H. CONGRESO DEL ESTADO DE CHIAPAS

LXVIII LEGISLATURA

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, diciembre de 2022.

Tabla de contenido

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 6º. Apartado A, fracción II y 16, párrafo segundo de nuestra Constitución Política Federal, así como por el artículo 3º. de la Constitución Política del Estado Libre y Soberano de Chiapas; el propósito es por un lado garantizar el acceso a la información pública que se encuentra en posesión de cualquier sujeto obligado y por la otra la protección de los datos personales, así como el derecho a solicitar el Acceso, Rectificación, Cancelación u Oposición de estos, los llamados derechos ARCO; y finalmente el derecho a la autodeterminación informativa, que en términos generales se refiere a la facultad de decidir por parte del titular, que datos entrega, a quien se los entrega y para efectos de que los entrega, y por parte del sujeto obligado, la obligación de brindar protección a la persona titular de los datos, lo que implica además de obtener su consentimiento, realizar un adecuado tratamiento de la información personal que proporciona, ya sea para la prestación de un servicio, realizar un trámite o como parte de nuestro quehacer laboral.

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 1°., 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.

Para armonizar el marco normativo en la materia, se emitió en el mes de agosto de 2017 la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, y el 01 de abril de 2020, la nueva Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, la cual contempla la normatividad en materia de protección de datos personales; y finalmente en mayo de 2020, se publica el Reglamento de Transparencia y Acceso a la Información Pública del Honorable Congreso del Estado de Chiapas, con el que se da vida a la Unidad de Transparencia de este poder legislativo.

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 diagnostico 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.

Lo anterior ha sido plasmado en este Documento de Seguridad, el cual 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.

Finalmente, es relevante mencionar que todo se realizó con el trabajo colaborativo de las áreas que conforman este recinto 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: Las direcciones, áreas y/o unidades administrativas del H. Congreso del Estado de Chipas, 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 si 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 e Transparencia, con la finalidad de construir, asesorar e informar, las acciones en materia de protección de datos personales.

LGPDPPSO: 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: Titular de las áreas que integran el H. Congreso, que manifestaron tratar datos personales.

Reglamento de Transparencia: El Reglamento de Transparencia y Acceso a la Información Pública del H. Congreso del Estado de Chiapas.

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

Del mismo modo, el presente documento una vez aprobado por el Comité de Transparencia del Honorable Congreso del Estado de Chiapas, siendo este la máxima autoridad en la materia, conforme a lo establecido en los artículos 113 y 114 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; 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.

Es importante mencionar que el Documento de Seguridad, es aplicable 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 los enlaces para elaborar el diagnóstico de los diversos tratamientos que se llevan a cabo en cada una de las áreas que conforman este H. Congreso. Este ejercicio sirvió para entender y tomar conciencia 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.

También este trabajo conjunto, sirvió para advertir que existen tanto obligaciones reciprocas entre algunas áreas internas; como obligaciones mínimas necesarias que se deben cumplir, ya sea como Responsable, Usuario o Enlace; como las que a continuación 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 que se realice un adecuado tratamiento de los datos personales conforme a los principios y deberes sustentados en la LGPDP y la LPDPPSOECH.
- El enlace, como representante de cada área, fungir como tal en coordinación con la Unidad de Transparencia.

- 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
- **Secretaria de Servicios Administrativos**:
  - Unidad de Tesorería
  - Unidad de Planeación
  - Unidad de Recursos Humanos
  - Unidad de Recursos Materiales
  - Unidad de Contabilidad
- **Dirección de Asuntos Jurídicos**
- **Contraloría Interna**
- **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 Atención al público, intérpretes y traductores en L.I.

- **Unidad de Informática:**
  - Área de Soporte Técnico y Redes
  - Área de Desarrollo de Sistemas

Es así como la Unidad de Transparencia integra este documento de seguridad con base en la información generada por las citadas unidades administrativas y conforme a los principios y deberes que en el siguiente capítulo se enunciaran.

Es relevante que las unidades administrativas realicen las acciones necesarias para cumplir con las obligaciones que establece este documento, de manera paulatina y progresiva, conforme a los recursos materiales y humanos necesarios, con estrategias interdisciplinarias en beneficio común.

