



DOCUMENTO DE SEGURIDAD

**EN
DATOS PERSONALES**

**HONORABLE
CONGRESO DEL
ESTADO DE CHIAPAS**



**DOCUMENTO DE SEGURIDAD EN MATERIA
DE PROTECCIÓN DE DATOS PERSONALES
EN POSESIÓN DEL
H. CONGRESO DEL ESTADO DE CHIAPAS**

COMITÉ DE TRANSPARENCIA

Tuxtla Gutiérrez, Chiapas.

TABLA DE CONTENIDO

I.	INTRODUCCIÓN	1
II.	GLOSARIO	3
III.	OBJETIVO	5
IV.	RESPONSABILIDADES DENTRO DEL PROGRAMA	5
V.	ALCANCE DEL DOCUMENTO DE SEGURIDAD	6
VI.	SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES	8
VII.	INVENTARIO DE TRATAMIENTO DE DATOS PERSONALES	11
VIII.	ANÁLISIS DE LA INFORMACIÓN DEL INVENTARIO DE DATOS PERSONALES	13
IX.	FUNCIONES Y RESPONSABILIDADES DE LOS TRATAMIENTOS O PROCESOS DE LOS DATOS PERSONALES	24
X.	LAS TRANSFERENCIAS DE LOS DATOS PERSONALES	31
XI.	RESGUARDOS DE SOPORTES FÍSICOS Y ELECTRONICOS	32
XII.	BITACORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A SEGURIDAD DE LOS DATOS PERSONALES	34
XIII.	ANÁLISIS DE RIESGO	35
A)	CLASIFICACIÓN DE DATOS PERSONALES	36
B)	METODOLOGÍA DEL ANÁLISIS DE RIESGO	37
C)	ANÁLISIS DE LA INFORMACIÓN	41
XIV.	ANÁLISIS DE BRECHA	43
XV.	GESTIÓN DE VULNERACIONES	45
XVI.	MEDIDAS DE SEGURIDAD	47
A)	IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD.	47
B)	PROCEDIMIENTO PARA ACTUAR ANTE POSIBLES INCIDENCIAS	50
XVII.	CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS	51
XVIII.	PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS	51
XIX.	PLAN DE CONTINGENCIA	52
XX.	TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES	53
XXI.	PLAN DE TRABAJO	53
XXII.	MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD	54
XIII.	PROGRAMA DE CAPACITACIÓN	56
XXIV.	ACTUALIZACIONES	57
XXV.	APROBACIÓN DEL DOCUMENTOS DE SEGURIDAD	58
XXVI.	REFERENCIAS BIBLIOGRAFICAS	60

I. INTRODUCCIÓN

La protección de datos personales es un derecho humano, y se entiende como toda información concerniente a una persona física identificada o identificable y está regulado por los artículos 6°. Apartado A, fracción II y 16, párrafo segundo, de nuestra Constitución Política Federal; así como, por el numeral 3°. de la Constitución Política del Estado Libre y Soberano de Chiapas; asimismo, los servidores públicos que tengan acceso a datos personales están obligados a conocer y aplicar las medidas que resulten necesarias para salvaguardar los mismos y garantizar la privacidad de las personas de que se traten, desde la obtención hasta la eliminación de dichos datos.

En ese sentido, resultan de gran relevancia las reformas y adiciones que en la materia se han realizado a nuestra Constitución Política Federal, para salvaguardar este derecho humano; mismas que dieron pauta para que el 26 de enero de 2017, se publicara en el Diario Oficial de la Federación, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, cuyo objetivo conforme al artículo 1º., párrafo tercero de la misma, 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.

Es por ello que está LXVIII legislatura del Honorable Congreso del Estado de Chiapas, a fin de dar cumplimiento a las obligaciones estipuladas en los artículos 45, 47, 48 y 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, y sabedores de que la protección de datos personales es un derecho fundamental autónomo e independiente del derecho a la información, siendo por lo tanto un activo que debe protegerse; se implementó un Sistema de Gestión de Protección de Datos Personales y mejora continua, para poder elaborar el Documento de Seguridad de Datos Personales de este poder legislativo, el cual contempla el ciclo PHVA (Planear-Hacer-Verificar y Actuar); para ello se inició con un diagnóstico a través de un inventario de datos personales, se conocieron las funciones y obligaciones de las personas que tratan datos personales, también se realizó el análisis de brecha de las medidas de seguridad y el análisis de riesgo de vulneraciones, así también se generaron las medidas de seguridad necesarias, se

planteó un programa de capacitación y finalmente la verificación o evaluación de las medidas de seguridad, para poder actualizar y mejorar paulatinamente.

El Documento de Seguridad, se define como un instrumento que describe las acciones relacionadas con las medidas de seguridad administrativas, físicas y técnicas, adoptadas por este Poder Legislativo, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que se encuentran bajo su resguardo, ello acorde al principio de responsabilidad y los deberes de confidencialidad y seguridad.

Es relevante mencionar que el contenido del documento de seguridad se realizó con la colaboración de las áreas que conforman este Poder legislativo y que manifestaron tratar datos personales, en coordinación con la Unidad de Transparencia y con la asesoría del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas; conforme a las disposiciones normativas, a efecto de visibilizar las acciones actuales y planear las futuras para el adecuado tratamiento de los datos personales.

II. GLOSARIO

Activo de información: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad.

Amenaza: A cualquier posible acto que pueda causar algún tipo de daño a los activos de información.

Archivo: Conjunto de expedientes y documentos legislativos y administrativos, que contienen información inherente al funcionamiento del H. Congreso del Estado de Chiapas, en cualquier soporte documental, en el ejercicio de sus atribuciones o en el desarrollo de sus actividades y que son organizados institucionalmente, respetando los principios de procedencia, orden original y ciclo vital de documento.

Áreas: Unidades administrativas que integran al H. Congreso del Estado de Chiapas, que cuentan o puedan contar, dar tratamiento y ser responsables de los datos personales.

Autodeterminación informativa: Es un derecho fundamental que habilita a la persona para decidir, por sí sola, sobre la difusión y utilización de sus datos personales con un fin determinado y con independencia del tipo de soporte (físico o electrónico) en el que se encuentren los datos personales.

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Comunicación: Toda comunicación de datos personales que se realiza entre áreas distintas dentro del H. Congreso del Estado de Chiapas.

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

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

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

Enlace: La persona designada por el titular de las áreas responsables para fungir como responsable entre el área y la Unidad de Transparencia, con la finalidad de construir, asesorar e informar, las acciones en materia de protección de datos personales.

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

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

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

LTAIPECH: Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

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

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

Responsable de área: Titulares de las unidades administrativas que integran el H. Congreso, que manifestaron tratar datos personales.

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

Sujeto Responsable: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Ayuntamientos, Órganos Constitucionales Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos, en este caso el H. Congreso del Estado de Chiapas.

Titular: Persona física a quien corresponden los datos personales.

Transferencias: Toda comunicación de datos personales que se realiza a persona o dependencia distinta del H. Congreso del Estado de Chiapas, ya sea dentro o fuera del territorio mexicano.

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, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Usuario: La persona que, por sus actividades laborales y atribuciones legales, tenga acceso a los datos personales.

Verificación: Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este documento.

Vulnerabilidad: Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

III. OBJETIVO

El presente Documento de Seguridad, provee el marco de trabajo necesario para la protección de datos personales en posesión de este Honorable Congreso del Estado de Chiapas, en conjunto con sus recursos administrativos, físicos y financieros, mismos en los que se debe garantizar su protección, a través de mecanismos, procedimientos y procesos internos que aseguren la salvaguarda de cada uno de ellos. Es a través de este Documento de Seguridad que se pretende establecer, implementar, operar, monitorear y mejorar las acciones encaminadas a la confidencialidad, integridad y disponibilidad de la información de carácter personal en posesión de los sujetos responsables.

El H. Congreso busca establecer mecanismos orientados al tratamiento de datos personales, de conformidad con la normatividad aplicable a la materia, identificando las vulnerabilidades o amenazas que representan un riesgo, para prevenir y en su caso lograr mitigarlas. En consecuencia, se promueve la adopción de mejores prácticas en la protección de datos personales, con la continua capacitación y sensibilización de los servidores públicos, para que juntos podamos ejecutar los mecanismos para el adecuado cumplimiento de los deberes y principios derivados de la legislación vigente en la materia.

IV. RESPONSABILIDADES DENTRO DEL PROGRAMA.

Está Sexagésima Octava Legislatura a través del Presidente de la Junta de Coordinación Política, interesado en generar e implementar el Documento de Seguridad en materia de Protección de Datos Personales, dio seguimiento durante toda su integración, con la finalidad de proporcionar una herramienta de apoyo

para la observancia de los mecanismos de transparencia, acceso a la información pública y protección de datos personales como temas fundamentales en la labor que desempeñan los servidores públicos adscritos al Honorable Congreso del Estado de Chiapas. Por lo que, de conformidad a lo establecido en el artículo 35 de la Ley General de Protección de Datos Personales y el 49 de la LPDPPSOECH, los que contemplan la obligatoriedad de contar con un documento de seguridad en el cual se incluya al menos el inventario de datos personales, las funciones y obligaciones de las personas que traten datos personales, el análisis de riesgos, el análisis de brecha, el plan de trabajo, los mecanismos de monitoreo y revisión de las medidas de seguridad, y un programa general de capacitación; damos cumplimiento a los principios y deberes establecidos en los artículos del 12 al 58 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Una vez aprobado el Documento de Seguridad por el Comité de Transparencia del Honorable Congreso del Estado de Chiapas, conforme a lo establecido en los artículos 113 y 114 de la LPDPPSOECH, con la finalidad de coordinar, supervisar y realizar las acciones necesarias para salvaguardar el derecho a la protección de los datos personales, así como su cumplimiento, será de observancia obligatoria para todos los servidores públicos que en el ejercicio de sus funciones traten datos personales.

V. ALCANCE DEL DOCUMENTO DE SEGURIDAD.

La aplicación del Documento de Seguridad, es obligatorio a todas las unidades administrativas que manifestaron tratar datos personales en el ejercicio de sus atribuciones conforme a los procesos que realizan cotidianamente, por tal razón para la construcción del mismo, se realizaron capacitaciones, contando con la participación de las áreas para elaborar el diagnóstico de los diversos tratamientos que se llevan a cabo en cada una de las unidades administrativas que conforman este H. Congreso del Estado. Este ejercicio sirvió para identificar de los tipos de datos personales que se tratan, así como de las personas responsables de cada tratamiento, también de las obligaciones y deberes que señala la normatividad, en su actuar laboral diario; desde que se obtiene, usa, registra, organiza, elabora, utiliza, difunde, almacena, maneja, aprovecha, comunica o transfiere datos personales, pasando por la conservación hasta su depuración o destrucción.

Obligaciones de las áreas internas del H. Congreso del Estado que tratan datos personales son las siguientes, mismas que se citan de manera enunciativa más no limitativa:

- ❖ Cumplir con los principios y deberes establecidos en la Ley de la materia para el adecuado tratamiento de los datos.
- ❖ Incentivar la capacitación y concientización de la ética profesional del personal.
- ❖ Impulsar las medidas necesarias para el adecuado tratamiento de los datos personales conforme a los principios y deberes sustentados en la LGPDP y la LPDPPSOECH.
- ❖ Conocer las consecuencias administrativas y legales, que implica un tratamiento indebido y que pueda generar perjuicio en el titular.
- ❖ Proponer las medidas de seguridad, esquemas de mejores prácticas, y demás estrategias que se consideren necesarias.

Así entonces, las unidades administrativas que forman parte del H. Congreso del Estado de Chiapas que deberán observar y ejecutar el Documento de Seguridad son las siguientes:

- ❖ Junta de Coordinación Política (JUCOPO)
- ❖ Mesa Directiva
- ❖ Secretaría de Servicios Parlamentarios:
 - Unidad de los Archivos de Trámite
 - Trámites legislativos
- ❖ Secretaría de Servicios Administrativos:
 - Unidad de Tesorería
 - Unidad de Planeación
 - Unidad de Recursos Humanos
 - Unidad de Recursos Materiales y Servicios Generales
 - Unidad de Contabilidad y Control Presupuestal
- ❖ Dirección de Asuntos Jurídicos
- ❖ Contraloría Interna
- ❖ Coordinación de Atención a municipios
- ❖ Instituto de Investigaciones Legislativas
 - Biblioteca "Mariano Robles Domínguez"
 - Hemeroteca
 - Archivo histórico "Ángel Robles Domínguez"
- ❖ Dirección de Comunicación Social

- ❖ Unidad de Transparencia
 - Área de Protección de Datos Personales
 - Área de Acceso a la Información Pública
- ❖ Unidad de Informática
 - Área de Soporte Técnico y Redes
 - Área de Desarrollo de Sistemas

VI. SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES.

El sistema de gestión de datos personales, es el conjunto de elementos y actividades interrelacionadas a través de las cuales el H. Congreso del Estado de Chiapas, garantiza el tratamiento de los datos personales que realiza como parte de su quehacer institucional, desde su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación que lleve a cabo; asimismo, con la intención de implementar, operar, monitorear, revisar y mejorar el tratamiento y seguridad de esos datos, conforme a lo previsto en la legislación de la materia. En ese sentido, se dio inicio al análisis e identificación de los procesos y tareas en los que, de acuerdo a las atribuciones y funciones de las áreas administrativas que integran al H. Congreso del Estado, realizan tratamientos de datos personales; asimismo, de conformidad con el artículo 47 de la LPDPPSOECH se elaboró un inventario de los datos personales para establecer y mantener las medidas de seguridad para la Protección de Datos Personales.

