CENTRO ESTATAL
DE CONTROL DE CONFIANZA
CERTIFICADO
GOBIERNO DE CHIAPAS

DOCUMENTO DE SEGURIDAD DE PROTECCIÓN DE DATOS PERSONALES DEL CENTRO ESTATAL DE CONTROL DE CONFIANZA CERTIFICADO.

CENTRO ESTATAL
DE CONTROL DE CONFIANZA
CERTIFICADO
GOBIERNO DE CHIAPAS

PRESENTACIÓN

El presente documento denominado Documento de Seguridad de Protección de Datos Personales del Centro Estatal de Control de Confianza Certificado del Estado de Chiapas, se elabora en el marco de las funciones siguientes:

El 26 de enero de 2017 se publicó la ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, en la cual se establecen las bases, procedimientos, principios, deberes y obligaciones que rigen el tratamiento de información de carácter personal, así como los derechos que tienen las/los titulares a la protección de sus datos personales en posesión del organismo de los poderes ejecutivo, Legislativo y Judicial en los tres niveles de gobierno.

El 30 de agosto de 2017 se publicó la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas, en la cual establecen que es de orden público y de observancia obligatoria en todo el territorio del Estado de Chiapas y tiene como objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de los sujetos obligados.

Bajo esta premisa, el Centro Estatal de Control de Confianza Certificado del Estado de Chiapas, es un sujeto obligado reconocido por las leyes antes citadas y tiene la obligación de cumplir con lo dispuesto en el marco normativo aplicable.

CENTRO ESTATAL
DE CONTROL DE CONFIANZA
CERTIFICADO
GOBIERNO DE CHIAPAS

MARCO NORMATIVO

El derecho a la protección de datos personales, materia de este documento, tiene su fundamentación en el marco jurídico siguiente:

- Constitución Política de los Estados Unidos Mexicanos.
- Ley de Transparencia y Acceso a la Información Pública de Estado de Chiapas.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.
- Ley de Responsabilidades Administrativas para el Estado de Chiapas.
- Ley del Sistema Estatal de Seguridad Pública del Estado de Chiapas.
- Ley de Archivos del Estado de Chiapas.
- Reglamento Interior del Centro Estatal de Control de Confianza Certificado.
- Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas.

CENTRO ESTATAL
DE CONTROL DE CONFIANZA
CERTIFICADO
GOBIERNO DE CHIAPAS

OBJETIVOS

El programa tiene como objetivos:

Promover el marco del trabajo necesario para la protección de los datos personales en posesión del Centro Estatal de Control de Confianza Certificado.

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

Establecer las directrices y herramientas necesarias, para garantizar la protección de los datos personales en posesión de las Direcciones, Unidades y Áreas, por medio de la sensibilización, capacitación, implementación, operación, revisión, mantenimiento y mejora de las acciones diseñadas por el tratamiento y la seguridad de los datos personales.

Promover la adopción de mejores prácticas en materia de protección de datos personales, a efecto de lograr una mayor participación de la comunidad del Centro Estatal de Control de Confianza Certificado con relación al ejercicio de los derechos ARCO, así como ofrecer proporcionar a la ciudadanía la certeza de que sus datos personales en posesión del Centro Estatal de Control de Confianza Certificado, están siendo tratados de conformidad con lo establecido en el marco normativo.

RESPONSABILIDADES

Con fundamento en lo dispuesto por los artículos 113 y 114 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas, que señala 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 con relación a 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, 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 ARCOS.
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. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.
VI. Coordinar el seguimiento y cumplimiento de las resoluciones emitidas por el Instituto.
VII. 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 presentara 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, y

Los resultados de las revisiones y auditorias.

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 este Centro, en ese sentido el programa se deberá hacer del conocimiento del Director General, a fin de que tome las medidas necesarias para que el mismo se observe en Centro Estatal de Control de Confianza Certificado del Estado de Chiapas.

La intervención del Director General 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 de Protección de Datos Personales en Posesión de los 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 de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas y los lineamientos correspondientes, el programa será de observancia obligatoria para todo los servidores públicos del sujeto obligado que en el ejercicio de sus funciones traten datos personales.

ALCANCE

El presente Programa de Datos Personales, aplica a todas las Direcciones, Unidades y Áreas del Centro Estatal de Control de Confianza Certificado, que en el cumplimiento de sus atribuciones recaban y tratan datos personales.

Se cubrirán todos los principios, deberes y obligaciones que establece los artículos 12, 13, 14 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas.

Por lo que atendiendo al Reglamento Interior, las Direcciones, Unidades y Áreas involucradas son:

I. Dirección General
II. Coordinación Operativa
III. Unidad de Apoyo Administrativo
IV. Unidad de Informática
V. Comisaría
VI. Unidad de Planeación
VII. Unidad de Asuntos Jurídicos
VIII. Dirección Ejecutiva y de Situación Patrimonial
IX. Dirección de Atención Psicológica
X. Dirección de Poligrafía
XI. Dirección de Investigación socioeconómica
XII. Dirección de Información, Registro y Cadena de Custodia
XIII. Dirección Médica y Toxicología

Es importante atender que también aplicará a todos el personal del servicio público que por sus funciones realicen algún tipo de tratamiento de datos personales, en este caso están obligados a conocer y aplicar las medidas de seguridad mínimas, en la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas.

Se destaca que la responsabilidad de la tarea, implica no solo tratar los datos personales con responsabilidad, si no también, guardar la debida confidencialidad y garantizar seguridad sobre la información a la que tenga acceso.

CONTEXTO INSTITUCIONAL

Se crea el Centro Estatal de Control de Confianza Certificado del Estado de Chiapas, en adelante "El Centro" como un Organismo Público Descentralizado de la Administración Pública Estatal, sectorizado al Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública, con personalidad jurídica y patrimonio propios, autonomía administrativa, presupuestal, técnica de gestión de operación, y de ejecución, mismo que atenderá los asuntos que la Ley del Sistema Estatal de Seguridad Pública, su Decreto de Creación, su reglamento interior y demás normativa aplicable le atribuyan, mediante Decreto No. 032 del Periódico Oficial número 006 de fecha 31 de diciembre de 2018, así como el Decreto No. 190 del Periódico Oficial 037 de fecha 05 de junio de 2019, por el que se reforman diversas disposiciones del Decreto por el que se crea el Centro Estatal de Control de Confianza Certificado del Estado de Chiapas.

"El Centro" tendrá como objeto fundamental evaluar y certificar a los integrantes de las instituciones de seguridad pública del Estado, a quienes se les aplicaran exámenes poligráficos, psicométricos, medico-toxicológico y socioeconómicos, a fin de garantizar la confiabilidad y certeza en la función que realizan para brindar un servicio apegado a la legalidad.

El Reglamento Interior, fue publicado mediante Decreto número 3229-A-2022, en el Periódico Oficial número 249 de fecha 19 de octubre de 2022 y establece la estructura orgánica del Centro y que para la realización de los estudios, condición, planeación y desempeño de las atribuciones, así como para el despacho de los asuntos de su competencia El Centro tiene los Órganos Administrativos siguientes:

I. Dirección General.
II. Coordinador Operativo.
III. Unidad de Apoyo Administrativo.
IV. Unidad de Informática

V. Comisaria.
VI. Unidad de Planeación.
VII. Unidad de Asuntos Jurídicos.
VIII. Dirección de Atención Psicológica.
IX. Dirección de Poligrafía.
X. Dirección de Investigación Socioeconómica.
XI. Dirección de Información, Registro y Cadena de Custodia.
XII. Dirección Ejecutiva y de Situación Patrimonial.
XIII. Dirección Médica y Toxicología.

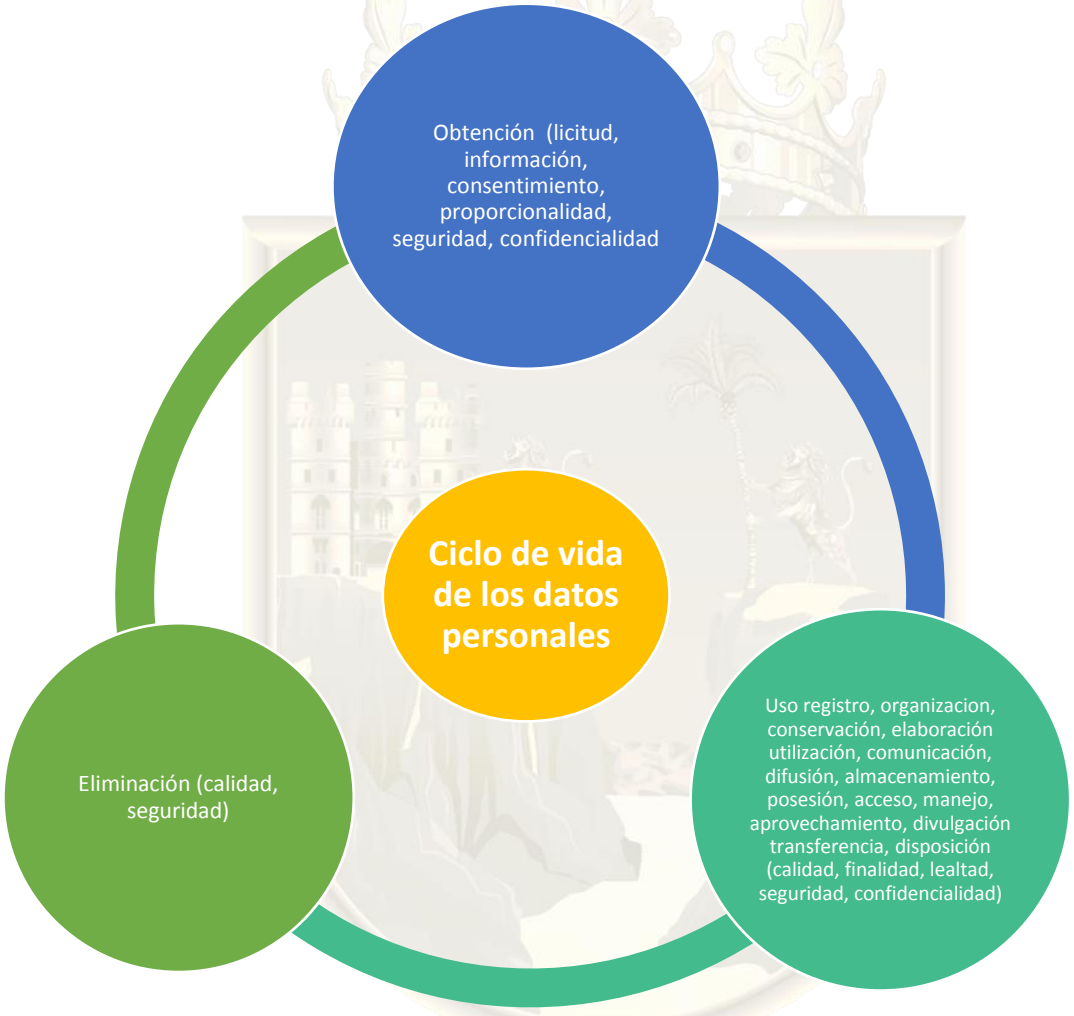
SISTEMA DE GESTION DE LOS DATOS PERSONALES

El tratamiento de datos personales que realicen las Direcciones, Unidades o Áreas deberá cumplir con los principios, deberes y obligaciones que prevé la Ley de Protección de Datos Personales en Posesión de los 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 identificaran las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las Direcciones, Unidades o Áreas de acuerdo con lo que establece la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas y los Lineamientos Generales, y según el ciclo de vida de los datos personales.

Asimismo, el Sujeto obligado procurara 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



LÍNEAS ESTRATÉGICAS

Lo anterior se lograra mediante la ejecución de las líneas estratégicas que a continuación se señalan:

Sensibilización.

Para aumentar el nivel de conocimiento del personal del servicio público del Centro, que se tiene sobre la protección de los datos personales, la Unidad de Transparencia emprenderá capacitaciones adecuadas de sensibilización, promoción y difusión de la materia.

