DOCUMENTO DE SEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES DEL CENTRO ESTATAL DE TRASPLANTES DEL ESTADO DE CHIAPAS

ÍNDICE

I. PRESENTACIÓN…….....3

II. OBJETIVOS DEL DOCUMENTO DE SEGURIDAD…….....4

III. GLOSARIO DE TÉRMINOS…….....5

IV. RESPONSABILIDADES DENTRO DEL PROGRAMA…….……7

V. ALCANCE DEL DOCUMENTO DE SEGURIDAD……..8

VI. SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES…….....9

VII. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTOS……..13

VIII. FUNCIONES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES……..…….....23

IX. PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD……..….26

X. ANÁLISIS DE RIESGO……27

XI. ANÁLISIS DE BRECHA……..……29

XII. MEDIDAS DE SEGURIDAD……29

XIII. MONITOREO DE LAS MEDIDAS DE SEGURIDAD……..32

XIV. PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES……..….33

XV. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD……33

I. PRESENTACIÓN.

La Protección de los Datos Personales garantiza la protección de la vida privada e intimidad de las personas, información que se puede ver vulnerada cuando la información personal se comparte con autoridades, instituciones, dependencias o entidades de la administración pública Federal, Estatal o Municipal.

Por tal razón en 2007, se realizaron reformas a la Constitución Política de los Estado Unidos Mexicanos, adicionando un segundo párrafo con siete fracciones al artículo 6º, con el propósito de garantizar el derecho de toda persona a la protección de sus datos personales, así como el derecho de las personas físicas para acceder gratuitamente a sus datos personales o a la rectificación de estos.

Posteriormente en 2016 se reformaron los artículos 16 y 73 Constitucionales. Se adiciona un segundo párrafo al artículo 16, con el propósito de garantizar el derecho de toda persona a la protección de sus datos personales, el acceso, rectificación, cancelación, así como a manifestar su oposición al tratamiento de estos. Se establece en el artículo 73 la facultad del Congreso Federal de legislar en materia de protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales, de todos los niveles de gobierno, así como el órgano garante encargado de velar por el cumplimiento de estos derechos.

En ese tenor el 26 de enero de 2017 se publicó en el Diario Oficial de la Federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados cuyo objeto según su artículo 1º, es establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de: cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito Federal, Estatal o Municipal.

En el presente documento se detallan las medidas de seguridad administrativas, físicas y técnicas con las que se contará en el Centro Estatal de Trasplantes del Estado de Chiapas “CETRA”, para garantizar la debida protección de los datos personales a los que se les da tratamiento en las unidades administrativas que los recaban.

El presente Documento de Seguridad para la Protección de Datos Personales, se dicta en cumplimiento de las disposiciones jurídicas vigentes y de conformidad a lo establecido en los artículos 3 fracción XIII y 29 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, publicada en el Periódico Oficial Número 045, de fecha 18 de junio de 2025.

II. OBJETIVOS DEL DOCUMENTO DE SEGURIDAD.

El presente documento es de observancia obligatoria y tiene como objetivo asegurar la integridad, confidencialidad y disponibilidad de los datos e información personal que se encuentra en posesión del Centro Estatal de Trasplantes del Estado de Chiapas, en su carácter de sujeto obligado, a la par que delimita las obligaciones de los responsables, encargados y usuarios de cada sistema y medidas de seguridad administrativas, físicas y técnicas que deberán implementarse para el correcto manejo de la información que se posee, conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en la protección de los datos personales, de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y demás normatividad aplicable.

El presente programa tiene como objetivos los siguientes:

1. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del Centro Estatal de Trasplantes del Estado de Chiapas.
2. Cumplir con las obligaciones que establecen las Leyes, los Lineamientos Generales y demás normatividad aplicable.
3. Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales a efecto de protegerlos de manera sistemática y continua, y;
4. Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que el programa se haya implementado de manera integral en la organización o bien, cuando se estime pertinente la implementación de buenas prácticas de tratamientos específicos.

El presente documento de seguridad fue elaborado por la Unidad de transparencia del Centro Estatal de Trasplantes del Estado de Chiapas y aprobado en su totalidad por el Comité de Transparencia.

III. GLOSARIO DE TÉRMINOS.

Bases de datos: Conjunto ordenado de datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Catálogo de bases de datos personales: Lista detallada del conjunto ordenado de bases datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

CETRA: Centro Estatal de Trasplantes del Estado de Chiapas.

Datos personales: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, 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.

Derechos ARCOP: Los derechos de acceso, rectificación, cancelación, oposición y portabilidad 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 la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Inventario de datos personales: Lista ordenada y detallada que posea el responsable o encargado, de cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a una persona física identificada o identificable.

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

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

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Medidas de seguridad administrativas: Políticas, acciones 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 medidas protocolos y controles para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento para prevenir el acceso no autorizado a sus instalaciones físicas, áreas críticas, recursos e información.

Medidas de seguridad técnicas: Conjunto de acciones, mecanismos y sistemas de los datos personales y los recursos involucrados en su tratamiento como revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.

Nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

Titular: La persona física a quien pertenecen los datos personales.

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

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

Transparencia para el Pueblo: Es un organismo público desconcentrado, sectorizado a la Secretaría Anticorrupción y Buen Gobierno, dotado de autonomía técnica y operativa, creado el 21 de marzo de 2025 en su carácter de autoridad garante federal para garantizar el derecho de acceso a la información en posesión de la administración pública federal.

