DOCUMENTO DE SEGURIDAD

PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES

Contenido

1. PRESENTACIÓN

Con fundamento en el artículo 6º apartado A, fracciones I y II de la Constitución Política de los Estados Unidos Mexicanos, en los que incorpora que toda persona tiene derecho al libre acceso a la información plural y oportuna y al derecho a la protección de sus datos personales, así como al acceso, rectificación, cancelación, oposición y portabilidad en los términos que determina la Ley.

En este sentido la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del estado de Chiapas, establece un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentra en posesión de sujetos obligados, entre los que figuran la Secretaría de Salud del Estado de Chiapas y el Instituto de Salud del Estado de Chiapas.

En observancia de esta ley y de conformidad con su artículo 45, se ha diseñado el presente documento de seguridad que tiene como propósito establecer los parámetros que guían el tratamiento de los datos personales al interior de la Secretaría de Salud del Estado de Chiapas y el Instituto de Salud del Estado de Chiapas, por las diferentes unidades administrativas que lo conforman.

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

El Documento de Seguridad busca crear un sistema de gestión para el tratamiento de los datos personales, que integre las acciones interrelacionadas para operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales.

Esto implica el planteamiento de acciones pertinentes para evitar la alteración, pérdida, transmisión y acceso no autorizado de los datos mediante la implementación de medidas físicas, administrativas y técnicas, tendientes a garantizar la seguridad e integridad de dichos datos con el seguimiento y observancia continua. Incluye además acciones que permitan controlar y verificar que el tratamiento de los datos personales se realice de acuerdo con los principios establecidos para la protección de los datos personales, implicando un compromiso con lo previsto en la ley y en los lineamientos generales, por parte de los funcionarios involucrados.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, es necesario señalar que todos y cada uno de los elementos que lo integran, constituyen un sistema interno para la gestión y tratamiento de los datos personales en posesión de la Secretaría de Salud del Estado de Chiapas y del Instituto de Salud del Estado de Chiapas, tal como lo indica el artículo 34 de la Ley de Protección de Datos Personales en posesión de sujetos obligados del estado de Chiapas, se entiende por sistema de gestión, al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

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

2. OBJETIVOS DEL DOCUMENTO DE SEGURIDAD

El presente documento de seguridad, tiene como objetivo:

I. Ofrecer el marco procedimental necesario para la protección de los datos personales en posesión de la Secretaría de Salud del Estado de Chiapas y el Instituto de Salud del Estado de Chiapas, como un medio para cumplir con las obligaciones que establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas (LPDPPSOCHIS), su Reglamento y sus Lineamientos Generales, así como la normatividad que derive de los mismos;

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

III. Promover la adopción de mejores prácticas en relación con la protección de datos personales, con la finalidad de establecer y mantener las medidas de seguridad de carácter administrativo, físico, informático y técnico para la protección de los datos personales.

3. RESPONSABILIDADES

De conformidad con lo dispuesto por el artículo 113 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas (LPDPPSOCHIS), el Comité de Transparencia del Sujeto Obligado, es la autoridad máxima en el mismo, en materia de protección de datos personales , teniendo 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, en esa tesitura dicho órgano tiene las siguientes funciones en este programa:

A. Elaborar, aprobar, coordinar y supervisar el Programa de Protección de Datos Personales, en conjunto con las áreas técnicas que estime necesario involucrar o consultar;
B. Proponer cambios y mejoras al mencionado Programa, a partir de la experiencia de su implementación;
C. Dar a conocer el Programa de PDP al interior del sujeto obligado;
D. Coordinar la implementación de dicho Programa en las unidades administrativas del sujeto obligado;
E. Asesorar a las unidades administrativas en la implementación de este Programa, con el apoyo de la Unidad de Transparencia y el Oficial de Datos Personales;
F. Presentar un informe anual al titular de la institución, en el que se describan las acciones realizadas para cumplir con lo dispuesto por este Programa;
G. Supervisar la correcta implementación del Programa;
H. Elaborar, aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con las áreas técnicas que estime necesario involucrar o consultar, y
I. Las demás que de manera expresa instruya el Titular de la Institución o las autoridades estatales en la materia.