El inventario de los datos personales contribuye a establecer el ciclo de vida de los datos personales, entendiendo que, una vez concluida la finalidad, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión, eliminación o destrucción, vinculado con el proceso de gestión documental implementado en el H. Congreso del Estado de Chiapas.



Así entonces, para el debido cumplimiento de las obligaciones establecidas en la LPDPPSOECH, los deberes que norman la protección de datos personales, son: el deber de confidencialidad y de seguridad; así mismo, los principios son: el de responsabilidad, proporcionalidad, licitud, finalidad, lealtad, consentimiento, calidad, e información; mismos que constituyen su aplicación obligatoria para los sujetos obligados, con el propósito de garantizar la integridad, disponibilidad y confidencialidad de la información personal, los que de manera sucinta se describen a continuación:

Principio de **proporcionalidad**, cada unidad administrativa debe tratar datos personales únicamente cuando resulten exclusivamente necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron, no se debe recolectar o usar datos, que no guarden estrecha relación con la finalidad del tratamiento.

El principio de **licitud**, se refiere a que cada tratamiento de datos personales está sujeto a las atribuciones o facultades que la normatividad aplicable confiere a cada una de las áreas; de esta manera nadie puede utilizar datos personales para actividades ilícitas, lo anterior implica que con las capacitaciones que se están implementando y que serán continuas los servidores públicos conocerán la normatividad en la materia para un correcto actuar.

Las acciones implementadas sirven para que el titular de los datos, conozca entre otras cosas, la finalidad del uso de sus datos personales, esto se realiza a través del Aviso de Privacidad, que se encuentra en su versión simplificada en cada una de las áreas que manifestaron tratar datos personales, y la versión integral, publicada en el portal de este Poder Legislativo, cumpliendo con el principio de **información**. El aviso de Privacidad cuenta con los siguientes elementos informativos: La manifestación de protección de datos personales, el área responsable del tratamiento de datos personales, la finalidad del tratamiento, los datos personales que se recaban, los mecanismos y medios para ejercer los derechos de Acceso, Rectificación, Cancelación u Oposición de datos personales (ARCO) y que a mediano plazo podrá realizarse el derecho de Portabilidad (ARCOP), el fundamento legal, así como la expresión de realizar transferencia de datos en los casos necesarios, la mención en su caso de tratar datos sensibles, y el medio electrónico mediante el cual el titular puede consultar el aviso de privacidad integral y la fecha de elaboración o actualización.

El principio de **consentimiento**, obliga al responsable del tratamiento, en caso de no estar dentro de alguna de las excepciones previstas en la normatividad, a solicitar el consentimiento del titular para el tratamiento de sus datos personales, este principio se cumple al hacer público el aviso de privacidad versión simplificada en el área y la versión integral en el portal de Internet de este H. Congreso del Estado. Este consentimiento puede ser expreso o tácito; el expreso se requiere cuando se tratan datos sensibles o se realizan transferencias, obteniéndose a través de huella dactilar, firma autógrafa o firma electrónica; en todos los demás casos es suficiente con que se ponga el aviso de privacidad a disposición, y el titular no se oponga al tratamiento, en este caso nos referimos al consentimiento tácito. En todos los casos el consentimiento debe ser libre, específico e informado.

El principio de **lealtad**, consiste en que el tratamiento de datos no solo debe ser legal sino también leal, es decir que el responsable no deberá obtener y tratar datos personales a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, por lo que deben otorgarse de manera voluntaria, cuidando que no exista error, mala fe, violencia o dolo.

Los principios de **calidad y finalidad**, son muy importantes y van vinculados en la práctica cotidiana, la LPDPPSOECH establece que los datos personales sean veraces, exactos, completos, correctos y actualizados, pero sobre todo que se suspenda de tratar información que ya no es necesaria para cumplir con las finalidades para los cuales fueron entregados en su momento.

Finalmente, el principio de **responsabilidad**, se refiere a que los responsables del tratamiento de los datos personales además de tomar las medidas necesarias para cumplir con los principios y obligaciones, deben realizar un esfuerzo adicional para observar las mejores prácticas y estándares en la protección de datos personales, y rindan cuentas con relación al uso y cuidado de la información personal que esté en su posesión. Por lo anterior, es necesario trabajar y pensar de forma preventiva, como dice la especialista en la materia Ann Cavoukian¹, “*Lo predeterminado es lo que manda*”, y si pensamos en el debido tratamiento de datos desde el principio y

¹ Cavoukian, A. (2011). Privacy by design: los 7 principios fundamentales. Disponible en: <https://www.acc.com/chapters/euro/upload/7foundationalprinciples-spanish.pdf>

no cuando la vulneración está dada, garantizaremos mejores niveles de tratamiento de la información de las personas.

Es importante precisar que, los responsables de las áreas que tratan datos personales, están obligados a generar acciones que estimen pertinentes para contar con el aviso de privacidad respectivo, previo al inicio de los procesos en los que se traten datos personales, por lo que es importante la capacitación a los servidores públicos de este poder legislativo, acción que se contempla en el programa de capacitación de este documento de seguridad.



Colocación de los Avisos de Privacidad Simplificado.

VII. INVENTARIO DE TRATAMIENTO DE DATOS PERSONALES

Por inventario de tratamiento de datos personales, se entiende al control documentado que se lleva de los tratamientos o procesos en los que tratan datos personales las áreas administrativas que integran el H. Congreso del Estado de Chiapas, realizado con orden y precisión.

Para dar cumplimiento a lo establecido en el artículo 47 fracción III, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, y para efecto de obtener un diagnóstico del conocimiento y tratamientos de datos personales, previa capacitación se elaboraron diversos formularios que fueron llenados por las distintas áreas administrativas, enfocándose en dos

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

actividades: 1) precisar que acción o procedimiento realizan y que tipo de datos personales son tratados por cada proceso, y 2) conocer el proceso de tratamiento que cada área efectúa, desde la recolección del dato hasta la conclusión del fin para el que fue proporcionado, así como su conservación o bien su destrucción. De acuerdo al análisis realizado de los distintos inventarios de datos personales, se desprendió qué son 18 áreas las que manifestaron tratar datos personales, las cuales fueron enlistadas en el apartado 3 de este documento.

Los rubros que integran el inventario de datos personales son los siguientes:

Medios de obtención de datos personales	<ul style="list-style-type: none"> • Manera en la que los sujetos responsables obtienen los datos personales de los titulares.
Tipo de datos personales tratados	<ul style="list-style-type: none"> • Datos personales necesarios para que el sujeto obligado pueda dar atención al tratamiento. Se diferencian entre sensibles y no sensibles.
Finalidades del tratamiento de datos personales	<ul style="list-style-type: none"> • Motivos por los que el sujeto responsable solicita los datos personales. Las finalidades deben ser concretas, lícitas, explícitas y legítimas
Áreas y servidores públicos con acceso al tratamiento	<ul style="list-style-type: none"> • Personas de los sujetos responsables que, conforme al ámbito de sus atribuciones, tratan los datos personales.
Medios de almacenamiento y conservación de los datos	<ul style="list-style-type: none"> • Medios en los que se almacenan los datos personales, puede ser en formato físico, electrónico o ambos.
Transferencias, comunicación o difusión	<ul style="list-style-type: none"> • Los datos personales que, en su caso puedan estar sujetos a una comunicación dentro o fuera del H. Congreso
Bloqueo, cancelación, supresión o destrucción de los datos	<ul style="list-style-type: none"> • Forma y tiempos del tratamiento de datos personales.

VIII. ANALISIS DE LA INFORMACIÓN DEL INVENTARIO DE DATOS PERSONALES.

A continuación, se muestra a manera de tablas el análisis de los tratamientos de datos personales:

a) Procesos o tratamientos por unidad administrativa y sus áreas correspondientes.

Órganos de Gobierno, Unidad Administrativa.	Área	Proceso o Tratamiento
Mesa Directiva	Presidencia	<ul style="list-style-type: none"> ❖ Programación de reuniones de trabajo con la representante del poder legislativo. ❖ Registro de atención al público
Junta de Coordinación Política	Presidencia	<ul style="list-style-type: none"> ❖ Registro de personas que solicitan audiencia, y programación de reuniones de trabajo. ❖ Propuestas al Pleno, para la integración de las Comisiones legislativas.
Unidad Administrativa.	Área	Proceso o Tratamiento
Secretaría de Servicios Parlamentarios	Unidad de los Archivos de Trámite	<ul style="list-style-type: none"> ❖ Solicitudes de Desincorporaciones de Predios del Patrimonio Municipal presentadas por los Ayuntamientos
	Trámites Legislativos	<ul style="list-style-type: none"> ❖ Propuestas de Nombramientos por Servidores Públicos.
Secretaría de Servicios Administrativos.	Unidad de Tesorería	<ul style="list-style-type: none"> ❖ Alta de nómina de los Diputados. ❖ Pago de Proveedores. ❖ Pago de Cheques.
	Unidad de Planeación y Presupuesto	<ul style="list-style-type: none"> ❖ Integrar y publicar formato de montos por ayudas y subsidios.
	Unidad de Recursos Humanos	<ul style="list-style-type: none"> ❖ Contratación y Alta de Personal. ❖ Altas y bajas en el IMSS. ❖ Inscripción y créditos INFONACOT. ❖ Elaboración y dispersión de nómina.

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

		<ul style="list-style-type: none"> ❖ Inscripción y créditos al INFONAVIT ❖ Respuestas a solicitudes de acceso a la información ❖ Elaboración de constancias ❖ Seguro de vida.
	Unidad de Contabilidad y Control Presupuestal	<ul style="list-style-type: none"> ❖ Resguardo de Información de operaciones financieras
	Unidad de Recursos Materiales y Servicios Generales	<ul style="list-style-type: none"> ❖ Directorio de proveedores. ❖ Generación de resguardos ❖ Requerimientos de los diputados (as)
Dirección de Asuntos Jurídicos	Jurídico	<ul style="list-style-type: none"> ❖ Actas administrativas. ❖ Contratos y convenios ❖ Procesos jurídicos
Contraloría Interna	Contraloría	<ul style="list-style-type: none"> ❖ Proceso de Acta-Entrega Recepción de Servidor es(as) Públicos (as) ❖ Atención y Seguimiento al Buzón de sugerencias y Quejas del H. Congreso del Estado de Chiapas. ❖ Seguro de Vida ❖ Declaración Patrimonial y de Intereses. ❖ Videocámaras ❖ Procedimientos de Responsabilidad Administrativa
Instituto de Investigaciones Legislativas	Investigación legislativa.	<ul style="list-style-type: none"> ❖ Investigaciones Legislativas ❖ Coordinación de visitas guiadas ❖ Control de oficios recibidos y emitidos por el Instituto ❖ Elaboración de la agenda legislativa
	Departamento de Biblioteca "Mariano Robles Domínguez"	<ul style="list-style-type: none"> ❖ Control de Acceso, y Control de Préstamos de Libros ❖ Control de Préstamos de Equipos de Cómputo.
	Departamento Hemeroteca	<ul style="list-style-type: none"> ❖ Trámite para Consulta de Diarios Locales.
	Departamento de Archivo Histórico "Ángel Robles Domínguez"	<ul style="list-style-type: none"> ❖ Préstamo de documentación para la consulta presencial (de usuarios internos externos al H. Congreso. ❖ Implementación de la clasificación archivística de la documentación generada en las áreas que integran el H. Congreso del Estado.

