brecha		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
Cubrir eventos (mediante captura de fotos y videos)	-Escritorio -Memoria externa con contraseña -Carpeta de archivo en la nube con contraseña	-Llave en los escritorios

Análisis de riesgo					
Tratamiento	**Tipo de dato**	**Volumen**	**Accesos**	**Entorno**	**Promedio de riesgo inherente**
Cubrir eventos (mediante captura de fotos y videos)	1	2	1	1	5
Promedio total	1	2	1	1	1.25

ÁREA DE RECURSOS MATERIALES Y SERVICIOS GENERALES

Análisis de Brecha		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
Procesos Licitatorios (Por Convocatoria Pública,	Escritorio Archivero	Archiveros con Llave

Invitación A Cuando Menos Tres Personas, Adjudicación Directa)	Computadoras con contraseña y Firewall	
Registro de Facturas en el Sistema Balance	Escritorio Archivero Computadoras con contraseña y Firewall	Archiveros con Llave

Análisis de riesgo					
Tratamiento	**Tipo de dato**	**Volumen**	**Accesos**	**Entorno**	**Promedio de riesgo inherente**
Procesos Licitatorios (Por Convocatoria Pública, Invitación A Cuando Menos Tres Personas, Adjudicación Directa)	2	1	2	2	1.5
Registro de Facturas en el Sistema Balance	2	1	1	2	1.5
Promedio total					1.5

DERECHOS HUMANOS

Análisis de Brecha		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
Quejas emitidas por la Comisión Nacional y Estatal delos derechos humanos	Escritorios Computadoras Archiveros	Ninguna

	Papelería	
Recomendaciones emitidas por la Comisión Nacional y Estatal de los derechos humanos	Escritorios Computadoras Archiveros Papelería	Ninguna
Medidas precautorias emitidas por la Comisión Nacional y Estatal de los derechos humanos	Escritorios Computadoras Archiveros Papelería	Ninguna

Análisis de riesgo					
Tratamiento	**Tipo de dato**	**Volumen**	**Accesos**	**Entorno**	**Promedio de riesgo inherente**
Quejas emitidas por la Comisión Nacional y Estatal delos derechos humanos	1	1	2	1	1.25
Recomendaciones emitidas por la Comisión Nacional y Estatal delos derechos humanos	1	1	2	1	1.25
Medidas precautorias emitidas por la Comisión Nacional y Estatal delos derechos humanos	1	1	2	1	1.25
Promedio total					1.25

ÁREA DE RECURSOS FINANCIEROS Y CONTABILIDAD

Análisis de Brecha		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
Registro en sistema informático de todas las personas que tramitan su viatico	Pagos por medio de cheques Computadoras con contraseña	Ninguna

Análisis de riesgo					
Tratamiento	**Tipo de dato**	**Volumen**	**Accesos**	**Entorno**	**Promedio de riesgo inherente**
Registro en sistema informático de todas las personas que tramitan su viatico	1	1	1	1	1
Promedio total					1

DIRECCION DE LA POLICIA ESTATAL DE TRANSITO

Análisis de Brecha		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
EXPEDICION DE PERMISOS PROVISIONALES PARA CIRCULAR SIN PLACAS Y SIN TARJETA DE C IRCULACION	Archivero Computadoras con contraseña	Llave en los archiveros
CONSTANCIA DE REVISIONES MECANICAS	Archivero	Llave en los archiveros

	Computadoras con contraseña	
IMPARTICION DE CURSOS DE MANEJO	Archivero Computadoras con contraseña	Llave en los archiveros
TRAMITE DE PAGOS POR APLICACIÓN DE MULTAS	Archivero Computadoras con contraseña	Un depósito para almacenar las garantías y documentación (placas, boletas de infracción)
EXPEDICION DE CONSTANCIAS DE NO INFRACCION PUBLICA Y PRIVADA	Archivero Computadoras con contraseña	Llave en los archiveros

