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

FEBRERO 2023

ÍNDICE

I. PRESENTACIÓN.....3

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

III. GLOSARIO DE TÉRMINOS.....4

IV. RESPONSABILIDADES DENTRO DEL PROGRAMA.....6

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.....12

VIII. FUNCIONES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES.....19

IX. PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD.....25

X. ANÁLISIS DE RIESGO.....26

XI. ANÁLISIS DE BRECHA.....29

XII. MEDIDAS DE SEGURIDAD.....31

XIII. MONITOREO DE MEDIDAS DE SEGURIDAD.....35

XIV. PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES.....35

XV. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD.....36

I. PRESENTACIÓN.

La Protección de los Datos Personales garantiza la protección de la vida privada e intimidad de las personas y garantiza que el tratamiento que estos reciban sea el adecuado como usuarios de un servicio o trámite o como parte del quehacer laboral, académico o empresarial, entre otros.

Por tal razón en 2007, se realizaron reformas a la Constitución para regular este derecho, adicionando un segundo párrafo con siete fracciones al artículo 6°, 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 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.

En 2016, se reformaron los artículos 16 y 73 Constitucionales, estableciendo 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 1°, 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 y 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 manejan.

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 artículo 49 y 50 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, publicada en el Periódico Oficial Número 315, de fecha 30 de agosto de 2017.

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 así como las 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 CETRA;

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, 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 e identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición 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.

INAI: Instituto Nacional de Acceso a la Información Pública y Protección de Datos Personales.

ITAIPCH: Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Chiapas.

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

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 113 y 114 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. Aprobar, supervisar y evaluar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley y demás disposiciones que resulten aplicables en la materia;

II. Coordinar, realizar y supervisar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del

responsable, de conformidad con las disposiciones previstas en la presente Ley y en las que resulten aplicables en la materia, en coordinación con el oficial de protección de datos personales, en su caso;

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

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

V. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y demás criterios que resulten aplicables en la materia;

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

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

VIII. Establecer programas de capacitación y actualización para los servidores públicos, en materia de protección de datos personales;

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

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

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

- Acciones realizadas por el Comité de Transparencia y la Unidad de Transparencia para cumplir con las obligaciones específicas que establece el Programa de Protección de Datos Personales 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 Centro Estatal de Trasplantes del Estado de Chiapas.

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 113 y 114 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 General, Ley y los Lineamientos Generales.

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 que trata el CETRA.

Para ello, el artículo 35 de la Ley General y 50 de la Ley, establecen los elementos mínimos que el documento de seguridad debe contener, siendo estos:

I. Inventario de datos;

II. Funciones y obligaciones de las personas que tratan datos;

III. Análisis de riesgos;

IV. Análisis de brecha;

V. Plan de trabajo;

VI. Mecanismos de revisión y monitoreo de las medidas de seguridad y,

VII. Programa general de capacitación.

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, como complemento, en lo dispuesto por los Lineamientos Generales y los documentos de apoyo publicados por el INAI.

La Delegación Administrativa, la Dirección de Registro y Asignación, el Área Jurídico Normativa, y la Unidad de transparencia, cubrirán los principios, deberes y obligaciones de la Ley contenidos en los artículos 12, 13 y 14.

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, los Lineamientos Generales 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:

Principio de licitud: el tratamiento de los datos personales será exclusivo de las facultades del responsable.

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 y los Lineamientos Generales.

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: se recabará el consentimiento del titular, de manera libre, específica e informada.

Principio de calidad: los datos personales deberán ser exactos y correctos, completos y actualizados.

Principio de proporcionalidad: los datos recabados deberán de ser estrictamente los necesarios, apropiados e indispensables y no excesivos para el cumplimiento de las finalidades.

Principio de información: se deberán comunicar, por medio del aviso de privacidad, las características de los tratamientos a los que se someterán los datos personales.