Transparencia para el Pueblo de Chiapas: Es un Órgano Administrativo Desconcentrado, jerárquicamente subordinado a la Secretaría Anticorrupción y Buen Gobierno, con plena autonomía administrativa, técnica, de gestión y de ejecución, así como con facultades de decisión y promoción para el adecuado desarrollo de sus atribuciones.
Que tiene por objeto garantizar, dentro de los sujetos obligados del Poder Ejecutivo del Estado de Chiapas y de los Municipios de la entidad, el cumplimiento de las obligaciones de transparencia, el ejercicio del derecho de acceso a la información pública y la protección de los datos personales, conforme a los principios y bases establecidos en los artículos 6°, Apartado A, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, así como en el artículo 5, fracciones XV y XVI, de la Constitución Política del Estado Libre y Soberano de Chiapas.

Unidades Administrativas: Órganos Administrativos con los que cuenta el CETRA, de acuerdo a su Reglamento Interior, para el despacho de los asuntos de su competencia.

IV. RESPONSABILIDADES DENTRO DEL PROGRAMA

Con fundamento a lo dispuesto en los artículos 77 y 78 de la Ley, que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones con relación a este programa:

I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los Datos Personales en la organización del responsable, de conformidad con lo previsto en la presente Ley y demás disposiciones aplicables en la materia;
II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los Derechos ARCO;
III. 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;
IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la Ley y demás criterios que resulten aplicables en la materia;
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. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Órgano Desconcentrado de la Secretaría o la Autoridad Garante competente, según corresponda;
VII. Establecer programas de capacitación y actualización para los servidores públicos, en materia de Protección de Datos Personales;
VIII. Dar vista al órgano de control interno u homólogo o 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; particularmente en casos relacionados con la declaración de inexistencia que realice el responsable.

Anualmente se presentará un informe, en las primeras dos semanas del mes de marzo de cada año y referirá al año inmediato anterior. Algunos de los elementos que pueden incluirse en el informe son:

- Estadística e información general sobre el cumplimiento de las obligaciones señaladas en el Programa de Protección de Datos Personales por parte de las unidades administrativas;
- Acciones realizadas por el Comité de Transparencia y la Unidad de transparencia para cumplir con las obligaciones específicas que establece el Programa de Protección de Datos Personales y
- Los resultados de las revisiones y auditorias.

Las unidades administrativas y la unidad de transparencia tendrán las funciones y responsabilidades que se describen en este programa.

Para que los objetivos planteados se logren con éxito, el programa requiere del apoyo e impulso del más alto nivel de la institución. En este sentido el programa se deberá hacer del conocimiento de su Directora General, a fin de que tome las medidas necesarias para que el mismo se observe en el CETRA.

La intervención de la Directora 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 77 y 78 de la Ley, al Comité de Transparencia en su carácter de máxima autoridad de datos personales en el CETRA.

Así mismo para que la implementación del programa de protección de datos personales tenga como resultado el cumplimiento integral de las obligaciones que establece la Ley y los Lineamientos Generales, el programa será de observancia obligatoria para todos los servidores públicos del CETRA, que en el ejercicio de sus funciones traten datos personales.

V. ALCANCE DEL DOCUMENTO DE SEGURIDAD

El presente documento será de observancia obligatoria para las unidades administrativas del CETRA y los servidores públicos adscritos a las mismas, que en el ejercicio de sus funciones traten datos personales, así como a las personas externas cuyos servicios contratados por el CETRA, estén relacionados con el tratamiento de estos.

El personal del CETRA que tenga acceso a los datos personales está obligado a conocer y aplicar el presente Programa y es aplicable en todas y cada una de las fases del tratamiento de los datos personales, iniciando desde la obtención de estos y finalizando con su eliminación.

El documento de seguridad se define como un instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales con que cuenta el CETRA.

Para ello, el artículo 29 de la Ley General establece los elementos mínimos que el documento de seguridad debe contener, siendo estos:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

El presente programa aplicará a todas las unidades administrativas que realicen tratamiento de datos personales en ejercicio de sus atribuciones, en ese sentido, en las páginas

siguientes, se abordará cada uno de los elementos que debe contener el documento de seguridad, con base en lo establecido en la Ley y demás disposiciones legales aplicables.

La Delegación Administrativa, el Área Jurídico Normativa, la Dirección de Planeación y Desarrollo, la Dirección de Registro y Asignación y la Unidad de Transparencia, cubrirán los principios, deberes y obligaciones de la Ley contenidos en los artículos 10, 11 y 12.

VI. SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES

El tratamiento de datos personales que realicen las unidades administrativas del CETRA, será a través del sistema de gestión que los sujetos responsables planifiquen, implementen, monitoreen y mejoren de manera continua, las medidas de seguridad administrativas, físicas y técnicas, conforme a lo establecido en la Ley General, la Ley y demás normatividad aplicable.

En este sentido, el responsable deberá monitorear y revisar las medidas de seguridad, supervisando lo siguiente:

- Nuevos activos
- Modificaciones necesarias
- Nuevas amenazas
- Posibilidad de nuevas vulneraciones
- Impacto de las amenazas valoradas, vulnerabilidades y riesgos
- Incidentes y vulneraciones de seguridad ocurridas.

Durante el ciclo de vida de los datos personales, el CETRA deberá contar con las versiones actualizadas de los inventarios de sistemas de tratamiento, avisos de privacidad simplificados e integrales y con el documento de seguridad institucional; documentos a través de los cuales se deberá garantizar el cumplimiento de los siguientes principios y deberes:

Principio de licitud: Implica que todo tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

Principio de finalidad: las finalidades del tratamiento de los datos personales deberán ser concretas a fin de no generar incertidumbre a las personas titulares de los datos personales; explícitas de modo que brinden claridad, acordes con los avisos de privacidad; lícitas al ser acordes con las atribuciones del responsable; y legítimas por contar con el consentimiento del titular de los datos. En el caso de que se requiera hacer un tratamiento distinto al de la finalidad para la cual se recabaron los datos personales se deberá considerar la expectativa razonable de privacidad de la persona titular basada en la relación que tiene con éste; la naturaleza de los datos, las consecuencias del tratamiento posterior de los datos personales para el titular y las medidas adoptadas para que el tratamiento posterior cumpla con las disposiciones previstas en la Ley General la Ley y demás normatividad aplicable.