Las unidades administrativas, el área coordinadora de archivos y la unidad de transparencia tendrán las funciones y responsabilidades que se describen más adelante en este documento.

Para que los objetivos planteados se logren con éxito, el Programa de Protección de Datos Personales requiere del total apoyo del Titular de la institución. En ese sentido, el Programa PDP ha sido presentado por el Comité de Transparencia que realiza esta función para ambos sujetos obligados la Secretaría del Salud del Estado de Chiapas y el Instituto de Salud del Estado de Chiapas, y ha sido aprobado por el Secretario de Salud del Estado de Chiapas, que a su vez ostenta la Dirección General del Instituto de Salud del Estado de Chiapas.

El titular, impulsará la debida implementación del Programa, pero no podrá suplir ni afectar las funciones del Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la organización.

Asimismo, para que la implementación del Programa PDP tenga como resultado el cumplimiento integral de las obligaciones que establece la LPDPPSOCHIS y los Lineamientos Generales, el Programa será de observancia obligatoria para todas las personas servidoras públicas del sujeto obligado que en el ejercicio de sus funciones traten datos personales,

Las unidades administrativas deberán realizar las acciones necesarias para cumplir con las obligaciones que establece este Programa, para lo cual deberán asignar los recursos materiales y servicios, así como los recursos humanos necesarios, y prever lo que se requiera en sus programas de trabajo.

4. ALCANCE DEL DOCUMENTO DE SEGURIDAD

El documento de seguridad aplica a todas las unidades administrativas que realicen tratamiento de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que efectúen, mismos que se encuentran bajo su estricta responsabilidad, tanto en medios físicos, como en medios electrónicos en los que se resguardan, operan y administran, con observancia de los principios, deberes y obligaciones que establecen las leyes aplicables.

Las unidades administrativas que forman parte de la Secretaría de Salud del Estado de Chiapas y el Instituto de Salud del Estado de Chiapas y que deberán observar el Programa de Protección de Datos Personales son las siguientes:

- ✓ La Oficina del Secretario de Salud
- ✓ La Dirección General del Instituto de Salud
- ✓ La Secretaría Técnica
- ✓ La Subdirección Jurídico Administrativa
- ✓ La Dirección de Administración y Finanzas
- ✓ La Dirección de Planeación y Desarrollo
- ✓ La Dirección de Infraestructura en Salud
- ✓ La Dirección de Atención Médica
- ✓ La Dirección de Salud Pública
- ✓ La Dirección de Salud Mental y Adicciones
- ✓ La Dirección de Protección Contra Riesgos Sanitarios
- ✓ Las Jurisdicciones Sanitarias
- ✓ Los Hospitales
- ✓ Y todas las unidades administrativas y de salud que de ellas dependan.

5. SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES

El Sistema de Gestión de Datos Personales es el medio por el la Secretaría de Salud del Estado de Chiapas y el Instituto de Salud del Estado de Chiapas garantizan el tratamiento de los datos personales que llevan a cabo como parte de sus funciones, desde su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación correspondiente; para lo cual, se establecen políticas y métodos orientados a salvaguardar la confidencialidad, integridad y disponibilidad de estos datos, de acuerdo con Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del estado de Chiapas y la Ley General de Transparencia y Acceso a la Información Pública del estado de Chiapas.