Principio de responsabilidad: adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en 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 en el CETRA

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

Para poder verificar el cumplimiento de las obligaciones previstas en el artículo 35, fracción I, de la Ley General y 50 fracción I, de la Ley, 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 33, fracción III de la Ley General, 47 fracciones II de la Ley, 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, 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, son 3 unidades administrativas del CETRA, que manifestaron dar tratamiento a datos personales con lo que se integró un inventario, con el objeto de atender dicha disposición legal, ello, 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 los cuales deberán publicarse en el Portal institucional del CETRA, específicamente, en https://cetra.chiapas.gob.mx/avisos.html.
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 datos 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, del responsable o encargado.

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 22 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	Fundamento legal
Dirección de Registro y Asignación	Registro de donadores voluntarios	A. Serán recabados y tratados para crear un banco de información de donadores voluntarios B. Serán recabados y tratados con fines estadísticos	2	Artículo 20 fracción III del reglamento Interior del CETRA
Dirección de Registro y Asignación	Generar Firmas electrónica al funcionariado	A. 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	Artículo 20 fracción XI del reglamento Interior del CETRA
Dirección de Registro y Asignación	Cuestionario electrónico	Serán recabados con fines estadísticos, para generar informes internos y/o los de carácter obligatorio del CETRA	2	Artículo 20 fracción V del reglamento Interior del CETRA

Área Jurídico Normativa	Elaboración de contratos, convenios, acuerdos	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	Artículo 18 fracción IV del reglamento Interior del CETRA
Área Jurídico Normativa	Procedimientos administrativos, laborales y judiciales seguidos en forma de juicio	Se le requerirá información correspondiente a datos personales para la tramitación, desahogo y conclusión de procedimientos laborales, seguidos en forma de juicio promovidos por el CETRA o en contra de este.	2	Artículo 18 fracciones I y VII del reglamento Interior del CETRA
Área Jurídico Normativa (Unidad Transparencia)	Atención a solicitudes de Información y de Datos Personales	Para la atención y seguimiento de las solicitudes de información pública y de datos personales.	2	Artículo 20 fracción III del reglamento Interior del CETRA
Área Jurídico Normativa (Unidad de Transparencia)	Recurso de revisión	Para la atención y seguimiento de recursos de revisión.	1	Artículo 18 fracción II del reglamento Interior del CETRA
Delegación Administrativa	Adjudicaciones	Serán recabados de acuerdo a los procedimientos establecidos para adjudicación. Para la integración de los expedientes que se generen con motivo del servicio acordado.	2	Artículo 17 fracción XVI del reglamento Interior del CETRA
Delegación Administrativa	Contratos	Se le requerirá de información correspondiente a datos personales para la celebración y suscripción de contratos	2	Artículo 17 fracción III del reglamento Interior del CETRA

