OFICINA DE
CONVENCIONES
Y VISITANTES

GOBIERNO DE CHIAPAS

Documento de seguridad para la Protección de Datos Personales.

Calzada Andrés Serra Rojas s/n, Col. El Retiro. CP. 29040. Piso 13 de la Torre Chiapas,
Tuxtla Gutiérrez, Chiapas. México.
Tel/Oficinas. (961) 61 8 75 30 ext. 68202 y 68203.
Web Site: www.ocvchiapas.com

Índice.

Introducción.-

El derecho de los datos personales es un derecho que está reconocido en la constitución política de los Estados Unidos Mexicanos en los artículos 6 apartado A, fracción II y 16, párrafo segundo, su regularización específica para el sector Público es la *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados,* por lo cual este documento de seguridad, es un instrumento que cuenta con las medias se seguridad administrativa y técnicas para dar el cumplimiento con la ley.

Así mismo, este documento tiene el propósito de controlar los sistemas de datos personales que se poseen, ya que todo tratamiento de datos personales que efectué el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, en relación con las atribuciones expresas que la normatividad aplicable les confiera.

Por lo cual el objetivo de contar con este documento es el de poder establecer los principales elementos que se debe que contar con los datos personales, para poder garantizar la disponibilidad, integridad y confidencialidad, así poder canalizar las posibles amenazas y riesgos de los cuales pueden ser objetos en el tratamiento de los datos personales.

Marco Jurídico.-

Para efectos del presente documento, la normatividad aplicable es la siguiente:

- Constitución Política de los Estados Unidos Mexicanos, última reforma publicada en el Diario Oficial de la Federación el 28 de mayo 2021.

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017.

- Lineamientos Generales de Protección de Datos Personales para el sector público, publicados en el Diario Oficial de la Federación el 26 de enero del 2018

- Lineamientos que establecen los parámetros, modalidades y procedimiento para la portabilidad de Datos Personales para el sector público, publicados en el Diario Oficial de la Federación el 12 de febrero del 2018

Objetivo y Alcance del Documentó

El siguiente documento tiene como objetivo lo siguiente:

En el marco de trabajo necesario para la protección de los datos personales en posesión del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, ya que tiene un medio para cumplir con las obligaciones que establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas (LPDPPSOCHIS) y los Lineamientos Generales, así como la normatividad que derive de los mismos.

Así como determinar las posibles vulnerabilidades, amenazas y riesgos de los que pueden ser objeto. así como la normatividad que derive de los mismos; estableciendo con ello, los elementos y actividades de gestión para la operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, y promover la adopción de mejores prácticas en relación con la protección de datos personales.

Estableciendo los elementos y actividades de gestión para la operación y control de los procesos que impliquen el tratamiento de datos personales, con la intención de protegerlos de manera sistemática y continua, además de 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 y técnico para la protección de los datos personales, emite el presente documento.

El alcance que tiene el documento de seguridad aplica para todos las dependencias u organismos públicos que realicen tratamientos 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 los espacios físicos como los medios electrónicos en los que se resguardan, operan y administran, con observancia de los principios, deberes y obligaciones que establece la ley.

Las unidades administrativas que forman parte de la Oficina de Convenciones y Visitantes, deberán observar el Programa de Protección de Datos Personales son las siguientes:

- Dirección del Centro de Convenciones y Visitantes.
- Dirección de Promoción, Ventas y Apoyo en Sitio
- Unidad de Apoyo administrativo
- Jurídico

El documento de seguridad está basada en la generación de la base de información fue generada por las antes mencionadas.

Sistema de Gestión de Datos Personales

Un sistema de gestión, es el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

La Oficina de Convenciones y Visitantes garantiza el tratamiento de los datos personales que lleva 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 de organización y planeación de los medios para 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 del instituto desarrollan 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 las bases físicas o electrónicas de datos; las finalidades del 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 que se desarrolla al interior de la Oficina de Convenciones y Visitantes.