Por lo anterior, se inició un proceso planeación para la organización de los datos personales tratados por ambos sujetos obligados, con el fin de garantizar la protección de datos, tomando como punto de partida la identificación de los procesos y tareas en los que, conforme a sus atribuciones, las distintas áreas de los sujetos obligados desarrollen tratamientos de datos personales. Para tal fin, se elaboró un formulario que facilitó a cada unidad administrativa, la identificación de los tratamientos que llevan a cabo como parte de su responsabilidad, considerando lo establecido en el artículo 47 de la Ley de Protección de Datos Personales del Estado de Chiapas; logrando con ello el levantamiento del inventario de datos, tratando de identificar, la categoría y tipo datos usados en cada tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican los archivos físicos, bases de datos electrónicas locales o en la nube; las finalidades del cada tratamiento, el nombre, cargo y adscripción de los servidores públicos que tienen acceso al tratamiento, además de, si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

Además, el inventario ha contribuido para la determinación del ciclo de vida de los datos personales, entendiendo que, una vez concluida la finalidad de los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, vinculado con el proceso de gestión documental de estos sujetos obligados.

Una vez integrados los inventarios de tratamientos y de datos, se estableció la metodología para el análisis de riesgo, con la intención de que se identificaran el valor de los datos y su ciclo de vida, así como el valor de exposición, las posibles consecuencias para los titulares por el uso indebido y/o posible vulneración y las condiciones de riesgo a los que podrían encontrarse expuestos por medidas de seguridad poco confiables. Lo anterior, permitió identificar la brecha entre las medidas de seguridad existentes y las medidas de seguridad propuestas por los especialistas en la materia, para que garanticen la seguridad de los datos, tanto administrativas, como físicas y técnicas.

A partir de esta identificación de posibles vulneraciones es factible prevenir posibles debilidades en la seguridad de los datos y las áreas de oportunidad, aun cuando no haya existido un daño real, mediante la identificación de la ineficiencia de los controles de acceso físico, electrónico y el inadecuado establecimiento de los esquemas de privilegios, sumado al poco conocimiento de procesos y responsabilidades en materia de protección de datos personales, además de la falta de

definición de perfiles y roles, falta de seguimiento y monitoreo a las medidas de seguridad, así como la inexistencia de mecanismos para garantizar la confidencialidad por parte del personal.

Las amenazas que se buscan prevenir pueden ser de diferentes tipos:

- Robo, extravío, copia o transferencia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizado.
- Pérdida o destrucción no autorizada o deseada.

El riesgo que puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada comprometiendo su confidencialidad, disponibilidad e integridad; y en este sentido, las medidas de seguridad por parte de cada dirección están orientadas justamente a proteger los datos personales. En el marco del sistema de gestión y política de seguridad institucional, se procurará:

- Tratar a los datos personales conforme a las atribuciones de Ley;
- Identificar a los servidores públicos ad intra, responsables del tratamiento de los datos personales.
- Que los tratamientos de datos personales estén sujetos a los principios de consentimiento siempre que sea posible;
- Responder al principio de información a los titulares sobre el uso que dará y sus finalidades;
- Mantener la actualización y pertinencia de los datos personales;
- Priorizar la supresión de los datos personales cuando haya concluido el proceso para el que fueron obtenidos;
- Ajustar el tratamiento de los datos personales a las finalidades para la que fueron obtenidos y estrictamente los necesarios para las finalidades;
- Obtener datos personales a través de medios legales, con respeto a la expectativa de privacidad del titular;
- Velar por el cumplimiento de los principios, estableciendo y manteniendo medidas de seguridad y de confidencialidad durante el ciclo de vida de los datos personales, en estricto respeto de los derechos de los titulares;
- Mantener actualizado el inventario de datos personales.

Buscando el logro de lo anterior, y tomando como punto de partida la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que, de acuerdo con otras experiencias y mejores prácticas tomadas como referencia, se encaminan a la mejora continua por parte de las personas involucradas en el tratamiento, en la búsqueda de lograr la salvaguarda del derecho a la privacidad y protección de datos personales, se han determinado las líneas de acción para el personal encargado de tratamiento de datos, con el propósito de generar mecanismos para el resguardo adecuado, actuando en apego a la LPDPPSO de Chiapas y los lineamientos correspondientes.

6. INVENTARIO DE TRATAMIENTOS Y DATOS PERSONALES

Cada una de las áreas administrativas realizara, con la asesoría de la Unidad de Transparencia, un diagnóstico de los tratamientos de datos personales que llevan a cabo, del cual se obtendrá el inventario de tratamientos y de datos personales realizados en el ejercicio de sus funciones.