Principio de lealtad: los datos personales no se deberán recabar por medios engañosos o fraudulentos; se privilegiarán los intereses de la persona titular para no dar lugar a discriminación o trato injusto; todos los datos personales recabados deberán de ser tratados conforme a lo señalado en los avisos de privacidad.

Principio de consentimiento: Consiste en el deber del responsable de recabar el consentimiento del titular, de manera libre, específica e informada.
Modalidades del consentimiento el consentimiento. Puede otorgarse por parte del titular de datos personales al Responsable en dos diferentes modalidades:

a) Expreso. - Se presenta cuando la voluntad del titular se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología aceptada.
b) Tácito. - Este tipo de consentimiento se da cuando habiéndose puesto a disposición del titular el aviso de privacidad, este no manifiesta su voluntad en sentido contrario. Por regla general será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente.

Tratándose de datos personales sensibles, el consentimiento que el responsable debe recabar será expreso y por escrito, esto es, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, según lo dispuesto en el artículo 15 párrafo cuarto de la Ley General.

Principio de calidad: Consiste en la obligación que tiene el responsable de adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que está tratando y se encuentren bajo su resguardo y posesión, a fin de que no se altere la veracidad de éstos y según se requiera para el cumplimiento de las finalidades concretas, explícitas lícitas y legítimas que motivaron su tratamiento.

Se presume que se cumple con él principio de calidad en los datos personales, cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario, según lo dispuesto en el artículo 17 párrafo primero de la Ley General.

Principio de proporcionalidad: consiste en la obligación que guarda el responsable de tratar única y exclusivamente los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad concreta, explícita lícita y legítima que justifica su tratamiento, según lo dispuesto en el artículo 19 de la Ley General.

Principio de información: Implica que el responsable deberá informar al titular a través del aviso de privacidad la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto, según lo dispuesto en el artículo 20, párrafo primero de la Ley General.

Por regla general, el aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que cuente el responsable. Para que el aviso de privacidad cumpla de manera eficiente con su función de informar, deberá estar redactado y estructurado de manera clara y sencilla, según lo dispuesto en el artículo 20, párrafos segundo y tercero de la Ley General.

Principio de responsabilidad: Es la obligación del responsable de adoptar los siguientes mecanismos de protección y seguridad en materia de tratamiento de datos personales:

I. Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales;
II. Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;
III. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
IV. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
V. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;
VI. Establecer procedimientos para recibir y responder dudas y quejas de las personas titulares;
VII. Diseñar, desarrollar e implementar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y
VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.

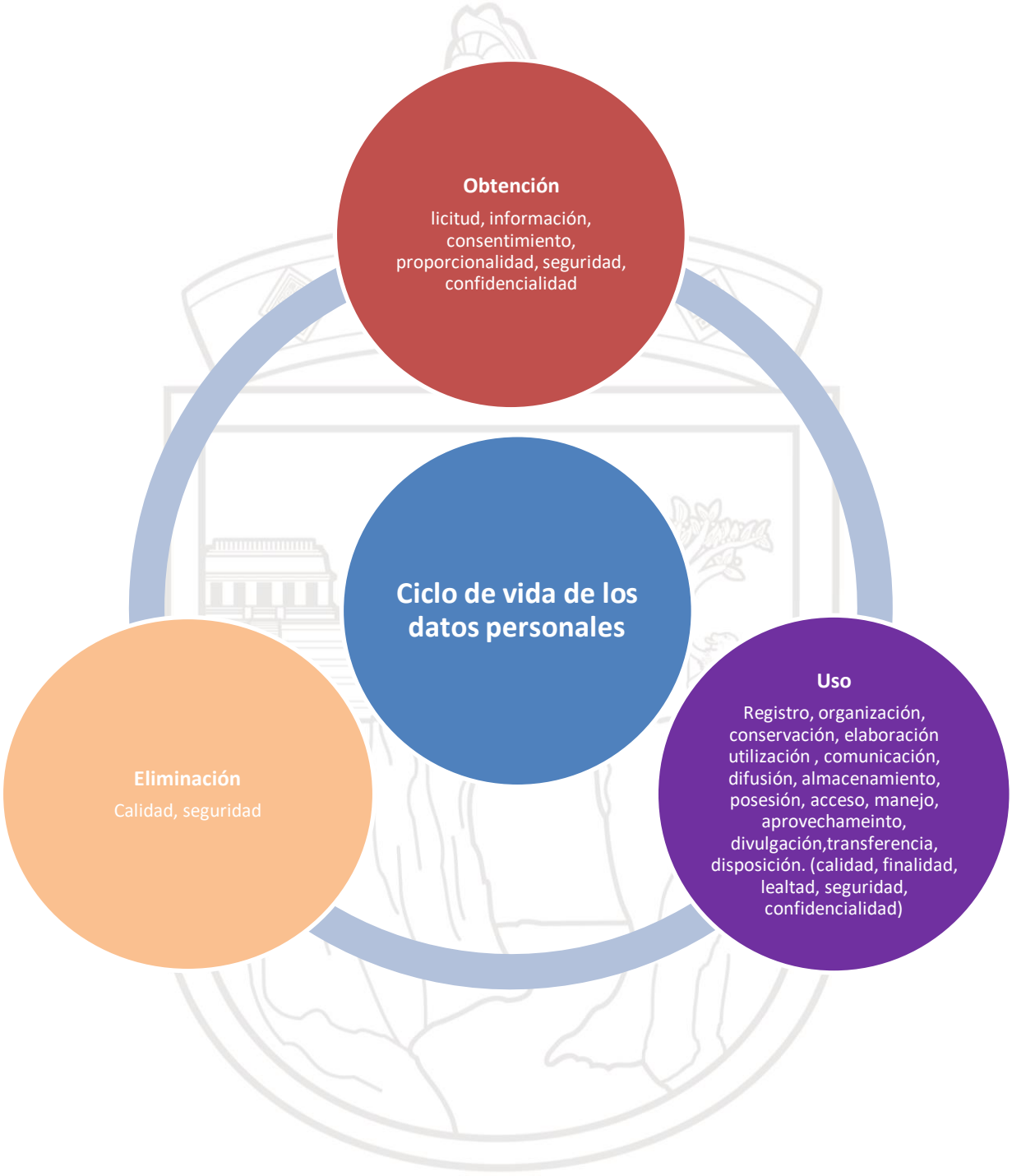
El deber de seguridad. - Implica que los titulares de los datos personales tengan el derecho a que la información personal que proporcionen a los responsables se resguarde bajo medidas de seguridad adecuadas, que eviten su pérdida, alteración, destrucción, daño o uso, acceso o tratamiento no autorizado.