Para ello, resulta fundamental que este Documento de Seguridad se conozca al interior del H. Congreso del Estado, por lo que el Comité de Transparencia se encargará de difundirlo entre los servidores públicos.

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 son utilizados por los servidores públicos en su labor cotidiana, con la intensión de implementar, operar, monitorear, revisar y mejorar el tratamiento y seguridad de esos datos, conforme a lo previsto en la legislación de la materia.

Vale la pena reflexionar que hoy en día todos estamos frente a enormes desafíos, este mundo no es un mundo de cambio progresivo, es un mundo de cambio

disruptivo, no da casi tiempo de irse adaptando, sino que nos tenemos que adaptar ya, y la mayoría de las veces sin prevención.

Nos encontramos en un momento en el que se está dando más importancia a los datos que a las personas, la sociedad es cautiva de la evolución tecnológica, por ello debemos ser cautelosos y proteger este derecho humano.

Así entonces, para el debido cumplimiento de las obligaciones establecidas en la Ley, pero sobre todo para conocer la situación que prevalece en la práctica cotidiana respecto a la protección de datos personales que son tratados al interior de este H. Congreso del Estado, de entrada, había que partir de un diagnóstico, como lo señalamos en el capítulo que antecede; por lo que primeramente, se implementaron talleres para impulsar la capacitación y una motivación conjunta, en pro de contar con el apoyo y sobre todo la buena disposición de los servidores públicos, para ejecutar los principios y deberes que norman la protección de datos personales, que son: deber de confidencialidad y de seguridad así como los principios de responsabilidad, proporcionalidad, licitud, finalidad, lealtad, consentimiento, calidad, e información; mismos que constituyen normatividad 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:

Se está trabajando con el cumplimiento al principio de **proporcionalidad**, para que cada área trate aquellos datos personales que resulten exclusivamente necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron. Por lo tanto, no se debe recolectar o usar datos que no guarden estrecha relación con la finalidad del tratamiento.

De igual manera, un principio relevante es el de **licitud**, que 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 relativa para un mejor actuar.

Por otra parte, se están implementando acciones para que el titular de los datos, sepa entre otras cosas, para que fines se utilizaran 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 la Unidad de Transparencia, 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); también contempla el fundamento legal, así como la expresión en su caso de realizar transferencia de datos, así como la mención en su caso de tratar datos sensibles, finalmente el medio electrónico mediante el cual el titular puede consultar el aviso de privacidad integral y la fecha de elaboración o actualización.

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.

También se contempla elaborar la descripción de los derechos ARCO Acceso, Rectificación, Cancelación y Oposición, así como la ruta a seguir para que los titulares puedan ejercer este derecho; lo que se publicara en el portal de transparencia.

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 cada una de las áreas y la versión integral en el portal de transparencia de este H. Congreso.

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, especifico 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.

Ahora bien, los principios de **calidad y finalidad**, son muy importantes y van vinculados en la práctica cotidiana, la Ley establece que los datos personales sean

veraces, exactos, completos, correctos y actualizados; por esta razón se está trazando la ruta de la capacitación constante, lo que genera a priori, una concientización del personal para mantener bases de datos actualizadas, pero sobre todo para que se deje de tratar información que ya no es necesaria para cumplir con las finalidades para los cuales fueron entregados; estamos en proceso de construcción, en donde el objetivo es que el servidor público pueda ser capaz primero de conocer y establecer para que fin trata la información, saber cuáles son los plazos de conservación de la información y una vez satisfecho el fin, bloquear, conservar o bien suprimir según sea el caso.