Por "inventario de tratamientos de datos personales" se entenderá los procedimientos en los que el área administrativa recaba datos personales para el desarrollo de sus funciones, el responsable de cada tratamiento, el medio por el que se recaban y almacenan los datos personales, así como las medidas de seguridad que permitan la protección de los mismos.

Así, en coordinación con las áreas, como resultado del proceso de análisis y actualización de la información, se logró identificar a 06 unidades administrativas que no realizan tratamiento de datos personales y 07 unidades administrativas que realizan tratamientos de datos personales, las cuales son:

- Dirección de Atención Medica y las Unidades de Salud
- Dirección de Salud Pública
- Banco de Sangre
- Área de Apoyo y Seguimiento
- Subdirección de Recursos Humanos
- Subdirección Jurídico Administrativa
- Unidad de Transparencia

Estos tratamientos se realizan en absoluto apego a sus funciones, a través de las diversas áreas que las integran y permiten el desarrollo de los procesos que realizan, para el cumplimiento de dichas funciones.

En relación con lo anterior, fue posible identificar 18 procesos que se desarrollan, y en los que se implican el tratamiento de datos personales. Mismas que a continuación se describen:

Unidad Administrativa	Proceso o Tratamiento
Dirección de Atención Medica y las Unidades de Salud	1. Expediente de prestadores de servicio social, prácticas profesionales e internistas.
Banco de Sangre	2. Evaluación de candidatos a ser donadores. 3. Pruebas de química sanguínea.
Área de Apoyo y Seguimiento	4. Proceso de entrega y recepción 5. Llenados de fichas de los datos personales solicitados por los órganos fiscalizadores 6. Registro único de servidores públicos para entidades federativas (RUSPEF)

Unidad Administrativa	Proceso o Tratamiento
Subdirección de Recursos Humanos	7. Reclutamiento de personal 8. Expediente único de personal 9. Credencialización 10. Nómina de pago de personal 11. Registro de asistencia del personal
Subdirección Asuntos Jurídicos	12. Pocedimientos seguidos en forma de juicio
Unidad de Transparencia	13. Solicitudes de Derechos ARCO
Dirección de Salud Pública	14. Listas de asistencia y registro de participantes

Como resultado del proceso de análisis, se identificaron también los datos personales utilizados en los tratamientos, mismos que corresponden a las tres categorías, tal como se señala a continuación:

Datos de Identificación: Nombre, firma, domicilio, CURP, RFC, número de seguridad social, cédula profesional, año de nacimiento o edad, antecedentes laborales, características físicas, correo electrónico, currículum vitae, datos académicos, datos de identificación, datos laborales, datos familiares, datos sindicales, imagen en fotografía, huella dactilar, huella digital, clave de elector, estado civil, teléfono, sexo, nacionalidad, nivel educativo, ocupación, títulos profesionales.

Datos Patrimoniales: Número de cuentas bancarias, estados de cuenta, clave interbancaria, institución bancaria, beneficiarios, datos de prestaciones, gratificaciones y obligaciones.

Datos Sensibles: Religión, datos de salud, datos sobre procedimientos judiciales o seguidos en forma de juicio, información genética, origen étnico o racial, otros datos biométricos.

Al respecto, se identificó que cada unidad administrativa tiene un medio propio para obtener los datos personales, y estos son: físicamente, correo electrónico, Internet o sistema informático, vía telefónica, siempre directamente del titular.

Cada unidad también se encarga de desarrollar estrategias para la protección de los datos personales, mediante archivos o bases de datos electrónicas simples, resguardadas en las computadoras de las personas servidoras públicas. No existe un sistema de base de datos institucional en el que puedan albergarse todos los datos personales.

Es por ello, que el Inventario de Datos del Instituto, a partir de los hallazgos identificados, se integra como un elemento del Sistema de Gestión de Datos Personales, que representa, junto con las medidas de seguridad, un instrumento útil para la implementación de las medidas correspondientes en materia de protección de datos personales.