Desarrollo de competencias.

Para el desarrollo adecuado de las competencias la Unidad de Transparencia, tomara los cursos y talleres que el Instituto de Transparencia y Acceso a la Información Pública del Estado de Chiapas; brinde sobre los diversos temas de capacitación en materia de protección de datos personales con la finalidad que el personal del servicio público estén debidamente capacitados en la normatividad de referencia.

Implementación, operación, revisión, mantenimiento y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.

La Unidad de Transparencia, velara por lo adecuado desarrollo de las líneas estratégicas, empezando con el debido cuidado que deberán tener el personal del servicio público, en cuanto el tratamiento de datos personales, ajustándose a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como los deberes y las acciones relativas a la seguridad y confidencialidad, que en todo momento deberán responder al marco normativo.

Es fundamental que el personal del servicio público, tenga pleno dominio de las obligaciones, en cuanto a la elaboración de los inventarios de tratamiento, de avisos de privacidad y del documento de seguridad.

Este último, deberá ser desarrollado por cada una de las Dirección, Unidad o Áreas, entendiéndolo como el documento que da cuenta de las medidas técnicas, físicas y administrativas para garantizar la confidencialidad, integridad y disponibilidad de los actos personales que obran en poder de las diversas unidades, áreas o direcciones.

No debe pasar desapercibido, que por la naturaleza del documento puede ser del interés de los ciudadanos y por lo tanto de carácter público, sin embargo, dependiendo de las categorías de los datos personales y los sistemas para su tratamiento, podría tener vocación de ser reservado, por lo que deberán de pasar a la consideración del Comité de Transparencia.

Esto significa, que los enlaces designados en materia de datos personales deberán tener la certeza que las medidas consideradas estarán adecuadamente protegidas, por lo tanto la Unidad de Transparencia, estará siempre atenta a los requerimientos de las Unidades, Áreas o Direcciones del Centro.

DESARROLLO DE LÍNEAS ESTRATÉGICAS

Sensibilización

Lograr sensibilizar al personal del servicio público del Centro, es decir contar con el conocimiento y compromiso, de la profunda relevancia que tiene los datos personales, lo anterior, le corresponde al personal del servicio público del Centro, asumir el compromiso de velar en todo momento por el adecuado tratamiento de los datos personales recabados, para lograrlo en el presente programa de protección de datos personales del Centro, encontraran el conjunto de actividades necesarias para concientizar al personal del servicio público, respecto de los diferentes aspectos relativos a la protección de datos personales, vistos desde la trascendencia del respecto a los derechos fundamentales, el derecho a la autodeterminación informativa es un elemento que le permite a la/el titular de los datos, decidir conscientemente con quien o que organización desea compartir su información, así como tener la garantía que estarán adecuadamente protegidos.

Desarrollo de competencias

Desde la creación del Centro Estatal de Control de Confianza Certificado, se dispuso a cumplir con toda normatividad aplicable, en la materia de protección de datos personales, en tal sentido, la Unidad de Transparencia llevara a cabo capacitaciones a las diversas unidades, áreas o direcciones, que en sus labores cotidianas realizan actividades vinculadas al tratamiento de datos personales y debe elaborar avisos de privacidad y atender solicitudes de ejercicio de derechos ARCO, además de contar con su documento de seguridad.

Implementación, operación, revisión, mantenimiento y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.

El personal del servicio público responsable del sistema de tratamiento de datos personales que poseen, deberán de adoptar las medidas para evitar que se produzca una vulneración de los mismos, respetando los principios de la protección de datos personales que constituyen el pilar mediante se articula este derecho y son de observancia obligatoria para todo aquel que interviene en el tratamiento de datos personales desde el momento de la obtención hasta la destrucción de los mismos.

A. Principios

***a.1. Principios de licitud*:** significa que el personal del servicio público deberán asumir un comportamiento ético y responsable, en el tratamiento de los datos personales que poseen en sus unidades, áreas o direcciones, sujetándose a las atribuciones o facultades que la normatividad aplicable les confiera.

***a.2. Principios de lealtad*:** de acuerdo con el principio de lealtad en la obtención de los datos personales, el personal del servicio público, no podrán obtener datos a través de medios engañosos, ni fraudulentos, lo que implica que no se recaben datos personales con dolo, mala fe, o negligencia, no tratar los datos de tal manera que genere discriminación o un trato injusto contra las/los titulares, no se vulnere la confianza de la/el titular con relación a que sus datos personales serán tratados conforme a lo acordado, se informe todos las finalidades del tratamiento en el aviso de privacidad.

a.3. Principios de consentimiento: el personal del servicio público, deberán contar con el consentimiento de la/el titular para el tratamiento de sus datos personales, para obtener el consentimiento tácito, expreso o expreso por escrito y dependiendo del tipo de datos personales, la solicitud del consentimiento deberá ir siempre ligada a las finalidades concreta del tratamiento que se informen en el aviso de privacidad, es decir el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general.

Aunado a ello, el consentimiento debe ser informado, por lo que previo a su obtención, es necesario que la/el titular conozca el aviso de privacidad, además de que debe ser libre tal y como lo refiere la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

a.4. Principios de información: el personal del servicio público se encuentran obligados a informar a las/los titulares, las características principales del tratamiento al que serán sometida su información personal, lo que se materializa a través del aviso de privacidad, a fin que los titulares puedan tomar decisiones informadas al respecto, y puedan ejercer su derecho de protección de su información personal.

***a.5. Principios de proporcionalidad*:** establece la obligación que el personal del servicio público, trataran solo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

a.6. Principios de finalidad: se entiende que el propósito, motivo o razón por el cual se tratan los datos personales y solo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas a la/el titular en el aviso de privacidad y en su caso consentida por este.

Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbres, dudas o confusión en la/el titular.

Explicita: tiene lugar cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.

Licitas: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conformo a lo previsto en el decreto de creación, reglamento y marco normativo.

Legitimas: cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento de la/el titular, salvo que se actualice alguna de las causales de excepción prevista en el artículo 18 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Así también, las unidades deberán evitar que las finalidades que describa en el aviso de privacidad sean inexactas, ambiguas o vagas como de manera enunciativa más no limitativa.

a.7. Principios de calidad: finalidad o finalidades para las que se vayan a tratar los datos personales estos deben ser exactos, correctos, o completos y actualizados.

El personal del servicio público, están obligados a:

- ✓ Adoptar las medidas que consideren convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, actualizados y correctos, a fin de que no se altere la veracidad de la información.

- ✓ Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo.

- ✓ Bloquear los datos personales antes de suprimirlos y durante el periodo de bloqueo solo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales.

- ✓ Eliminar los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación de conformidad con lo establecido por la Ley de Archivos del Estado de Chiapas.

- ✓ Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales.

A efecto de cumplir con el principio de calidad, es necesario tomar en consideración los siguientes aspectos.

Conservación de los datos personales

El plazo de conservación de los datos personales no debe exceder el tiempo estrictamente necesario para llevar a cabo las finalidades que justificaron el tratamiento, ni aquel que se requiera para cumplir:

- ✓ Las disposiciones legales establecidas en la Ley de Archivos del Estado de Chiapas.
- ✓ Las disposiciones aplicables en la materia de que se trate.
- ✓ Los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.
- ✓ El periodo de conservación.

Conclusión del plazo de conservación

Una vez concluido el plazo de conservación y siempre que no exista disposición legal o reglamentaria que establezca lo contrario, las Direcciones, Unidades o Áreas, deben proceder a la supresión de los datos personales, en este caso, deberán informarlo a la

Coordinación del Sistema Institucional de Archivos para que este haga de conocimiento y solicite la aprobación ante el Archivo General de Estado.

Además, en cuanto a los datos personales sensibles, el responsable debe realizar esfuerzos razonables para limitar el periodo de tratamiento al mínimo indispensable.

a.8. Principio de responsabilidad: el principio de responsabilidad cierra el círculo con relación a los principios que regulan la protección de los datos personales, este principio establece la obligación de las Direcciones, Unidades o Áreas de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación y demostrar antes las/los titulares y el órgano garante, que cumple con sus obligaciones en torno a la protección de los datos personales, bajo este principio el personal del servicio público responsable del tratamiento están obligados a velar por la protección de los datos personales aun y cuando los datos estén siendo tratados por encargados.

B. Confidencialidad y seguridad.

La protección de los datos personales además de principios y obligaciones encuentra base en dos deberes:

***b.1. deber de confiabilidad*:** por confidencialidad, se entiende que se deben establecer controles o mecanismos que tengan por objeto que todas aquellas personas del servicio público, que traten datos personales, en cualquier fase del tratamiento, mantengan en secreto la información, así como evitar que la información sea revelada a personas no autorizadas y prevenir la divulgación no autorizada de la misma.

El personal del servicio público, tiene la obligación de guardar la debida confidencialidad respecto de los datos personales que son tratados en la Dirección, Unidad o Áreas, para evitar causar un daño a la/el titular, de no ser así, un tercero no autorizado podría tener acceso a determinada información y hacer mal uso de esta.

b.2. deber de seguridad: para una efectiva protección de datos personales es necesaria la implementación de un sistema de gestión de seguridad de datos personales, que permita planificar, implementar, monitorear y mejorar las medidas de seguridad de carácter administrativos, físico y técnico, a través de una serie de actividades, interrelacionadas y documentadas tomando en consideración los estándares en materia de protección de datos personales y seguridad.

En este sentido las personas del servicio público con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectué, deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, perdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y relación laboral que mantenga con el Centro Estatal de Control de Confianza Certificado del Estado de Chiapas, debiendo subsistir esta obligación después de finalizar su relación con esta.

C. Inventario de datos personales y de los sistemas de tratamiento.

Al respecto, la normatividad describe como inventario de datos personales a que datos personales se tiene, cual tipo son sensibles o no, cuantos sistemas de datos tienes y en que soportes se tiene la información, si es un documento físico o se encuentra en formato electrónico.

Es necesario que el enlace designado de protección de datos personales de cada dirección, unidad o área, cuente con el apoyo del Oficial de Protección de Datos Personales, para la identificación de los principales tipos de activos que pueden ser considerados al interior del Centro.

Dicho catálogo de inventario de tratamiento de datos personales, que realicen las direcciones, unidades o áreas, a través del personal de servicio público, contendrá las finalidades, tipos de datos tratados, formatos de almacenamientos, lista del personal al servicio público que tiene acceso al tratamiento, en su caso, nombre o razón social del encargado, así como de los destinarios de la transferencias.

Para contar con dicho inventario y sistemas de tratamiento, es importante que el personal del servicio público, designados como enlaces en materia de protección de datos personales realicen los siguientes elementos relevantes:

1. **¿Qué tratamiento de datos personales realizan las direcciones, unidades o áreas?**

   El personal del servicio público deberá identificar cada uno de los procesos de las direcciones, unidades o áreas en la que trata datos personales en cumplimiento en el marco de su competencia y facultades para atender un trámite.

   Es importante recordar que un dato personal es cualquier información correspondiente a una persona física identificada o cuya identidad se puede conocer a través de esa información, por ejemplo nombre, apellidos, CURP, numero de pasaporte, número

de teléfono, dirección de correo electrónico, número de tarjeta de crédito, datos profesionales, laborales o académicos, salarios entre otros.

2. **¿Qué personas o dirección, unidad o área está a cargo de estos procesos y que por tanto sea la administradora de las base de datos o archivos que se generen con motivo de dichos tratamientos?**

   Hay que identificar o definir si el área, unidad o dirección está a cargo del proceso en donde se tratan los datos personales, según las atribuciones o facultades normativas, además del personal al servicio público que tiene acceso al tratamiento.

   Aunado a ello, el tratamiento se entiende la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

   En ese sentido, se deberán identificar las personas, áreas, dirección o unidad del centro, que realicen cualquiera de las actividades antes señaladas, así como identificar qué actividad en concreto realizan con los datos personales, por ejemplo: si los recaban y almacenan; si los recaban transfieren o acceden a los mismos.