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 faltantes 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:

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

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 la Ley;
- Responder al principio de información a los titulares sobre el uso que dará y sus finalidades;
- Que los tratamientos de datos personales estén sujetos al principio de consentimiento siempre que la Ley lo permita;
- Identificar a los servidores públicos de la Oficina de Convenciones y Visitantes los responsables del tratamiento de los datos personales;
- Priorizar la supresión de los datos personales cuando haya concluido el proceso para el que fueron obtenidos;
- Mantener la actualización y pertinencia de los datos personales;
- Mantener actualizado el inventario de datos personales que maneja la Oficina de Convenciones y Visitantes;
- Obtener datos personales a través de medios legales, con respeto a la expectativa de privacidad del titular;

En base en lo anterior, la Oficina de Convenciones y Visitantes determina las pautas de acción del personal encargado de tratamiento de datos personales con intención a generar su correcto resguardo, buscando en todo momento actuar en apego a las disposiciones de la LGPDPPSO y los Lineamientos de la materia, siempre en consideración de la protección del derecho a la privacidad y protección de datos de las personas.

Con base en 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 experiencia 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 logar 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.

Inventario De Tratamientos y Datos Personales

Para el debido cumplimiento de las obligaciones es necesario que cada una de las unidades administrativas realice un diagnóstico de los tratamientos de datos personales que llevan a cabo.

El diagnóstico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en este Instituto.

Por "inventario de tratamientos de datos personales" se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas del Instituto, realizado con orden y precisión.

Así, en coordinación con las áreas, como resultado del proceso de análisis y actualización de la información, se logró identificar a las unidades administrativas son las siguientes:

- Dirección del Centro de Convenciones y Visitantes.
- Dirección de Ventas y Apoyo en Sitio
- Unidad de Apoyo administrativo
- Recursos humanos
- Jurídico

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 26 procesos que se desarrollan, que implican el tratamiento de datos personales. Mismas que a continuación se describen:

Dirección del Centro de Convenciones y Visitantes.	**Proceso o Tratamiento**
Ventas	**Contrato de Prestación de Servicios** **Convenios con Medios de Comunicación Impresos**

Dirección de Promoción, Ventas y Apoyo en Sitio.	**Proceso o Tratamiento**
Ventas y Apoyo en Sitio	**Apoyo en Sitio** **Promoción del Destino**

Unidad de Apoyo Administrativo.	**Proceso o Tratamiento**
Recursos Humanos	**Movimiento Nominal de Alta de personal de Nuevo Ingreso**
	Movimiento Nominal de Baja de Personal
	Movimiento Nominal de Recategorización
	Movimiento de Alta al IMSS
	Movimiento de Baja al IMSS
	Movimientos de Altas y Bajas al INFONAVIT
	Declarachiapas
	Manejo del Expediente
	Evaluación al Personal
	Cursos o capacitaciones
	Manejo de Nómina de sueldos

Unidad de Apoyo Administrativo.	Proceso o Tratamiento
Financieros	Elaboración de Facturas Electrónicas
	Pago a Proveedores
Materiales	Resguardo de Bienes Muebles
	Adquisición de Bienes y/o Servicios

Jurídico.	Proceso o Tratamiento
Ventas	Convenios De Colaboración, Concertación Y/O Prestación De Servicios
	Denuncias Por Incumplimiento A Las Obligaciones De Transparencia
	Juicios y/o Procedimientos Seguidos En Forma De Juicio

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:

De identificación:

- Nombre, firma, domicilio, CURP, RFC, número de seguridad social, cédula profesional, año de nacimiento o edad, antecedentes laborales, características físicas, correo electrónico, Curriculum vitae, datos académicos, datos de identificación, datos laborales, datos familiares, datos personales contenido en documento para acreditar personalidad del representante, datos personales contenidos en la identificación oficial presentada por la persona física, datos sindicales, descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil, entre otros),imagen en fotografía y/o video, huella dactilar, huella digital, menor de edad, clave de elector, estado civil, teléfono, sexo, nacionalidad, nivel educativo, ocupación, sexo, títulos profesionales.

Patrimoniales:

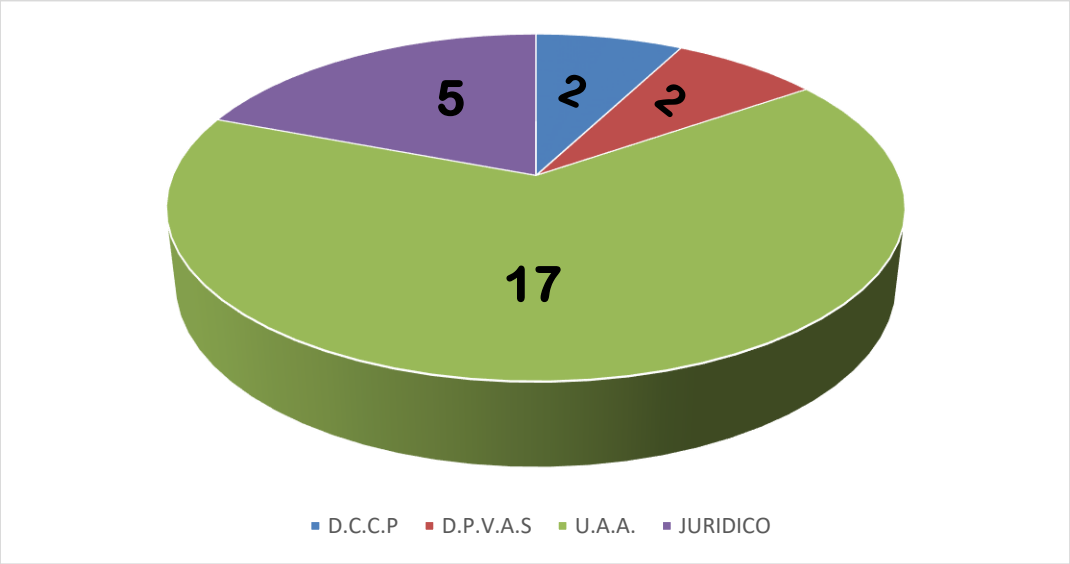
- Número de cuentas bancarias, estados de cuenta, CLABE interbancaria, institución bancaria, facturas, beneficiarios, datos contenidos en declaraciones patrimoniales, descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil, entre otros).

Sensibles:

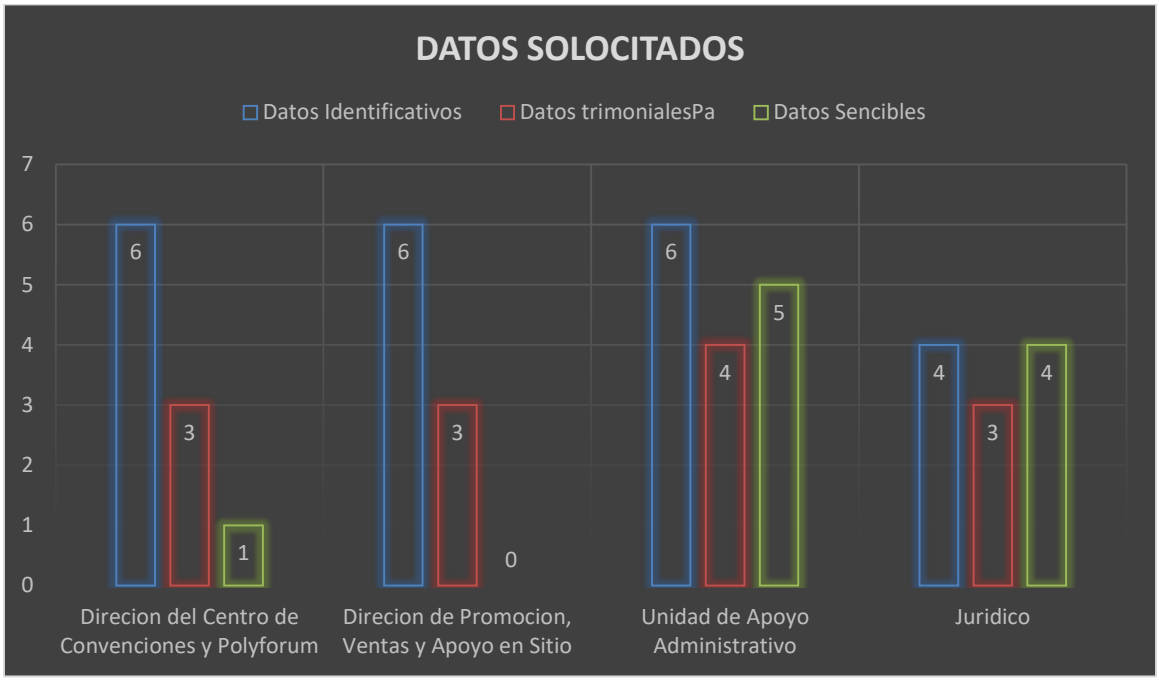
- Circunstancias socioeconómicas, creencias religiosas, filosóficas o morales, datos de salud, datos sobre procedimientos judiciales o seguidos en forma de juicio, discapacidad, estado de interdicción o incapacidad legal. información genética, información migratoria, lengua indígena, origen étnico o racial, otros datos biométricos, pertenencia a pueblo indígena.