En este mismo sentido, ayuda a trazar las rutas para la capacitación en materia de protección de datos hacia los funcionarios del Instituto, como una vía de fortalecimiento en la operación de los procesos en que se tratan datos, en la búsqueda de sensibilizar y preparar a los responsables y encargados de los mismos, para que el tratamiento se realice de conformidad con los estándares nacionales e internacionales en la materia.

7. FUNCIONES Y RESPONSABILIDADES DE TRATAMIENTOS DE DATOS PERSONALES

Como resultado de la identificación de los procesos en los que intervienen datos personales, relacionado en el Inventario de Datos Personales, por las áreas que integran las unidades administrativas correspondientes al interior del Instituto, resulta importante definir estas actividades con las funciones y facultades establecidas en el Reglamento Interior, que otorga a las personas servidoras públicas responsables de dicho tratamiento; lo anterior, a fin de dar cumplimiento al principio de legalidad que debe atender todo servidor público. Por lo anterior, a continuación, se ilustran las funciones otorgadas por el reglamento interior de este Instituto a quienes llevan a cabo tratamientos de datos personales.

DIRECCIÓN DE ATENCION MEDICA	
Tratamientos	**Atribuciones o funciones para el tratamiento**
1. Expediente de prestadores de servicio social, prácticas profesionales e internistas.	En coordinación con la Secretaría de Salud Federal se recabaran los datos y documentos necesarios para estos tratamientos.

BANCO DE SANGRE	
Tratamientos	**Atribuciones o funciones para el tratamiento**
2. Evaluación de candidatos a ser donadores.	Registrar al paciente para revisar si es válido (idóneo) para ser donador de sangre.
3. Pruebas de química sanguínea.	En caso de ser candidato valido a ser donador, se realizarán los análisis de química sanguínea que arrojarán datos personales sensibles.

AREA DE APOYO Y SEGUIMIENTO	
Tratamientos	**Atribuciones o funciones para el tratamiento**
4. Proceso de entrega y recepción	Vigilar la elaboración de las actas de entrega y recepción de los servidores y cargos públicos.
5. Llenados de fichas de los datos personales solicitados por los órganos fiscalizadores	Presentar a los Órganos Fiscalizadores las fichas de datos personales solicitadas.
6. Registro único de servidores públicos para entidades federativas (RUSPEF)	Notificación de inicio, de resultados y de cierre de los distintos órganos fiscalizadores.

SUBDIRECCIÓN DE RECURSOS HUMANOS	
Tratamientos	**Atribuciones o funciones para el tratamiento**
7. Reclutamiento de personal	Vigilar el cumplimiento de convocatorias de contratación de personal.
8. Expediente único de personal	Crear el expediente de personal de los servidores públicos.
9. Credencialización	Crear las identificaciones del personal de la Institución.

10. Nómina de pago de personal	Generar los pagos, retenciones y operaciones de nómina del personal.
11. Registro de asistencia del personal	Registrar por diferentes medios la asistencia.

SUBDIRECCIÓN JURÍDICO ADMINISTRATIVA	
Tratamientos	**Atribuciones o funciones para el tratamiento**
12. Juicios y/o procedimientos seguidos en forma de juicio	Atender los procesos judiciales y extrajudiciales en los que se involucra personal de la Institución.

UNIDAD DE TRANSPARENCIA	
Tratamientos	**Atribuciones o funciones para el tratamiento**
13. Solicitudes de derechos ARCO	Atender las solicitudes de Acceso, Rectificación, Cancelación y Oposición de Datos Personales.

DIRECCIÓN DE SALUD PÚBLICA	
Tratamientos	**Atribuciones o funciones para el tratamiento**
14. Listas de asistencia y registro de participantes.	Dar constancia del registro de asistencias o participación para los diferentes eventos, capacitaciones, actos o reuniones.