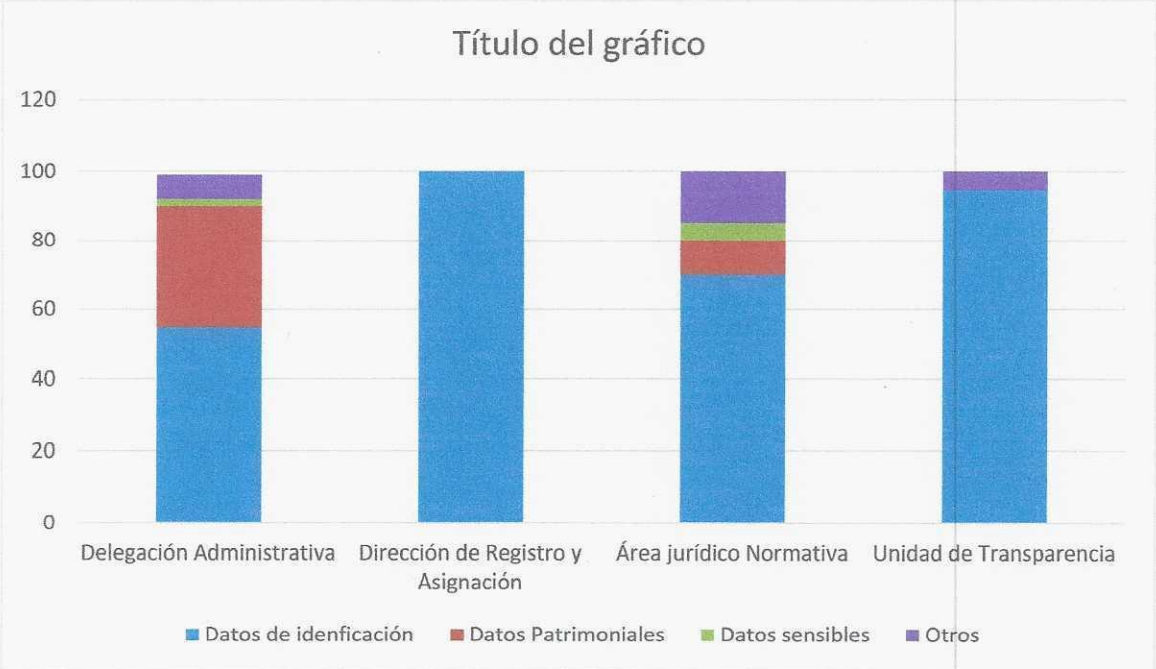
Delegación Administrativa	Seguros y Fianzas	A. Para los seguros y fianzas se le requerirá de información correspondiente a datos personales derivado de los procedimientos de adquisiciones de bienes o servicios. B. Se le requerirá de datos personales para la tramitación del seguro de vida.	2	Artículo 17 fracción XVI del reglamento Interior del CETRA
Delegación Administrativa	Facturas	Para la adquisición de un bien o servicio requerido para el cumplimiento de las funciones del CETRA.	2	Artículo 17 fracción XVI del reglamento Interior del CETRA
Delegación Administrativa	Resguardo de bienes	Para la contratación de proveedores, pedidos, órdenes de servicios que serán utilizados para la integración de os expedientes que se elaboren con motivo de los servicios prestados	2	Artículo 17 fracción XVII del reglamento Interior del CETRA
Delegación Administrativa	Comités y Subcomités de Adquisiciones, Arrendamientos y Servicios	Para la contratación de proveedores, pedidos, órdenes de servicios que serán utilizados para la integración de los expedientes que se elaboren con motivo de los servicios prestados al CETRA.	2	Artículo 17 fracción XVII del reglamento Interior del CETRA
Delegación Administrativa	Viáticos	Para la justificación de viáticos para las reuniones, cursos y/o eventos a los que deban asistir en el estado o a nivel nacional, como personal del CETRA.	2	Artículo 17 fracción I del reglamento Interior del CETRA
Delegación Administrativa	Ordenes de pago	Para realizar el pago por la adquisión de	2	Artículo 17 fracción XVI del

		bienes o servicios que el CETRA requiera		reglamento Interior del CETRA
Delegación Administrativa	Bancos	Para la apertura de cuentas bancarias derivado de los procedimientos para el pago de bienes y servicios que el CETRA, requiera.	2	Artículo 17 fracción XVI del reglamento Interior del CETRA
Delegación Administrativa	Expedientes del personal	Para integrar su expediente como personal del CETRA.	2	Artículo 17 fracción I del reglamento Interior del CETRA
Delegación Administrativa	Registro y control de puestos y plazas	Para el registro y control de puestos y plazas integran el CETRA.	2	Artículo 17 fracción II del reglamento Interior del CETRA
Delegación Administrativa	Nómina	Para el resguardo de los documentos legales y/o administrativos que surjan de la relación laboral como personal del CETRA.	2	Artículo 17 fracción XI del reglamento Interior del CETRA
Delegación Administrativa	Control de asistencia	Para el registro de asistencia de entradas y salidas, como personal del CETRA	2	Artículo 17 fracción I del reglamento Interior del CETRA
Delegación Administrativa	Descuentos	Para aplicar los descuentos por retardos o faltas de asistencia de acuerdo a la normatividad aplicable	2	Artículo 17 fracción XI del reglamento Interior del CETRA
Delegación Administrativa	IMSS	Para realizar su alta ante el Instituto Mexicano del Seguro Social (IMSS), como personal de nuevo ingreso del CETRA.	2	Artículo 17 fracción I del reglamento Interior del CETRA