Estos datos son utilizados en 26 procesos, de los cuales dos le corresponden a la Dirección de Centro de Convenciones y Polyforum, dos a la Dirección de Promoción, Ventas y Apoyo en Sitio, dieciocho a la Unidad de Apoyo Administrativo, y en lo que respecta al Área Jurídica tiene cinco procesos. Asimismo, en 26 procesos se utilizan datos personales de identificación, mientras que en 8 se recabaron datos personales patrimoniales y en lo que se refiere a datos sensibles, se manejan en 12 tratamientos.

PROCESOS POR UNIDAD ADMINISTRATIVA.



En relación con los datos solicitados, todas las unidades administrativas solicitan datos de identificación, mientras que la Dirección de Administración y Finanzas, la Dirección Jurídica, la Unidad de Transparencia y el Área Recursos humanos solicitan datos patrimoniales, por otro lado, estas unidades administrativas manejan datos sensibles; tal como se presenta en la gráfica.



Es posible apreciar que Unidad de Apoyo Administrativo y Finanzas es la que desarrolla el mayor número de procesos en los que intervienen tratamientos de datos personales, dada la naturaleza de sus funciones, lo anterior, debido a que las áreas que la integran cuentan con atribuciones para administrar los recursos humanos, materiales y financieros del Instituto; lo cual implica que los procesos correspondientes a la protección de datos personales sean aplicados con mayor cuidado y puntualidad, a manera de garantizar que este derecho se cumpla. No obstante, en las otras áreas, aunque en menor medida, se implementa algún tipo de proceso con tratamiento de datos; por tanto, la estrategia de protección debe ser entendida como una acción de frecuencia generalizada.

Con respecto a que cada Dirección y Unidad Administrativa tiene un medio propio para obtener los datos personales, y estos son: físicamente, correo electrónico, Internet o sistema informático, vía telefónica, Plataforma Nacional de Transparencia, y servicios de mensajería instantánea (WhatsApp); 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 los datos personales.

Es por ello, que el Inventario de Datos de la Oficina de Convenciones y Visitantes, a partir de los hallazgos identificados en su actualización, 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. En apego a lo anterior, el Inventario de Datos Personales del Instituto de Transparencia, se consolida como un elemento más de la política implementada para la observancia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en su artículo 35 párrafo I, dando certeza a la ciudadanía sobre el destino de los datos recabados por este Órgano Garante.

Funciones y Responsabilidades del Tratamiento de Datos Personales

Del trabajo de identificación de los procesos en los que intervienen datos personales, relacionado en el Inventario de Datos Personales, por las áreas que integran las Direcciones y Unidades Administrativas correspondientes al interior de la Oficina de Convenciones y Visitantes, es 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 la Oficina de Convenciones y Visitantes quienes llevan a cabo tratamientos de datos personales.

Dirección o Unidad Administrativa	Nombre y Cargo de las o los funcionarios que tratan Datos personales	Tratamientos
Dirección del Centro de Convenciones y Polyforum	Lic. Amaratha Trujillo Figueroa Directora del Centro de Convenciones y Polyforum	Contrato de Prestación de Servicios
	Irma Dalia Sánchez Morales Jefa de Ventas	Convenios con Medios de Comunicación Impresos
	Laura Lucia Arguello Utrilla Ejecutiva de Ventas	
Dirección de Promoción, Ventas y Apoyo en Sitio.	Lic. Iván Álvarez Toledo. Director de Promoción Ventas y Apoyo en Sitio	Apoyo en Sitio
	Marycarmen Escobar Velázquez Ejecutiva de Ventas	Promoción del destino
	Elsa Margarita Osuna Ruiz Ejecutiva de Ventas	

Dirección o Unidad Administrativa	Nombre y Cargo de las o los funcionarios que tratan Datos personales	Tratamientos
Unidad de Apoyo Administrativo	Lorena Del Carmen Rincón Velázquez Jefa de Recursos Humanos Nancy Rosas Martínez Asistente de Recursos Humanos	Movimiento Nominal de Alta de personal de Nuevo Ingreso
		Movimiento Nominal de Baja de Personal
		Movimiento Nominal de Promoción de Personal
		Movimiento Nominal de Recategorización
		Movimiento de Alta al IMSS
		Movimiento de Baja al IMSS
		Movimientos de Altas y Bajas al INFONAVIT
		Declarachiapas
		Manejo del Expediente
		Evaluación al Personal
		Cursos o capacitaciones
		Manejo de Nómina de sueldos
	Francisco Javier Bashulto Salinas Jefe de Financieros Daniel Flores Vera Encargado de presupuestos Claudia Luz Corzo Santos Encargada de Ingresos Propios	Elaboración de Facturas Electrónicas
		Pago a Proveedores
	Dionicio Domínguez Yuca Encargado de Materiales	Resguardo de Bienes Muebles
		Adquisición de Bienes y/o Servicios
Jurídico	Gilberto Enrique Tinajero Velázquez Jurídico	Convenios de colaboración, concertación y/o prestación de servicios
		Denuncias por incumplimiento a las obligaciones de transparencia
		Juicios y/o procedimientos seguidos en forma de juicio
		Contratos
		Laudos