En ese sentido, los responsables se encuentran obligados a resguardar los datos personales en bases de datos protegidas con medidas de seguridad administrativas, físicas o técnicas, según lo dispuesto en el artículo 25 de la Ley General.

El deber de confidencialidad. - Consiste en la obligación del responsable de establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo, según lo dispuesto en el artículo 36 de la Ley General.

Para ello, se identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las unidades administrativas del CETRA, de acuerdo con lo que establece la Ley General y según el ciclo de vida de los datos personales.

Desarrollo de la Política de Gestión de los Datos Personales



VII. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

Para poder verificar el cumplimiento de las obligaciones previstas en el artículo 29, fracción I, de la Ley General, es necesario contar con un diagnóstico de cada uno de los procesos que involucran tratamiento de datos personales. Este diagnóstico se realiza a través de la elaboración de un "inventario de tratamiento" de datos personales, el cual debe formar parte del documento de seguridad.

Para garantizar orden y precisión en los inventarios, se deben tener en consideración los elementos mínimos establecidos en los artículos 58 y 59 de los Lineamientos Generales.

Inventario de datos personales artículo 58, con relación a lo previsto en el artículo 29, fracción I de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:

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

Ciclo de vida de los datos personales en el inventario de estos, artículo 59. Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos Generales, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:

I. La obtención de los datos personales;
II. El almacenamiento de los datos personales;
III. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
V. El bloqueo de los datos personales, en su caso, y
VI. La cancelación, supresión o destrucción de los datos personales. El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo

de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar.

En ese sentido, las 4 unidades administrativas del CETRA, dan tratamiento a datos personales con lo que se integró un inventario, con el objeto de atender dicha disposición legal, con el apoyo y orientación de la unidad de transparencia y en el cual se señalan los tratamientos que actualmente se realizan siendo coincidentes con los avisos de privacidad elaborados y publicados en el Portal institucional del CETRA, específicamente, en https://cetra.chiapas.gob.mx/avisos-de-privacidad-2/

Las distintas secciones del inventario de tratamientos de datos personales del CETRA se conforman de la siguiente manera:

Medios de obtención de los datos personales	•Manera en la que los sujetos responsables obtienen los datos personales de los titulares. Puede ser de manera directa o indirecta.
Finalidad del tratamiento	• Motivos por los que el sujeto responsable solicita los datos personales. Las finalidades deben de ser concretas, lícitas, explicitasy legítimas.
Datos personales que se obtienen para el tratamiento	• Datos personales necesarios para que el sujeto obligado pueda dar atención al tratamiento. Se diferencian entre sensibles y no sensibles.
Medios de almacenamiento	• Medio en el que se almacenan los datos personales, puede ser en formato físico, electrónico o ambos
Servidores públicos con acceso al tratamiento	•Personas de los sujetos responsables que, conforme al ámbito de sus atribuciones, tratan los daots personales
Transferencia	• Los datos personales que, en su caso, pueden estar sujetos a una comunicación dentro o fuera del territorio mexicano realizada a persona distinta del titular, o del CETRA

Para el debido cumplimiento de las obligaciones que se establecen en este documento, fue necesario que cada una de las unidades administrativas realizaran un diagnóstico de los tratamientos de datos personales que llevan a cabo.

A partir de ello y como parte del proceso de mejora continua, la unidad de transparencia realizó, en coordinación con las áreas competentes, un estudio en donde se determinó la existencia de 21 tratamientos de datos personales.

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 el CETRA.

Por inventario de datos personales se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas del CETRA, las cuales realizan el tratamiento con una finalidad definida por sus funciones y en pleno ejercicio de sus facultades, tal y como se señala en el siguiente cuadro:

Unidad Administrativa	Tratamiento	Finalidad	Personas que tienen acceso
Dirección de Registro y Asignación	Cuestionario electrónico	A. serán recabados con fines estadísticos, para generar informes internos y/o los de carácter obligatorio del CETRA.	2
Dirección de Registro y Asignación	Generar Firmas electrónica al funcionariado	A. Sus datos personales serán recabados y tratados para la creación de su firma electrónica. B. Para el resguardo de los documentos personales, legales y/o administrativos que tengan relación directa con la creación de su firma electrónica.	2
Área Jurídico Normativa	Elaboración de convenios, contratos, acuerdos y demás actos jurídicos relacionados	Se le requerirá de información correspondiente a datos personales para la celebración y suscripción de documentos tales como convenios, contratos acuerdos y demás actos de la misma naturaleza.	2
Área Jurídico Normativa	Atención a solicitudes de Información pública y de Datos Personales	Para la atención y seguimiento de las solicitudes de información pública y de datos personales.	2