   Asimismo podrá darse el caso en que dos unidades, direcciones o áreas, estén a cargo de un proceso mediante el cual se recaban los datos personales y que administren las bases de datos correspondientes de manera conjunta, en ese sentido para definir quien está a cargo del proceso mediante el cual recaban los datos personales y que, por tanto, administre las bases de datos o archivos correspondientes en necesario analizar la función que realiza cada área, dirección o unidad dentro del proceso y las atribuciones o facultades normativas que resulten aplicables.

3. **Una vez que haya sido identificado los tratamientos de los cuales estén a cargo las unidades, áreas o direcciones, será necesario determinar lo siguiente, de acuerdo con el ciclo de vida de los datos personales, es necesario realizar el inventario de protección de datos personales.**

3. **a. ¿Cómo se obtiene los datos personales?**

1. Directamente de la/el titular
2. De manera personal, con la presencia física de la/el titular de los datos personales o su representante, en su caso.
3. Vía telefónica.

4. Por correo electrónico.
5. Por internet o sistema informático.
6. Por escrito presentado directamente en las oficinas del sujeto obligado.
7. Por escrito enviado por mensajería
8. Mediante una trasferencia.
9. Quien transfiere los datos personales y para que fines.
10. Medio por lo que se realiza la transferencia.
11. De una fuente de acceso a la información.

3. b. ¿Qué tipo de datos personales se tratan? ¿Son sensibles?

Se sugiere hacer un listado de todos los datos personales que se recaban y utilizan para las distintas actividades que realicen el personal del servicio público, en el marco de sus facultades y atribuciones legalmente conferidas, siendo importante la distinción de los datos personales sensibles, a continuación se describen las siguientes categorías de datos personales y sus niveles.

Datos identificativos: Nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyente (RFC), Clave Única de Registro de Población (CURP), Clave de elector, Matricula del Servicio Militar Nacional, numero de pasaporte, lugar y fecha de nacimiento nacionalidad, edad, fotografía y demás análogos.
Nivel: Básico.

Datos electrónicos: Las direcciones electrónicas, tales como el correo no oficial, dirección IP (protocolo de internet), dirección MAC (dirección Media Acces Control o Dirección de Control de Acceso al Medio)
(Nivel: Básico).

Datos laborales: Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencia laborales, referencias personales, solicitudes de empleo, hoja de servicio y además análogos.
(Nivel: Básico).

Datos académicos: Trayectoria educativa, calificaciones, títulos, cedula profesional, certificados y reconocimientos y demás análogos.
(Nivel: Básico).

Datos de salud: El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detención de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumos de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona.
(Nivel: Alto).

Datos patrimoniales: Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales y demás análogos.
(Nivel: Medio).

Datos sobre procedimiento administrativos: La información relativa a una persona que se encuentra sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en material laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del derecho.
(Nivel: Medio).

Datos de tránsito y movimientos migratorios: información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria.
(Nivel: Básico).

Datos biométricos: Huellas dactilares, ADN, geometría de la mano, característica de iris y retina y demás análogos.
(Nivel: Alto).

Datos sensibles: Origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias religiosas, filosóficas, la pertenencia a sindicatos, la salud y preferencia sexual.
(Nivel: Alto).

Datos personales de naturaleza pública: aquellos que por mandato legal sea accesibles al público.
(Nivel: Básico).

3. **c. ¿Dónde se almacenan y realiza el tratamiento de los datos personales?**

- Sección, serie y subserie de archivos
- Formato en que se encuentra la base de datos: físico y/o electrónico

- Ubicación de la base de datos

3. **d. ¿Para qué finalidades se utilizan los datos personales?**

Las finalidades son acciones más específicas de los procesos de los que derivan los tratamientos de datos personales: por ejemplo el procedimiento podría ser "**contratación de personal**" y la finalidades "**evaluación curricular para la selección de personal**".

En este punto, será necesario identificar cada una de las finalidades concretas para las cuales se tratan los datos personales, lo cual se vincula de manera directa con las actividades en las cuales se utilizan los datos personales, por ejemplo, nomina, o expediente de personal, tramite o servicios que realizan las dependencias o sujetos obligados.

También, no deberá de pasar por desapercibido, si se requiere el consentimiento o no de las/los titulares y el tipo de consentimiento (tácito o expreso y por escrito), y en caso de que no se requiera, definir que supuestos (fracciones del artículo 18 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas).

Asimismo, se deberá señalar el marco jurídico que da facultades para el tratamiento de datos personales (disposición, normativa, fracción, inciso, párrafo).

3. **e. ¿Quién tiene acceso a la base de datos o archivos (sistemas de tratamiento) y a quien se comunican los datos personales al interior de los sujetos obligados?**

Se deberá identificar el catálogo del personal del servicio público al interior del Centro Estatal de Control de Confianza Certificado.

3. **f. ¿Intervienen encargados en el tratamiento de los datos personales?**

Es necesario identificar el nombre del encargado y el número de contrato, pedido o convenio correspondiente.

3. **g. ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?**

La comunicación de datos personales puede ser de la/el titular de los datos o con otro sujeto responsable, resulta necesario que se identifique a quien se comunican los datos personales y para que fines, esto es, autoridades a terceros externos al Centro.

3. h. ¿Se difunden los datos personales?

Hay que señalar si los datos personales se difunden y el fundamento jurídico.

3. i. ¿Cuál es el plazo de conservación de los datos personales?

Este plazo tendría que estar definido en los instrumentos de clasificación archivística, por lo que es necesario identificar a qué serie documental pertenecen los archivos o base de datos en los que están contenidos los datos personales.

3. j. ¿Cómo se suprimen los datos personales?

El personal del servicio público, deberá de adoptar medidas necesarias para mantener exactos, completo, correctos y actualizados los datos personales en su posesión, esto es, políticas, métodos y técnicas orientadas a la supresión definitiva de estos, de tal manera que la probabilidad de recuperación o reutilizarlos sea mínimo.

Se deberán de considerar los siguientes atributos y el o los medios de almacenamiento, físico y/o electrónicos en los que se encuentren datos personales.

- Irreversibilidad: que el proceso utilizado no permita recuperar los datos personales.
- Seguridad y Confidencialidad: Que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refiere las leyes aplicables.
- Favorable al medio ambiente: Que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.

A mayor abundamiento, cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso.

Una vez que concluya el plazo de conservación de los mismos. Los plazos de conservación de los datos personales no deberán exceder aquellos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las

disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

D) Aviso de Privacidad

El aviso de privacidad es el documento que deberán las unidades, áreas o direcciones, poner a disposición de la/el titular de forma física, electrónica o en cualquier formato, a partir del momento en el que se recaben sus datos personales como el objeto de informarle los propósitos del tratamiento de los mismos.

La puesta a disposición del aviso de privacidad implica que el personal al servicio público, deberán de publicar en un lugar visible, accesible y gratuito, en el cual la/el titular, de manera informada, cuente con la posibilidad de conocer el tratamiento que se les dará o su datos personales, en todo caso el aviso de privacidad deberá estar ubicado en un lugar visible y que facilite su consulta, esto último también tiene como finalidad acreditar ante el Órgano Garante el cumplimiento de su obligación.

Para la elaboración de los avisos de privacidad, será necesario que las unidades direcciones o áreas soliciten la opinión y asesoría de la Unidad de Transparencia, para analizar las finalidades que se realizaran por el personal del servicio público, en el ámbito de sus atribuciones para el debido tratamiento de los datos personales que posean.

d.1. Modalidades del Aviso de Privacidad

Existen dos modalidades del aviso de privacidad, simplificado e integral

El Simplificado debe contener lo siguiente:

- La denominación del Responsable.
- La finalidad del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieran el consentimiento de la/el titular.

a. Las autoridades, poderes, entidades, órganos y organismo gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y

b. Finalidades de estas transferencias.

- Los mecanismos y medios disponibles para que la/el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento de la/el titular, y
- El sitio donde se podrá consultar el aviso de privacidad integral.

Por otra parte, el aviso de privacidad integral deberá contener, además de lo citado con anterioridad al menos la información siguiente:

- El domicilio del responsable.
- Los datos personales que serán sometidos a tratamientos, identificando aquellos que son sensibles.
- El fundamento legal que faculta al responsable para llevar acabo el tratamiento.
- Las finalidades del tratamiento para las cuales se obtienen los datos personales distinguiendo aquellas que requieren el consentimiento de la/el titular.
- Los mecanismo, medios y procedimientos disponibles para ejercer los derechos ARCO;
- El domicilio de la Unidad de Transparencia, y
- Los medios a través de los cuales el responsable comunicara a las/los titulares los cambios al aviso de privacidad.

Finalmente para conocer los formatos de avisos de privacidad que deberán de utilizar las unidades, áreas o direcciones, se agregan al presente programa las plantillas de los avisos de privacidad simplificado e integral. **Anexo I.**

d.2. Medidas Compensatorias.

Las medidas compensatorias son los mecanismos alternos para dar a conocer a las/los titulares el aviso de privacidad simplificado, a través de su difusión por medios masivos de comunicación u otros mecanismos de amplio alcance.

El personal del servicio público deberá de instrumentar medidas compensatorias cuando resulte imposible dar a conocer a la/el titular el aviso de privacidad simplificado de manera directa o ello exija esfuerzos desproporcionados.

Imposibilidad de dar a conocer a la/el titular el aviso de privacidad de forma directa: se presenta cuando el responsable no cuenta con los datos personales necesarios que les permitan tener un contacto directo con la/el titular ya sea porque no existen en sus

archivos, registros, expedientes, bases o sistemas de datos personales, o bien porque los mismo se encuentran desactualizados, incorrectos, incompletos o inexactos.

Esfuerzos desproporcionados para dar a conocer a la/el titular el aviso de privacidad de forma directa: cuando el número de las/los titulares sea tal, que el hecho de poner a disposición de cada uno de estos el aviso de privacidad, de manera directa, le implique al responsable un costo excesivo atendiendo a su suficiencia presupuestaria, o comprometa la vialidad de su presupuesto programado o la realización de sus funciones o atribuciones que la normatividad aplicable le confiera, o altere de manera significativa aquellas actividades que lleve a cabo cotidianamente en el ejercicio de sus funciones o atribuciones.

Obtención directa de los datos personales: cuando la/el titular proporciona personalmente sus datos personales a quien representa al responsable o a través de algún medio que permita su entrega directa como podrían ser sistemas o medios electrónicos, ópticos, sonoros, visuales, vía telefónica, internet o cualquier otra tecnología o medio físico.

Los avisos de privacidad serán actualizados o en su caso, elaborados por cada unidad, área o dirección, que trate datos personales, según sus atribuciones, la unidad de transparencia proporcionara asesoría, verificara su correcta elaboración y difusión en el portal de este centro.

d.3. Consentimiento

El personal del servicio público, deberá contar con el consentimiento de la/el titular de los datos personales, salvo que se actualice alguna de las excepciones de los artículos 18, 94 y 95 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

- Elaborar su respectivo aviso de privacidad, revisando la necesidad y legalidad de su tratamiento para cumplir con la finalidad de que se trate, a fin de que quede debidamente justificada la obtención y uso de los datos personales.

- Identificar las finalidades para cuales se requiere el consentimiento de las/los titulares.

- En caso de que las finalidades o tratamiento establecidos en el aviso de privacidad encuadre con la hipótesis de los artículos 18, 94 y 95 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, la unidad, área o dirección estará exenta de solicitar al usuario su consentimiento.

Una vez que se ponga a disposición de la/el titular el aviso de privacidad, las unidades, áreas o direcciones, deberán observar los casos en que se requiera consentimiento tácito o expreso, dependiendo el tipo de datos personales.