Análisis de riesgo					
Tratamiento	**Tipo de dato**	**Volumen**	**Accesos**	**Entorno**	**Promedio de riesgo inherente**
EXPEDICION DE PERMISOS PROVISIONALESPARA CIRCULAR SIN PLACAS Y SIN TARJETA DE CIRCULACION	1	1	1	2	1.25
EXPEDICION DE REVISIONES MECANICAS	1	1	1	2	1.25
IMPARTICION DE CURSOS DE MANEJO	1	1	1	2	1.25
TRAMITE DE PAGOS POR APLICACIÓN DE MULTAS	1	1	1	2	1.25

EXPEDICION DE CONSTANCIAS DE NO INFRACCION PUBLICA Y PRIVADA	1	1	1	2	1.25
Promedio total					1.25

DIRECCIÓN DE LA POLICÍA FUERZA CIUDADANA

Análisis de Brecha		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
Movimiento de personal (alta y baja)	Archivero Computadoras con contraseña Programas con contraseña Carpetas Sobres	Llave en los archiveros
Integración de expediente de los elementos de la Institución.	Archivero Computadoras con contraseña Programas con contraseña Carpetas Sobres	Llave en los archiveros
Medidas de protección de violencia de Genero	Archivero Computadoras con contraseña Memorias externas	Falta de archiveros

Análisis de riesgo

Tratamiento	Tipo de dato	Volumen	Accesos	Entorno	Promedio de riesgo inherente
Movimiento de personal (alta y baja)	4	2	3	3	3
Integración de expediente de los elementos de la Institución	4	2	3	3	3
Medidas de protección de violencia de Genero	4	2	4	2	3
Promedio total					9

AREA DE RECURSOS HUMANOS

Análisis de Brecha		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
Guarda y custodia de archivo de nominas	Archivero Computadoras con contraseña.	Sistema de registro de entradas y salidas
Programación De Exámenes	Archivero Computadoras Con Contraseña.	Ninguno
Promociones	Archivero Computadoras Con Contraseña.	Ninguno

Evaluaciones	Usuario Y Contraseña Personalizada En El Sistema De Declaracionesc3.	Ninguno
Movimiento De Personal	Maquinas Conectadas A Internet	Software con mayor capacidad
Pago	Sistema Digital De Información Del Persona E Información	Software con mayor capacidad
Incapacidades	Sistema Digital De Información Del Persona, Información Del Personal, Control De Incapacidades,	Software con mayor capacidad
Tramites De Pensiones Y Jubilación	Sistema Digital De Información Del Persona, Información Del Personal	Archiveros
Tramites De Seguro De Vida	Sistema Digital De Información Del Persona, Información Del Personal	Archiveros
Gastos Fúnebres	Sistema Digital De Información Del Persona E Información	Archiveros
Constancias	Sistema Digital De Información Del Persona E Información	Archiveros
Elaboración de oficios	Archivero Computadoras con contraseña	Llave en los archiveros

Análisis de riesgo

Tratamiento	Tipo de dato	Volumen	Accesos	Entorno	Promedio de riesgo inherente
Guarda y custodia de archivo de nominas	1	2	1	2	1.5
Programación De Exámenes	1	2	1	2	1.5
Promociones	1	2	1	2	1.5
Evaluaciones	1	2	1	2	1.5
Movimiento De Personal	1	2	1	2	1.5
Pago	1	2	1	2	1.5
Incapacidades	3	1	2	4	2.5
Tramites De Pensiones Y Jubilación	1	1	2	2	1.5
Tramites De Seguro De Vida	1	1	2	2	1.5
Gastos Fúnebres	2	1	2	2	1.7
Constancias	2	1	1	1	1.2
Elaboración de oficios	1	2	1	2	1.5
Promedio total	1.3	1.5	1.3	2	1.5

-GESTION DE VULNERACIONES.