Área Jurídico Normativa	Recurso de revisión en materia de acceso a la información y datos personales	Para la atención y seguimiento de recursos de revisión.	1
Área Jurídico Normativa	Procedimientos administrativos y laborales seguidos en forma de juicio	A. Se requerirá de información correspondiente a datos personales para la práctica de actuaciones y diligencias a las que se hagan acreedores como trabajadores al servicio del CETRA, que permitan llegar a una resolución de carácter administrativo. B. Se requerirá información correspondiente a datos personales para la tramitación, desahogo y conclusión de procedimientos laborales, seguidos en forma de juicio C. Se requerirá información correspondiente a datos personales para la tramitación, desahogo y conclusión de procedimientos seguidos en forma de juicio en contra del CETRA D. Se requerirá información correspondiente a datos personales para la tramitación, desahogo y conclusión de	2

		procedimientos laborales, seguidos en forma de juicio promovidos por el CETRA	
Delegación Administrativa	Adquisiciones, arrendamiento de bienes muebles y contratación de servicios	A. Sus datos personales serán recabados de acuerdo a los procedimientos establecidos para la adquisición, arrendamiento de bienes muebles y contratación de servicios. B. Para la integración de los expedientes que se generen con motivo de la adquisición de bienes o servicios.	2
Delegación Administrativa	Certificado de seguro de vida	Se requerirá de información correspondiente a datos personales para el certificado de Seguro de Vida y el posterior cobro por el monto asegurado en caso de muerte como trabajador al servicio del CETRA.	2
Delegación Administrativa	Facturas	Se requerirá de información correspondiente a datos personales para la emisión de las facturas por la adquisición de un bien o servicio requerido por el CETRA	2
Delegación Administrativa	Resguardo de mobiliario y bienes informáticos	Se requerirá de información correspondiente a	2

		datos personales para el registro y control de los responsables del resguardo de mobiliario y bienes informáticos del CETRA.	
Delegación Administrativa	Viáticos	Se requerirá de información correspondiente a datos personales para justificar el pago de viáticos de las reuniones, cursos y/o eventos a los que deban asistir en el estado o a nivel nacional, como personal del CETRA.	2
Delegación Administrativa	Órdenes de pago	Se requerirá de información correspondiente a datos personales para realizar el pago de bienes o servicios que el CETRA requiera	2
Delegación Administrativa	Apertura de cuentas	Se requerirá de información correspondiente a datos personales para la apertura de cuentas bancarias que así lo requieran para el pago de bienes y servicios.	2
Delegación Administrativa	Expedientes del personal	Se requerirá de información correspondiente a datos personales para integrar y resguardar su expediente como personal al servicio del CETRA.	2

Delegación Administrativa	Control de puestos y plazas	A. Para el registro y control de puestos y plazas de personal que integra el CETRA. B. Para el resguardo de los documentos legales y/o administrativos que surjan de la relación laboral como personal del CETRA.	2
Delegación Administrativa	Registro en el Sistema de Nóminas de Gobierno del Estado de Chiapas	A. Se requerirá de información correspondiente a datos personales para integrar su expediente como personal de nuevo ingreso del CETRA, para su registro en el Sistema de Nóminas de Gobierno del Estado de Chiapas. B. para el resguardo de los documentos legales y/o administrativos que surjan de la relación laboral como personal del CETRA.	2
Delegación Administrativa	Control de asistencia	Se requerirá de información correspondiente a datos personales para el control de asistencia e incidencias (salidas, vacaciones, permisos y/o incapacidades) como personal del CETRA.	2
Delegación Administrativa	Descuentos	Se le requerirá de información	2

		correspondiente a datos personales para aplicar los descuentos por retardos o faltas de asistencia de acuerdo a la normatividad aplicable.	
Delegación Administrativa	Alta ante el Instituto Mexicano del Seguro Social	Para realizar su alta ante el Instituto Mexicano del Seguro Social (IMSS), como personal de nuevo ingreso del CETRA.	2

1) A continuación se describen las categorías de datos personales, que el **CETRA**, requiere, de acuerdo con el Catálogo de Datos Personales que cada Unidad Administrativa reportó, los cuales son:

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, datos de identificación oficial y referencias personales.
Datos biométricos: huella dactilar.
Datos laborales: Centro de trabajo, puesto o cargo que desempeña, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información generada durante los procedimientos de reclutamiento, selección, contratación.
Datos académicos: trayectoria educativa, título, cédula profesional, certificados y reconocimientos.
Datos patrimoniales y/o financieros: ingresos, egresos y cuentas bancarias, beneficiarios y declaraciones patrimoniales.
Datos legales: situación jurídica de la persona o de su representante (capacidad legal, estado de interdicción, juicios, procesos administrativos, entre otros)
Datos de salud: estado de salud físico presente y pasado, estado de salud mental presente y pasado.
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 **CETRA**.

b. Personas externas que prestan algún servicio para el **CETRA**, por adjudicaciones, contratos, seguros, fianzas, factura, resguardo de bienes, órdenes de pago.

c. Personas externas que participan en actividades como: capacitaciones, cursos, diplomados, registro de donadores voluntarios,
d. Personas con las que se sigan procedimientos administrativos o en forma de juicio.
e.
f. Servidores públicos que requieran firman electrónica.

g. Personas que deseen ejercer sus derechos de **ARCOP**

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

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

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

4) Transferencias de los datos personales:

Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 16 y 64 de la Ley.

Unidad administrativa:	Nombre de la unidad responsable del tratamiento al interior del CETRA.
Fecha de elaboración o última actualización:	Especificar la fecha a partir de la cual se realiza la modificación al tratamiento.
Nombre del tratamiento (proceso):	Nombre que refleje la finalidad para la cual son tratados los datos personales del sistema en cuestión.
Fundamento jurídico que habilita el tratamiento:	Disposición normativa que permite al CETRA realizar el tratamiento en cuestión.
Atribuciones de la unidad administrativa para realizar el tratamiento:	Disposición normativa que otorga atribuciones a la unidad administrativa responsable para realizar el tratamiento en cuestión.