ANÁLISIS DE RIESGO

De acuerdo con el artículo 50 de la LPDPPSOCHIS, 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 de la Oficina de Convenciones y Visitantes, con respeto a la integridad de las personas.

La evaluación de riesgos de los datos personales forma parte de la serie de elementos que integran el documento de seguridad, cuyo propósito es garantizar la confidencialidad, integridad y disponibilidad de los datos personales en posesión de la Oficina de Convenciones y Visitantes.

Así mismo, 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:

I. El valor de los datos personales de acuerdo con su clasificación previamente definitiva y su ciclo de vida;
II. Los requerimientos regulatorios, código de conducta o mejores prácticas de un sector específico;
III. Las consecuencias y negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; y

IV. 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.

De los anteriores, se identificó que se trabaja sobre todo con dos categorías: Datos de Identificación y datos sensibles, ya que como datos patrimoniales se recaban Numero de cuentas bancarias, estados de cuenta, CLABE interbancaria, institución bancaria, facturas, beneficiarios, datos contenidos en declaraciones patrimoniales, y Descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil).

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 autorizada.
- Pérdida o destrucción no autorizada.

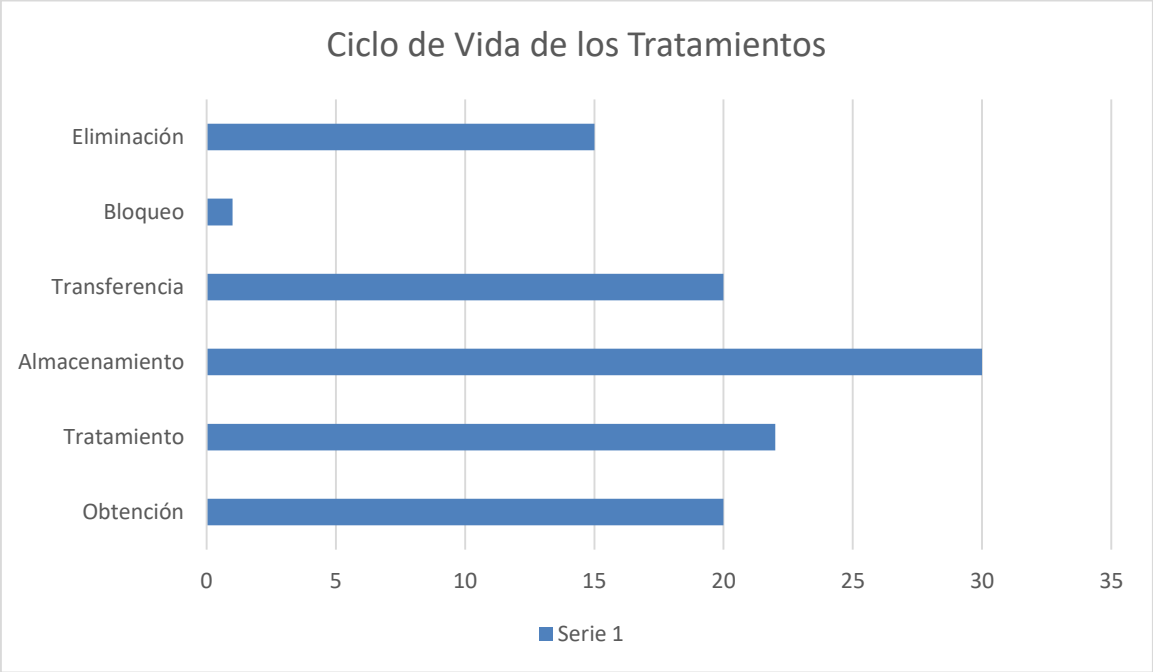
A partir de lo anterior, se consideró una probabilidad baja, media o alta de que la amenaza suceda en las distintas etapas de vida y tipo de datos personales. Además, se tomó en cuenta la consecuencia desfavorable que podría sufrir el titular en caso de vulneración, la cual puede ser leve, moderada o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