Finalmente nos referiremos al principio de **responsabilidad**, el que implica prácticamente la ejecución del presente documento, porque la intensión es que no solo quede en letra muerta, sino que trascienda a la vida diaria en el actuar de este poder legislativo; una manera de hacerlo realidad es aplicando el **deber de seguridad**, estableciendo las medidas de seguridad físicas, administrativas y técnicas necesarias para observar las mejores prácticas y estándares en la protección de datos personales. Esto se realizó partiendo del trabajo conjunto con las diversas áreas, mediante el análisis de brecha y de riesgo, los que se analizarán en el capítulo correspondiente de este Documento de Seguridad; igualmente se contempla un programa de verificaciones para observar las mejores prácticas, la constante actualización y las adecuaciones necesarias, esto implica recursos tanto físicos como económicos para que en un futuro no muy lejano, trabajemos y pensemos de forma preventiva, aún estamos a tiempo, como dice la especialista en la materia Ann Cavoukian[1], "*Lo predeterminado es lo que manda*", y si pensamos en el debido tratamiento de datos desde el principio y no cuando la vulneración

[1] Cavoukian, A. (2011). Privacy by design: los 7 principios fundamentales. Disponible en: https://transparencia.congresochiapas.gob.mx/bibliografias/los_7_principios_fundamentales.pdf

está dada, garantizaremos mejores niveles de tratamiento de la información de las personas.

Así entonces y después de haber señalado como se está dando cumplimiento a los principios normativos en la materia, debemos mencionar que también se realizó el diagnóstico de los diferentes tratamientos de datos personales por cada una de las áreas, esto fue mediante un inventario de datos personales, en el cual se identificó, primeramente: los procesos que se realizan, los datos que tratan, así como las atribuciones; también se conocieron los responsables en cada tratamiento, se generaron los avisos de privacidad; también se observó la importancia de actualizar el portal de transparencia el cual ya se está diseñando, entre otras acciones que en el siguiente capítulo se precisan.

Colocación de los Avisos de Privacidad Simplificado.

Una vez obtenidos y concentrados los distintos formularios, se procedió a su análisis, lo que dio pauta a continuar con los talleres para después obtener el análisis de riesgo y el análisis de brecha, concluyendo con la conformación de las medidas de seguridad y finalmente el programa de capacitación y verificación.

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, se implementó la estrategia de solicitar mediante oficio a los titulares de las áreas administrativas; primeramente nombrar a un enlace para estar en constante comunicación con el área de Protección de Datos Personales de la Unidad de Transparencia, posteriormente y previa capacitación se elaboraron diversos formularios que fueron remitidos para ser llenados por las distintas áreas administrativas; enfocándose en dos 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.

Talleres de Capacitación

De acuerdo al análisis realizado de los distintos inventarios de datos personales, se desprendió qué son 20 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	•Manera en la que los sujetos responsables obtienen los datos personales de los titulares.
Tipo de datos personales tratados	•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	•Motivos por los que el sujeto responsable solicita los datos personales. Las finalidades deben ser concretas, licitas, explicitas y legitimas
Áreas y servidores públicos con acceso al tratamiento	•Personas de los sujetos responsables que, conforme al ámbito de sus atribuciones, tratan los datos personales.
Medios de almacenamiento y conservación de los datos	•Medios en los que se almacenan los datos personales, puede ser en formato físico, electrónico o ambos.
Transferencias, comunicación o difusión	•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	•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.