Medio de obtención de los datos personales		
Señalar el o los medios a través de los cuales se obtienen los datos personales en este tratamiento. Si es más de un medio, se deberá indicar un medio por fila. (columna 1)	Describir el medio, por ejemplo, la fuente de acceso público, URL, domicilio, número telefónico, entre otros.	En caso de seleccionar la opción otros, especificar el medio de obtención.

Tercero que transfiere los datos personales, en su caso	Finalidades de la transferencia recibida, en su caso
Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar el nombre del tercero o terceros que realizan la transferencia.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar para qué finalidades se realiza dicha transferencia. Se deberá utilizar la misma fila por cada tercero que transfiere los datos personales.

Datos personales	Datos sensibles
Indicar cada uno de los datos personales que se tratan o sus categorías, uno por fila.	Señalar si el dato personal es sensible o no.

Formato de la base de datos	Ubicación base de datos	
Señalar el o los formatos en los que se encuentra la base de datos del tratamiento.	Señalar la ubicación de la base de datos. Si es más de uno, se deberá indicar uno por fila.	En caso de seleccionar la opción otro, especificar la ubicación.

Sección de archivos	Serie de archivos	Subserie de archivos
Indicar clave de identificación de la sección a la que corresponde el tratamiento, de conformidad con el Cuadro General de Clasificación Archivística.	Indicar clave de identificación de la serie a la que corresponde el tratamiento, de conformidad con el Cuadro General de Clasificación Archivística.	Indicar clave de identificación de la subserie a la que corresponde el tratamiento, de conformidad con el Cuadro General de Clasificación Archivística.

Finalidades del tratamiento	¿Requiere consentimiento?	Supuesto del artículo 22 que se actualiza, en su caso	Tipo de consentimiento
Indicar cada una de las finalidades del tratamiento, las cuales deberán ser explícitas y concretas. Una	Indicar si la finalidad requiere o no el consentimiento del titular.	En caso de que la finalidad no requiera el consentimiento del titular, señalar el o los supuestos del artículo 18 de la Ley que se actualizan.	En caso de que la finalidad requiera el consentimiento del titular, señalar el tipo de consentimiento que se necesita.

Servidores públicos que tienen acceso a la base de datos	Área de adscripción	Finalidad del acceso
Señalar los puestos de las personas servidoras públicas que tienen acceso a la base de datos del tratamiento correspondiente. Uno por fila.	Definir unidad administrativa a la que está adscrito el puesto.	Señalar con qué fines tienen acceso las personas servidoras públicas antes identificados. Uno por fila, según corresponda.

¿Se realizan transferencias?	Tercero al que se transfieren los datos personales, en su caso	Finalidades de la transferencia	Requiere consentimiento para su transferencia
Señalar si se realizan o no transferencias en el marco del tratamiento.	Señalar el nombre, razón o denominación social de los terceros a los que se transfieren los datos personales, cuando ello sea posible, o bien, su categoría. Uno por fila.	Señalar las finalidades para las cuales se transfieren los datos personales por cada uno de los terceros.	Señalar si la transferencia requiere o no consentimiento.

Supuestos artículos 18 y 95 que se actualizan, en su caso	Tipo de consentimiento que se requiere para la transferencia	¿La transferencia requiere la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico?	Supuesto del artículo 95 de la Ley que se actualiza, en su caso
En caso de que la transferencia no requiera consentimiento, señalar los supuestos que se actualizan.	En caso de que la finalidad de la transferencia requiera el consentimiento del titular, señalar si se requiere el tácito o el expreso y por escrito.	Indicar si la transferencia requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, según el artículo 66 de la Ley.	Señalar el supuesto que en su caso se actualiza, si no se requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico.

Difusión de los datos personales	Fundamento jurídico para la difusión
Indicar si en el tratamiento se realiza la difusión de los datos personales.	Indicar el fundamento jurídico que ordena la difusión de los datos personales.

Plazo de conservación	Bloqueo	Observaciones
Señalar el plazo de conservación de los datos personales, de conformidad con lo establecido en el Cuadro General de Clasificación Archivística..	Señalar periodo en el que estarán bloqueados los datos personales.	Espacio libre para hacer aclaraciones y precisiones.

VIII. FUNCIONES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES.

Las Unidades Administrativas encargadas de tratar datos personales son:

- Delegación Administrativa
- Dirección de Registro y Asignación
- Dirección de Planeación y Desarrollo
- Área Jurídico Normativa, y
- Unidad de transparencia.

Las personas que desempeñan los puestos anteriormente mencionados, tienen como funciones y obligaciones las siguientes:

a. Garantizar la seguridad en el tratamiento de datos personales, esto con la finalidad de evitar algún riesgo, como la pérdida, robo, alteración o acceso no autorizado.
b. Garantizar la debida protección de los datos personales, conforme a la Ley y las demás disposiciones aplicables en la materia.
c. Implementar medidas de seguridad físicas, técnicas y administrativas convenientes para el tratamiento diario de los datos personales.
d. Garantizar la confidencialidad de los datos personales derivada de los procedimientos que tienen a su cargo.
e. Conocer y aplicar las acciones derivadas de este Documento de Seguridad.

f. Garantizar el cumplimiento de los derechos ARCOP a los titulares de los datos personales

El personal que labora en el Centro Estatal de Trasplantes del Estado de Chiapas que por razón de sus funciones deba tratar con datos personales, deben brindar el adecuado tratamiento y protección mismos que para efectos del presente, se refieren a continuación:

Responsable: La persona titular del sujeto responsable.
Enlace: La persona designada por el responsable para la administración y custodia de los datos personales recabados.
Usuario: La persona que, por sus actividades laborales y atribuciones legales, tenga acceso a los datos personales.