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

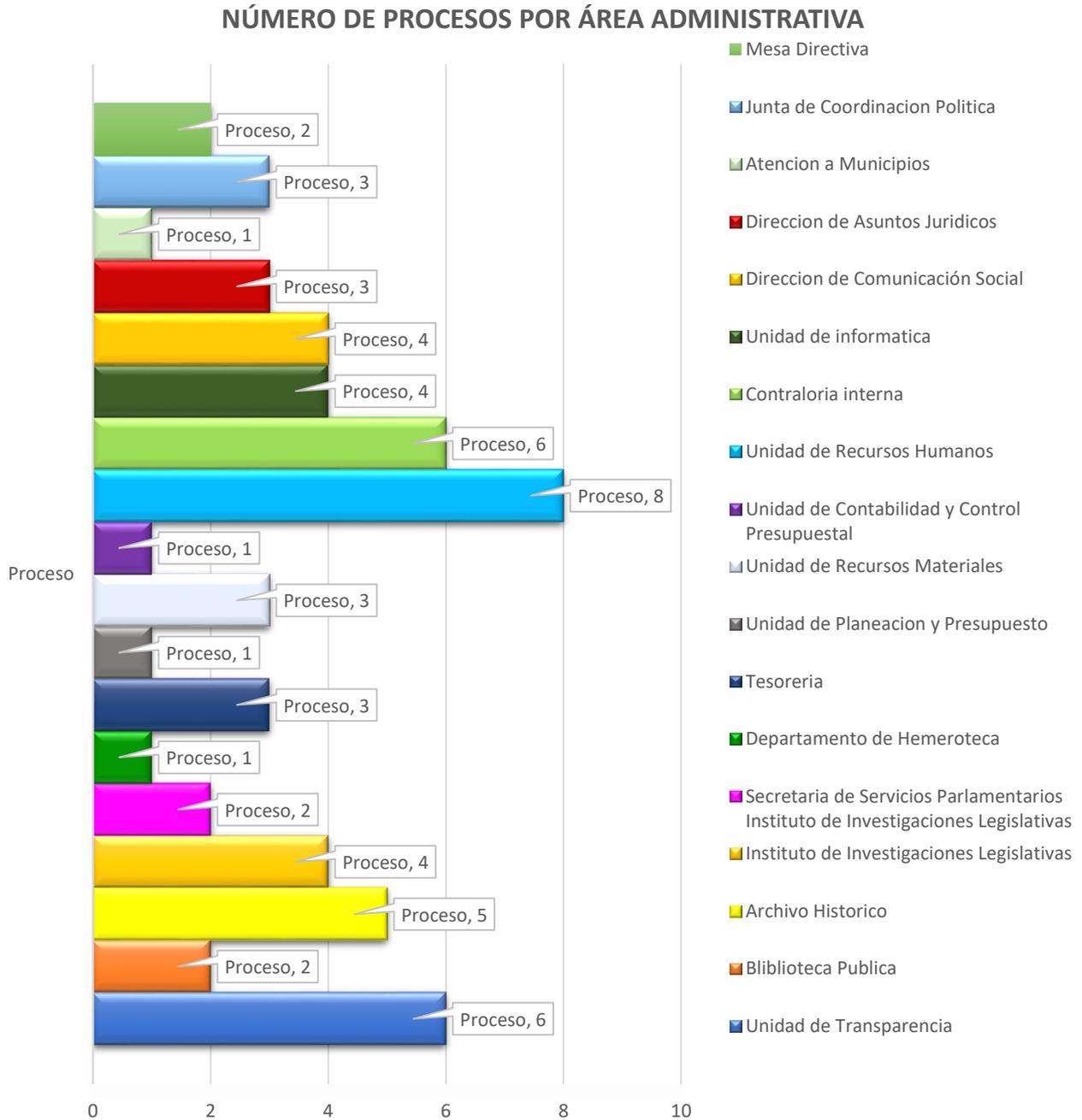
		<ul style="list-style-type: none"> ❖ Brindar Asesorías y capacitación en materia de archivos al personal del H. Congreso del Estado. ❖ Atender solicitudes de información del portal de Transparencia, áreas internas del H. Congreso del Estado. ❖ Préstamo de documentación para trámites de las áreas internas del H. Congreso del estado.
Dirección de Comunicación Social	Dirección	<ul style="list-style-type: none"> ❖ Monitoreo de la síntesis informativa ❖ Proceso Informativo para medios de comunicación ❖ Cobertura de eventos y producción de material gráfico y audiovisual. ❖ Servicios de Publicidad
Coordinación a Atención de Municipios	Coordinación	<ul style="list-style-type: none"> ❖ Atender los asuntos Relacionados con los Municipios.
Unidad de Transparencia	Área de Acceso a la Información Pública	<ul style="list-style-type: none"> ❖ Trámite de solicitudes de Acceso a la Información Pública y de Derechos ARCO ❖ Directorio de enlaces (Capacitación y Reuniones de Trabajo). ❖ Atención a requerimientos del ITAIPCH ❖ Atención a denuncias por incumplimiento a las obligaciones de transparencia y Recursos de Revisión.
	Área de Protección de Datos Personales.	<ul style="list-style-type: none"> ❖ Directorio de enlaces (Capacitación y Reuniones de Trabajo). ❖ Atención a requerimientos del ITAIPCH (Procedimientos de Verificación)
Unidad de Informática	Área de Desarrollo y Sistemas.	<ul style="list-style-type: none"> ❖ Directorios de Diputados del H. Congreso del Estado de Chiapas. ❖ Credencialización Oficial del personal del H. Congreso. ❖ Solicitudes de Servicio Web del H. Congreso del Estado de Chiapas.
	Área de soporte técnico	<ul style="list-style-type: none"> ❖ Solicitudes de servicio.

Cuadro 1. Tratamientos por área administrativa.

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

En la siguiente gráfica se refleja el número de procesos por unidad o área administrativa.



Cuadro 2. Número de procesos por área administrativa.

Con la gráfica anterior, es posible determinar que el área administrativa con mayor número de procesos es la Unidad de Recursos Humanos con un total de 10 procesos,

mientras que el Departamento de Hemeroteca, únicamente tiene 1 proceso o tratamiento.

b) Tratamiento de datos personales por categoría o tipo de dato.

Del mismo modo, se observó que principalmente se realiza el tratamiento de datos de tipo identificativo, laboral y patrimonial (este último únicamente en las declaraciones patrimoniales respecto de los servidores públicos); así también, se tratan datos identificativos de titulares externos, como son proveedores, o ciudadanos que participan en alguna convocatoria para ocupar cargos públicos, o bien, en relación a la designación o ratificación de servidores públicos por parte del Poder Legislativo del Estado de Chiapas, así como, en relación a algún proceso jurídico de la Competencia del H. Congreso del Estado.

Ahora bien, por lo que se refiere a datos sensibles, únicamente tres áreas manifestaron tratar por lo menos alguno de los datos de esta categoría, pudiendo ser datos de salud, origen, o características físicas; finalmente se identificó el tratamiento de datos de menores de edad hijos de los/as trabajadores (as) del H. Congreso del Estado, exclusivamente para el registro de seguridad social, en el seguro de vida o en la declaración patrimonial.

En la siguiente gráfica se representan las categorías o tipos de datos personales que son tratados en las áreas administrativas.



Cuadro 3. Tipos de datos personales tratados por área administrativa.

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

Podemos concluir que la categoría de datos personales que mayormente son tratadas, son la de carácter identificativo, en segundo término, los datos laborales, académicos, seguidos por los que tratan datos sensibles y finalmente los patrimoniales.

Asimismo, se observó que la unidad administrativa con más tratamientos de datos personales es la Secretaría de Servicios Administrativos, esto debido a las funciones que desempeña cada una de las áreas que la integran como son: Recursos humanos, tesorería, planeación, recursos materiales y contabilidad.

c) Fundamento legal de los procesos y los medios de obtención de los datos personales.

Así también y con la intención de dar cumplimiento al principio de legalidad, en el inventario de datos personales las áreas administrativas del H. Congreso del Estado, en la siguiente tabla se especifica el fundamento legal de sus tratamientos y los medios de obtención de los datos:

UNIDAD ADMINISTRATIVA	ÁREAS	PROCESO	FUNDAMENTO	MEDIO DE OBTENCIÓN DE DATOS
JUNTA DE COORDINACIÓN POLÍTICA	Presidencia	Registro de personas que solicitan audiencia, y programación de reuniones de trabajo.	Artículo 17 de la sección primera de la Ley Orgánica del H. Congreso del Estado de Chiapas.	Por comunicación interna
		Propuestas al pleno para la integración de las Comisiones Legislativas.	Artículo 15 de la sección primera de la Ley Orgánica del H. Congreso del Estado de Chiapas	
		Videocámaras	Artículo 17, inciso E) de la Ley Orgánica del H. Congreso del Estado de Chiapas	
(SECRETARÍA DE SERVICIOS ADMINISTRATIVOS)	Unidad de Tesorería	Altas de nóminas de los Diputados	Artículo 6to. de la Constitución Política Federal, apartado A.	De manera personal
		Pago de cheques	Artículo 45, numeral 1, inciso A de la Ley Orgánica del H. Congreso el Estado	
		Pago de proveedores.	Artículo 6to. de la Constitución Política Federal, apartado A.	Por comunicación interna

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

		Plantilla de Alta	Artículo 45. Inciso B de la Ley Orgánica del H. Congreso el Estado.	De manera personal.
		Altas y bajas al IMSS	Artículo 2 de la Ley Federal del Trabajo y del Seguro Social.	De manera personal
		Inscripción y Créditos INFONACOT	Artículo 132 fracción XXVI de la Ley Federal del Trabajo.	Vía portal de internet o sistema informático.
		Elaboración y dispersión de nomina	Artículo 45 incisos B de la Ley Orgánica del H. Congreso del Estado de Chiapas.	Por comunicación interna
		Inscripción y Créditos INFONAVIT	Artículo 132 fracción XXVI y XXVI Bis. Ley Federal del Trabajo. Artículo 42- Reglamento de Inscripción, pago de aportaciones y entero de descuentos al INFONAVIT	Por comunicación interna De manera personal. Vía portal de internet o sistema informático
		Elaboración de Constancias	Artículo 45, numeral 1, inciso B de la Ley Orgánica del H. Congreso del Estado de Chiapas.	De manera personal
	Unidad de Recursos Humanos	Seguro de Vida	Artículo 45, numeral 1, inciso B de la Ley Orgánica del H. Congreso del Estado de Chiapas	Por comunicación interna
		Respuestas de las solicitudes del Portal de Transparencia.	Artículo 60 de la Ley de Transparencia y Acceso a la información. Art. 6to. Constitución Política de los Estados Unidos Mexicanos.	Por comunicación interna Escrito o formato presentado directamente en el H. Congreso del Estado de Chiapas.
		Contratación y prestación de servicios y compras.	Artículo 45, inciso C de la Ley Orgánica del H. Congreso del Estado.	De manera personal
	Unidad de Recursos Materiales	Orden de pago.	Artículo 45 inciso C de la Ley Orgánica del H. Congreso del Estado.	De manera personal
		Resguardo de Información	Artículos 6, 7, 9, 11, 12 de la Ley de Archivos del Estado de Chiapas	Por comunicación interna
	Unidad de Contabilidad y Control Presupuestal	Resguardo de Información de operaciones financieras.	Artículos 6, 7, 9, 11, 12 de la Ley de Archivos del Estado de Chiapas	Por comunicación Interna

	Unidad de Planeación y Presupuesto	Integrar y Publicar formato de montos por ayudas y subsidios.	Artículos 9 fracciones I, IX, y XIV, 14, 56, 58 y 67, último párrafo de la Ley General de Contabilidad Gubernamental y cuarto transitorio del Decreto por el que se reforma.	Por comunicación interna
DIRECCIÓN DE COMUNICACIÓN SOCIAL	Dirección de Comunicación Social	Servicios de publicidad	Artículos 18, 47, fracción III, 50, 51, 52, 53, 54, 55, 56, 57, 58, 95 y 96 de LPDPPSOECH.	Por comunicación interna
		Cobertura de eventos y producción de material gráfico y audiovisual	Artículos 18, 47, fracción III, 50, 51, 52, 53, 54, 55, 56, 57, 58, 95 y 96 de LPDPPSOECH.	De manera personal Por comunicación interna Vía telefónica Vía correo electrónico
		Proceso informativo para medios de comunicación	Artículos 18, 47, fracción III, 50, 51, 52, 53, 54, 55, 56, 57, 58, 95 y 96 de LPDPPSOECH.	De manera personal Por comunicación interna Vía telefónica Vía correo electrónico
		Monitoreo de la síntesis informativa	Artículos 18, 47, fracción III, 50, 51, 52, 53, 54, 55, 56, 57, 58, 95 y 96 de LPDPPSOECH.	De manera personal Por comunicación interna Vía telefónica Vía correo electrónico
CONTRALORÍA INTERNA	Contraloría	Seguro de vida.	Artículo 51 de la ley del Servicio Civil del Estado y los Municipios de Chiapas, Fracción XIII	Vía correo electrónico de manera personal
		Declaración patrimonial y de interés.	Artículo 32, 33 y 34 de la Ley de Responsabilidades Para el Estado de Chiapas	Vía portal de internet o sistema informático
		Buzón de sugerencias, propuestas y quejas.	Artículo 55 fracción IV de la Ley Orgánica del Congreso del estado de Chiapas y artículo 90 al 93 de la Ley de Responsabilidades Administrativas para el Estado de Chiapas	Vía correo electrónico y de manera personal

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

		Acta Entrega-Recepción	Artículo 7 de la Ley de Responsabilidades Administrativas del Estado de Chiapas; 1,3,9,13, 25, 26, 27, 29, 30, 31 y 45 de la Ley que establece el Proceso de Entrega Recepción de la Administración Pública del Estado de Chiapas	De manera personal
		Procedimientos de Responsabilidad Administrativa	Artículo 55, numeral 1, fracciones III, IV y V de la Ley Orgánica del Congreso del Estado de Chiapas Artículo 90 al 93 de la Ley de Responsabilidades Administrativas para el Estado de Chiapas	De manera personal
		Videocámaras	Artículo 55, numeral 1, fracción VIII de la Ley Orgánica del Congreso del estado de Chiapas	De manera personal
Coordinación a Atención de Municipios	Coordinación	Atender los asuntos Relacionados con los Municipios.	Artículo 54 de la Ley Orgánica del H. Congreso el Estado	Por comunicación interna
UNIDAD DE TRANSPARENCIA	Área de Acceso a la Información Pública	Atención a solicitudes de acceso a la información pública y de Derechos ARCO.	Artículo 5, fracción XXXV, 6 y 7 de la LPDPPSOECH. Artículo 68 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.	Plataforma Nacional de Transparencia, vía correo electrónico Por Oficialía de Partes
		Directorio de enlaces (Capacitación y reuniones de trabajo).	Artículo 60, fracción IV de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.	Electrónica y personal
		Atención a denuncias por incumplimiento a las obligaciones de transparencia y Recursos de Revisión	Artículo 5 fracción XXXV 6 y 7, 49 al 58 de la LPDPPSOECH, 60 y70 de la ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, y Art. 61 del Reglamento de Transparencia del H. Congreso del Estado de Chiapas.	Electrónica y personal
		Atención de Requerimientos del ITAIPCH		