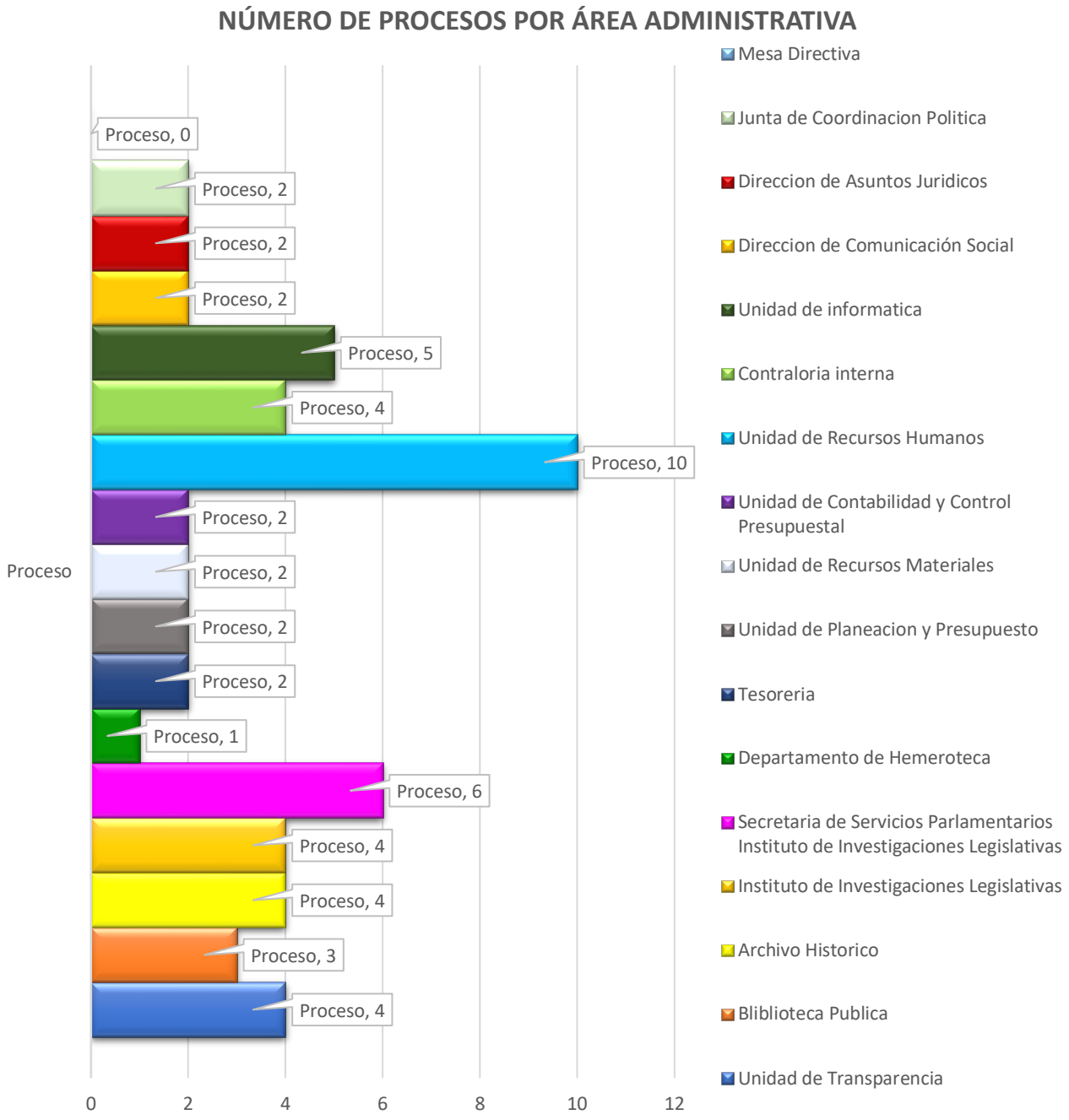
Órganos de Gobierno, Unidad Administrativa.	Área	Proceso o Tratamiento
MESA DIRECTIVA		
Junta de Coordinación Política	JUCOPO	❖ Registro de personas que solicitan audiencia, y programación de reuniones de trabajo. ❖ Propuestas al Pleno, para la integración de las Comisiones legislativas.
Secretaría de Servicios Parlamentarios	Unidad de los Archivos de Trámite	❖ Recepción de solicitudes de apoyo de intervención. ❖ Solicitudes de desincorporaciones de bienes inmuebles. ❖ Recepción de iniciativas de Ley y puntos de acuerdo. ❖ Recepción de propuestas para nombramientos de funcionarios públicos.
	Trámites Legislativos	❖ Tramites de las solicitudes de desincorporaciones de bienes inmuebles. ❖ Tramites de las propuestas de nombramientos.
Secretaría de Servicios Administrativos.	Unidad de Tesorería	❖ Pago de nóminas Diputados. ❖ Pago de Proveedores
	Unidad de Planeación y Presupuesto	❖ Elaborar el anteproyecto del Presupuesto de Egresos con cotizaciones de proveedores.