Para tal efecto, las funciones y obligaciones mínimas que deberán atender quienes conforme a sus atribuciones realicen el tratamiento de datos personales en cada sujeto responsable, son las siguientes:

Tipo	Funciones	Obligaciones
Responsable	1. Comunicar al personal del sujeto responsable el contenido del documento de seguridad. 2. Observar los principios y deberes establecidos en la Ley de la materia para el adecuado tratamiento de los datos. 3. Incentivar la capacitación del personal. 4. Establecer canales de comunicación con la Unidad de transparencia, a fin de obtener asesoría u orientación sobre el tratamiento de datos personales.	1. Coordinar la implementación de medidas de seguridad para el tratamiento de datos. 2. Verificar que los accesos a los sistemas de información garanticen niveles de seguridad adecuados. 3. Comunicar al responsable designado conforme al art. 85 de la Ley General las vulneraciones de datos que se hayan suscitado. 4. Autorizar la realización de copias de respaldo y/o recuperación de los datos personales. 5. Informar, por lo menos una vez al año, al responsable designado conforme al art. 85 de la Ley General respecto de nuevos tratamientos de datos o de la actualización de

		medidas de seguridad implementadas.
Enlace	1. Observar los principios y deberes establecidos en la Ley de la materia para el adecuado tratamiento de los datos. 2. Velar para que se realice un adecuado tratamiento de los datos personales, conforme a los principios y deberes establecidos en la Ley. 3. Fungir como enlace con la Unidad de transparencia. 4. Proponer al responsable, la implementación y o actualización de medidas de seguridad, así como el desarrollo o adopción de esquemas de mejores prácticas, conforme a las disposiciones legales aplicables.	1. Supervisar la implementación de medidas de seguridad para el tratamiento de datos. 2. Llevar una bitácora de los accesos a los datos personales con que cuentan. 3. Informar al responsable de las vulneraciones suscitadas. 4. Elaborar el informe que el responsable debe remitir al responsable designado conforme al art. 85 de la Ley General. 5. Remitir a la Unidad de transparencia el inventario de tratamiento de datos personales, cuando esta lo solicite, se realice un nuevo tratamiento de datos o se actualicen las medidas de seguridad. 6. Mantenerse actualizado en los cursos, talleres o programas de capacitación relacionados con la materia.
Usuario	1. Observar los principios y deberes establecidos en la ley de la materia para el adecuado tratamiento de los datos. 2. Conocer las implicaciones legales y administrativas que conlleva el tratamiento indebido o no autorizado de datos personales.	1. Utilizar los datos personales a los que tenga acceso, únicamente para el desempeño de sus atribuciones. 2. Guardar secreto y confidencialidad de los datos a los cuales tenga acceso.

	3. Proponer la implementación de medidas de seguridad o esquemas de mejores prácticas que, en su caso, estime necesarias.	3. Abstenerse de borrar, destruir, dañar, alterar, sustraer, modificar o divulgar cualquier información relacionada con datos personales, sin que tenga la debida autorización expresa para ello. 4. Informar sobre cualquier anomalía, error, imprecisión o fallo que detecten en los datos a los cuales tengan acceso.

Cada uno de los responsables según el ámbito de su competencia están obligados a generar sus avisos de privacidad previa al inicio de cada tratamiento, para lo cual la Unidad de transparencia del Centro Estatal de Trasplantes del Estado de Chiapas será la encargada de auxiliar y orientar a los responsables en el proceso de elaboración de los avisos de privacidad para su posterior aprobación del Instituto de Transparencia Acceso a la Información Pública y Protección de Datos Personales del Estado de Chiapas.

IX. EL PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE LAS MEDIDAS DE SEGURIDAD.

Una vez identificados los factores de riesgo de los datos personales objeto de tratamiento por parte de los responsables del CETRA, y con el análisis de brecha en donde se han identificado las medidas de seguridad faltantes que conlleve a garantizar la seguridad y confidencialidad se presentan las acciones a desarrollar conforme a lo siguiente:

1. [redacted]
2.
3.
4.
5.
6.

7. [redacted]
8.

ACCIÓN	ENCARGADO	TEMPORALIDAD
1	Unidad de transparencia	Permanente
2	Unidad de transparencia	Permanente
3	Comité de Transparencia	Anual
4	Unidad de transparencia	Permanente
5	Área de archivo y Dirección de Registro y Asignación	Anual
6	Unidad de transparencia y Dirección de Registro y Asignación	Permanente
7	Unidad de transparencia	Anual
8	Cada titular de Área Administrativa que recabe datos personales	Permanente

X. ANÁLISIS DE RIESGO.

El presente análisis identifica el riesgo inherente a los datos personales en el tratamiento que reciben por el CETRA al ejercer sus atribuciones, de manera que pueda ser controlado por la institución para satisfacer el derecho humano a la autodeterminación informativa. La Ley General establece la necesidad de contar con un análisis de los riesgos a los cuales se puede enfrentar el tratamiento de los datos personales durante su ciclo de vida; para muestra, en el documento denominado Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales, emitidas por el INAI, se indican los incidentes más comunes:

1. [redacted]
2.
3.
4.
5.

Los Lineamientos Generales de Protección de Datos Personales para el Sector Público, emitidos por INAI, indican en su artículo 60 que el análisis de riesgos de los datos personales tratados debe contemplar los siguientes aspectos:

- Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.
- El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.
- El valor y exposición de los activos involucrados en el tratamiento de los datos personales.
- Las consecuencias negativas para los titulares de los datos personales, que puedan derivar en una vulneración de seguridad.
- El riesgo inherente, la sensibilidad, las posibles consecuencias de vulneración para los titulares, las transferencias y vulneraciones previas ocurridas sobre los datos personales, así como el número de titulares de éstos y el riesgo por su valor potencial, además del desarrollo tecnológico.