En cuanto a la valoración del riesgo por el tipo de dato en cada proceso en el que las unidades administrativas de la Oficina de Convenciones y Visitantes tratan datos personales, se señaló una escala del 1 al 4, representándose de la forma siguiente:

Tipo de Dato	Riesgo	Nivel de Riesgo
Datos identificativos	Bajo	1
Datos laborales, de domicilio laborales, patrimoniales, procedimientos administrativos	Medio	2
Datos de tránsito y movimientos migratorios; de salud, biométricos	Medio	3
Datos sensibles	Alto	4

Como resultado del levantamiento de información para el análisis de riesgo y de brecha, se identifica que la Oficina de Convenciones y Visitantes se cuenta con 4 unidades administrativas en las que tienen lugar tratamientos de datos personales para el desarrollo de los 26 procesos como se ilustra a continuación:

Al respecto, 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 en un 30%; mientras que el periodo que implica menor riesgo es el de bloqueo con un 1%.



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 autorizada.
- 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.

El análisis de brecha es de naturaleza diagnóstica y contribuye a conocer las áreas de oportunidad por cada tratamiento. A su vez, esta información da sustento a las políticas y mecanismos institucionales en materia de protección de datos personales que se han aprobado por el Comité de Transparencia para atenderlas de manera paulatina y en coordinación con cada una de las áreas.

Las medidas de seguridad administrativa, físicas y técnicas que actualmente se aplican para la Oficina de Convenciones y Visitantes 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:

a) Medidas Administrativas

- Diseño y ejecución de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.
- 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.
- Diseño e implementación de una carta responsiva por parte del personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.
- Aplicación de estrategias de seguridad, para el resguardo de los expedientes, con observancia de criterios vinculados con el sistema de gestión documental.

- Previsión de reportes de incidencias, mediante la elaboración e implementación de los formularios correspondientes.

b) Medidas Técnicas

- 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.
- 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 a la Dirección de Verificación y Tecnologías de la Información.
- Procurar la utilización de una cuenta de correo electrónico oficial para fines relacionados con las actividades laborales, evitando remitir datos personales.
- 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.
- Cuidar que en los equipos de impresión no se dejen olvidados documentos que contengan datos personales.

c) Medidas Físicas

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

CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

Los sistemas tecnológicos de la Oficina de Convenciones y Visitantes son bastante básicos, por lo que no se aplican controles de identificación y autenticación de usuarios sofisticados. La única medida que se implementa es el uso de contraseñas par el acceso a los equipos de cómputo, repositorios y cuentas de correo institucionales; mismas que son controladas por el Área de Informática.

LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

La Oficina de Convenciones y Visitantes en cuenta con el área de informática que cuenta con 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 requieran.

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 debe 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.

Debido a que la Oficina de Convenciones y Visitantes no se cuenta con algún sistema tecnológico complejo, tampoco se ha diseñado un plan de contingencia institucional en esos términos, todo se deriva de las medidas de seguridad implementadas de manera específica en cada área. Sin embargo, se cuenta con la posibilidad de recuperar los datos almacenados en las unidades de almacenaje con las que cuenta cada área.

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

- Los reportes de vulneración.
- Designación de personas encargadas de o Reportar la vulneración, o Realizar la investigación para identificar la causa y responsable de la vulneración.

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 la Oficina de Convenciones y Visitantes de manera sistemática y organizada, un sistema de técnicas para la supresión y borrado seguro, todo se hace de acuerdo con la iniciativa y posibilidad de cada área; por lo que este proceso será parte del plan de trabajo a desarrollar en el futuro inmediato. Por lo anterior, es posible afirmar que será necesaria la implementación de técnicas para la supresión y el borrado seguro que considere tanto métodos físicos que se basan en la destrucción de los medios de almacenamiento físicos electrónicos; como lógicos, basados en la limpieza de los datos almacenados en los equipos de cómputo a través de la desmagnetización y la sobre – escritura.

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 o la destrucción de medios de almacenamiento electrónicos.

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.

MONITOREO DE LAS 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 de la Oficina de Convenciones y Visitantes, 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.

La Dirección de Capacitación será la encargada de dicho monitoreo, en tanto la Oficina de Convenciones y Visitantes no cuente con una Dirección en materia de Protección de Datos Personales