		❖ Integrar y publicar formato de montos por ayudas y subsidios.
	Unidad de Recursos Humanos	❖ Contratación y Alta de Personal. ❖ Trámites de altas y bajas en el IMSS y pagos de cuotas obrero patronal. ❖ INFONACOT. ❖ Elaboración de nómina. ❖ Inscripción al INFONAVIT ❖ Créditos ante INFONAVIT ❖ Certificación a INFONACOT ❖ Solicitudes de información y obligaciones de la Plataforma Nacional de Transparencia. ❖ Timbrado de nomina ❖ Elaboración de constancias
	Unidad de Contabilidad	❖ Resguardo de Información ❖ Procesos Contables
	Unidad de Recursos Materiales y Serv. Generales.	❖ Contratación y prestación de Servicios y Compras. ❖ Orden de pago
Dirección de Asuntos Jurídicos	Jurídico	❖ Trámites Jurídicos ❖ Notificaciones Procesos Jurídicos
Contraloría Interna	Contraloría	❖ Proceso de Acta-Entrega Recepción de Servidor(a) Publico(a) ❖ Atención y Seguimiento al Buzón de sugerencias y Quejas del H. Congreso del Estado de Chiapas. ❖ Seguro de Vida ❖ Declaración Patrimonial y de Intereses.
Instituto de Investigaciones Legislativas	Investigación legislativa.	❖ 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”	❖ Control de Acceso, Control de Préstamos de Libros, Control de Equipos de Cómputo. (matutino y vespertino)
	Departamento Hemeroteca	❖ Préstamo de Diarios locales para consulta.

	Departamento de Archivo Histórico "Ángel Robles Domínguez"	❖ 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. ❖ 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.
Dirección de Comunicación Social	Dirección	❖ Registro de las personas que solicitan audiencia, para generar un control de las mismas. ❖ Agenda de los posibles eventos
Unidad de Transparencia	Área de atención al público, intérpretes y traductores en lenguas indígenas.	❖ Atención al portal de Transparencia ❖ Directorio de enlaces.
	Área de Protección de Datos Personales.	❖ Directorio de enlaces, para capacitación y verificación y seguimiento como parte del programa de seguridad en protección de datos personales ❖ Atención a solicitudes de derechos ARCO.
Unidad de Informática	Área de Desarrollo y Sistemas.	❖ Directorios de Diputados y Funcionarios Públicos 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. ❖ Declaración Patrimonial y de Interés
	Área de soporte técnico	❖ Para dar trámite a las solicitudes de servicios que se hacen llegar para la revisión, mantenimiento y dictaminación del parque informático.

Cuadro 1. Tratamientos por área administrativa.

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



Cuadro 2. Número de procesos por área administrativa.

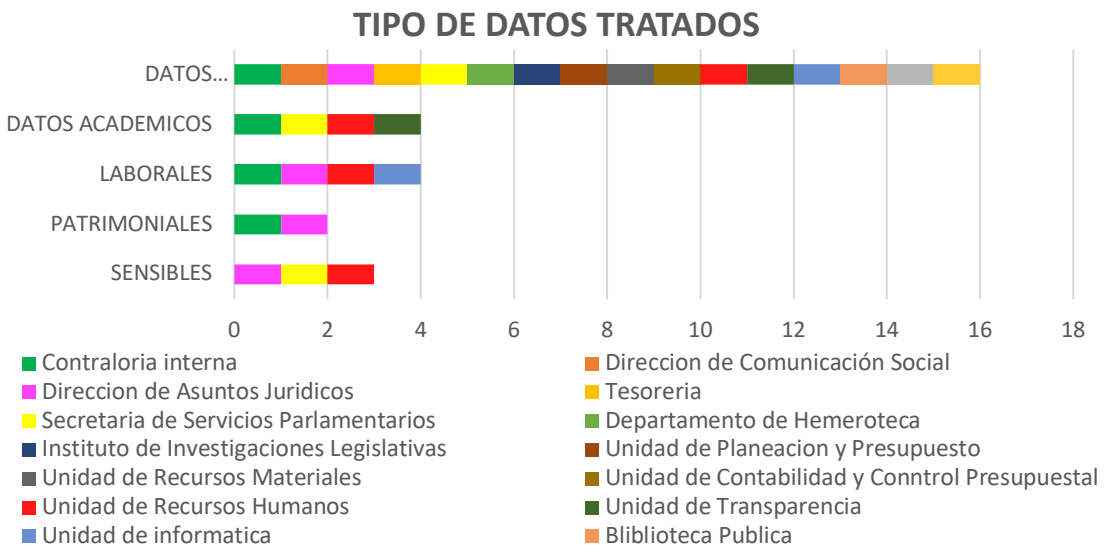
Como se puede observar, la unidad administrativa con mayor número de procesos es la Unidad de Recursos Humanos con 10 procesos, mientras que la que menos procesos tiene es el Departamento de Hemeroteca con 1 proceso o tratamiento.