Los datos mencionados en la tabla corresponden a los tratamientos realizados por el CETRA, de los cuales 15, realiza la Delegación Administrativa; 3, la Dirección de Registro y Asignación; 2, el Área jurídico Normativa y 2 la Unidad de Transparencia. Asimismo en todos se solicitan

datos personales de identificación y solo la Delegación Administrativa y el Área Jurídico Normativa, solicitan datos sensibles tal y como se representa en la siguiente gráfica.

Datos Personales solicitados por unidad administrativa



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: 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, información de dependientes económicos.

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, antecedentes laborales.

Datos académicos: trayectoria educativa, título, cédula profesional, certificados.

Datos patrimoniales y/o financieros: Cuenta bancaria, Clabe bancaria estandarizada, ingresos, egresos, beneficiarios, descuentos personales y declaraciones patrimoniales.

Datos legales: situación jurídica de la persona y de su representante, documento que acredite su personalidad como titular 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**.

c. Personas externas que participan en actividades como: capacitaciones, cursos, diplomados, que requieran firman electrónica, registrarse como donadores voluntarios, ejercer sus derechos de **ARCO**, adjudicaciones, contratos, seguros, fianzas, facturas, resguardo de bienes, órdenes de pago, procedimientos seguidos en forma de juicio.

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 18 y 95 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 de la 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

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 18 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 por fila.	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, y
- Área Jurídico Normativa, (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 ARCO 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 y 117 de la Ley 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 y 117 de la Ley, 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	1. Supervisar la implementación de medidas de seguridad para el tratamiento de datos.

	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.	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 debe remitir al responsable designado conforme al art. 85 de la Ley General y 117 de la Ley. 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. Abstenerse de borrar, destruir, dañar, alterar, sustraer, modificar o

	3. Proponer la implementación de medidas de seguridad o esquemas de mejores prácticas que, en su caso, estime necesarias.	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 la 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 conlleven a garantizar la seguridad y confidencialidad se presentan las acciones a desarrollar conforme a lo siguiente:

1. Promover e impulsar la capacitación en materia de protección de datos personales a todos los sujetos responsables para abatir la falta de conocimiento por parte del personal de nuevo ingreso;

2. Identificar necesidades de capacitación en temas específicos en la implementación de la Ley, como lo pueden ser: Obligaciones de la protección de datos personales; elaboración de avisos de privacidad y establecimiento de medidas de seguridad;

3. Aprobar el Programa de Capacitación;
4. Proponer la implementación de políticas de traslado seguro de la información en la cual se contienen datos personales mediante medidas de seguridad que eviten la vulneración de la información;

5. Impulsar la generación de procesos de digitalización de información que contiene datos personales;

6. Sensibilizar sobre la importancia de la generación de copias de respaldo de la información que contiene datos personales para minimizar el posible daño por pérdida de estos por razones de causas naturales o casos fortuitos;

7. Actualizar el inventario de datos personales para la posible detección de nuevos tratamientos o la modificación de estos:

8. Promover la revisión periódica de las medidas de seguridad a efecto de identificar posibles deficiencias en sus procesos de implementación; para lo cual el sujeto responsable remitirá, por lo menos una vez al año, un informe al responsable designado conforme al art. 85 de la Ley General y 117 de la Ley, que dé cuenta de esta revisión.

En relación con lo anterior, a continuación, se presenta el Plan de Trabajo a desarrollarse:

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 RIESGOS.