8. ANALISIS DE RIESGO

De acuerdo con el artículo 50 de la LPDPPSOCH, el análisis de riesgo y brecha forma parte del documento de seguridad, como un medio para identificar las medidas de seguridad implementadas y, en relación con ello, las amenazas de vulneración en que se encuentran los datos personales.

El análisis sirve para identificar el riesgo inherente a los datos personales en el tratamiento a que son sometidos en el ejercicio de las funciones del Sujeto Obligado, con respeto a la integridad de las personas.

La evaluación de riesgos de los datos personales tiene como propósito, garantizar la confidencialidad, integridad y disponibilidad de los datos personales en posesión del ISECH.

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

a. Los requerimientos regulatorios, código de conducta o mejores prácticas de un sector específico;
b. El valor de los datos personales de acuerdo con su clasificación previamente definitiva y su ciclo de vida;
c. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
d. Las consecuencias y negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; y
e. Los factores previstos en el artículo 47 de la Ley Estatal.

Bajo esta premisa, para analizar los riegos de los datos personales que son objeto de tratamiento por el Instituto, se aplicó un instrumento para clasificar los datos utilizados, a partir de la categorización existente en la ley:

Datos de Identificación o Contacto: Que se refieren a información por la que se identifica a una persona y/o permiten su contacto como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población, edad, entre otros.

Datos Patrimoniales: Son aquellos que comprenden la información que se encuentra vinculados al patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.

Datos Sensibles: Se refiere a la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleve a un riesgo grave para éste, tales como, el origen étnico, el estado de salud presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

Se identificó que se trabaja con las tres categorías: Datos de Identificación, Datos Patrimoniales y datos sensibles.

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

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

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizado.
- Pérdida o destrucción no autorizada.

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

En cuanto a la valoración del riesgo por el tipo de dato en cada proceso en el que las unidades administrativas del Instituto tratan datos personales, se señaló una escala del 1 al 3, representándose de la forma siguiente:

TIPO DE DATO	RIESGO INHERENTE	NIVEL DE RIESGO
Datos identificativos y laborales	Bajo	1
Datos patrimoniales, procedimientos administrativos	Medio	2
Datos sensibles y de salud	Alto	3

Como resultado del levantamiento de información para el análisis de riesgo y de brecha, se identifica que en el Instituto se cuenta con 7 unidades administrativas en las que tienen lugar tratamientos de datos personales para el desarrollo de los 26 procesos como se ilustra a continuación:

Área	Tratamientos
Dirección de atención médica	**1**
Banco de Sangre	**2**
Área de apoyo y seguimiento	**3**
Subdirección de recursos humanos	**5**
Subdirección Jurídico Administrativa	**1**
Unidad de Transparencia	**1**
Dirección de Salud Pública	**1**

Hay que señalar además que la etapa del ciclo de vida (obtención, tratamiento, almacenamiento, transferencia, bloqueo y eliminación) en la que los datos personales se encuentran más vulnerables, es en el periodo de almacenamiento.

Las amenazas a las que se ven expuestos son básicamente:

- ✓ Robo, extravío o copia no autorizada.
- ✓ Uso, acceso o tratamiento no autorizado.
- ✓ Daño, alteración o modificación no autorizado.
- ✓ Pérdida o destrucción no autorizada

Siendo la más alta, la de robo, extravío o copia no autorizada y la de menor riesgo es daño, alteración o modificación no autorizada.

Finalmente, como parte del análisis es posible establecer que el nivel de riesgo es mayormente medio, debido que se trabaja sobre todo con datos de identificación, en algunos casos con datos sensibles y se utilizan en mínimos procesos datos patrimoniales. Los datos personales se mantienen a resguardo en computadoras personales con contraseña, archiveros ubicados en las unidades administrativas y espacios dedicados a Archivos de Expedientes Clínicos.

Podemos observar que por las funciones que se desempeñan en las áreas administrativas, el riesgo es bajo, es así como el nivel medio prevalece con mayor porcentaje en las direcciones de Atención Médica y Salud Pública, las cuales tratan datos sensibles.