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

	Área de Protección de Datos Personales.	Atención de Requerimientos del ITAIPCH (Procedimientos de Verificación)	60 y 70 de la ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, y Art. 61 del Reglamento de Transparencia del H. Congreso del Estado de Chiapas.	Vía electrónica o de manera personal
		Directorio de enlaces (Capacitación y reuniones de trabajo).	Artículo 60, fracción IV de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.	Electrónica y personal
MESA DIRECTIVA	Presidencia	Programación de Reuniones de Trabajo con la representante del Poder Legislativo.	Artículo 43 inciso A) y F) de la Ley Orgánica del H. Congreso del Estado de Chiapas.	Escrito o formato presentado directamente en el H. Congreso.
		Registro de atención al público.	Artículo 23 de la Ley Orgánica del H. Congreso del Estado de Chiapas.	
SECRETARIA DE SERVICIOS PARLAMENTARIOS	Secretaria de Servicios Parlamentarios	Solicitudes de desincorporaciones de predios del patrimonio municipal presentadas por los ayuntamientos	Artículo 43 incisos A) y F) de la Ley Orgánica del H. Congreso del Estado de Chiapas.	Escrito o formato presentado directamente en el H. Congreso. Por comunicación interna. Escrito o formato presentado directamente en el H. Congreso
		Propuestas de nombramientos de Servidores públicos.	Artículo 43 de la Ley Orgánica del H. Congreso del Estado de Chiapas.	Por comunicación interna.
INSTITUTO DE INVESTIGACIONES LEGISLATIVAS	Instituto	Control de oficios	Artículo 47 de la Ley Orgánica del H. Congreso del Estado de Chiapas	Escrito o formato presentado directamente en el H. Congreso. Directamente del titular.
		Agenda legislativa.	Artículo 47 de la Ley Orgánica del H. Congreso del Estado de Chiapas	Escrito o formato presentado directamente en el H. Congreso
		Coordinación de visitas por orden de la Mesa Directiva	Artículo 47 de la Ley Orgánica del H. Congreso del Estado de Chiapas	Escrito presentado al Congreso

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

		Investigaciones Legislativas	Artículo 47 de la Ley Orgánica del H. Congreso del Estado de Chiapas	Por comunicación interna
	Biblioteca	Préstamos de material bibliográfico	Artículo 45 fracción 1 Ley de Protección de Datos Personales en Posesión de Sujeto Obligado	De manera personal. Escrito presentado directamente en el H. Congreso
		Registro de acceso y uso de los equipos de cómputo.	Artículo 47, numeral 1, fracción II, inciso C) de la Ley Orgánica del H. Congreso del Estado de Chiapas. Artículo 45 fracción 1 de la Ley de Protección de Datos Personales en Posesión de Sujeto Obligado	De manera personal. Escrito presentado directamente en el H. Congreso
	Hemeroteca	Consulta a Diarios Locales	Artículos 4, 5 fracción XXXV, 6 y 7 de la LPDPPSOECH	De manera personal. Escrito o formato presentado directamente en el H. Congreso.
	Archivo Histórico	Brindar asesorías y capacitación al personal del H. Congreso del Estado.	Ley de Archivos del Estado de Chiapas	De manera personal
		Atender solicitudes de información del portal de transparencia.	Ley de Archivos del Estado de Chiapas	Por comunicación interna Vía correo electrónico
		Préstamo de documentación para tramites de las áreas internas del H. Congreso del Estado	Artículo 4, 5, fracción XXXV, 6 y 7 de la LPDPPSOECH.	Por transferencia. Vía correo electrónico
		Préstamo de Documentación para consulta archivística	Artículo 4, 5, fracción XXXV, 6 y 7 de la LPDPPSOECH.	Transferencia o Vía correo electrónico De manera personal.
		Implementación de la clasificación archivística de la documentación en las áreas que integran el H. Congreso del Estado	Ley de Archivos del Estado de Chiapas Ley Orgánica del Congreso del Estado	

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN DE ASUNTOS JURÍDICOS	Dirección	Actas Administrativas	Art. 49 de la Ley Orgánica del H. Congreso del Estado de Chiapas	Escrito o formato presentado directamente en el H. Congreso.
		Procesos jurídicos	Art. 49 de la Ley Orgánica del H. Congreso del Estado de Chiapas Artículo 4, 5, fracción XXXV, 6 y 7 de la LPDPPSOECH.	Por transferencia. Vía correo electrónico
		Contratos y convenios	Art. 49 de la Ley Orgánica del H. Congreso del Estado de Chiapas	De manera personal
INFORMÁTICA	Área de Desarrollo y Sistemas	Solicitudes de servicio web del H. Congreso del Estado de Chiapas	Artículo 6º de la Política Federal y Art. 38 de la LPDPPSOECH.	Escrito o formato presentado directamente en el H. Congreso.
		Directorio de diputados	Artículo 6º de la Constitución Política Federal y Art. 38 de la LPDPPSOECH.	Vía portal de internet o sistema informático
		Credencialización oficial del personal del H. Congreso	Artículo 6º de la Constitución Política Federal y Art. 38 de la LPDPPSOECH.	Escrito o formato presentado directamente en el H. Congreso.
	Área de Soporte Técnico	Solicitudes de servicio	Artículo 75 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas	A solicitud de las áreas del H. Congreso

Cuadro 4. Proceso o tratamiento, fundamento y medios de obtención de los datos personales por área administrativa.

IX. FUNCIONES Y RESPONSABILIDADES DE LOS TRATAMIENTOS O PROCESOS DE DATOS PERSONALES.

Otro aspecto importante que deriva de la elaboración del presente documento, es el de precisar quiénes son los servidores públicos responsables que tratan datos personales dentro de los procesos cotidianos del día a día, esto con la intención por una parte de generar mayor sensibilización en ellos de la importancia de la seguridad de los datos tratados, porque lo que se debe proteger más que datos, es proteger los derechos de las personas; y por otro lado, implica una obligación de cumplimiento y una consecuencia en caso contrario.

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

Como lo refiere el Comisionado Javier Diez de Urdanivia, retomando el termino *compliance* - que significa el cumplimiento regulatorio, el cual obliga al cumplimiento del mandato constitucional que por un lado establece los derechos de la autodeterminación de los datos personales y por el otro la garantía de la protección de los mismos, cuando empieza el vínculo jurídico entre el titular de los datos y un tercero o sujeto obligado, que en este caso es el H. Congreso del Estado de Chiapas.

“La protección de datos personales es un entrenamiento complejo de principios”², esta protección se da cuando hay un vínculo jurídico entre un titular y otro o varios entes. Derivado de lo anterior y para dar cumplimiento, **en la siguiente tabla se puede observar el nombre del área, los procesos, la finalidad y los usuarios o servidores públicos que realizan los procesos.**

En la siguiente tabla se puede observar los procesos, la finalidad y los usuarios o servidores públicos que tratan datos personales:

PROCESO, FINALIDAD Y USUARIO				
UNIDAD ADMINISTRATIVA	ÁREAS	PROCESO	FINALIDAD DEL TRATAMIENTO	USUARIOS DEL PROCESO
JUNTA DE COORDINACIÓN POLÍTICA.	PRESIDENCIA	Registro de personas que solicitan audiencia, y programación de reuniones de trabajo.	Consulta	Dr. Víctor Hugo Guzmán Zarate
		Videocámaras	Seguridad	Dr. Víctor Hugo Guzmán Zarate
		Propuestas al pleno para la integración de las comisiones legislativas.	Consulta	Dr. Víctor Hugo Guzmán Zarate
SECRETARÍA DE SERVICIOS ADMINISTRATIVOS	UNIDAD DE TESORERÍA	Alta de nómina de diputados.	Para pago	Lic. Consuelo Gómez Román
		Pago de cheques		
		Pago de proveedores.		

² Comisionado Javier Diez de Urdanivia, inai, Conferencia en “La Ruta de la Privacidad 2022”, 26 de enero de 2022.

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

		Contratación y Alta de personal	No se cuentan	C.P. Yeri Ruíz Ruíz Lic. Carolina Ochoa García Lic. Karina Herrera Obregón
	UNIDAD DE RECURSOS HUMANOS	Altas y bajas en el IMSS	Para ser ingresados a los servicios de salud del IMSS	Lic. José Luis Ramírez Hernández Ing. Tomas Morales San Cristóbal
		Inscripción y Créditos INFONACOT	Para conocer a quienes se les aplicaran las deducciones. Para el resguardo de información de los trabajadores Contar con información para el trabajador	
		Elaboración y dispersión de nómina	Elaboración de nomina Pago de salario de trabajadores	Lic. Carolina Ochoa García Cp. José Isidro Ovando Pérez
		Inscripción y créditos al INFONAVIT.	Movimientos de afiliación al INFONAVIT	Ing. Tomas Morales San Cristóbal
			Descuento por crédito INFONAVIT	
		Solicitudes de información y obligaciones de la plataforma nacional.	Dar cumplimiento a las obligaciones de transparencia	
		Seguro de vida	Seguridad Social	Lic. José Luis Ramírez Hernández
		Elaboración de constancias.	Declaración anual	Ing. David Paredes Trinidad
	UNIDAD DE RECURSOS MATERIALES	Directorio de proveedores	Para realizar acciones de cotizaciones, compras y/o adquisiciones con los proveedores	Ing. José Alfredo Jiménez Reyes, Ing. Jessica del Rosario Sánchez Paz

		Generación de Resguardos	Para control y resguardo de los bienes muebles del H. Congreso del Estado	Lic. Anabeli Morales Gonzales
		Atención a Requerimientos de los diputados	Para realizar acciones de requerimientos o solicitudes de los diputados	C.P Raúl Alexis García Hidalgo
	UNIDAD DE CONTABILIDAD	Resguardo de Información	Resguardar la información de manera digital	C.P. Carlos Alberto López Consospo,
	UNIDAD DE PLANEACIÓN Y PRESUPUESTO	Integrar y Publicar formato de montos por ayudas y subsidios.	Integrar y publicar trimestralmente formato de montos pagados por ayudas y subsidios	Lic. Christian Miguel Salinas C.P Martha Elena Mendoza C.P. Laura Lilia Arrevillaga Cano
DIRECCIÓN DE COMUNICACIÓN SOCIAL	DIRECCIÓN DE COMUNICACIÓN SOCIAL	Servicios de Publicidad	Registro de personas que realizan la cobertura de las actividades legislativas.	Lic. Karla Irina Mendiola Calvo. Lic. Arturo Tomas Torres Guzmán
		Cobertura de eventos y Producción de material gráfico y Audiovisual.	Registro de personas que realizan la cobertura de las actividades legislativas.	Lic. Karla Irina Mendiola Calvo. Lic. Arturo Tomas Torres Guzmán
		Proceso informativo para medios de comunicación	Registro de personas que realizan la cobertura de las actividades legislativas.	Lic. Karla Irina Mendiola Calvo. Lic. Arturo Tomas Torres Guzmán
		Monitoreo de la síntesis informativa	Registro de personas que realizan la cobertura de las actividades legislativas.	Lic. Karla Irina Mendiola Calvo. Lic. Arturo Tomas Torres Guzmán
CONTRALORÍA INTERNA	CONTRALORÍA INTERNA CONTRALORÍA INTERNA	Buzón de Sugerencias, Propuestas, Quejas y Denuncias.	Recibir y dar seguimiento	Lic. Jorge David Barragán Gordillo y Personal de sistemas de la Unidad de Informática del H. Congreso del Estado de Chiapas

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

		Declaración patrimonial y de interés publico	Seguimiento para el cumplimiento	C.P María de los Ángeles Ramírez Camera y Personal de sistemas de la Unidad de Informática del H. Congreso del Estado de Chiapas
		Seguro de Vida	Datos póliza SDV Asignación de beneficiario Autorización del asegurado Datos para póliza SDV	Lic. Mariana Guadalupe Domínguez López
		Acta-Entrega Recepción	Forman parte del contenido del Acta Entrega Recepción, en el apartado de identificación del servidor publico	Mtra. María Luisa Robles Prado Mtro. Carlos Ernesto Ozuna Hodich Mtro. Alberto Vázquez Penagos Lic. Víctor Rafael Hernández Marroquín Lic. Jorge David Barragán Gordillo C.P. Iliana Zenteno Díaz Lic. Angélica C.P María De Los Ángeles Ramírez Camera Lic. Mariana Guadalupe López Domínguez
		Procedimientos de Responsabilidad Administrativa	Tramite de expedientes	Ing. Guadalupe Morales Marín Mtro. Alberto Vázquez Penagos Mtro. Carlos Ernesto Ozuna Hodich Mtra. María Luisa Robles Prado Lic. Víctor Rafael Hernández Marroquín.
COORDINACIÓN DE ATENCIÓN A MUNICIPIOS	COORDINACIÓN	Atender los Asuntos relacionados con los Municipios	La tramitación y solución de los asuntos planteados	C. Kenia Lisbeth Jiménez Alegría

UNIDAD DE TRANSPARENCIA	ÁREA DE ACCESO A LA INFORMACIÓN PÚBLICA	Atención de solicitudes de Acceso a la Información Pública y de Derechos ARCO	La tramitación y respuesta de las solicitudes	Lic. Silvia Molina Ruíz Lic. Magdalena Pablo Hernández Lic. Rodolfo Ruiz Padilla	
		Atención a denuncias de las obligaciones de Transparencia	Tramitación de los expedientes	Lic. Silvia Molina Ruíz Lic. Magdalena Pablo Hernández	
		Atención a requerimientos del ITAIPCH	Brindar cumplimiento a los distintos requerimientos	Lic. Silvia Molina Ruíz Lic. Magdalena Pablo Hernández Lic. Rodolfo padilla Ruiz	
		Directorio de Enlaces (Capacitación y reuniones de trabajo)	Comunicación efectiva	Lic. Silvia Molina Ruíz Lic. Magdalena Pablo Hernández	
	ÁREA DE PROTECCIÓN DE DATOS PERSONALES	Directorio de Enlaces (capacitación y reuniones de trabajo)	Comunicación efectiva	Lic. Rodolfo Ruiz Padilla C. Carolina Trejo Altuzar	
		Atención a requerimientos del ITAIPCH (Procedimientos de Verificación)	Tramitación del procedimiento de verificación	Lic. Rodolfo Ruiz Padilla C. Carolina Trejo Altuzar	
	MESA DIRECTIVA	PRESIDENCIA	Programación de Reuniones de Trabajo con la Representante de la Mesa Directiva	Atención a los temas concernientes a la Presidencia de la Mesa Directiva	Lic. Azucena Caridad Meza Ruiz
			Registro de Atención al Público	Brindar atención a la ciudadanía	Lic. Azucena Caridad Meza Ruiz
SERVICIOS PARLAMENTARIOS	SECRETARIA DE SERVICIOS PARLAMENTARIOS	Solicitudes de Desincorporaciones de Predios del Patrimonio Municipal presentadas por los Ayuntamientos	Tramitación de las solicitudes	Lic. Laura Vázquez Coutiño	
		Propuestas de Nombramientos de Servidores Públicos	Designación de servidores públicos	Lic. Laura Vázquez Coutiño	