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. Robo de información en documentos y medios de almacenamiento desechados incorrectamente;

2. Empleados que acceden a datos personales sin la autorización correspondiente;

3. Empleados que revelan información a otras personas a través de engaños;

4. Robo o pérdida de equipos de cómputo, laptops, teléfonos inteligentes, tabletas, o memorias extraíbles con información personal, y;

5. Acceso ilegal a las bases de datos personales por un externo.

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,

[redacted]

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

En el CETRA se considera como vulneraciones comunes, por lo que hace a los datos personales que [redacted]

- [redacted]

Por su parte, los datos personales contenidos [redacted] presentan riesgos por su propia naturaleza como lo son:

- [redacted]

[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:

Análisis de Brecha		
Área Jurídico Normativa		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
1. Elaboración de contratos, convenios, acuerdos	Clasificación de los archivos físicos Clasificación de los archivos electrónico [redacted]	[redacted]
2. Procedimientos administrativos, laborales y judiciales seguidos en forma de juicio	Clasificación de los archivos físicos Clasificación de los archivos electrónico [redacted]	[redacted]
Unidad de transparencia		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
1. Atención a solicitudes de Información y de Datos Personales	Clasificación de los archivos físicos Clasificación de los archivos electrónico [redacted]	[redacted]
2. Recurso de revisión	Clasificación de los archivos físicos Clasificación de los archivos electrónico [redacted]	[redacted]

Análisis de Brecha		
Dirección de Registro y Asignación		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
Registro de donadores voluntarios	[redacted]	[redacted]

Generar Firmas electrónica al funcionariado	[redacted]	[redacted]
Cuestionario electrónico	[redacted]	[redacted]

Análisis de Brecha		
Delegación Administrativa		
Tratamiento	**Medidas implementadas**	**Medidas faltantes**
1.- Adjudicaciones	Clasificación física de la información procesada. Archivos electrónicos de la información procesada. [redacted]	[redacted]
2.- Contratos	Clasificación física de la información procesada. Archivos electrónicos de la información procesada.	[redacted]
3.- Seguros y Fianzas	Clasificación física de la información procesada. Archivos electrónicos de la información procesada.	[redacted]
4.- Facturas	Clasificación física de la información procesada. Archivos electrónicos de la información procesada.	[redacted]
5.- Resguardo de bienes	Clasificación física de la información procesada. Archivos electrónicos de la información procesada. [redacted]	[redacted]
6.- Comités y Subcomités de Adquisiciones, Arrendamientos y Servicios	Clasificación física de la información procesada. Archivos electrónicos de la información procesada.	[redacted]
7.- Viáticos	Clasificación física de la información procesada. Archivos electrónicos de la información procesada.	[redacted]

8.- Ordenes de pago	Clasificación física de la información procesada. Archivos electrónicos de la información procesada.	[redacted]
9.- Bancos	Clasificación física de la información procesada. Archivos electrónicos de la información procesada.	[redacted]
10.- Expedientes del personal	Clasificación física de la información procesada. Archivos electrónicos de la información procesada.	[redacted]
11.- Registro y control de puestos y plazas	Clasificación física de la información procesada. Archivos electrónicos de la información procesada.	[redacted]
12.- Nómina	Clasificación física de la información procesada. Archivos electrónicos de la información procesada.	[redacted]
13.- Control de asistencia	Clasificación física de la información procesada. Archivos electrónicos de la información procesada.	[redacted]
14.- Descuentos	Clasificación física de la información procesada. Archivos electrónicos de la información procesada.	[redacted]
15.- IMSS	Clasificación física de la información procesada. Archivos electrónicos de la información procesada.	[redacted]

XII.MEDIDAS DE SEGURIDAD

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

Medidas de Seguridad Administrativas.

1. **Capacitación:** El personal involucrado en el tratamiento de los datos personales deberá asistir a los cursos de capacitación implementados por el Comité de Transparencia.

2. **Clasificación de los archivos físicos:** Identificar o incluir la base de datos en soporte físico en el Catálogo de Disposición Documental para tener control del ciclo de vida a que deben estar sujetos los archivos administrativos.