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

Del mismo modo, se observó que principalmente se realizan 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 se inscriben a algún proceso de nombramiento, designación o ratificación por parte del Poder Legislativo, o bien por algún proceso jurídico.

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 o bien de familiares, 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.

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 intensión de dar cumplimiento al principio de legalidad, en el inventario de datos personales se pidió que cada usuario de los diversos tratamientos, especificará el fundamento legal de sus tratamientos, lo cual se plasma en la siguiente tabla; de igual forma en la última columna de la tabla, se puede observar los medios por los cuales los usuarios de los tratamientos obtienen los datos personales.

UNIDAD ADMINISTRATIVA	ÁREAS	PROCESO	FUNDAMENTO	MEDIO DE OBTENCION DE DATOS
JUNTA DE COORDINACIÓN POLÍTICA.	JUCOPO	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 Chapas.	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.	Por comunicación interna
(ÁREAS DE LA SECRETARÍA DE SERVICIOS ADMINISTRATIVOS)	UNIDAD DE TESORERÍA	Pago de nóminas diputados, personal estructuras y confianza.	Artículo 6to. de la Constitución Política Federa, apartado A.	De manera personal con la presencia física del titular.
		Pago de proveedores.	Artículo 6to. de la Constitución Política Federal, apartado A.	Por comunicación interna

	UNIDAD DE RECURSOS HUMANOS	Contratación y Alta de personal	Artículo 45. inciso B de la Ley Orgánica del H. Congreso el Estado.	De manera personal.
		Tramites de altas y bajas en el IMSS y pagos de cuotas obrero patronal	Artículo 2 de la Ley Federal del Trabajo y del Seguro Social.	De manera personal.
		INFONACOT	Artículo 132 frac. XXVI de la Ley Federal del Trabajo.	Vía portal de internet o sistema informático.
		Elaboración de nomina	Artículo 45 incisos B de la ley Orgánica del H. Congreso del Estado de Chiapas.	Por comunicación interna
		Inscripción al INFONAVIT.	Artículo 132 fracción XXVI y XXVI Bis. Ley Federal del Trabajo.	Por comunicación interna
		Créditos ante INFONAVIT.	Artículo 42-Reglamento de Inscripción, pago de aportaciones y entero de descuentos al INFONAVIT.	De manera personal. Vía portal de internet o sistema informático
		Certificación a INFONACOT.	Artículo 132 fracción XXVI y XXVI Bis. Ley Federal del Trabajo.	Vía correo electrónico
		Solicitudes de información y obligaciones de la plataforma nacional.	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.
		Timbrado de nómina.	129 y 129 A de la Ley de Impuestos Sobre la Renta.	Por comunicación interna
		Elaboración de constancias.	Artículo 45 de la ley Orgánica del H. Congreso del Estado de Chiapas.	Por comunicación interna
	UNIDAD DE RECURSOS MATERIALES	Contratación y prestación de servicios y compras.	Artículo 45 inciso C de la Ley Orgánica del H. Congreso del Estado.	De manera personal