INSTITUTO DE INVESTIGACIONES LEGISLATIVAS	INSTITUTO DE INVESTIGACIONES LEGISLATIVAS	Control de oficios	Consulta	Lic. Violeta del Carmen de la Cruz Ramírez
		Coordinación de visitas guiadas por orden de la Mesa Directiva	Consulta y estadísticas	Dra. Tatyana Penagos Coello
		Agenda legislativa	Investigación	Dra. Tatyana Penagos Coello
		Investigaciones legislativas	Trámites	Dra. Tatyana Penagos Coello
	BIBLIOTECA	Prestamos de Material Bibliográfico	Control de acceso Control de préstamos de libros Control de equipo de cómputo.	Dulzura Zarate Mandujano María Teresa Galdámez vera Martha Laura Escobar Flores
		Registro de acceso y uso de los equipos de computo	Control de acceso Control de préstamos de libros Control de equipo de cómputo.	Dulzura Zarate Mandujano María teresa Galdámez vera Martha Laura Escobar Flores
	HEMEROTECA	Consulta a Diarios Locales	Registro de usuarios	Lic. María Soledad Culebro Espinoza Lic. Martha Martínez Ballinas
	ARCHIVO HISTÓRICO	Brindar asesorías y capacitaciones al personal del H. Congreso del Estado.	Capacitación	Mtro. Hugo Alberto Ruis Flores Coordinador de las Áreas de Archivo
		Implementación de la clasificación archivística de la documentación en las áreas que integran el H. Congreso del Estado	Los datos personales recabados son utilizados únicamente para el acto o efecto para el cual son solicitados, posteriormente se eliminan.	Mtro. Hugo Alberto Ruis Flores Coordinador de las áreas de Archivo
		Préstamo de documentación para tramites de las áreas internas del H. Congreso del Estado	Registro de usuarios	Mtro. Hugo Alberto Ruis Flores Coordinador de las áreas de Archivo

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

		Préstamo de documentación para consulta archivística	Registro de usuarios	C. Fernando Zapata García
DIRECCIÓN DE ASUNTOS JURÍDICOS	DIRECCIÓN DE ASUNTOS JURÍDICOS	Actas administrativas	Trámite	Lic. Gustavo Fernández Díaz
		Contratos y convenios.	Consulta	Lic. Gustavo Fernández Díaz
		Procesos jurídicos	Trámite	Lic. Gustavo Fernández Díaz
UNIDAD DE INFORMATICA	AREA DE DESARROLLO DE SISTEMAS	Credencialización oficial del H. Congreso del Estado de Chiapas	La elaboración de la credencialización	Ing. Orbelin Galindo Mancilla
		Directorio de Diputados	Registrar los directorios de los diputados	
		Solicitudes de servicio web	Para dar trámite a las solicitudes	
	AREA DE SOPORTE TÉCNICO	Solicitudes de servicio	Para dar trámite a las solicitudes	Ing. Francisco Javier Gordillo Escobar.

Cuadro 5. Contiene los procesos o tratamiento, la finalidad de los mismos y los usuarios que los tratan.

X. LAS TRANSFERENCIAS DE DATOS PERSONALES.

Para efecto de saber cómo se intercambia la información que contiene datos personales de acuerdo a los distintos procesos o tratamientos, se consideraron dos conceptos, el primero que es la comunicación interna, que consiste en el traslado de información de un área a otra, pero siempre dentro del H. Congreso del Estado y el segundo la transferencia, que consiste en el traslado de información que contiene datos personales a instituciones, dependencias, organismos, poderes, entre otros, para cumplimentar los procesos específicos necesarios del Poder Legislativo.

Así entonces y derivado de las funciones de los servidores públicos en las distintas áreas, se encontró que solamente algunas realizan transferencia de datos personales a otras dependencias o instituciones fuera del H. Congreso; tal como se muestra a continuación:

Sujeto obligado receptor	Tipo de datos
Secretaría de Hacienda	<ul style="list-style-type: none"> ✓ Identificativos ✓ Laborales ✓ Patrimoniales
Instituto Mexicano del Seguro Social IMSS	<ul style="list-style-type: none"> ✓ Identificativos ✓ Laborales ✓ Patrimoniales ✓ Sensibles (de salud)
Instituto del Fondo Nacional para el Consumo de los Trabajadores INFONACOT	<ul style="list-style-type: none"> ✓ Identificativos ✓ Laborales ✓ Patrimoniales
Instituto del Fondo Nacional de la Vivienda para los Trabajadores INFONAVIT	<ul style="list-style-type: none"> ✓ Identificativos ✓ Laborales ✓ Patrimoniales
Institución bancaria	<ul style="list-style-type: none"> ✓ Identificativo ✓ Laborales ✓ Patrimoniales
Poder Ejecutivo del Estado de Chiapas	<ul style="list-style-type: none"> ✓ Identificativos ✓ Académicos

Ante este contexto, es posible concluir que el inventario de datos Personales del H. Congreso del Estado de Chiapas, a partir de los hallazgos identificados en la matriz de acciones, en donde se correlacionan las diferentes categorías de datos personales, con el tipo de tratamiento que las personas realizan en base a sus funciones y obligaciones, se constituye como un elemento del Sistema de Gestión de Datos Personales, que junto con el análisis de riesgo y las medidas de seguridad, representan un instrumento de evidencia para la implementación de directrices de la política en materia de protección de datos, con la intención de fortalecer el conocimiento y la estructura de los responsables y los usuarios, para que sus tratamientos se lleven a cabo conforme a los estándares nacionales e internacionales.

XI. RESGUARDOS DE SOPORTES FÍSICOS Y ELECTRÓNICOS

Las medidas de seguridad para el resguardo de los soportes físicos se llevan a cabo con la finalidad de evitar la alteración, pérdida o acceso no autorizados, son las siguientes:

- ✓ Manejo de bitácora de control de acceso a archivos, expedientes o sistemas que contienen datos personales, en caso de ser persona distinta al usuario responsable;
- ✓ Resguardo de documentos e información en lugares seguros, archiveros, cajones, gavetas, puertas de oficinas con cerraduras y llaves;
- ✓ Control de personas con acceso a archivos que contengan información con datos personales;
- ✓ Registro y autorización de la entrada y salida de archivos que contengan información y datos de carácter personal e indicar los detalles básicos del traslado (solicitante, objeto de la solicitud, fecha, entre otros).
- ✓ 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.
- ✓ Solicitar a la instancia competente de archivos, la asesoría y orientación para el proceso de la baja documental.

En relación, a las medidas de seguridad para el resguardo de los soportes electrónicos de los datos personales, y evitar la alteración, pérdida o acceso no autorizados a los mismos, se enumeran de la forma siguiente:

- Seguimiento del programa de mantenimiento preventivo y correctivo anual de los equipos de cómputo, que implementó la Unidad de Informática;
- Implementación de un programa y lineamientos por la Unidad de Informática, en el que se contemple el uso y la seguridad del hardware, software y la red, en donde se establezca lo siguiente:
 - Contar con un inventario de dispositivos informáticos.
 - Capacitación a los usuarios para que realicen respaldo y resguardo de la información;
 - Los equipos informáticos y periféricos son propiedad del H. Congreso del Estado y para uso exclusivo de actividades concernientes a este;
 - La red local y el acceso a internet, será exclusivamente para uso laboral;
 - Evitar guardar información personal en los equipos de cómputo;
 - Únicamente se usarán las de redes sociales, cuentas de correo o aplicaciones instaladas y/o autorizadas por la Unidad de Informática;

- Evitar abrir correos electrónicos de destinatarios desconocidos, ni descargar contenido dudoso.
- Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas;
- Contar con equipos adecuados para poder segmentar la red local, para brindar acceso a internet a usuarios externos y evitar exponer los recursos informáticos del H. Congreso. Así como la segmentación (subredes) para las áreas que tratan datos personales de riesgo alto.
- El usuario que realiza los procesos de alto riesgo es responsable de resguardar la información en la carpeta asignada por la Unidad de Informática, para realizar el respaldo de manera periódica.
- Implementación de niveles y esquema de privilegios, para que el usuario lleve a cabo las actividades que requiere de acuerdo con sus funciones.

XII. BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A SEGURIDAD DE LOS DATOS PERSONALES

Las bitácoras de acceso, operación cotidiana y vulneraciones, serán emitidas por las áreas del H. Congreso del Estado de Chiapas, mismas que contendrán de conformidad con el artículo 53 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Chiapas, lo siguiente:

- ✓ La fecha en que ocurrió la vulneración
- ✓ El motivo de la vulneración se seguridad, y
- ✓ Las acciones correctivas implementadas de forma inmediata y definitiva.

Asimismo, este H. Congreso del Estado deberá informar sin dilación alguna al titular, y según corresponda, al Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, en relación con las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en un plazo máximo de 72 horas, contemplando en el informe, lo señalado por el artículo 55 de la Ley de la materia:

- ✓ La naturaleza del incidente
- ✓ Los datos personales comprometidos
- ✓ Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses
- ✓ Las acciones correctivas realizadas de forma inmediata
- ✓ Los medios donde puede obtener mayor información al respecto.

XIII. ANALISIS DE RIESGO

La siguiente acción denominada análisis de riesgos y de brecha, está enfocada a la seguridad de los datos personales, y es considerada uno de los grandes retos a nivel institucional, sobre todo porque nos enfrentamos a la constante y cada vez más novedosa evolución y uso de las tecnologías de la información, pues actualmente los datos personales tienen mucho valor, generalmente son recabados y utilizados para finalidades comerciales, incluso se dice que estamos en proceso de la cuarta revolución industrial, en donde los datos de cada ser humano son el activo con más valor cuantitativo.

No podemos decir aún, que para el sector público dejen de tener valor, pues el impacto, y por tanto el riesgo, se valora en términos del costo derivado del valor de los activos afectados, además de los daños producidos en el propio activo, como pueden ser los siguientes:

- ✓ “Daños personales
- ✓ Pérdidas financieras
- ✓ Interrupción de servicios
- ✓ Perdida de reputación”³
- ✓ Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.

Así entonces y conforme a la normatividad, misma que señala que es obligación de los sujetos obligados el determinar los riesgos existentes y la posibilidad de mitigarlos a través de un análisis cualitativo, sobre el impacto y la probabilidad de que una amenaza vulnere la seguridad, tanto en la información de los datos personales como en los recursos involucrados, lo que dará pauta a la implementación de medidas de seguridad.

Bajo esta premisa, para analizar los riesgos de los datos personales que son objeto de tratamiento por el H. Congreso del Estado de Chiapas, se aplicó un instrumento para, clasificar los datos utilizados, a partir de la siguiente categorización de Datos Personales, de manera enunciativa más no limitativa:

³ “Recomendaciones para conocer las principales amenazas a los datos personales”, P.15, INAI, Edición. -abril de 2021

a) Clasificación de datos personales

1) **De identificación**, que se refieren a información por la que se identifica a una persona y/o permiten su contacto como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población o la fecha de nacimiento.

2) **Laborales**, son aquellos que hacen referencia a nombramiento, capacitación, puesto o cargo, domicilio de trabajo, correo institucional, teléfono institucional, trayectoria profesional.

3) **Académicos**, se refieren a la trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos y constancias.

4) **Patrimoniales**, que comprenden la información que se encuentran vinculados al patrimonio de una persona como, por ejemplo, cuentas bancarias, estados de cuenta, clave interbancaria, bienes muebles e inmuebles, los créditos, las tarjetas de débito, los cheques o las inversiones.

5) **Datos en procedimientos administrativos seguidos en forma de juicio y/o judiciales.**

La información relativa a una persona que se encuentra sujeto a un procedimiento administrativo seguido en forma de juicio y demás análogos.

6) **Sensibles**, que consideran la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleva un riesgo grave para éste como, por ejemplo, datos de **salud**, el **origen étnico o racial**, **ideológicos** (las creencias religiosas, filosóficas, afiliación política o sindical, pertenencia a organizaciones religiosas o de la sociedad civil), **vida sexual**; y con la evolución de la tecnología ya también se consideran como sensibles los datos **biométricos** (ADN, huella dactilar, reconocimiento facial, imagen de iris y retina, geometría de la mano, reconocimiento de la voz u otros análogos); los datos **electrónicos particulares** (Número de Identificación Personal (NIP), correos electrónicos particulares, contraseñas, entre otros) y las **características físicas** (color de piel, color de iris, color de cabello, señas particulares, discapacidades, entre otros).

Ante este escenario, resulta importante la valoración de los **riesgos de los datos personales** que se tratan, con el propósito de detectar las áreas de oportunidad y mejora necesaria, para un adecuado tratamiento. Lo que nosotros queremos lograr es generar una cultura de prevención, es decir prever y así evitar lo inesperado. Partiremos primero del reconocimiento de que hay ciertos escenarios de riesgo, los cuales queremos mitigar a través de la mejora continua.

b) Metodología del Análisis de Riesgo

La metodología de análisis de riesgo que empleamos, establece un proceso que consiste en identificar y correlacionar los elementos que intervienen en el riesgo, como lo son:

El activo, que en este caso se refiere a los datos personales, **Las amenazas**, que son factores externos que tienen el potencial de dañarlos y, **Los escenarios de vulneración**, que en este caso son dos: el primero, es el número de veces que se accede a la información, y el segundo, el entorno mediante el cual se accede a la información.