La Ley General en sus artículos 32, fracción I, y 33, fracción IV, 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 General, la valoración de los riesgos de los datos personales forma parte de los elementos mínimos que debe contener el instrumento que describe y da cuenta, en lo general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas (Documento de seguridad), en este caso, por el CETRA, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de ese tipo de datos bajo su posesión. Aunado a lo anterior,

Los factores a considerar en el análisis de riesgos son los señalados en el Artículo 32 de la Ley General, esto es:

I. [redacted]
II.
III.
IV.
V.
VI.
VII.
VIII.

En el CETRA se considera como vulneraciones comunes las siguientes:

[redacted]

Por su parte, los datos personales contenidos en un sistema electrónico presentan riesgos por su propia naturaleza [redacted]

XI. ANÁLISIS DE BRECHA.

Las Unidades Administrativas del CETRA, analizaron las medidas de seguridad existentes, así como aquellas que podrían implementarse para la protección de datos personales. Las cuales se expresan en la tabla siguiente:

Medidas implementadas	Medidas faltantes
[redacted]	

XII. MEDIDAS DE SEGURIDAD

Medidas de Seguridad Administrativas

A. [redacted]

B.

C.

D.

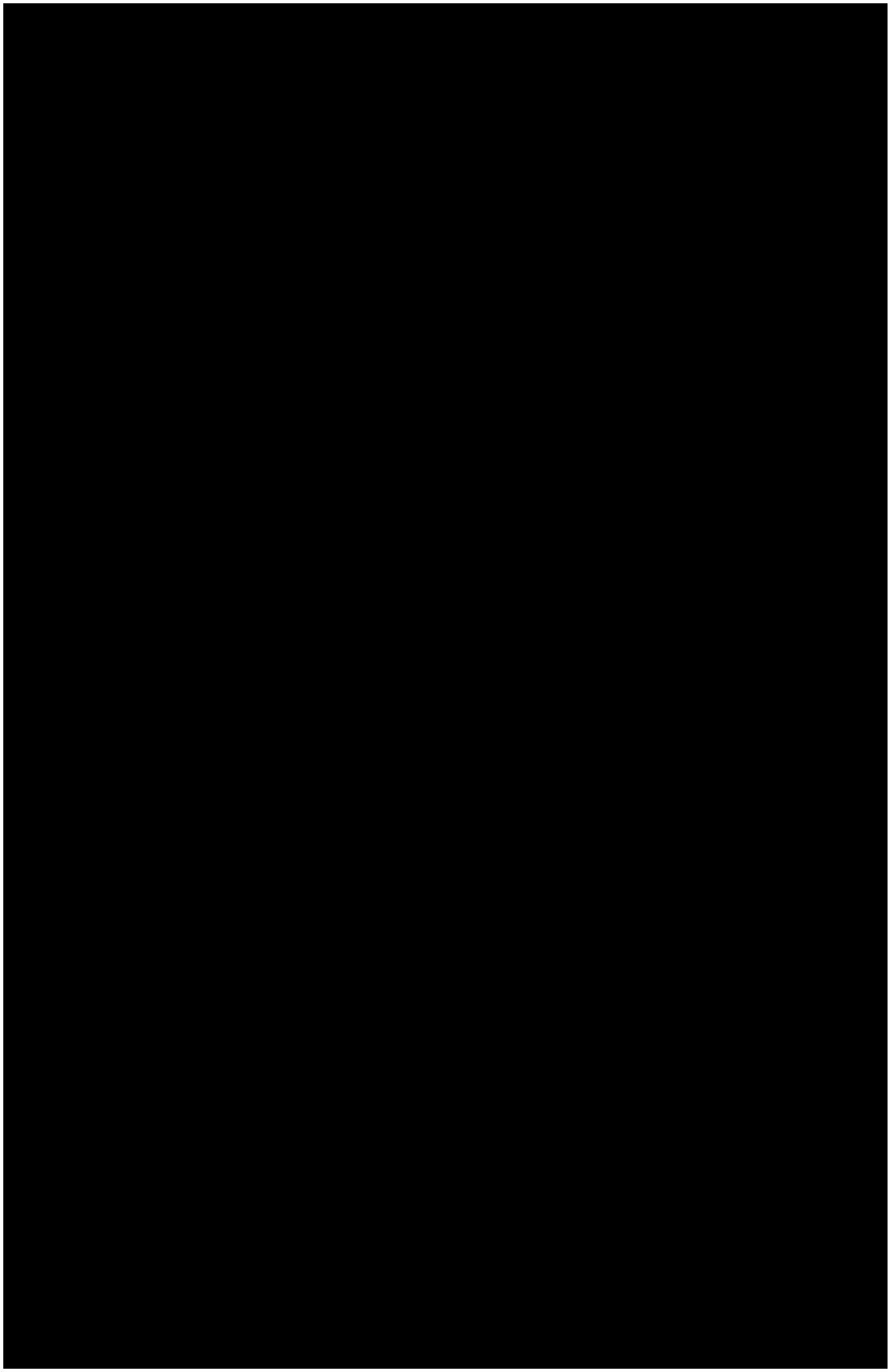
E.

F.

G.

H.

I.



J. [redacted]

K.

Medidas de seguridad físicas

A. [redacted]

B.

C.

D.

Medidas de Seguridad Técnicas

A. [redacted]

B.

C.

D. [redacted]

E.

F.

G.

H.

I.

J.

XIII. MONITOREO DE LAS MEDIDAS DE SEGURIDAD

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

1. [redacted]

2. [redacted]

3. [redacted]

4. [redacted]

5. Vigilar que el ingreso de personas sea a través de los accesos correspondientes, plenamente identificados.

XIV. PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

El personal de la Dirección de Datos Personales capacitará al personal del ICAI en materia de protección de datos personales una vez 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 Administrativas tenga la necesidad de capacitación, se solicitará la programación del curso.

XV. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD.

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

Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.

Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.

Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad, e

Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Cuando surjan documentos, formatos, recomendaciones, etc. por parte del Transparencia para el Pueblo para la mejora del documento de seguridad