E) Derechos ARCO

El acrónico ARCO está conformado por las iniciales de los derechos de Acceso, Rectificación, Cancelación y Oposición de los datos personales, y que las/los titulares pueden ejercer, consiste en:

Derecho de Acceso: es el derecho que tiene la/el titular de solicitar el acceso a sus datos personales que se encuentran en las bases de datos, sistemas, archivos, registros o expedientes del responsable que lo posee, almacena o utiliza, así como de conocer información relacionada con el tratamiento que se da a su información personal.

Derecho de Rectificación: es el derecho que tiene la/el titular de solicitar la rectificación o corrección de sus datos personales, cuando estos sean inexactos o incompletos o no se encuentren actualizados, en otras palabras puede solicitar a quien posea o utilice su datos personales que los corrija cuando los mismos sean incorrectos, desactualizados o inexactos.

Derecho de Cancelación: es el derecho que tienen las/los titulares de solicitar que sus datos personales se eliminen de los archivos, registros, expedientes, sistemas, base de datos del responsable que lo trata, aunque hay que tomar en cuenta que no en todos casos se podrá eliminar sus datos personales, principalmente cuando sea necesarios por alguna cuestión legal o para cumplimiento de obligaciones.

Derecho de Oposición: es el derecho que tiene la/el titular de solicitar que sus datos personales no se utilicen para una determinada finalidad, no para la totalidad de estas, también en este caso como en el anterior, no siempre se podrá impedir el uso de los datos cuanto estos sean necesarios por motivos legales o para cumplimiento de obligaciones.

El personal del servicio público, deben tener conocimiento que como cualquier otro derecho, el de protección de datos personales tiene límites, por lo que bajo ciertas circunstancias los derechos ARCO, no podrán ejercerse o su ejercicio se verá limitado por cuestiones de seguridad nacional, orden, seguridad y salud públicos, así como por derechos de terceros.

Las causas por las que el responsable puede negar el ejercicio de los derechos ARCOS son:

- La/el titular de los datos personales o su representante no haya acreditado su identidad.
- El responsable no es competente para atender la solicitud.

- Existe un impedimento legal.
- Se puede afectar los derechos de terceros personas.
- Cuando el ejercicio de los derechos ARCO pudiera obstaculizar procesos judiciales o administrativos.
- Cuando sean necesarios para proteger intereses jurídicamente tutelados de la/el titular.
- Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por la/el titular.
- Cuando los datos sean parte de información de las entidades sujetas a regulación y supervisión financiera del sujeto obligado, o.
- Cuando en función de sus atribuciones del sujeto obligado, el uso, resguardo y manejo sean necesarios para mantener la integridad, estabilidad y permanencia del estado mexicano.

Cabe resaltar, aunque no proceda el ejercicio de derechos ARCO, las unidades, áreas o direcciones, están obligadas a responder la solicitud e informar las causas de improcedencia.

Luego entonces el derecho a la protección de datos personales es un derecho personalísimo, solamente las/los titulares o sus representantes podrán solicitar el ejercicio de los derechos ARCO, por lo que es indispensable acreditar la identidad.

F) Transferencias.

El personal del servicio público, responsable del tratamiento de los datos personales deberá de comprender que la transferencia es toda comunicación de datos personales, dentro o fuera del territorio, a persona distinta de la/el titular, del responsable o del encargado.

Es decir la comunicación de datos entre el responsable y el encargado, NO se considera transferencia, a ese tipo de comunicaciones se les llama remisiones, es importante señalar que los responsables no están obligados a solicitar el consentimiento de las/los titulares para la realización de remisiones, ni informarlas en el aviso de privacidad, contrario a lo que ocurre con la transferencias.

La/el titular haya otorgado su consentimiento para la transferencia se realice, salvo los casos de excepción previsto en el artículo 18, 94 y 95 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

No se requerirá el consentimiento de las/los titulares, para realizar transferencias, algunos de los supuestos son:

- Cuando una ley así lo disponga;
- Cuando las transferencias que se realicen entre responsables, para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivo el tratamiento;
- Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- Para el reconocimiento o defensa de derechos de la/el titular ante autoridades competente;
- Para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica;
- Cuando exista una situación de emergencia;
- Asistencia sanitaria;
- Los datos se encuentren en fuentes de acceso público;
- Los datos personales sean sometidos a un procedimiento de disociación;
- La/el titular de los datos sea una persona reportada como desaparecida;
- Transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal;
- A petición de una autoridad u organismo extranjero, competente en su carácter de receptor, cuya facultades sea homologas;
- Transferencia necesaria para un contrato celebrado o por celebrar en interés de la/el titular;
- La transferencia sea necesaria por razones de seguridad;

G) Documento de Seguridad

El documento de seguridad es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad, técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Para su elaboración resulta indispensable la participación del personal del servicio público responsable del tratamiento de los datos personales de todas las unidades, áreas o direcciones, en el ámbito de su competencia quienes, para este fin, serán coordinadas por el personal de la Unidad de Transparencia quien orientará y verificará la integración del documento, mismo que se conforma por lo siguiente:

- El inventario de datos personales;
- Las funciones de las personas que tratan datos;
- El análisis de riesgos;

- El análisis de brecha;
- El plan de trabajo;
- Los mecanismo de monitoreo y revisión;
- El programa de capacitación.

El documento de seguridad, podrá sufrir actualizaciones considerando los siguientes eventos:

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

Es importante destacar que la seguridad de los datos personales deberá observarse durante todo su ciclo de vida, desde su obtención hasta su eliminación.

H) Vulneraciones

La vulneración de datos personales además de las que señalen las leyes respectivas y la normatividad aplicable, se consideraran como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos de obtención hasta su eliminación.

- La pérdida o destrucción no autorizada;
- El robo, extravió o copia no autorizada;
- El uso, acceso o tratamiento no autorizado, o
- El daño, la alteración o modificación no autorizada

El personal del servicio público, responsable de los sistemas de tratamiento de los datos personales que poseen, deberán de notificar inmediatamente a sus respectivos enlaces de protección de datos personales, cuando se actualice alguno de los puntos considerados anteriormente, debiendo contener lo siguiente:

- La naturaleza del incidente o vulneración ocurrida;

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

Una vez que se cuente con cada uno de los puntos anteriores descritos el enlace de protección de datos personales deberá de notificarlo a la Unidad de Transparencia, para que este a su vez, lo informe al Instituto de Transparencia, Acceso a la Información Pública del Estado de Chiapas de monitorear y revisar la eficacia y eficiencia del Programa.

La Unidad de Asuntos Jurídicos en conjunto con la Unidad de Transparencia, realizará revisión cuando crea conveniente, a efecto de coadyuvar con el personal del servicio público, responsable del tratamiento de los datos personales a fin de que se garantice la observancia obligatoria de los principios de protección de datos personales prevista en la normatividad.

MEJORA CONTINUA DEL PROGRAMA

Con finalidad de comprobar el cumplimiento del programa, el comité de transparencia realizara las siguientes acciones:

1. requerirá a la Unidad de Transparencia, el informe de resultados de los programas de sensibilización y desarrollo de competencias diseñadas para el adecuado tratamiento y la seguridad de los datos personales.

2. a través de la Unidad de Transparencia, se requerirá a todas las unidades, áreas o direcciones, de ser el caso la elaboración del aviso de privacidad integral y/o simplificado, cuando de acuerdo a sus actividades, funciones y atribuciones realizan tratamiento de datos personales, este requerimiento se realizara de manera preventiva finalizado el periodo de capacitación y en una segunda etapa, una vez realizado el levantamiento del inventario, aquellas áreas universitarias que resulten faltantes.

3. una vez realizado el diagnóstico y que la Unidad de Transparencia cuente con el inventario de datos personales, el Comité de Transparencia tomara en cuenta las áreas de oportunidad para las medidas de seguridad físicas, administrativas y técnicas, la que quedaran establecidas en el correspondiente "documento de seguridad" que será propuesto como prioritario en la siguiente política institucional de protección de datos personales.

Con las acciones señaladas, se ensaya el nivel de cumplimiento de las disposiciones establecidas en el presente programa y la emisión de recomendaciones por parte del Comité de Transparencia para dar cumplimiento a las obligaciones que en materia de protección de datos personales que establece el marco normativo.

El Comité de Transparencia, realizara las recomendaciones que estime conveniente en materia de protección de datos personales, teniendo como finalidad fundamental que las unidades, áreas, o direcciones, adopten acciones preventivas y correctivas:

1. acción preventiva (deberán documentarse): las encaminadas a evitar cualquier incumplimiento a lo establecido en el presente Programa. Para las acciones preventivas se podrán llevar a las siguientes actividades:

a) Analizar y revisar las posible causas de incumplimiento;
b) Determinar que otras causas de incumplimiento podría desencadenarse a partir de ciertas situaciones de riesgo para el tratamiento de datos personales;
c) Evaluar las acciones necesarias para evitar que el incumplimiento ocurra;
d) Determinar e implementar estas acciones;
e) Documentar e implementar estas acciones;
f) Revisar la eficacia de las acciones preventivas tomadas.

2. acciones correctivas que deberán documentarse: las encaminadas a eliminar las causas de incumplimiento con relación a lo previsto en este documento, para las acciones previstas se podrán llevar a la siguientes actividades:

a) Analizar y revisar el incumplimiento;
b) Determinar las causas que dieron origen al cumplimiento;
c) Evaluar las acciones necesarias para evitar que el incumplimiento vuelva a ocurrir;
d) Proponer acciones y establecer un plazo para su cumplimiento;
e) Documentar resultados de las acciones tomadas, y

f) Revisar la eficacia de las acciones correctivas tomadas.

Resulta trascendental tener presente que el objetivo de las acciones denominadas correctivas, es eliminar las causas que generaron el incumplimiento a lo establecido en el presente programa, o bien, reducir su grado de prevalencia.

Finalmente, es importante que sea el primer programa en materia de protección de datos que se elabora por la Unidad de Transparencia.

DEFINICIONES OPERACIONALES

Activo. La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales que tenga valor para la organización.

Aviso de Privacidad. Documento de forma física, electrónica o en cualquier formato que es generado por el responsable y puesto a disposición de las/los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Base de Datos. Conjunto ordenado de dato personales bajo criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procedimiento, almacenamiento y organización.

Bloqueo. La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabadas, con el único propósito de determinar posibles responsables en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de estas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido este, se procederá a su cancelación en la base de datos que corresponde.

Consentimiento. Manifestación de la voluntad libre, especifica e informada de la/el titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

Comité de Transparencia. Instancia a la que hace referencia el artículo 62 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

Datos Personales. Cualquier información concerniente a una persona física identificada o identificable, se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos Personales Sensibles. Aquellos que se refieran a la esfera más íntima de la/el titular, o cuya utilización indebida pueda dar origen de discriminación o con lleve a un riesgo grave para este. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones.

Derechos ARCO. Los derechos de acceso, rectificación, cancelación y reposición al tratamiento de datos personales.

Documento de Seguridad. Instrumento que describe y da cuenta, de manera general, sobre las medidas de seguridad técnicas, físicas y administrativas, adoptadas por el responsable para garantizar confidencialidad, integridad y disponibilidad de los datos personales que posee.

Encargado. Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Fuentes de Acceso Público. Aquellas base de datos, sistemas o archivos que por disposición de la ley pueda ser consultada públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso el pago de una contraprestación, tarifa o contribución, no se considerara fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga procedencia ilícita, conforme a las disposiciones por la presente ley y demás normativa aplicable.

Instituto. Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado.

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

Lineamiento. Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas.

Medidas de Seguridad Administrativas. Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de Seguridad Físicas. Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, de manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

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

Medidas de seguridad técnicas. Conjunto de acciones y mecanismo que se valen de la tecnología relacionadas con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento, de manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificado y autorizados.
b) Generar esquema de privilegios para que el usuario lleve a cabo las actividades que requieren con motivo de sus funciones.
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del Software y Hardware.
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Programa. Programa de Protección de Datos Personales.

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

Revisión. Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continúo de los contenidos establecidos en este programa.