Debe entenderse por vulneraciones de datos personales a “la materialización de las amenazas pudiendo estar enfocadas a la pérdida o destrucción no autorizada de los datos personales en posesión de los Sujetos Obligados que realizan el tratamiento de los datos, el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, así como el daño, alteración o modificación no autorizada.

En este sentido la LGPDPPSO, señala en su artículo 52º, que por vulneraciones de seguridad debe entenderse, en cualquier fase del tratamiento de datos, al menos, las siguientes:

a) La pérdida o destrucción no autorizada;

b) El robo, extravío o copia no autorizada;

c) El uso, acceso o tratamiento no autorizado, o

d) El daño, la alteración o modificación no autorizada.

En caso de ocurrir una vulneración de seguridad, el responsable deberá 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 si fuese el caso a efecto de evitar que la vulneración se repita.

Cada unidad administrativa de esta secretaria de Seguridad y Protección Ciudadana, deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa, la fecha en la que ocurrió, el motivo de ésta y las acciones.

Por lo que, la Bitácora de Vulneraciones atiende en sus términos lo establecido en el artículo 53º de la LGPDPPSO.

Así mismo, debe ser conservado por las unidades administrativas para el registro histórico de las vulneraciones que se presenten a lo largo del tiempo. Además, si la vulneración tiene el riesgo de repercutir significativamente en los derechos de sus titulares de los datos personales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

Artículo 55º de la LGPDPPSO:

El responsable deberá informar al titular al menos lo siguiente:

I) La naturaleza del incidente;

II) Los datos personales comprometidos;

III) Las recomendaciones y medidas que éste pueda adoptar para proteger sus intereses;

e) Las acciones correctivas realizadas de forma inmediata, y

f) Los medios donde puede obtener más información al respecto.

Ahora bien, cuando se presente alguna de las situaciones enunciadas, con el propósito de asegurar un control adecuado en el momento que ocurren las vulneraciones y garantizar la no repetición de éstas, es necesario implementar las siguientes acciones:

1. La persona que observe o conozca sobre una vulneración de datos personales, deberá informar inmediatamente a la persona responsable de seguridad de datos personales (RESPONSABLE) designada en el área de su adscripción.

2. Por su parte, la persona RESPONSABLE deberá informar inmediatamente sobre la vulneración a la persona titular del área de su adscripción y entablar contacto con la Unidad de Transparencia, para informar el hecho y que ésta disponga lo conducente para orientar y acompañar en las gestiones que deban documentarse, las cuales deben realizarse con celeridad para garantizar la eficacia de las medidas adoptadas.

3. La persona RESPONSABLE coordinará las acciones preventivas que se estimen convenientes al interior del área de su adscripción para asegurar el cese inmediato de la vulneración.

4. Una vez implementadas las acciones preventivas, se deberá documentar, a través de los formatos señalados.

5. Identificada y registrada esta información, se deberán implementar y planear las acciones correctivas de corto plazo, en coordinación con la Unidad de Transparencia y las áreas competentes para subsanar la vulneración y evitar posteriores incidentes.

6. En caso de que se deba informar a los titulares o al Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales sobre una vulneración que ponga en riesgo sus derechos patrimoniales o morales, la Unidad de Transparencia realizará los requerimientos internos necesarios para recabar información suficiente y emitirá las comunicaciones correspondientes.

7. Al final de este proceso, deberá concluirse la información de la Bitácora de Registro de Vulneraciones.

Es importante señalar que la versión original de los documentos generados se firmará

por la persona RESPONSABLE y permanecerá bajo resguardo del área involucrada.

8.-REDACCIÓN DE MEDIDAS DE SEGURIDAD.

Las medidas generales de seguridad administrativas, físicas y técnicas con las que actualmente cuenta la Secretaría de Seguridad y Protección Ciudadana para mantener la confidencialidad e integralidad 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:

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, impartido mediante el Campus Virtual de Capacitación del organismo garante.