Seguridad de la información: La gestión de datos médicos confidenciales debe ser segura y protegida contra amenazas cibernéticas. Riesgos como fugas de datos, accesos no autorizados o malware son preocupaciones importantes.

Cumplimiento normativo: Las instituciones de salud deben cumplir con regulaciones para garantizar la privacidad y seguridad de la información médica. El incumplimiento puede acarrear multas y dañar la reputación de la organización.

Gestión de riesgos operativos: Esto implica identificar y mitigar riesgos en los procesos administrativos, como errores en la facturación, problemas en la gestión de inventario o dificultades en la logística hospitalaria.

Seguridad del paciente: Los protocolos de seguridad y calidad en la atención médica deben ser sólidos para minimizar errores médicos, riesgos de infecciones nosocomiales y otros eventos adversos que puedan afectar a los pacientes.

Riesgos financieros: La gestión ineficiente de recursos financieros puede tener un impacto en la calidad de la atención médica. Por ejemplo, mala gestión de costos, facturación incorrecta o retrasos en los pagos pueden afectar la sostenibilidad financiera.

9. ANALISIS DE BRECHA

Las medidas de seguridad administrativas, físicas y técnicas que actualmente se aplican en el ISECH para mantener la confidencialidad e integralidad de la información, protegiendo los datos personales contra daño, pérdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado e impedir la divulgación no autorizada, son las siguientes:

Medidas Administrativas

1. Diseño y desarrollo de un modelo de capacitación permanente en materia de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), impartido a quienes laboran en el Instituto.
2. Aplicación de estrategias de seguridad, para el resguardo de los expedientes, con observancia de criterios vinculados con el sistema de gestión documental.
3. Diseño e implementación de una carta responsiva por parte del personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.
4. Previsión de reportes de incidencias, mediante la elaboración e implementación de los formularios correspondientes.

Medidas Físicas

1. Protección de documentos e información resguardándolos en archivos físicos de trámite, asegurados con llave.
2. Disponer de instalaciones aseguradas con llave para mantener control de acceso de personas a espacios de resguardo de información.
3. Aplicar la firma de cartas de confidencialidad con el personal que trata datos personales.

Medidas Técnicas

1. Garantizar la seguridad de los datos personales, utilizando claves de usuario y contraseñas de manera individual y evitar compartirlas, prestarlas o registrarlas a la vista de otras personas, y que estas sean seguras al incluir: caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero.
2. Cuando se identifique algún caso en el que las claves de usuario y/o contraseña hayan sido utilizadas por un tercero, notificar de manera inmediata al área de Informática, para las prevenciones conducentes.
3. Procurar la utilización de una cuenta de correo electrónico oficial para fines relacionados con las actividades laborales, evitando remitir datos personales.
4. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de restringir el acceso a los datos personales que pudieran mantenerse en archivos y equipos.
5. Cuidar que en los equipos de impresión no se dejen olvidados documentos que contengan datos personales

10. CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

Los sistemas tecnológicos del Instituto son bastante básicos, por lo que solo se aplican controles de identificación y autenticación de usuarios. La única medida que se implementa es el uso de contraseñas par el acceso a los equipos de cómputo, repositorios y cuentas de correo institucionales.

11. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

El ISECH cuenta con repositorios para el almacenaje y respaldo de la información de algunos equipos; sobre todo la que se genera en correos institucionales, la página web institucional y sistemas de salud pública; lo que, posibilita los procedimientos de respaldo y recuperación de la información; además, en cada área los respaldos de datos personales se llevan a cabo de acuerdo con las posibilidades identificadas de manera particular. En algunos casos se realizan respaldos en la nube de diferentes sistemas operativos, así como en discos duros y otros medios portátiles controlados y administrados por los responsables de cada tratamiento, que permiten el respaldo y la recuperación de los datos personales cuando así se requiera.