Por lo tanto, el valor de riesgo de los datos personales tratados al interior de las áreas que conforman el H. Congreso del Estado, se basará en la fórmula $Z(A + B + C)^n$, en donde **A** es **el tipo de datos tratado**, **B** el **número de veces que acceden**, y **C** el **tipo de entorno en que son tratados**, y el factor **n**, es el número de combinaciones posibles entre las mismas.

En los rubros A y C, se pueden sumar uno o más tipos de datos, mientras que en el rubro B, solo se puede elegir uno; esto nos da la posibilidad de distintas combinaciones (factorial **n**) (**anexo 1**), las cuales nos dieron la oportunidad de determinar un porcentaje de valor cuantitativo a cada rubro A, B y C; dicho porcentaje se representó en la gráfica de calor (**anexo3**), arrojando un porcentaje de riesgo latente.

Al primer rubro (A) denominado Riesgo por tipo de datos, y que a su vez se integra de 3 categorías de datos, se le asignó un porcentaje del 50%; dividido entre los mismos; al segundo rubro (B) titulado Riesgo por número de veces de acceso, que se integra por 4 categorías, se le asignó un porcentaje del 20% dividido entre los mismos, y al tercer rubro (C) denominado Riesgo por tipo de entorno, que se integra por 4 categorías, se le asignó un porcentaje del 30% dividido entre los mismos (**anexo 3**).

Esta gráfica de calor se trabajó de manera digital, en la que conforme se va seleccionando cada rubro se van sumando, y el marcador de semáforo, arroja el nivel de riesgo.

Como se describió en el **cuadro 3** de este documento, vale la pena precisar que los datos personales que son tratados en el H. Congreso son los siguientes:

- ✓ Datos identificativos,
- ✓ Datos académicos,
- ✓ Datos laborales,
- ✓ Datos de familiares,
- ✓ Datos patrimoniales,
- ✓ Sensibles:
 - De salud
 - Ideológicos
 - Características físicas

La tipología enunciada se retomó de lo plasmado en el inventario de datos personales por los usuarios y responsables de áreas en los diversos tratamientos de datos. A este rubro se le suma el riesgo por el número de veces que cada sujeto responsable accede a los datos personales que a continuación se hace referencia.

B.- Riesgo por el número de veces que se accede.

El riesgo por el número de veces que se accede a la información que contiene datos personales, es una vulnerabilidad, por lo que se consideró que el grado de vulnerabilidad es mayor cuando se accede más número de veces a la información que se pretende proteger, en un intervalo de 24 horas. Determinándose los siguientes rangos por número de veces que se accede:

- ✓ De 01-05 veces
- ✓ De 06 a 10 veces
- ✓ De 11 a 20 veces
- ✓ Más de 20 veces

Así entonces, se encontró que la mayoría de las áreas accede de 1 a 5 veces, mientras que sólo 5 áreas manifestaron acceder de 6 a 10 veces, como se puede observar en la siguiente tabla.

Órganos de Gobierno, Unidades Administrativas y Áreas	No. de veces que acceden	
	De 1 a 5	De 6 a 10
JUNTA DE COORDINACIÓN POLÍTICA	3*	
MESA DIRECTIVA	2	

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

SECRETARIA DE SERVICIOS PARLAMENTARIOS		
Unidad de Archivo y Correspondencia	1*	
Unidad de Trámites Legislativos	1*	
SECRETARÍA DE SERVICIOS ADMINISTRATIVOS		
Unidad de Tesorería	3*	
Unidad de Planeación y Presupuesto	1*	
Unidad de Recursos Humanos	8*	
Unidad de Recursos Materiales	3*	
Unidad de Contabilidad y Control Presupuestal	2*	
INSTITUTO DE INVESTIGACIONES LEGISLATIVAS	4*	1*
Departamento de Biblioteca	1*	2*
Departamento de Hemeroteca	1*	
Área de Archivo Histórico	5*	
DIRECCIÓN DE ASUNTOS JURÍDICOS	3*	
CONTRALORÍA INTERNA	5*	1*
DIRECCIÓN DE COMUNICACIÓN SOCIAL	2*	
UNIDAD DE TRANSPARENCIA		
Área de Acceso a la Información Pública	4*	
Área de Protección de Datos Personales	2*	
UNIDAD DE INFORMATICA		
Área de Desarrollo y Sistemas	3*	*
Área de Soporte Técnico		1*
COORDINACIÓN DE ATENCIÓN A MUNICIPIOS	1*	

*Número de procesos por área. **Cuadro 7. Descripción del número de veces que acceden por proceso.**

Finalmente, a este parámetro se le suma el riesgo por el tipo de entorno, por el que se accede a los diversos procesos o tratamientos de datos, que es el siguiente:

C.- Riesgo por el tipo de entorno

Este rubro se refiere a los entornos desde los cuales se acceden a los datos personales, entre mayor sea la anonimidad para acceder, mayor riesgo de vulnerarse la seguridad, y pueden ser:

- Físico (archiveros de la unidad)
- Equipo de computo
- Red

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

- Nube (intranet, Dropbox, google, drive, etc.)

En este rubro, cada área expuso el entorno a que accede al ejercer sus funciones y tratar datos personales, observándose que puede ser que traten datos en el entorno físico, como pueden ser expedientes, carpetas, recopiladores, libretas, entre otras, y/o en un equipo de cómputo, o bien hacen uso de una red o incluso a través de la nube, o en todas. En la siguiente tabla se puede observar a que entornos acceden las distintas áreas.

ÓRGANOS DE GOBIERNO, UNIDADES Y ÁREAS	TIPO DE ENTORNO			
	FÍSICO	PC	RED	NUBE
JUNTA DE COORDINACIÓN POLÍTICA	✓	✓		
Coordinación de atención a municipios	✓	✓		
ÁREAS DE LA SECRETARÍA DE SERVICIOS ADMINISTRATIVOS:				
Unidad de Tesorería	✓	✓		
Unidad de Recursos Humanos	✓	✓	✓	✓
Unidad de Recursos Materiales	✓	✓	✓	✓
Unidad Contabilidad	✓	✓	✓	
Unidad de Planeación y Presupuesto	✓	✓	✓	
DIRECCIÓN DE COMUNICACIÓN SOCIAL	✓	✓		
CONTRALORIA INTERNA	✓	✓	✓	✓
ÁREAS DE LA UNIDAD DE TRANSPARENCIA:				
Área de Acceso a la Información Pública	✓	✓	✓	✓
Área de Protección de Datos Personales	✓	✓	✓	
MESA DIRECTIVA	✓	✓		
ÁREAS DE LA SECRETARIA DE SERVICIOS PARLAMENTARIOS:				
Unidad de los Archivos de Trámite	✓	✓	✓	
Trámites Legislativos	✓	✓	✓	
INSTITUTO DE INVESTIGACIONES LEGISLATIVAS	✓	✓	✓	✓
Biblioteca	✓	✓	✓	
Hemeroteca	✓			
Archivo Histórico	✓	✓	✓	
DIRECCIÓN DE ASUNTOS JURÍDICOS	✓	✓	✓	
ÁREAS DE LA UNIDAD DE INFORMATICA				
Área de Desarrollo y Sistemas	✓	✓	✓	✓
Área de Soporte Técnico	✓			
TOTAL DE ÁREAS POR TIPO DE ENTORNO	18	16	14	6

Cuadro 8. Descripción de los tipos de entorno a los que acceden las distintas áreas.

c) Análisis de la información

Con esta metodología, integrando los tres factores obtuvimos un valor cuantitativo del nivel de riesgo latente de datos personales.

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

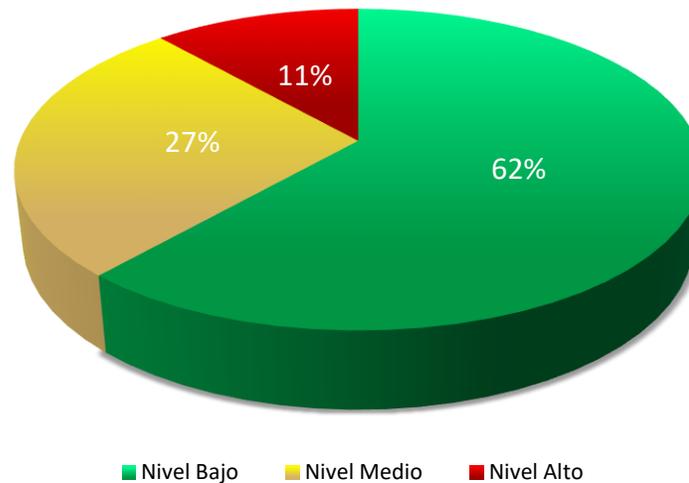
Así entonces, y considerando los tres parámetros para calcular el nivel de riesgo latente, que se obtuvo del análisis de semáforo en las gráficas de calor (**anexo 3**) de cada una de las áreas, se concluye que, las unidades administrativas que resultaron con nivel de riesgo alto (color rojo) en sus tratamientos de datos personales, son la Unidad de Recursos Humanos y la Dirección de Asuntos Jurídicos con dos procesos cada una, seguidas de la Unidad de Informática y Contraloría con un proceso, esto implica que sus procesos relativos a la protección de datos personales, sean aplicados con mayor atención y cuidado, con la intención de garantizar que el derecho a la protección de datos personales se cumpla.

Para mayor comprensión se muestra la siguiente tabla:

NIVEL DE RIESGO POR ÁREA Y NÚM. DE PROCESOS					
NIVEL BAJO	POR ÁREA	NIVEL MEDIO	POR ÁREA	NIVEL ALTO	POR ÁREA
ARCHIVO HISTORICO	5	INFORMATICA	1	INFORMATICA	1
HEMEROTECA	1	TRANSPARENCIA	1	CONTRALORÍA	2
BIBLIOTECA	2	CONTRALORIA INTERNA	4	DIRECCIÓN ASUNTOS JURIDICOS	3
INFORMATICA	2	RECURSOS HUMANOS	2	RECURSOS HUMANOS	2
CONTABILIDAD	1	PLANEACIÓN	1	JUNTA DE COORDINACIÓN POLÍTICA	1
COMUNICACIÓN SOCIAL	4	INVESTIGACIONES LEGISLATIVAS	2		
PLANEACIÓN	1	RECURSOS MATERIALES Y SERVICIOS GENERALES	2		
INVESTIGACIONES LEGISLATIVAS	2				
TESORERÍA	3				
PARLAMENTARIOS	2				
RECURSOS HUMANOS	4				
TRANSPARENCIA	5				
JUNTA DE COORDINACIÓN POLÍTICA	2				
MESA DIRECTIVA	2				
COORDINACIÓN DE ATENCIÓN A MUNICIPIOS	1				
TOTAL DE PROCESOS					
	37		13		9

Cuadro 8. Descripción del semáforo de nivel de riesgo, que tienen los procesos de cada área.

NIVEL DE RIESGO DE LAS ÁREAS DEL H. CONGRESO DEL ESTADO



Cuadro 9. Representación gráfica del porcentaje de riesgo, conforme a los procesos que tratan las áreas del Honorable Congreso del Estado de Chiapas.

De lo anterior se desprende que la mayor parte de las áreas que integran el H. Congreso del Estado de Chiapas, mantiene un nivel de riesgo bajo.

XIV. ANALISIS DE BRECHA

El análisis de brecha consiste en identificar la distancia que existe entre las medidas de seguridad existentes y las medidas que falta implementar, esto considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento.

A su vez, esta información da sustento a las medidas de seguridad administrativas, físicas y técnicas en materia de protección de datos personales, acordadas con cada una de las áreas y aprobadas por el Comité de Transparencia, para atenderlas de manera paulatina.

En esta tesitura, nuestra herramienta consistió en un formato denominado “Análisis de Brecha” (**anexo 4**), el cual fue llenado por los responsables de cada área de acuerdo a sus procesos en los que tratan datos personales; este documento contiene una serie de medidas a manera de preguntas, para responder si se cuenta

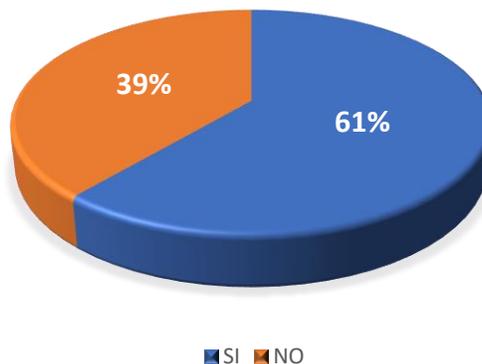
o no con ellas y un campo más de observaciones; en este instrumento se consideraron 3 rubros a saber:

- 1) Medidas de seguridad basadas en la cultura general y del entorno físico;
- 2) Medidas de seguridad del entorno físico; y
- 3) Medidas de seguridad del entorno digital.

Del análisis realizado de las encuestas se concluyó que, el 61.22 % de las áreas manifestaron realizar las medidas de seguridad mínimas, mientras que el 38.78% refieren que no se cumplen dichas medidas. Por lo que nuestra meta es que paulatinamente con las acciones de sensibilización y capacitación susceptibles de aplicarse, se fortalezcan las medidas administrativas, físicas y técnicas, para así garantizar y dar certeza del cumplimiento de los principios que rigen el derecho constitucional de protección de los datos personales en posesión del H. Congreso del Estado de Chiapas.

Representación gráfica del análisis de brecha respecto a las medidas de seguridad existentes y faltantes.