2. Implementación de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.

3. Resguardo de los expedientes bajo los criterios, directrices y lineamientos para la atención de los expedientes técnicos

4. Mecanismos de control desarrollados conforme a lo establecido en los lineamientos del Sistema de Gestión de Documentos institucional.

5. Suscripción de una carta responsiva por parte de los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.

6. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.

Medidas físicas

1. Resguardo de documentos e información en archivos físicos de trámite y concentración.

2. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información.
3. Limitar el número de personas con acceso a archivos físicos.
4. Procurar suscribir responsivas de confidencialidad con el personal que trata datos personales
5. Resguardo de llaves en oficinas de acceso restringido

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 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.

-CONTROL DE IDENTIFICACION Y AUTENCICACION DE USUARIOS.
En esta Secretaría de Seguridad y Protección Ciudadana no se aplican controles de identificación y autenticación de usuarios sofisticados. La única medida que se implementa es el uso de contraseñas par el acceso a los equipos de cómputo, repositorios y cuentas de Correo institucionales; mismas que son controladas por la Unidad de Tecnologías y Gestión de la Información adscrita a la misma.

- LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.
La recuperación de la información se lleva a cabo de acuerdo con las posibilidades identificadas de manera particular. En algunos casos se realizan respaldos en la nube de diferentes sistemas operativos, así como en discos duros y otros medios portátiles

controlados y administrados por los responsables de cada tratamiento, que permiten el respaldo y la recuperación.

-PLAN DE CONTINGENCIA.

Ante la pérdida total o parcial de datos personales en posesión de este sujeto obligado, se debe contar con un plan de contingencia.

Con la evaluación de riesgos y la elaboración de las medidas de seguridad aplicables para prevenir las posibles vulneraciones a las que consiste en la aplicación de las medidas de seguridad tratadas en párrafos anteriores, mismas que están sujetas a cambios por eventualidades no contempladas, por ello la importancia de señalar que el presente se trata de un plan de contingencia no limitativo. nos vemos expuestos, nos encontramos con que el plan de contingencias de este sujeto obligado

Lo anterior toda vez que en la actualidad existen cambios y grandes avances que van modificando la organización de la información, y al igual existan riesgos inminentes que día a día evolucionan.

Con la aplicación de las medidas de seguridad establecidas previamente en este documento se buscan minimizar los riesgos o vulneraciones, pero a su vez se intenta propiciar el restablecimiento de los datos personales en el menor tiempo posible ante cualquier eventualidad. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada área administrativa en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo.

Mismas en las que nos podremos apoyar con las bitácoras de vulneración existentes en cada unidad administrativa, las cuales cuentan con información especifica de los tratamientos, en las que se sigue una investigación al respecto; apoyado así también, de la información resguardada en USB y/o en la nube.

En el actual panorama digital, la seguridad informática es una preocupación constante debido a las amenazas y vulnerabilidades a las que están expuestos los sistemas y datos.

Para garantizar la protección de la información y prevenir intrusiones no autorizadas, se han desarrollado protocolos de seguridad informática que establecen medidas y procedimientos a seguir.

Protocolos de seguridad informática

Los protocolos de seguridad informática son conjuntos de reglas y procedimientos diseñados para proteger los sistemas y la información frente a posibles ataques. Estos protocolos incluyen medidas como el uso de firewalls, antivirus, encriptación de datos y autenticación de usuarios.

- Uso de firewalls: Los firewalls funcionan como barreras de seguridad que controlan y filtran el tráfico de red, permitiendo o bloqueando determinados accesos de acuerdo con las reglas establecidas.
- Antivirus: Los antivirus son herramientas que detectan, bloquean y eliminan programas maliciosos, como virus, malware y spyware, protegiendo así los sistemas de posibles infecciones.
- Encriptación de datos: La encriptación es el proceso de codificar la información para que solo las partes autorizadas puedan acceder a ella. Esto garantiza que, en caso de interceptación, los datos se mantengan seguros y protegidos.
- Autenticación de usuarios: La autenticación de usuarios es un proceso que verifica la identidad de los usuarios que intentan acceder a un sistema o red. Esto se logra mediante la utilización de contraseñas, certificados digitales o autenticación biométrica.