Riesgo. Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Sujeto Obligado. Cualquier autoridad, entidad órgano y organismo de los Poder Ejecutivo

CENTRO ESTATAL
DE CONTROL DE CONFIANZA
CERTIFICADO
GOBIERNO DE CHIAPAS

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

Centro. Centro Estatal de Control de Confianza Certificado del Estado de Chiapas.

Titular. Persona física de sexo femenino y masculino a quien le corresponden los datos personales.

Responsable Sujeto obligado de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Oficial. Persona responsable de la gestión, aplicación y administración ante el Instituto de Transparencia, Acceso a la información Pública del Estado de Chiapas.

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

Tratamiento. Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionada con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Área, Dirección o Unidad. Áreas, Unidades o Direcciones a la que se le confiere especificas en el reglamento interior estatuto orgánico o instrumento normativo equivalente que sea superior a un manual de organización.

Por cada Dirección, Unidad o Área señalada en el apartado de "ALCANCE" deberá redactar su aviso de privacidad integral y simplificado por cada tratamiento que trate de acuerdo a la redacción siguiente:

Anexo I

AVISO DE PRIVACIDAD INTEGRAL DE ----------.
(Indicar a que tramite, servicio o procedimiento se refiere)

DOMICILIO

El Centro Estatal de Control de Confianza Certificado (El Centro), con domicilio ubicado en la avenida 1era Sur, esq. 2ª Oriente, número 290, colonia Centro, C.P. 29000, Tuxtla Gutiérrez, Chiapas; a través de su (nombre de la unidad, área o dirección) es responsable del tratamiento de los datos personales que nos proporcione, los cuales serán protegidos conforme a lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, y de más normatividad que resulten aplicable.

FINALIDAD DE USO Y TRATAMIENTO DE SUS DATOS PERSONALES.

(Nombre de la unidad, área o dirección) hace de su conocimiento que la finalidades del tratamiento aplicado a sus datos personales son los siguientes y no requiere de su consentimiento (si fuera el caso contrario, indicar si requieren consentimiento expreso).

(Describir cada una de la finalidad para las cuales se recaban los datos personales)

DATOS PERSONALES QUE SERÁN SOMETIDOS A TRATAMIENTO.

Para llevar a cabo las finalidades descritas en el presente aviso de privacidad recabaremos los siguientes datos personales

(Enlistar casa uno de los datos personales recabados)

Así mismo se recabaran datos personales de carácter sensible como:

(Describir el tipo de datos que se trate o en caso contrario indicar expresamente: "se informa que no se recaban datos personales sensibles").

FUNDAMENTO LEGAL

El tratamiento de sus datos personales se realiza con fundamento en los artículos 5, 12, 14, 19, 20, 22, 23, 26, 31, 34, 37, 39 y demás relativos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como los artículos 58, 70, 71, 146, 149, 150 y

151 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, así como el (fundamento que le compete a su área, unidad o dirección) del Reglamento Interior del Centro Estatal de Control del Confianza Certificado, y demás normativas que resulten aplicables.

FINALIDAD DE USO Y TRATAMIENTO DE SUS DATOS PERSONALES.

Los Datos Personales que aquí se recaben se utilizarán para los principales fines:

Se recabaran sus datos personales como nombre y firma, sus datos personales, serán utilizados con la finalidad de llevar a cabo la celebración del convenio de colaboración entre el H. ayuntamiento y el Centro Estatal de Control de Confianza Certificado, con el objetivo de llevar un mejor seguimiento a los proceso de evaluación que se someten.

TRANSFERENCIA DE DATOS PERSONALES

Se informa que no se realizarán transferencias de datos personales, salvo aquellas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados, con fundamento en el artículo 18 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

DONDE SE PUEDEN EJERCER LOS DERECHOS DE ACCESO, CORRECCIÓN/ RECTIFICACION, CANCELACIÓN U OPOSICIÓN DE DATOS PERSONALES (DERECHOS ARCO).

Usted podrá ejercer sus derechos de acceso, rectificación cancelación u oposición de sus datos personales (ARCO) directamente antes la Unidad de Transparencia de estas instalaciones, ubicado en la Avenida 1ª Sur, esq. 2ª Oriente, número 290, colonia Centro, C.P. 29000, Tuxtla Gutiérrez, Chiapas; C.P. 29000, o bien, a través de la Plataforma Nacional de Transparencia (http://www.plataformadetransparencia.org.mx/) o en el correo electrónico control_confianza@transparencia.chiapas.gob.mx. Si desea conocer el procedimiento para el ejercicio de estos derechos puede acudir a la Unidad de Transparencia, enviar un correo electrónico a la dirección antes señala.

Medios para presentar recurso de revisión:

A través de la Plataforma Nacional de Transparencia:
http://www.plataformadetransparencia.org.mx/

Correo electrónico: control_confianza@transparencia.chiapas.gob.mx

Presencial: ubicado en la Avenida 1ª Sur, esq. 2ª Oriente, número 290, colonia Centro, C.P. 29000, Tuxtla Gutiérrez, Chiapas; C.P. 29000

CAMBIO EN EL AVISO DE PRIVACIDAD

En caso de realizar cambios en el Aviso de Privacidad se realizará por medio presencial y en nuestra página de internet: www. controldeconfianza.chiapas.gob.mx

ANEXO II

AVISO DE PRIVACIDAD SIMPLIFICADO DE ----------.
(Indicar a que tramite, servicio o procedimiento se refiere)

El Centro Estatal de Control de Confianza Certificado (El Centro), con domicilio ubicado en la avenida 1era Sur, esq. 2ª Oriente, número 290, colonia Centro, C.P. 29000, Tuxtla Gutiérrez, Chiapas; a través de su (nombre de la unidad, área o dirección) es responsable del tratamiento de los datos personales que nos proporcione, los cuales serán protegidos conforme a lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, y de más normatividad que resulten aplicable.

Sus datos personales serán utilizados con la finalidad de (describir la finalidad para las cuales se recaban los datos personales)

Usted podrá consultar el aviso de privacidad integral en www.controldeconfianza.chiapas.gob.mx, así como en la (nombre de la unidad, área o dirección) de este Organismo Descentralizado.

CENTRO ESTATAL
DE CONTROL DE CONFIANZA
CERTIFICADO
GOBIERNO DE CHIAPAS

INVENTARIO DE TRATAMIENTO 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 diagnostico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en este Centro Estatal de Control de Confianza Certificado del Estado de Chiapas.

Por inventario de tratamientos de datos personales se entenderá el control documentado que se llevará de los tratamientos que realizan las Direcciones, Unidades y Áreas del Centro Estatal de Control de Confianza Certificado del Estado de Chiapas.

1. A continuación se describen las categorías de datos personales con los que cuenta el Centro, esto según el formato que se llenó por casa Dirección, Unidad o Área, lo cuales se anexan al final de este documento.

Datos de identificación y contacto: nombre, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, firma autógrafa, edad, fotografía y referencias personales.

Datos biométricos: huella dactilar.

Datos Laborales: puesto o cargo que desempeña, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información generada durante los procedimientos de reclutamiento, selección y contratación y experiencia/capacitación laboral.

Datos Académicos: trayectoria educativa, título, cédula profesional, certificados, y reconocimientos.

Datos Patrimoniales y/o Financieros: ingresos, egresos y cuentas bancarias.

Datos sobre pasatiempos, entretenimiento y diversión: pasatiempos, aficiones, deportes que práctica y juegos de interés.

Datos Legales: Situación jurídica de la persona (juicios, amparos, proceso administrativos, entre otros.)

Datos de Salud: estado de salud físico presente, pasado o futuro y estado de salud mental presente, pasado, o futuro.

Datos personales de naturaleza pública: datos que por mandato legal son de acceso público.

2. Personas de quienes se obtienen los datos personales:

a) Personas que laboran en el Centro.
b) Personas externas que prestan sus servicios en diferentes Instituciones de Seguridad Pública del Estado, que se somete a evaluación de control de confianza.
c) Personas externas que participan en actividades que llevan a cabo las direcciones, unidades o áreas del Centro. (capacitaciones, contratos, concursos etc.).

Los datos personales se recaban por medio de documentos presentados y/o por el llenado de formularios físicos y/o electrónicos por las/los titulares de los datos personales.

3. Nivel de seguridad de los datos personales a los que se les da tratamiento en el Centro:

Por mayor garantía de seguridad en los datos personales y en las bases de datos personales, físicas o electrónica, donde se concentran los mismos, las medidas de seguridad que se implementaran corresponden a un nivel de seguridad medio o alto, siempre garantizando la confidencialidad, integridad y disponibilidad de los datos personales, tal y como lo expresa la Ley.

4. Transferencias de los datos personales:

Todas transferencia de datos personales, sea esta estatal, o nacional se encuentra sujeta al consentimiento de la /el titular, salvo en las excepciones previstas en los artículos 16,68 y 72 de la Ley.

5. Catálogo de base de tratamientos de datos personales de las direcciones, unidades o áreas del Centro:

Dirección, Unidad o Área	Tratamiento
Dirección General	✓ Recepción
Dirección Médica y Toxicología	✓ Proceso de evaluación de Médico Toxicología ✓ Integración de Expedientes de M-T

Dirección de Información, Registro y Cadena de Custodia	✓ Emitir el Certificado Único Policial (CUP) ✓ Integración de Resultados
Dirección Ejecutiva y de Situación Patrimonial	✓ Declaraciones Patrimoniales ✓ Investigación de Presunta Responsabilidad ✓ Programación de Evaluaciones
Dirección de Atención Psicológica	✓ Proceso de evaluación psicológicas
Dirección de Poligrafía	✓ Proceso de evaluación de poligrafía
Dirección de Investigación socioeconómica	✓ Proceso de evaluación de socioeconómica ✓ Proceso de investigación de antecedentes ✓ Proceso de investigación documental
Unidad de Apoyo Administrativo	**Recursos Humanos** ✓ Infonavit y Fonacot ✓ Hacienda e Imss (movimiento nominales y afiliaciones) ✓ Expediente Personal y Nóminas **Recursos Materiales y Servicios** ✓ Integración de contratos ✓ Solicitudes de pasajes aéreos **Recursos Financieros** ✓ Orden de Pago
Unidad de Informática	✓ Tarjeta Institucional ✓ Resguardo Temporal ✓ Creación de Usuario ✓ Cámara de Vigilancia
Comisaria	✓ realización de acciones tendientes a evaluar el desempeño general de la entidad y vigilar su correcto funcionamiento y administración.
Unidad de Planeación	✓ Integración de Información de Planeación
Unidad de Asuntos Jurídicos	✓ Convenio ✓ Procedimientos Judiciales ✓ Solicitudes de Transparencia

Entre esto se recaban lo siguientes datos personales, para llevar acabo los tratamientos antes señalados.