		Orden de pago.	Artículo 45 inciso C de la Ley Orgánica del H. Congreso del Estado.	De manera personal
	UNIDAD DE CONTABILIDAD	Resguardo de Información	Artículos 6, 7, 9, 11, 12 de la Ley de Archivos del Estado de Chiapas	Por comunicación interna
		Procesos contables.	Artículo I, II, XVI, XVII, XVIII, XIX Ley de Contabilidad Gubernamental, Artículos XL, XLI Normatividad Contable del Estado de Chiapas.	Por comunicación interna
	UNIDAD DE PLANEACIÓN Y PRESUPUESTO	Elaborar el anteproyecto del Presupuesto de Egresos con cotizaciones de proveedores.	Artículo 344 del Código de la Hacienda Pública del Estado de Chiapas.	Por comunicación interna
		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
DIRECIÓN DE COMUNICACIÓN SOCIAL	DIRECIÓN DE COMUNICACIÓN SOCIAL	Registro de las personas que solicitan audiencia, para generar un control de las mismas.	Artículos 18, 95 y 96 de LPDPPSOECH, así como los artículos 47, fracción III,50 al 58.	De manera personal Por comunicación interna Vía telefónica Vía correo electrónico
		Agenda de los posibles eventos.		
CONTRALORÍA INTERNA	CONTRALORÍA INTERNA	Proceso de Acta-Entrega Recepción de servidor(a) público.	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 con la presencia física del titular de los datos personales o, en su caso, su representante.

		Atención y seguimiento al buzón de sugerencias y quejas del H. Congreso del Estado de Chiapas	Artículo 55 fracción IV de la Ley Orgánica del Congreso del estado de Chiapas y articulo 90 al 93 de la Ley de Responsabilidades Administrativas para el Estado de Chiapas.	Escrito o formato presentado directamente en el H. Congreso del Estado de Chiapas.
		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.	Ley de Responsabilidades Para el Estado de Chiapas articulo 32,33 y 34	Vía portal de internet o sistema informático
UNIDAD DE TRANSPARENCIA	ÁREA DE ATENCIÓN AL PÚBLICO, INTERPRETES Y TRADUCTORES EN LAS LENGUAS INDÍGENAS	Atención al portal de transparencia.	Artículo 5 fracción XXXV, 6 y 7 de la LPDPPSOECH, 68 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.	Vía portal de internet o sistema informático Vía correo electrónico Por comunicación interna
		Directorio de enlaces.		
	ÁREA DE PROTECCIÓN DE DATOS PERSONALES.	Directorio de enlaces para capacitación.	Artículo 5 fracción XXXV 6 y 7, 49 al 58 de la LPDPPSOECH, 68 de la ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, y Art. 64 del Reglamento de Transparencia del H. Congreso del Estado de Chiapas.	De manera personal con la presencia física del titular de los datos personales o, en su caso, su representante.
		Atención a las solicitudes de derechos ARCO		
MESA DIRECTIVA	MESA DIRECTIVA			
SERVICIOS PARLAMENTARIOS	UNIDAD DE LOS ARCHIVOS DE TRÁMITE	Recepción de solicitudes de apoyo de intervención	Art. 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.
		Solicitudes de desincorporaciones de bienes inmuebles.	Art. 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.

		Recepción de iniciativas de Ley y puntos de acuerdo.	Art. 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. Por comunicación interna.
		Recepción de propuestas para nombramientos de funcionarios públicos.	Art. 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
	TRÁMITES LEGISLATIVOS	Trámites de las solicitudes de desincorporaciones de bienes inmuebles.	Art. 43 de la Ley Orgánica del H. Congreso del Estado de Chiapas.	Por comunicación interna.
		Trámites de propuestas de nombramientos.	Art. 43 de la Ley Orgánica del H. Congreso del Estado de Chiapas.	Por comunicación interna
INSTITUTO DE INVESTIGACIONES LEGISLATIVAS	INSTITUTO DE INVESTIGACIONE LEGISLATIVAS	Investigaciones legislativas	Artículo 47 de la Ley Orgánica	Escrito o formato presentado directamente en el H. Congreso.
		Coordinación de visitas guiadas	Ley Orgánica del Congreso del Estado.	
		Control de oficios recibidos y emitidos por el instituto	Artículo 47 de la Ley Orgánica del H. Congreso	Escrito o formato presentado directamente en el H. Congreso. Directamente del titular.
		Elaboración de la agenda legislativa.	Artículo 47 de la Ley Orgánica	Escrito o formato presentado directamente en el H. Congreso
	BIBLIOTECA	*Control de acceso. *Control de préstamos de libros. *Control de equipos de cómputo.(Matutino y Vespertino)	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