3. [redacted]

4. **Bitácora de vulneraciones:** Implementar un control informativo en donde se reporten los tipos de vulneraciones con los siguientes datos: fecha y lugar en donde se produjo, nombre y cargo de quien notifica la incidencia, nombre y cargo de la persona a la que se le comunica, y las medidas que se implementaron para subsanar la misma. Toda vulneración deberá notificarse, también, a la Unidad de Transparencia para que tome las acciones pertinentes. Si la vulneración trasciende a una posible afectación directa de los titulares de los datos personales, especialmente en sus derechos patrimoniales o en su esfera más íntima (datos sensibles), se deberá notificar a los titulares afectados para que tomen las medidas pertinentes para la defensa de sus derechos.

5. [redacted]

6. [redacted] en desuso o que hayan cumplido su finalidad o el tiempo de conservación dispuesto para el archivo administrativo. Solicitar a Dirección de Registro y Asignación que proporcione un programa para el borrado integral de la información, o en su defecto, reinicio de los equipos o medios de almacenamiento a los valores de origen. Además, [redacted]

7. **Clasificación de los archivos electrónicos:** Identificar y etiquetar las bases de datos en soporte electrónico con el nombre del Tratamiento de Datos Personales conforme al Inventario reportado por el área.

8. **Responsable de seguridad:** designar un responsable de seguridad para coordinar y verificar las medidas de seguridad establecidas en el Documento de Seguridad.

9. **Transferencias:** realizar transferencias con las medidas de confidencialidad necesarias. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.

Medidas de seguridad físicas

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

Medidas de Seguridad Técnicas.

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

2. [redacted]

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

4. Utilizar el correo electrónico para fines relacionados con las actividades laborales, evitando remitir datos personales.

5. [redacted]

6. No difundir, transmitir o compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.

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

8. 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 los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.

9. 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.

10. Notificar las bajas de accesos a los sistemas de información o de tratamiento de datos personales, con oportunidad, para restringir el acceso a dichos datos por personal no autorizado.

[redacted]

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

XIV. MONITOREO DE LAS MEDIDAS DE SEGURIDAD.

Las medidas de seguridad administrativas, físicas y técnicas serán de aplicación obligatoria a todas las bases de datos personales que manejan las personas a cargo de la Delegación Administrativa, Dirección de Registro y Asignación, Área Jurídico Normativa y Unidad de Transparencia, esto de acuerdo a sus funciones y obligaciones.

XV. PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

El Comité de Transparencia capacitará al personal del CETRA 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.

Uno de los factores esenciales para la implementación de los controles y demás medidas de seguridad, la actualización y mejora continua del inventario de datos personales, el apego a la normatividad, así como la concientización en la materia por parte del personal involucrado en el tratamiento de datos personales, es el conocimiento y capacitación, por lo que el aprovechamiento de los recursos y herramientas que el INAI ha dispuesto para su uso y obtención de beneficios, se propone que a través del Comité de Transparencia, en coordinación con la Unidad de Transparencia, se desarrolle un programa de capacitación focalizada, mediante el cual profundice en el conocimiento de la materia por parte de los servidores públicos que intervienen en el tratamiento de datos personales.

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

I. Introducción al derecho a la protección de datos personales.

- Principios.
- Deberes.
- Sistemas de datos personales.
- Medidas de seguridad.
- Procedimientos y sanciones
- Derechos ARCO (acceso, rectificación, cancelación y oposición)

.

- Medios de defensa.

II. La LGPDPPSO y sus Lineamientos.
   - Antecedentes.
   - ¿A quién aplica?
   - ¿Qué objeto tiene?

III. Fundamentos conceptuales de la LPDPSOCH.
   - Inventario
   - Medidas de seguridad.
   - Análisis de brecha y de riesgo.
   - Funciones y obligaciones.

IV. Relevancia de los Avisos de Privacidad.
- Consentimiento.
- Deber de información.
- Finalidades del tratamiento de los datos.

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 de la capacitación.

XVI. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD.

El presente documento de seguridad se actualizará cuando ocurran 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;

IV. Para la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

V. Cuando surjan documentos, formatos, recomendaciones, etc. por parte del INAI para la mejora del documento de seguridad