Datos Personales Identificativos	Datos Personales Patrimoniales	Datos Personales Sensibles
• Nombre de persona física (titular de los datos personales, representante, terceros interesados, promovente, persona autorizada para recibir notificaciones, entre otros. • Firma • CURP • RFC • Teléfono fijo o celular • Domicilio • Correo electrónico • Datos laborales • Fotografía • Escolaridad • Antecedentes • Cedula profesional • Año de nacimiento o edad • Beneficiarios • Características físicas • Curriculum vitae • Datos académicos • Datos laborales • Menor de edad • Nacionalidad • Nivel educativo • Ocupación • Sexo • Títulos profesionales	• Descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil, entre otros. • Cuenta interbancaria	• Datos sobre procedimientos judiciales o seguimiento en forma de juicio. • Religión • Origen • Datos de salud • Vida sexual • Circunstancias socioeconómicas • Creencias religiosas, filosóficas o morales • Discapacidad • Estado de interdicción o incapacidad legal • Lengua indígena • Origen étnico o racial • Pertenencia a pueblo indígena • Datos biométricos

CENTRO ESTATAL DE CONTROL DE CONFIANZA CERTIFICADO
GOBIERNO DE CHIAPAS

• Nombre • Estado civil • Empleo actual • Cartilla de servicio militar nacional • Huella dactilar		

Cada Área, Unidad o Dirección, realizara el tratamiento con una finalidad definida por sus funciones, tal como se señala en el cuadro siguiente

Dirección, Unidad o Área	Tratamiento	Finalidad
Dirección General	✓ Recepción	✓ Se solicita los datos de la persona, con la finalidad de identificarlo.
Dirección Médica y Toxicología	✓ Proceso de evaluación de Médico Toxicología ✓ Integración de Expedientes de M-T	✓ En ambos se requiere los datos para el Proceso de Evaluación Medico y Toxicología
Dirección de Información, Registro y Cadena de Custodia	✓ Emitir el Certificado Único Policial (CUP) ✓ Integración de Resultados	✓ Para entrega del Formato Único de Evaluación, donde se encuentra los datos personales de los elementos, así como los cursos recibidos para la emisión de CUP. ✓ Para emitir un Resultado Único de Control de Confianza.
Dirección Ejecutiva y de Situación Patrimonial	✓ Declaraciones Patrimoniales ✓ Investigación de Presunta Responsabilidad ✓ Programación de Evaluaciones	✓ Mantener actualizado el padrón de declarantes y promover la presentación de las declaraciones patrimoniales. ✓ Preparar el inicio de expediente de investigación por la presunta responsabilidad en la omisión de presentación de la declaración de situación patrimonial. ✓ Programar las Evaluaciones de Control de Confianza Certificado.
Dirección de Atención Psicológica	✓ Proceso de evaluación psicológicas	✓ Para Identificar a la persona en la Aplicación de Pruebas y Entrevista e Integración del expediente de la Evaluación Psicológica.

Dirección de Poligrafía	✓ Proceso de evaluación de poligrafía	✓ Proceso de evaluación poligráfica con el objetivo de identificación en entrevista de evaluación e integración del expediente poligráfico.
Dirección de Investigación socioeconómica	✓ Proceso de evaluación de socioeconómica ✓ Proceso de investigación de antecedentes ✓ Proceso de investigación documental	✓ Elaborar informes de investigación socioeconómica, con base a los datos vertidos y obtenidos ✓ La finalidad de los datos recibidos es para cumplir con los requisitos del proceso de la evaluación socioeconómica. ✓ La finalidad de los datos recibidos es para cumplir con los requisitos del proceso de la evaluación socioeconómica.
Unidad de Apoyo Administrativo	**Recursos Humanos** ✓ Infonavit y Fonacot ✓ Hacienda e Imss (movimiento nominales y afiliaciones) ✓ Expediente Personal y Nóminas **Recursos Materiales y Servicios** ✓ Integración de contratos ✓ Solicitudes de pasajes aéreos **Recursos Financieros** ✓ Orden de Pago	**Recursos Humanos** ✓ Para dar alta, baja y modificaciones de salarios, así como verificar si el trabajador se encuentra vigente. ✓ Para realizar movimientos nominales de alta, promoción y baja en el Sistema de Nómina NECH. ✓ Integrar documentos para Expedientes del Personal del Centro. **Recursos Materiales y Servicios** ✓ Para llevar a cabo la integración de los contratos de compraventa y servicio de este Centro. ✓ Para realizar la compra de boletos de pasajes aéreos **Recursos Financieros** ✓ Gestionar el pago correspondiente a los proveedores, viáticos y servicios básicos
	✓ Tarjeta Institucional	✓ Para la realización de la tarjeta institucional,

Unidad de Informática	✓ Resguardo Temporal ✓ Creación de Usuario ✓ Cámara de Vigilancia	para permitir la identificación. ✓ Realizar el resguardo temporal de equipos informáticos para un control interno de la ubicación de dichos equipos. ✓ identificar al usuario que se le dará acceso a los sistemas. ✓ Mantener la Seguridad dentro del Edifico del Centro Evaluador.
Comisaria	✓ evaluar el desempeño	✓ Realización de acciones tendientes a evaluar el desempeño general de la entidad y vigilar su correcto funcionamiento y administración.
Unidad de Planeación	✓ Integración de Información de Planeación	✓ Para informar ante la Secretaría de Hacienda el presupuesto ejercido por concepto de montos pagados por ayudas y subsidios.
Unidad de Asuntos Jurídicos	✓ Convenio ✓ Procedimientos Judiciales ✓ Solicitudes de Transparencia	✓ Se realiza el convenio de colaboración de los Honorables de Ayuntamientos, para llevar acabo las evaluaciones de control de confianza. ✓ Se requieren los datos del procedimiento para tener conocimiento del juicio. ✓ Realizar la contestación de las solicitudes de transparencia.

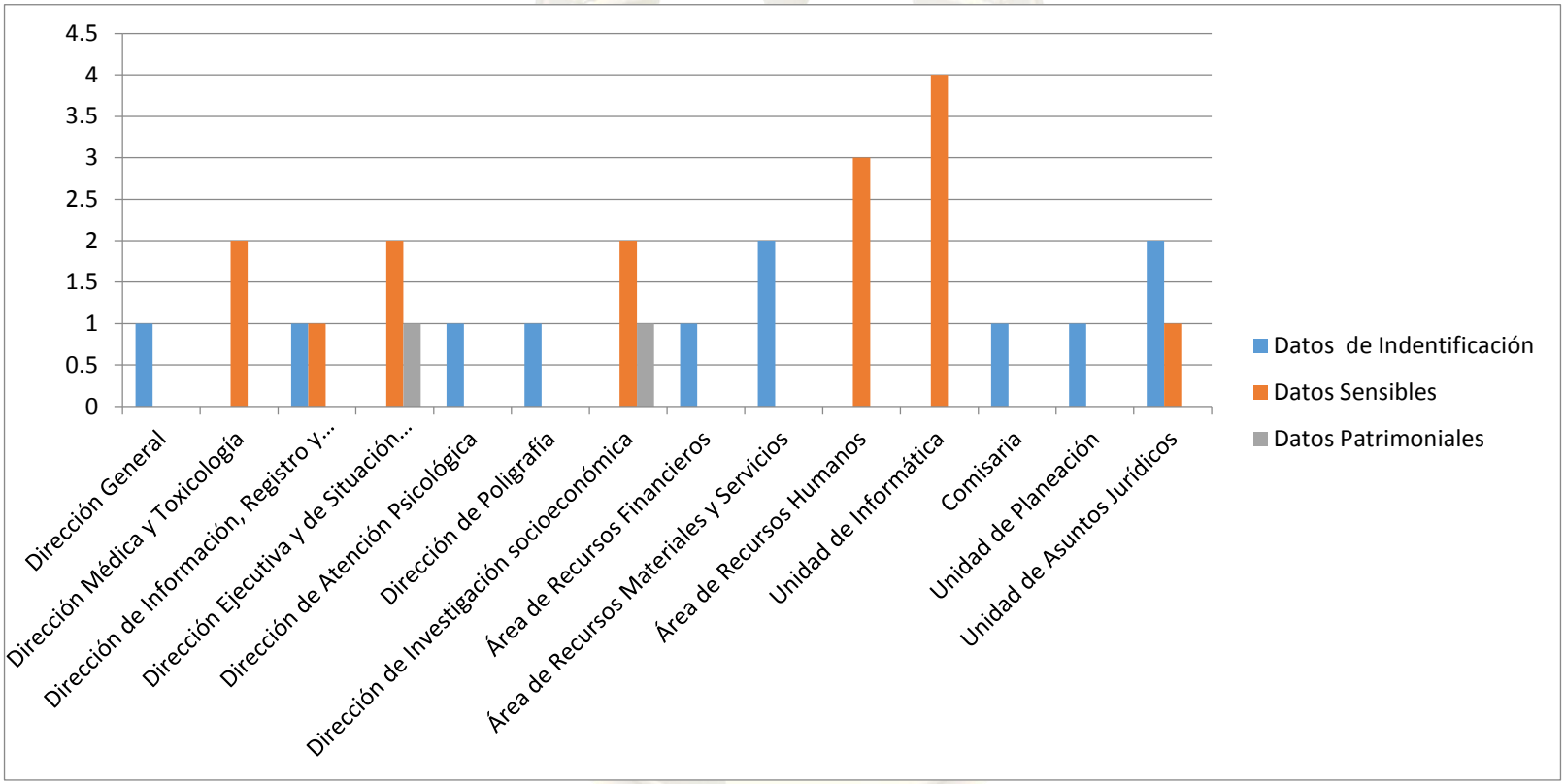
Como parte del proceso, se transfiere datos personales a las siguientes instituciones y se difunden a otras áreas, con la finalidad señalada en el cuadro anterior.

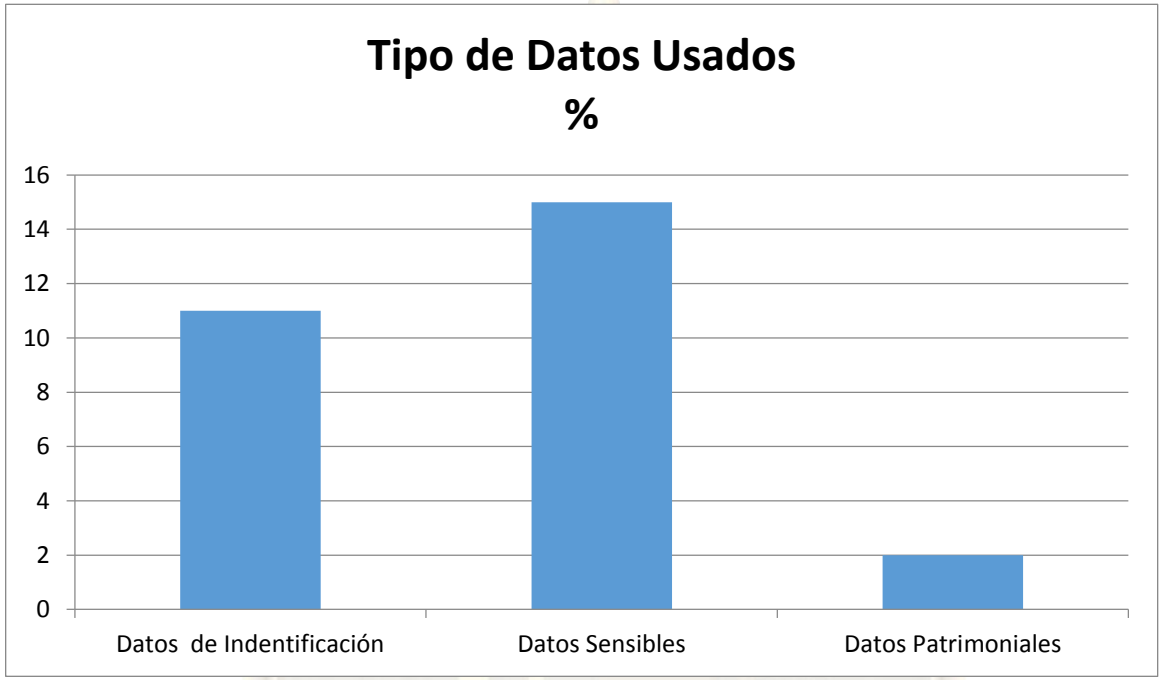
Dirección, Unidad o Área	Institución donde se realiza la transferencia
Dirección Médica y Toxicología	✓ Empresa Laboratorio Clínico Azteca, S.A.P.I. de C.V.
Dirección de Información, Registro y Cadena de Custodia	✓ Secretaria de Seguridad y Protección Ciudadana. ✓ Fiscalía General del Estado. ✓ H. Ayuntamientos Municipales ✓ Centro Estatal de Control de Confianza de Tabasco. ✓ Centro Estatal de Control de Confianza de Quintana Roo.