12. EL PLAN DE CONTINGENCIA

Dentro de la seguridad informática se denomina plan de contingencia, a la definición de acciones a realizar, recursos a utilizar y personal a emplear en caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización. Es decir, es la determinación precisa del quién, qué, cómo, cuándo y dónde ocurrió, en caso de producirse una anomalía en el sistema de información.

El plan de contingencia es elaborado anualmente por el Área de Informática y considerar todos los componentes del sistema: Datos críticos, equipo lógico de base, aplicaciones, equipos físicos y de comunicaciones, documentación y personal.

Además, debe contemplar también todos los recursos auxiliares, sin los cuales el funcionamiento de los sistemas podría verse seriamente comprometido: suministro de potencia; sistemas de climatización; instalaciones; etc.

Para contar con un sistema de seguridad fortalecido, es necesario contar con el protocolo de actuación en caso de contingencia, que incluya

- Los reportes de vulneración,
- Designación de personas encargadas de

- Reportar la vulneración,
- Realizar la investigación para identificar la causa y responsable de la vulneración,

- Método para la notificación de los titulares afectados y
- Procedimientos para la recuperación de la información

13. LAS TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES

La destrucción y borrado de información es un tema de vital importancia para proteger la privacidad, confidencialidad, integridad y disponibilidad de la información, y en particular de los datos personales; debe hacerse bajo procedimientos que garanticen que fueron eliminados en su totalidad y que no pueden ser recuperados, y utilizarse de manera indebida.

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

Lo anterior implica algunas acciones, entre las que podemos contar:

- Capacitación al personal para acercarse al conocimiento de lo que son las técnicas para la supresión y el borrado seguro
- Diseño de un lineamiento para garantizar el proceso
- Adquisición de trituradoras para la destrucción de los documentos
- Implementación de herramientas digitales para
  - la destrucción de medios de almacenamiento electrónicos,
  - la desmagnetización y sobre escritura de los equipos de cómputo

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

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

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

15. MONITOREO DE MEDIDAS DE SEGURIDAD

Como parte del programa de protección de datos personales, es importante la supervisión de las medidas de seguridad técnicas y físicas, como un elemento para la mejora continua, que permite definir nuevas formas de monitoreo, de acuerdo con las necesidades surgidas al interior del Instituto, como son:

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

16. PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

La aplicación del Programa de Protección de Datos Personales en el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales, requiere como un factor esencial, la formación y sensibilización de las personas servidoras públicas, de tal forma que pueda garantizarse la actualización y mejora continua del inventario de datos personales, la observancia de la normatividad, por lo que se propone un programa de capacitación en el tema de protección de datos personales que favorezca la profundización en el conocimiento del tema por parte de quienes intervienen en el tratamiento de datos personales. A manera de propuesta, se han considerado los siguientes temas:

1) La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en Chiapas.

✓ Antecedentes, Principios, Alcances, Objetivo e Implicaciones

2) Obligaciones en la observancia de la LPDPPSOCHIS

✓ Deberes, Medidas de seguridad, Procedimientos y sanciones, Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) y Medios de defensa.

3) El programa de protección de datos personales

✓ Sistemas de datos personales, Inventario y Base de Datos, Medidas de seguridad, Análisis de brecha y riesgo y Funciones y obligaciones.

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

✓ Contenido: Integral, simplificado, Consentimiento, Deber de información y Finalidades del tratamiento de los datos.

5) Implementación de medidas de seguridad

✓ Esquema de privilegios en el acceso, Registro y control de accesos a las bases de datos, Identificación y autenticación de usuarios, Almacenamiento, respaldo y recuperación de la información y Técnicas para la supresión y borrado seguro de la información

_____

Dr. Francisco Arturo Mariscal Ochoa
Encargado del Despacho de la Secretaría de salud del Estado de Chiapas
y de la Dirección del instituto de salud del Estado de Chiapas

_____

Dra. Dora Leticia Martínez Sol
Secretaria Técnica
Revisión

_____

Ing. José de Jesús Pacheco Velazquez
Responsable de la Unidad de Transparencia
Elaboración