ANALISIS DE BRECHA



Cuadro 10. Representación gráfica del porcentaje de las medidas de seguridad que si se realizan y las que aún no se contemplan.

Por lo antes descrito es de gran importancia la implementación y ejecución del programa de capacitación, concientización, sensibilización, así como la consumación de las medidas de seguridad, como política estratégica; y de esta manera estar en condiciones de cumplir con el objetivo planteado en el documento de seguridad, sustentado en la normatividad vigente.

XV. GESTIÓN DE VULNERACIONES:

De conformidad con el artículo 52 de la LPDPPSOECH además de las que señalen las leyes y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos personales, al menos, las siguientes:

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

De lo anterior, se procede a exponer el mecanismo que las áreas o unidades administrativas deberán efectuar cuando:

1. Se materialice una alerta de seguridad en cualquier fase del tratamiento de datos personales
2. Se materialice una vulneración de seguridad en cualquier fase del tratamiento de datos personales

La Unidad de Transparencia del H. Congreso del Estado informará sin dilación alguna al titular y al Instituto sobre las vulneraciones ocurridas que de forma significativa afecten los derechos patrimoniales o morales del titular, en un plazo máximo de setenta y dos horas, una vez que se confirme que ocurrió la vulneración, y se inicie la implementación de las acciones encaminadas a detonar un proceso de revisión exhaustiva que determine la magnitud de la afectación, esto con el fin de que el titular de los datos personales, tome las medidas correspondientes y defienda sus derechos.

De conformidad con el artículo 55 de la LPDPPSOECH el H. Congreso del Estado a través de la Unidad de Transparencia deberá informar al Instituto y al titular, al menos lo siguiente:

- 1) La naturaleza del incidente
- 2) Los datos personales comprometidos
- 3) Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses
- 4) Las acciones correctivas realizadas de forma inmediata, y
- 5) Los medios donde puede obtener mayor información al respecto.

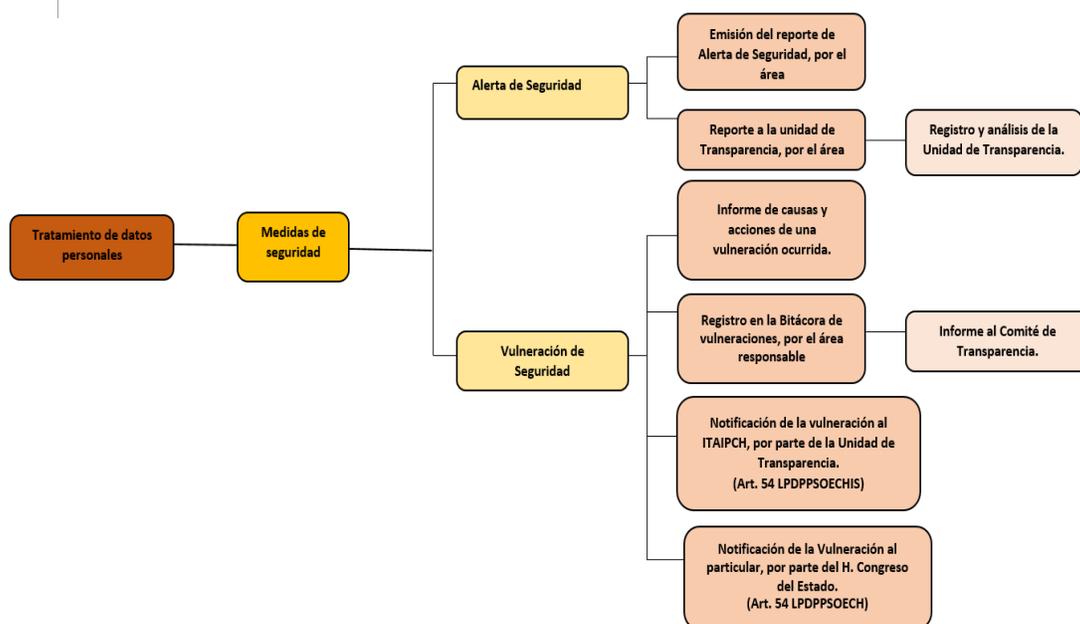
HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

Para la comprensión de los mecanismos antes referidos, resulta elemental distinguir entre una alerta y una vulneración de seguridad, la diferencia entre ambos conceptos, se exponen de la forma siguiente:

Alerta de seguridad	Vulneración de seguridad
Detección de una amenaza que, de haberse materializado en un daño, hubiera implicado una afectación en la seguridad de los datos personales.	Afectación acaecida a los datos personales en cualquier fase de un tratamiento, que haya generado: <ol style="list-style-type: none"> 1. Su pérdida o destrucción no autorizada. 2. El robo, extravío o copia no autorizada. 3. El uso, acceso o tratamiento no autorizado. 4. El daño, la alteración o modificación no autorizada
No implica la materialización de una vulneración.	Implica un daño a los activos del H. Congreso del Estado de Chiapas, como pueden ser las bases de datos, el personal, el hardware, software, archivos o documentos electrónicos o en papel.
Advierten una anomalía o cambio inesperado o no deseado.	Riesgo materializado que afecta de manera significativa los derechos patrimoniales o morales de los titulares de los datos personales.

Cuadro sinóptico que muestra el procedimiento o mecanismo a seguir al materializarse la vulneración de seguridad de la información que afecta los datos personales en cualquier fase del tratamiento:



XVI. MEDIDAS DE SEGURIDAD

La normatividad establece que se entenderá como medidas de seguridad al conjunto de acciones, actividades, controles o mecanismos administrativos, físicos y técnicos que permiten proteger toda información que contenga datos personales. El artículo 45 de la LPDPPSOECH dispone que con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o bien su uso, acceso o tratamiento no autorizado, así como garantizar su confiabilidad, integridad y disponibilidad.

Las medidas de seguridad como ya se mencionó, se abordan desde tres modalidades:

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

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

A) Implementación de Medidas de Seguridad.

Por consiguiente, las medidas generales de seguridad que se implementaran en las áreas que conforman el H. Congreso del Estado de Chiapas son las siguientes:

Medidas Administrativas.- De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

1. Adopción de un esquema de capacitación permanente en materia de Protección de Datos Personales en posesión de Sujetos Obligados, impartido por el INAI (Cursos virtuales), o bien por el Organismo Garante en la entidad;

así como a través de los talleres presenciales que impartirá la Unidad de Transparencia de este Poder Legislativo;

2. Cuidar la seguridad de los recursos humanos, previo a la contratación, durante y una vez que haya culminado sus funciones; dando a conocer a todo el personal el Manual de Inducción y el Código de Ética, obteniendo el compromiso de su cumplimiento con una carta de confidencialidad, como una buena práctica en la materia;
3. Normalización de las Instalaciones eléctricas, para un adecuado funcionamiento de equipos de cómputo;
4. Prevenir el acceso no autorizado a las instalaciones físicas, áreas críticas, recursos e información; mediante instalación de cámaras en áreas estratégicas, en la medida de lo posible.
5. Tener el control por escrito de visitantes a la entrada de las instalaciones del H. Congreso, tanto en Palacio Legislativo como en el primer piso del Edificio Plaza.
6. Implementación de identificación de servidores públicos del H. Congreso, mediante la portación de credencial oficial;
7. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas (ventanas de cristal, prever inundaciones, incendios, y descargas eléctricas);
8. Implementación de formatos de entrada y salida de préstamo de documentos o expedientes requeridos en las áreas que se tratan datos personales;
9. Monitoreo, revisión y/o actualización en su caso de las medidas de seguridad.
10. Actualizar el presente documento de seguridad conforme al artículo 51 de la LPDPPSOECH.

Medidas Físicas.- De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

1. Bitácora de control de acceso a archivos, expedientes o sistemas que contienen datos personales, en caso de ser persona distinta al usuario responsable;
2. Resguardo de documentos e información en lugares seguros, archiveros, cajones, gavetas, puertas de oficinas con cerraduras y llaves;
3. Limitar y delimitar a las personas con acceso a archivos que contengan información con datos personales, quienes deberán acudir a las capacitaciones en la materia;

4. Autorizar y registrar la entrada y salida de archivos que contengan información y datos de carácter personal e indicar los detalles básicos del traslado (solicitante, objeto de la solicitud, fecha, entre otros).
5. Incorporar en su labor diaria la gestión y archivo de los documentos dirigidos a garantizar su correcta conservación, la localización de estos y la consulta de la información, (clasificación archivística) con el propósito de agilizar el ejercicio de los derechos ARCO;
6. Mantener política de escritorio limpio; evitar dejar a la vista documentación con información relevante; prever y evitar derrame de líquidos;
7. Usar hojas recicladas que no contengan datos personales;
8. Solicitar a la instancia competente de archivos, la asesoría y orientación para el proceso de la baja documental;
9. Contemplar medidas adecuadas para la destrucción de documentos, como la trituración o incineración;
10. Suprimir los datos personales, una vez que haya concluido la finalidad para la que fueron recabados y los mismos hayan dejado de ser pertinentes, observando en todo momento la normatividad aplicable;
11. Informar inmediatamente de cualquier incidente al superior jerárquico, (llenar y seguir los pasos del formato correspondiente).

Medidas Técnicas.- De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- Seguimiento del programa de mantenimiento preventivo y correctivo anual de los equipos de cómputo, que implementó la Unidad de Informática;
- Implementación de un programa y lineamientos por la Unidad de Informática, en el que se contemple el uso y la seguridad del hardware, software y la red, en donde se establezca lo siguiente:
 - Contar con un inventario de dispositivos informáticos.
 - Capacitación a los usuarios para que realicen respaldo y resguardo de la información;
 - Los equipos informáticos y periféricos son propiedad del H. Congreso del Estado y para uso exclusivo de actividades concernientes a este;
 - La red local y el acceso a internet, será exclusivamente para uso laboral;
 - Evitar guardar información personal en los equipos de cómputo;
 - Únicamente se usarán las de redes sociales, cuentas de correo o aplicaciones instaladas y/o autorizadas por la Unidad de Informática;

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS

ÁREA DE PROTECCIÓN DE DATOS PERSONALES

- Evitar abrir correos electrónicos de destinatarios desconocidos, ni descargar contenido dudoso.
- Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas.
- Contar con equipos adecuados para poder segmentar la red local, para brindar acceso a internet a usuarios externos y evitar exponer los recursos informáticos del H. Congreso. Así como la segmentación (subredes) para las áreas que tratan datos personales de riesgo alto.
- El usuario de los procesos de alto riesgo es responsable de la información que resguarda en la carpeta asignada por la Unidad de Informática, para realizar el respaldo de manera periódica.
- Implementar Directorio Activo.
- Implementación de niveles y esquema de privilegios, para que el usuario lleve a cabo las actividades que requiere de acuerdo con sus funciones.
- Borrar o eliminar de la papelera de reciclaje y del escritorio de los equipos de cómputo los documentos o archivos electrónicos que no sean necesarios para el desarrollo de funciones.
- Implementar técnicas de borrado seguro de la información, de acuerdo con los dispositivos que se tengan.
- 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.
- Contemplar medidas adecuadas para la destrucción de los medios de almacenamiento electrónicos, como la desintegración, pulverización entre otros;
- Informar inmediatamente de cualquier incidente al superior jerárquico, (**anexo 5 y 6**), situación que deberá de informar a la Unidad de Informática, para realizar las medidas necesarias y dar pronta atención. (Tómese como incidente toda alteración, daño, robo, extravió o copia, pérdida, transmisión y acceso no autorizado, o alguna otra que vulnere la información confidencial del usuario).

B) Procedimiento a efectuar ante posibles incidencias

Se implementaron 2 formatos que contienen el procedimiento para identificar, registrar y notificar en caso de alguna vulneración (**anexos 5 y 6**).

Lo anterior servirá también para llevar una bitácora de las vulneraciones ocurridas en las distintas áreas, que dará pauta a identificar las causas y también las acciones preventivas y correctivas a realizar.

XVII. CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

La implementación en los equipos de cómputo de claves o contraseñas personales por cada usuario, lo que permitirá tener una seguridad e identificación de quien accede a equipos de cómputo, repositorios o cuentas de correo electrónico institucionales, mediante éstos mecanismos los sistemas tecnológicos serán monitoreados por la Unidad de Informática. Asimismo se cuenta con las actualizaciones periódicas de la instalación de programas de antivirus, lo que garantiza una eficaz y eficiente conservación de la información que se encuentra en archivos digitales.

Asimismo, por cualquier mal uso de estos medios electrónicos será causa de falta o sanción administrativa conforme al Manual de Inducción y los lineamientos para el buen uso de los bienes informáticos, ambos del H. Congreso del Estado y la normatividad aplicable.

XVIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Es importante implementar mecanismos que permitan la elaboración de copias de respaldo y la recuperación de datos personales, una vez que las medidas de seguridad han sido vulneradas. En ese sentido, en los casos de que los datos personales se encuentren en soporte físico se procurara que el respaldo se efectúe mediante la digitalización de los documentos, es decir, que se cuente con el soporte físico, pero además, se cuente con el archivo electrónico, por ejemplo el respaldo de nubes, discos duros, memorias externas, por el personal que maneja los datos personales o tratamientos de éstos. Asimismo, cuando los datos personales se encuentren en soportes electrónicos se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción, garantizando su restablecimiento al estado en que se encontraban al tiempo de producirse la pérdida involuntaria o destrucción accidental.

De igual forma, se tomará en consideración lo siguiente:

- ✓ Se analizara las medidas que de acuerdo con la magnitud de la pérdida involuntaria o destrucción accidental ocurrida, lo anterior con la finalidad de

encontrar las herramientas idóneas y eficaces que permitan el restablecimiento o recuperación de los datos personales.