	✓ Servicio de Protección Federal. ✓ Secretaría de Hacienda del Estado
Dirección Ejecutiva y de Situación Patrimonial	✓ Secretaria de Seguridad y Protección Ciudadana. ✓ Fiscalía General del Estado. ✓ H. Ayuntamientos Municipales ✓ Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana. ✓ Instituto de Formación Policial. ✓ Instituto Mexicano del Seguro Social (IMSS). ✓ Instituto Nacional Electoral (INE) ✓ Secretaría de Hacienda del Estado ✓ Registro Civil ✓ Coordinación Operativa, Centro Estatal de Control de Confianza Certificado. ✓ Comisión Federal Electoral (CFE).
Dirección de Investigación socioeconómica	✓ Instituciones Educativas. ✓ Secretaria de Defensa Nacional. ✓ Subsecretaria de Ejecución de Sanciones Penales y Medidas de Seguridad. ✓ Secretaria de Hacienda del Estado.
Unidad de Apoyo Administrativo	**Recursos Humanos** ✓ Instituto del Fondo Nacional de la Vivienda (INFONAVIT) ✓ Instituto del Fondo Nacional para el Consumo de los Trabajadores (INFONACOT) ✓ Coordinación General de Recursos Humanos de la Secretaría de Hacienda del Estado de Chiapas ✓ Instituciones de Seguros ✓ Servicio de Administración Tributaria ✓ Secretaría de la Honestidad y Función Pública del Estado de Chiapas. **Recursos Materiales y Servicios** ✓ Dirección de Adquisiciones de la Oficialía Mayor del Estado. **Recursos Financieros**

	✓ Secretariado Ejecutivo del Sistema de Estatal de Seguridad Pública
Unidad de Planeación	✓ Secretaría de Hacienda del Estado

Cuando se trata datos personales sensibles, el consentimiento es expreso mediante una carta de consentimiento o una leyenda en el formulario para recabar datos mismos que son firmados por el Titular en el área, unidad o dirección donde se le requiera sus datos personales sensible, tal y como se presenta en la gráfica.





TIPO DE DATOS POR TRATAMIENTO

N°	Dirección , Unidad o Área	Datos de Identificación	Datos Sensibles	Datos Patrimoniales
1	Recepción	1		
2	Proceso de evaluación de Médico Toxicología		1	
3	Integración de Expedientes de M-T		1	
4	Emitir el Certificado Único Policial (CUP)	1		
5	Integración de Resultados		1	

6	Declaraciones Patrimoniales			1
7	Investigación de Presunta Responsabilidad		1	
8	Programación de Evaluaciones		1	
9	Proceso de evaluación psicológicas	1		
10	Proceso de evaluación de poligrafía	1		
11	Proceso de evaluación de socioeconómica			1
12	Proceso de investigación de antecedentes		1	
13	Proceso de investigación documental		1	
14	Infonavit y Fonacot		1	
15	Hacienda e Imss (movimiento nominales y afiliaciones)		1	
16	Expediente Personal y Nóminas		1	
17	Integración de contratos	1		
18	Solicitudes de pasajes aéreos	1		
19	Orden de Pago	1		
20	Tarjeta Institucional		1	
21	Resguardo Temporal		1	
22	Creación de Usuario		1	
23	Cámara de Vigilancia		1	
24	Realización de acciones tendientes a evaluar el desempeño general de la entidad y vigilar su correcto funcionamiento y administración.	1		
25	Integración de Información de Planeación	1		
26	Convenio	1		
27	Procedimientos Judiciales		1	
28	Solicitudes de Transparencia	1		
	Total	**11**	**15**	**2**

CENTRO ESTATAL
DE CONTROL DE CONFIANZA
CERTIFICADO
GOBIERNO DE CHIAPAS

ANÁLISIS DE RIESGO Y DE BRECHA

El Presente análisis identifica el riesgo inherente a los datos personales en el tratamiento que reciben por Centro Estatal de Control de Confianza Certificado al ejercer sus atribuciones, de manera que pueda ser controlado por la institución para satisfacer el derecho humano a la autodeterminación informativa.

La LPDPPSOCHIS 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, la valoración de los riegos 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 (documentos de seguridad), en este caso, por el Centro Estatal de Control de Confianza Certificado, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de ese tipo de datos bajo su posesión.

La Unidad de Transparencia realizará una matriz de análisis de riesgos aplicadas a las Unidades, Direcciones o Áreas del Centro, que tratan datos personales de la cual emanara el documento de análisis de riesgo que contendrá por lo menos lo siguiente:

a. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.
b. El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida.
c. El valor y exposición de los activos involucrados en el tratamiento de los datos personales.
d. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.
e. El riesgo inherente a los datos personales tratados, considerando los activos, las amenazas y las vulnerabilidades.
f. La sensibilidad de los datos personales tratados.
g. Las posibles consecuencias de una vulneración para los titulares,
h. La transferencia de datos personales que se realicen.
i. 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.

CENTRO ESTATAL DE CONTROL DE CONFIANZA CERTIFICADO
GOBIERNO DE CHIAPAS

En general se tiene que el Centro Estatal de Control de Confianza Certificado del Estado de Chiapas, cuenta con 14 unidades administrativas en las que se da tratamiento de datos personales mediante 28 procesos como se visualiza a continuación:

Dirección , Unidad o Área	Datos de Identificación	Datos Sensibles	Datos Patrimoniales
Dirección General	1		
Dirección Médica y Toxicología		2	
Dirección de Información, Registro y Cadena de Custodia	1	1	
Dirección Ejecutiva y de Situación Patrimonial		2	1
Dirección de Atención Psicológica	1		
Dirección de Poligrafía	1		
Dirección de Investigación socioeconómica		2	1
Área de Recursos Financieros	1		
Área de Recursos Materiales y Servicios	2		
Área de Recursos Humanos		3	
Unidad de Informática		4	
Comisaria	1		
Unidad de Planeación	1		
Unidad de Asuntos Jurídicos	2	1	

Bajo esta premisa para analizar los riesgos de los datos personales que son objeto de tratamiento por el Centro Estatal de Control de Confianza Certificado del Estado de Chiapas, 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 pueda dar origen a discriminación o con lleva un riesgo grave para este como por ejemplo, el origen étnico, el estado de salud presente o futuro, la creencias religiosas, la opinión política o la orientación sexual.

De los anteriores, se identificó que se trabaja con número de categorías 1,2 y 3: Datos de Identificación, Datos Patrimoniales, Datos Sensibles.

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

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

1. Robo, extravío o copia no autorizada.
2. Uso, acceso o tratamiento no autorizado.
3. Daño, alteración o modificación no autorizado.
4. Pérdida o destrucción no autorizada.

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 el 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 del Centro Estatal de Control de Confianza Certificado 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 electrónicos, de domicilio, laborales, patrimoniales, procedimientos administrativos	Medio	2
Datos sensibles	Alto	3

I. Clasificación de datos personales

El responsable debe identificar los tipos de datos personales que se tratan, la sensibilidad de los mismos y el número de titulares para determinar el valor de riesgo inherente de los datos para un tercero no autorizado.

Datos con riesgo inherente bajo

Esta categoría considera información general concerniente a una persona física identificada o identificable, como por ejemplo datos de identificación y contacto o información académica o laboral, tal como nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo y lugar de trabajo, idioma o lengua, escolaridad, cedula profesional, información migratoria, entre otra información que no refiera a los siguientes tres categorías.

Datos riesgo inherente medio

Esta categoría contempla los datos que permiten conocer la ubicación física de la persona, tales como la dirección física, información relativa al tránsito de las personas dentro y fuera del país, y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más, por ejemplo: dependencia, beneficiarios, familiares, referencias laborales, referencias personales, etc.

También son datos de riesgo inherente medio aquellos que permitan inferir el patrimonio de una persona, que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados. Incluye el número de tarjeta bancaria de crédito y/o débito.

Son considerados también, los datos de autenticación con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros) firma autógrafa y electrónica, fotografías, identificaciones oficiales, inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona.

Dentro de esta categoría se toman en cuenta los datos jurídicos tales como antecedentes penales, amparos, demandas, contratos litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil penal o administrativa.

Datos con riesgo inherente alto

Esta categoría de datos contempla a los datos personales sensibles, que de acuerdo a la Ley incluyen datos de salud los cuales se refieren a la información médica donde se documente el estado de salud física y mental, pasado, presente o futuro; información genética; origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o con lleve un riesgo grave para la/el titular.

Los datos de mayor riesgo son los que de acuerdo a su naturaleza derivan en mayor beneficio para un atacante, por ejemplo:

Información adicional de tarjeta bancaria que considera el número de la tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido de la misma, por ejemplo fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN).

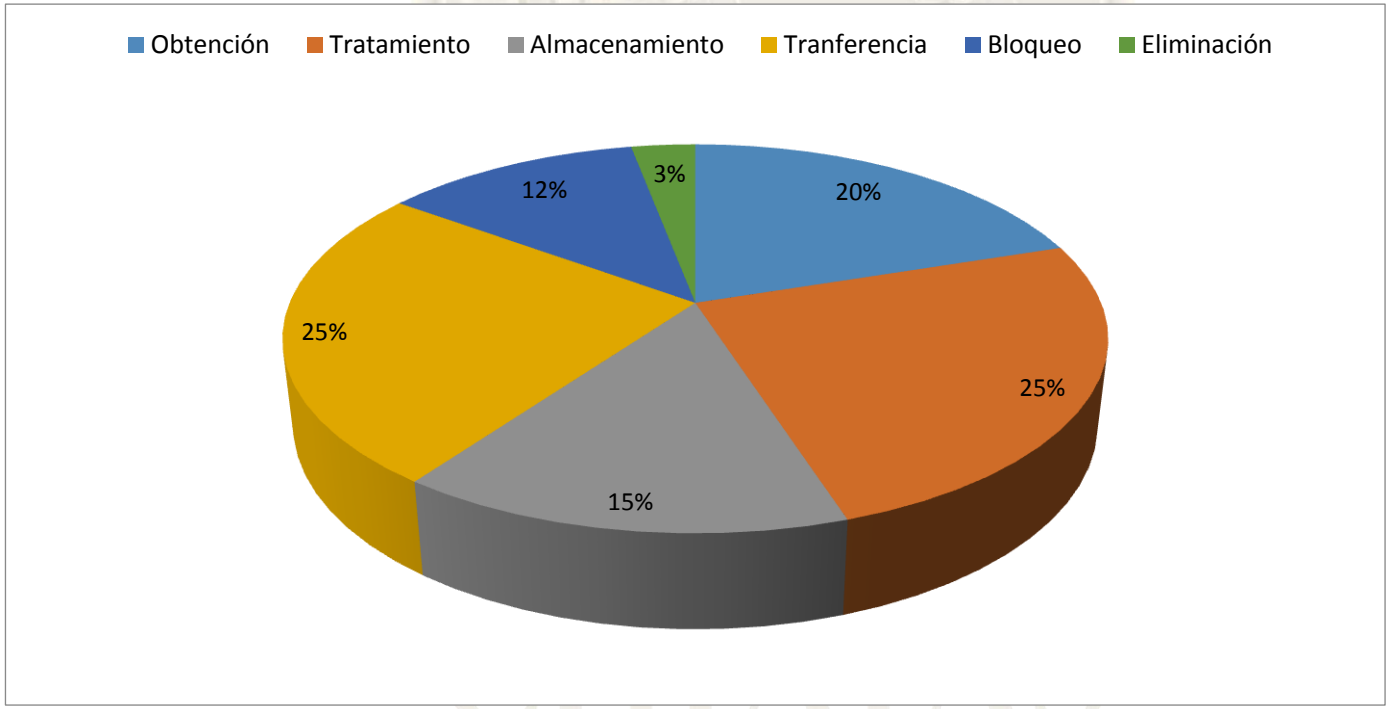
Las personas de alto riesgo son aquellas cuya profesión, oficio o condición están expuestas a una mayor probabilidad de ser atacadas debido al beneficio económico o reputacional que sus datos personales pueden representar para un atacante, por ejemplo, líderes políticos, religiosos, empresariales, de opinión y cualquier otra persona que sea considerada como personaje público. Asimismo se considera a cualquier persona cuya profesión esté relacionada con la impartición de justicia y seguridad nacional. Tratar datos de personas de alto riesgo involucra que la base de datos contiene nombres de figuras públicas que pueden ser reconocidas a primera vista, así como información personal donde se infiera o se relacione explícitamente con su profesión, puesto o cargo en combinación con datos de identificación como nombre, domicilio, entre otros.