Protección de la información confidencial

La protección de la información confidencial es fundamental para garantizar la privacidad y la integridad de los datos. Para ello, es necesario establecer protocolos y medidas específicas orientadas a proteger la información más sensible de una organización o individuo.

- Control de acceso: Se deben establecer políticas de control de acceso que regulen quiénes pueden acceder a la información confidencial y bajo qué condiciones. Esto incluye la asignación de permisos y restricciones de acceso.
- Respaldos y almacenamiento seguro: Realizar copias de seguridad periódicas y almacenarlas de forma segura es esencial para garantizar la disponibilidad y recuperación de la información en caso de pérdida o daño.

- Políticas de seguridad de la información: Establecer políticas claras y concisas sobre el manejo de la información confidencial, incluyendo aspectos como la clasificación de datos, la destrucción segura y la protección contra fugas de información.
- Formación y concienciación: La formación y concienciación del personal acerca de las mejores prácticas en seguridad informática es crucial para garantizar una protección efectiva de la información confidencial. Esto incluye la educación sobre la importancia de contraseñas seguras, el phishing y otras técnicas de ingeniería social.

-TECNICAS UTILIZADAS PARA LA SUPRESION Y BORRADO SEGURO DE LOS DATOS PERSONALES.

hasta el momento no se han desarrollado en esta Secretaría, de manera sistemática y organizada, un sistema de técnicas para la supresión y borrado seguro, todo se hace de acuerdo con la iniciativa y posibilidad de cada área; por lo que este proceso será parte del plan de trabajo a desarrollar en el futuro inmediato. Por lo anterior, es posible afirmar que será necesaria la implementación de técnicas para la supresión y el borrado seguro que considere tanto métodos físicos que se basan en la destrucción de los medios de almacenamiento físicos electrónicos; como lógicos, basados en la limpieza de los datos almacenados en los equipos de cómputo a través de la desmagnetización y la sobre escritura.

-PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD.

Conforme al análisis de brecha, es importante generar acciones que permitan la seguridad de la información, así como de su localización, para resolver de manera eficaz el acceso, rectificación, corrección u oposición de las personas titulares de la información; por lo que a continuación se presentan las actividades generales que se planea realizar:

- Celebración de reuniones de trabajo con los jefes de área 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.

9. MONITOREO DE MEDIDAS DE SEGURIDAD.

Los sistemas tecnológicos de la Secretaría de Seguridad y Protección Ciudadana, son bastante básicos, por lo que no se aplican controles de identificación y autenticación de usuarios sofisticados. La única medida que se implementa es el uso de contraseñas par el acceso a los equipos de cómputo, repositorios y cuentas de correo institucionales; mismas que son controladas por la Dirección de Tecnologías de la Información.

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. Revisar la actualización permanente del esquema de contraseñas conforme a las pantallas de parametrización de los sistemas, verificando que los valores se encuentren determinados conforme a la política.

2. Monitorear que todas las cuentas que se dan de alta para otorgar acceso a la red, sea validada en el campo correspondiente a la contraseña, a fin de asegurar el uso.

3. Revisar el cumplimiento de protocolos

10. PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

La aplicación del programa de protección de datos personales en la Secretaria de Seguridad y Protección Ciudadana, 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:

I) La Ley General de protección de datos personales en posesión de sujetos obligados en Chiapas.

-Antecedentes

-Principios.

-Alcances

-Objetivo

- Implicaciones

II) Obligaciones en la observancia de la Ley General 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

-Sistemas de datos personales.

-Inventario y Base de Datos.

- Medidas de seguridad.

- Análisis de brecha y de 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