- ✓ Analizar las medidas correctivas que permitan evitar la reincidencia de las acciones que propiciaron la vulneración de los datos personales.

XIX. PLAN DE CONTINGENCIA

Se denomina como plan de contingencias para la protección de la información, a la definición de acciones a realizar, recursos a utilizar, y el personal a emplear en caso que se produzca un acontecimiento de carácter intencional o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos del H. Congreso del Estado.

Clasificación de la contingencia:

De acuerdo al tipo de contingencia es posible determinar el grado de afectación.

Grado 1, son las más bajas que van desde fallas eléctricas, fallas con la conexión de internet y que pueden ser resueltas por el mismo personal del H. Congreso del Estado.

Grado 2, Son las contingencias provocadas por un siniestro y por su alcance pueden afectar severamente la operatividad del Poder Legislativo, por ejemplo una inundación o un incendio, en estos casos se requiere tanto del apoyo de personal del H. Congreso del Estado, como del Cuerpo de Bomberos y de Protección Civil Municipal o Estatal del Estado.

Por lo anterior, es necesario contar con un protocolo de actuación que se denominará Plan de Contingencia del H. Congreso del Estado, de manera enunciativa más no limitativa, deberá contener:

- Consideraciones principales
- Reporte de Vulneración
- Designación de Personas
- Aviso de las vulneraciones al titular de datos
- Investigación de la vulneración ocurrida
- Medidas de prevención y conservación de archivos
- Medidas preventivas ante los siguientes siniestros:
 - Incendio
 - Terremoto o sismo
 - Inundaciones por lluvia

- Robo
- Huelga o Manifestaciones
- Amenazas informáticas (hackeo informático)

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

Cuando se deba realizar la destrucción de documentos o de medios electrónicos, con los medios que se consideren más adecuados y para demostrar el cumplimiento de esta medida de seguridad se deberá generar evidencia de dicho proceso, con actas circunstanciadas de hechos, fotografías o bitácoras, para garantizar que los datos fueron eliminados en su totalidad y que no hay forma alguna que permita su recuperación o bien, que puedan ser utilizados de manera indebida.

Las acciones que deben utilizarse para la supresión y borrado seguro de los datos personales son los siguientes:

- 1. Métodos físicos:** Trituración mediante trituradoras, en caso de no contar con este elemento se debe realizar mediante un corte cruzado, es decir cortar el documento de forma vertical y luego horizontal obteniéndose fragmentos muy diminutos, lo cual hace prácticamente imposible de volverlos a unir.
- 2. Métodos de destrucción de los medios de almacenamiento electrónicos:** Se realiza mediante la desintegración, consistente en la separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir, así como, mediante la pulverización entre otros.
- 3. Métodos lógicos:** De sobre-escritura, que consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software. De igual manera, borrar o eliminar de la papelera de reciclaje y del escritorio de los equipos de cómputo los documentos o archivos electrónicos que no sean necesarios para el desarrollo de funciones e Implementar técnicas de borrado seguro de la información, de acuerdo con los dispositivos que se tengan.

XXI. PLAN DE TRABAJO

Son acciones que se van a determinar con cada área o unidad administrativa correspondientes para adoptar un plan de trabajo que permita la implementación

de medidas de seguridad faltantes para el cumplimiento cotidiano de las políticas de gestión y tratamiento de datos personales de este Poder Legislativo.

Este Plan de Trabajo debe determinar las actividades generales que se deben realizar al interior del H. Congreso del Estado. Es importante recapitular que el Documento de Seguridad ofrece una radiografía del Poder Legislativo en materia de protección de los datos personales; asimismo, presenta áreas de oportunidad; de igual forma, constituye un insumo para la toma de decisiones por parte de las instancias competentes en materia.

Derivado de lo anterior, el Plan de Trabajo será una herramienta complementaria y de instrumentalización del Documento de Seguridad previamente aprobado por el Comité de Transparencia, cuyos objetivos fundamentales serán los siguientes:

- ✓ La implementación de medidas de seguridad pendientes en cada uno de los tratamientos de datos personales identificados; y,
- ✓ Consolidar y preservar los niveles de protección de los datos personales a través de mecanismos de monitoreo y revisión.

XXII. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Una manera de mejora continua es a través del monitoreo y revisión de las medidas de seguridad implementadas, amenazas y vulneraciones a las que están sujetos los datos personales contenidos en los sistemas y/o bases de datos personales, lo que permite definir nuevos controles por ejemplo la revisión y actualización de las contraseñas utilizadas para resguardar los datos personales en equipos de cómputo, o bien realizar actualizaciones sustentadas de los mecanismos implementados, y por su puesto monitorear las medidas de seguridad ya establecidas, recordemos que todo es susceptible de mejorar.

Al respecto, la Unidad de Transparencia será el área administrativa encargada de ejecutar el mecanismo de monitoreo y revisión de las medidas de seguridad implementadas en la protección de los datos personales, el cual se integrara por dos etapas, es decir, por la etapa de monitoreo y la de verificación, asimismo, este procedimiento se llevará a cabo de manera semestral.

La etapa de monitoreo consistirá en el requerimiento por parte de la Unidad de Transparencia del Reporte de Seguridad de Datos Personales, el cual deberá ser emitido por las áreas que, son responsables de los procesos de datos personales.

La etapa de verificación consistirá en el análisis por parte de la Unidad de Transparencia a través del Área de Protección de Datos Personales, del Reporte de Seguridad de Datos Personales, concluyéndose con un dictamen de seguridad de datos personales en el que se plasmen las recomendaciones o requerimientos que se consideren pertinentes.

En el reporte de seguridad de datos personales, se precisaran lo siguiente:

- ✓ Acciones desarrolladas para la ejecución de las medidas de control existentes
- ✓ Manifestación de si existe alguna actualización o modificación respecto de las medidas de seguridad y controles implementados en el tratamiento de datos personales que realice. De ser así, deberán incluir una explicación de tal actualización o modificación
- ✓ Indicar de manera clara la actualización de los aspectos siguientes:
 - La incorporación de nuevos activos en el tratamiento que realiza, como podrían ser una actualización o modificación en el hardware o software del sistema utilizado, personal de nuevo ingreso a cargo del tratamiento o cualquier otro recurso humano o material que tenga impacto en el tratamiento de los datos personales.
 - El surgimiento de nuevas amenazas en el tratamiento de los datos.
 - La posibilidad de que las nuevas amenazas que originen una vulnerabilidad en el tratamiento de datos.

Posteriormente, La Unidad de Transparencia analizará los reportes de seguridad de datos personales remitidos por las instancias, verificando especialmente lo siguiente:

1. La efectividad de las medidas de seguridad y control respecto del tratamiento.
2. La implementación de controles preventivos y correctivos.
3. La gestión interna de nuevas amenazas, vulnerabilidades e incrementos en el impacto de probables daños.
4. Avances de cumplimiento conforme al Plan de Trabajo.

Concluido el ciclo de examinación, se elaborará un dictamen de seguridad en el que se detallaran las recomendaciones o los requerimientos que resulten pertinentes en materia de seguridad, lo que será notificada a las áreas correspondientes, se procurara, señalar la manera en que deberán ser desahogadas las recomendaciones y/o requerimientos.

XXIII. PROGRAMA DE CAPACITACIÓN

La coordinación de la capacitación en el tema, corresponde a la Unidad de Transparencia bajo la tutela del Comité de Transparencia, de conformidad a los artículos 66 fracción V y 114 fracción VIII de las leyes de Transparencia y Acceso a la Información Pública, así como la de Protección de Datos Personales en Posesión de Sujetos Obligados ambas del Estado de Chiapas respectivamente; contemplándose al menos los siguientes temas:

- ❖ **Derechos ARCO (acceso, rectificación, cancelación y oposición) de Datos Personales.**
- ❖ **Introducción al derecho a la protección de datos personales**
 - Teoría y normatividad en materia de Datos Personales
 - Principios que regulan el tratamiento de datos personales, deberes y obligaciones de los sujetos responsables.
 - Causas de responsabilidad administrativa.
- ❖ **Relevancia del Aviso de Privacidad**
 - Simplificado
 - Integral
- ❖ **Inventario de datos personales y los rubros que lo integran**
- ❖ **Información confidencial/reservada**
- ❖ **Medidas de seguridad y vulneraciones**
 - Incidencias
 - Medidas de Seguridad, (administrativas, físicas y técnicas).
- ❖ **Gestión de Vulneraciones de Seguridad**
 - Vulneraciones
 - Mecanismo ante una vulneración
- ❖ **Medidas Preventivas y evitar vulneraciones de datos personales**
 - Controles de identificación y autenticación de usuarios
 - Procedimiento de respaldo y recuperación de datos
 - Técnicas para la supresión y borrado seguro de los datos personales
- ❖ **Controles o mecanismos de Confidencialidad**
- ❖ **Que es el Plan de Contingencia**
- ❖ **Que es el Plan de trabajo**

❖ Mecanismos de monitoreo y revisión de las medidas de seguridad

Cuando así se amerite, se establecerán reuniones de trabajo con las unidades administrativas a efecto de identificar y concertar debilidades y fortalezas que propicien alternativas de solución, técnicas, físicas y administrativas a desarrollar a mediano y largo plazo. El Programa de Capacitación podrá prever la impartición de cursos a través del personal del área de Protección de Datos Personales de la Unidad de Transparencia, así como aquella proporcionada por el Organismo Garante en la entidad o incluso por el INAI, de forma virtual o presencial.

XXIV. ACTUALIZACIONES

Conforme al artículo 51 de la ley estatal de la materia, el presente documento de seguridad deberá ser actualizado por el responsable de manera periódica y por los siguientes eventos:

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

Cuando se realicen cambios o actualizaciones en los tratamientos, usuarios, normatividad o medidas de seguridad, deberá actualizarse el presente documento de seguridad y ser aprobado por el Comité de Transparencia.

En caso de que los servidores públicos incumplan con las obligaciones establecidas en este Documento de Seguridad, podrán incurrir en responsabilidad administrativa, conforme al artículo 191 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, y demás normatividad aplicable en la materia; así también, podrán ser sancionados conforme a la Ley de Responsabilidades Administrativas para el Estado de Chiapas.

Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

El artículo 57 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, exige el establecimiento de controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de estos, obligación que subsistirá aún después de finalizar sus relaciones laborales con el H. Congreso del Estado de Chiapas; en ese contexto, la Unidad de Transparencia en conjunto con las áreas que resulten competentes elaboraran el documento que contenga los controles o mecanismos de confidencialidad a que hace alusión el citado dispositivo.

La obligación de confidencialidad se considera expuesta al materializarse alguna de las vulneraciones de seguridad, situación que puede presentarse en cualquiera de las fases del tratamiento de datos, es decir, desde su obtención hasta su cancelación, supresión o eliminación. Dichas vulneraciones pueden afectar de manera significativa los derechos patrimoniales o morales de los titulares.

XXV. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

El presente documento de seguridad fue aprobado de forma unánime por los integrantes del Comité de Transparencia del Honorable Congreso del Estado de Chiapas, conforme a sus atribuciones mediante Acta de la Trigésima Quinta Sesión Extraordinaria de fecha dos de diciembre del año dos mil veintidós.

De conformidad con el artículo 51 de la LPDPPSOECH, con fecha veintiuno de agosto del dos mil veintitrés, se lleva a cabo la actualización del Documento de Seguridad.

XXVI. REFERENCIA BIBLIOGRÁFICA

- ✓ Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación, 5 de febrero de 1917, última reforma publicada en el D.O.F., el 28 de mayo de 2021.
- ✓ Constitución Política del Estado Libre y Soberano de Chiapas, última reforma publicada en el Periódico Oficial el 28 de octubre d 2021.
- ✓ Decreto Promulgatorio del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y Protocolo adicional al Convenio para Europa para la Protección de las

personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos. (Convenio No.108 del Consejo Europeo); DOF, 28 de septiembre de 2018, Secretaría de Gobernación.

- ✓ Ley General de Transparencia y Acceso a la Información Pública, Diario Oficial de la Federación, 04 de mayo de 2015, última reforma publicada en el D.O.F. el 20 de mayo de 2021.
- ✓ Lineamientos Generales de Protección de Datos Personales para el Sector Público. ACT-PUB/19/12/2017.10
- ✓ Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, publicada en el Periódico Oficial con fecha 22 de diciembre de 2021. Decreto No. 016.
- ✓ Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, comentada. INAI, 2018.
- ✓ Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, publicada en el Periódico Oficial, con fecha 30 de agosto del año 2017. Decreto No. 239.
- ✓ Ley de Responsabilidades Administrativas para el Estado de Chiapas, última reforma publicada en el Periódico Oficial de fecha 19 de agosto de 2020. Decreto No. 261.
- ✓ Ley del Servicio Civil del Estado y los Municipios de Chiapas, última reforma publicada en el Periódico Oficial con fecha 31 de diciembre de 2016. Decreto No. 44.
- ✓ Reglamento de Transparencia y Acceso a la Información Pública del Honorable Congreso del Estado de Chiapas, publicado en el Periódico Oficial con fecha 04 de mayo de 2020.
- ✓ Recomendaciones para conocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo, Instituto Nacional de Transparencia, Acceso a la Información y Protección de datos Personales, Edición abril de 2021.
- ✓ Conferencia: en “La Ruta de la Privacidad 2022”, inai; 22 de enero de 2022.

- ✓ Ann Kavoukian, "Los siete principios fundamentales de la privacidad por diseño", <https://www.studocu.com/co/document/servicio-nacional-de-aprendizaje/analisis-y-desarrollo-de-sistemas-de-informacion/modulo-1-apuntes-1/13209410>
- ✓ https://micrositios.inai.org.mx/covid-19/?page_id=155