El responsable o encargado deberá documentar los tipos de datos que tiene en tratamiento y su riesgo inherente, para uso en las siguientes secciones de la metodología. Se debe incluir todos los tipos de datos que se tiene en tratamiento.

El proceso de análisis de riesgos considera la evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. Contempla la identificación de activos, el estudio de causas y consecuencias de la amenaza y vulnerabilidades en los sistemas de tratamiento de datos personales, y permite establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad.

ETAPA DE MAYOR Y MENOR VULNERABILIDAD

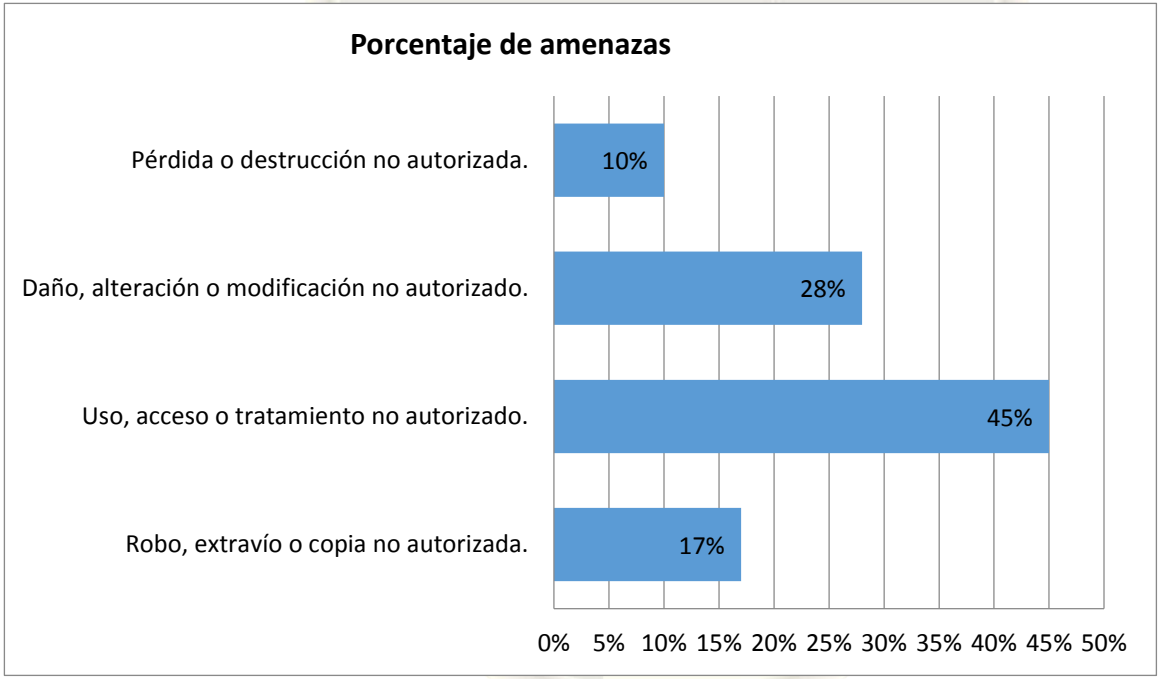
La identificación de la etapa de mayor y menor vulnerabilidad es el resultado de la valoración que se haga al distribuir porcentajes a la etapas del tratamiento (obtención, tratamientos, almacenamiento, transferencia, bloqueo y eliminación), analizando cuales el riesgo para cada etapa, de acuerdo con las medidas de seguridad que implementamos y los diferentes entornos.



Las amenazas a las que se ven expuestos son básicamente:

1. Robo, extravío o copia no autorizada.
2. Uso, acceso o tratamiento no autorizado.
3. Daño, alteración o modificación no autorizado.
4. Pérdida o destrucción no autorizada.

Siendo las más alta, la de robo, extravío o copia no autorizada y la de menor riesgo es daño, alteración o modificación no autorizada, como se muestra en la tabla siguiente:



CENTRO ESTATAL
DE CONTROL DE CONFIANZA
CERTIFICADO
GOBIERNO DE CHIAPAS

ANÁLISIS DE LA INFORMACIÓN

La unidad administrativa que observa mayor estado de vulnerabilidad y riesgo de los datos personales es de la siguiente manera como se desglosa:

No.	Tratamiento	Tipo de Dato	Volumen	Accesos	Entorno	Promedio de Riesgo Inherente
1	Proceso de Evaluación Socioeconómica	Datos sensibles	Menos de 10,000	40	Físico	3.00
2	Proceso de Evaluación de Médica-Toxicología	Datos de tránsito y movimientos migratorios, de salud, biométricos	Menos de 10,000	20	Equipo de cómputo	2.50
3	Integración de Resultados	Datos sensibles	Menos de 10,000	20	Físico	2.50
4	Integración de Expediente de Médica-Toxicología	Datos de tránsito y movimientos migratorios, de salud, biométricos	Menos de 10,000	10	Equipo de cómputo	2.25
5	Proceso de investigación de antecedentes	Datos sensibles	Menos de 10,000	10	Físico	2.25
6	Proceso de investigación documental	Datos sensibles	Menos de 10,000	10	Físico	2.25
7	Proceso de evaluación psicológicas	Identificativos	Menos de 10,000	30	Equipo de cómputo	2.25
8	Programación de Evaluaciones	Datos de tránsito y movimientos migratorios, de salud, biométricos	Menos de 10,000	10	Equipo de cómputo	2.25
9	Declaraciones Patrimoniales	Datos laborales, patrimoniales, procedimientos administrativos	Más de 10,000	10	Equipo de cómputo	2.25
10	Proceso de Evaluación Poligráficas	Identificativos	Menos de 10,000	20	Equipo de cómputo	2.00
11	Expediente Personal y Nóminas	Datos sensibles	Menos de 1,000	10	Físico	2.00
12	Cámara de Vigilancia	Datos sensibles	Menos de 100	10	Equipo de cómputo	2.00
13	Resguardo Temporal de Equipos Informáticos	Datos laborales, patrimoniales, procedimientos administrativos	Menos de 1,000	10	Físico	1.50
14	Creación de Usuarios al personal para Acceso a los Sistemas del CECCC	Datos laborales, patrimoniales, procedimientos administrativos	Menos de 1,000	10	Físico	1.50
15	Investigación de Presunta Responsabilidad	Datos laborales, patrimoniales, procedimientos administrativos	Menos de 1,000	10	Físico	1.50
16	Proceso Judiciales	Datos laborales, patrimoniales, procedimientos administrativos	Menos de 100	10	Físico	1.25

17	Certificado Único Policial	Identificativos	Menos de 1,000	10	Físico	**1.25**
18	Integración de Información planeación	Identificativos	Menos de 1,000	10	Físico	**1.25**
19	Hacienda e Imms (movimiento nominales y afiliaciones)	Identificativos	Menos de 1,000	10	Físico	**1.25**
20	Infonavit y Fonacot	Identificativos	Menos de 1,000	10	Físico	**1.25**
21	Tarjetas Institucionales	Datos laborales, patrimoniales, procedimientos administrativos	Menos de 100	10	Físico	**1.25**
22	Órdenes de pago	Identificativos	Menos de 1,000	10	Físico	**1.25**
23	Convenios	Identificativos	Menos de 100	10	Físico	**1.00**
24	Recepción	Identificativos	Menos de 100	10	Físico	**1.00**
25	Solicitudes (transparencia).	Identificativos	Menos de 100	10	Físico	**1.00**
26	Integración de Contratos	Identificativos	Menos de 100	10	Físico	**1.00**
27	Solicitudes de pasajes aéreos	Identificativos	Menos de 100	10	Físico	**1.00**
28	Evaluación el desempeño general de la entidad y vigilar su correcto funcionamiento y administración.	Identificativos	Menos de 100	10	Físico	**1.00**
	Total					**1.67**

Finalmente, como parte del análisis es posible establecer que el nivel de riesgo es mayormente bajo, debido que se trabaja sobre todo con datos de identificación, en algunos casos con datos patrimoniales y son en unos tratamientos se solicita un dato sensible.

Asimismo, los datos personales corresponden a menos de 400 personas, lo que reduce el nivel de riesgo y se mantienen a resguardo en computadoras personales con contraseña y en archiveros con llave, así como un sistema de video vigilancia de seguridad las 24 horas al día.

PLAN DE TRABAJO

Las medias generales de seguridad administrativa, físicas y técnicas con las que actualmente cuenta el Centro Estatal de Control de Confianza Certificado, para mantener la confidencialidad e integridad de la información, así como para proteger los datos personales contra daño, perdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado, e impedir la divulgación no autorizada, son las siguientes:

Medidas Administrativas

a. Canalizar a cada dirección, unidad o áreas, que trate datos personales, la encuesta sobre el estado actual del cumplimiento de las obligaciones en materia de datos personales para que sea contestada y así poder conocer las unidades, áreas o direcciones con las cuales se trabajara.

b. Capacitar al personal del Centro, en materia de datos personales.

c. Implementar medidas de seguridad físicas, administrativas y técnicas para la debida protección de los datos personales.

d. Conformar el aviso de privacidad con lo que requiera la ley de acuerdo a los tratamientos que este centro realiza.

e. Llevar acabó revisión de seguimiento y de verificación, esto con el objetivo de corroborar el cumplimiento de las obligaciones que marca la ley.

f. Conformar la carpeta de evidencia del cumplimiento de las obligaciones.

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

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

Medidas Físicas

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

b. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información.

c. Limitar el número de personas con acceso a archivos físicos.

d. Procurar suscribir responsivas de confidencialidad con el personal que trata datos personales.

e. Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales.

f. Resguardo de llaves en oficinas de acceso restringido.

Medidas Técnicas

a. Utilizar claves de usuario y contraseñas de manera personal y evitar compartirlas, prestarlas o registrarla a la vista de otras personas.

b. Establecer y utilizar contraseña robustas, es decir, del amenos ocho caracteres alfanuméricos y especiales, evitando que sean iguales al nombre de usuario.

c. Notificar de manera inmediata a la Dirección, Unidad o Área los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero.

d. 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.
e. 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 actividades laborales.

f. Evitar el acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio; es decir únicamente al personal que por sus funciones y facultades laborales lo requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.

g. Borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo los documentos o archivos electrónicos que nos son necesarios para el desarrollo de funciones.

CENTRO ESTATAL
DE CONTROL DE CONFIANZA
CERTIFICADO
GOBIERNO DE CHIAPAS

LAS MECANISMO DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Las medidas de seguridad administrativas, físicas y técnicas serán de aplicación a todas las bases de datos personales que manejan las personas a cargo de la dirección, unidad o áreas mencionadas en la fracción IV del presente documento.

LOS PROGRAMAS DE CAPACITACIÓN Y ACTUALIZACIÓN

El personal de la Unidad de Transparencia, capacitará al personal del Centro, en materia de protección de datos personales dos veces al año, la fecha se designará en el transcurso del mismo, esto con la intención de que todos estén presentes.

En caso de que en el transcurso del año se presente alguna modificación a la ley de la materia, surja alguna actualización en el tema o alguna de las Unidades, Áreas, o Direcciones, tenga la necesidad de capacitación, se solicitará la programación del curso.

Asimismo, el personal de la Unidad de Transparencia, estará en capacitación constante por medio de cursos/o talleres presenciales o en línea por parte del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas.

ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

El presente documento de seguridad se actualizará cuando ocurran los siguientes eventos:

a. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.
b. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.
c. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a l seguridad, e
d. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.