	HEMEROTECA	Prestamos de Diarios locales para consulta.	Art 4 y 5 fracción XXXV 6 y 7 de la LPDPPSOECH	De manera personal. Escrito o formato presentado directamente en el H. Congreso.
	ARCHIVO HISTORICO	Prestamos de documentación para la consulta presencial (de usuarios internos externos al H. Congreso)	Ley de Archivos del Estado de Chiapas Ley Orgánica del Congreso del Estado	De manera personal Escrito o formato presentado directamente en el H. Congreso
		Implementación de la clasificación archivística de la documentación generada en las áreas que integran al H. Congreso	Ley de Archivos del Estado de Chiapas	
		Brindar asesorías y capacitación en materia de archivo 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, áreas internas del H. Congreso	Ley de Archivos del Estado de Chiapas	Por comunicación interna Vía correo electrónico
DIRECCIÓN DE ASUNTOS JURÍDICOS	DIRECCIÓN DE ASUNTOS JUÍDICOS	Trámites jurídicos	Artículo 4, 5 fracción XXXV 6 y 7 de la LPDPPSOECH.	Por transferencia. Vía correo electrónico
		Notificaciones procesos jurídicos	Artículo 4, 5 fracción XXXV 6 y 7 de la LPDPPSOECH.	Transferencia.Vía correo electrónico De manera personal.
INFORMÁTICA	ÁREA DE DESARROLLO Y SISTEMAS	Directorios de Diputados y Funcionarios Públicos del H. Congreso del Estado de Chiapas	Artículo 6°. de la Constitución Política Federal y Art. 38 de la LPDPPSOECH.	Escrito o formato presentado directamente en el H. Congreso.
		Credencialización oficial del personal del H. Congreso	Artículo 6°. de la Constitución Política Federal y Art. 38 de la LPDPPSOECH.	Escrito o formato presentado directamente en el H. Congreso.

		Solicitudes de servicio web del H. Congreso del Estado de Chiapas	Artículo 6°. de la Política Federal y Art. 38 de la LPDPPSOECH.	Escrito o formato presentado directamente en el H. Congreso.
		Declaración Patrimonial y de Interés	Artículo 6°. de la Constitución Política Federal y Art. 38 de la LPDPPSOECH.	Vía portal de internet o sistema informático
	ÁREA DE SOPORTE TÉCNICO	Para dar trámite a las solicitudes de servicios que se hacen llegar para la revisión, mantenimiento y dictaminarían del parque informático.	Artículo 6°.de la Constitución Política Federal y Art. 38 de la LPDPPSOECH.	Escrito o formato presentado directamente en el H. Congreso.

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

d) Funciones y responsabilidades de los tratamientos o procesos de datos personales.

Uno de los aspectos importantes que se derivaron 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 intensión 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.

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 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 una primera instancia, se pudo observar que servidores públicos tratan datos personales, lo que resulta importante, porque son a los primeros que se capacitaran para sensibilizar y en consecuencia lograr que de manera natural se proteja la información y los procesos por los que se traten datos personales.

Así entonces en la siguiente tabla se puede observar de acuerdo al área, los procesos, la finalidad y los usuarios o servidores públicos que los tratan

PROCESO, FINALIDAD Y USUARIO				
UNIDAD ADMINISTRATIVA	ÁREAS	PROCESO	FINALIDAD DEL TRATAMIENTO	USUARIOS DEL PROCESO
JUNTA DE COORDINACIÓN POLÍTICA.	JUCOPO	Registro de personas que solicitan audiencia, y programación de reuniones de trabajo.	Consulta	Junta de Coordinación Política
		Propuestas al pleno para la integración de las comisiones legislativas.		
(ÁREAS DE LA SECRETARÍA DE SERVICIOS ADMINISTRATIVOS)	UNIDAD DE TESORERÍA	Pago de nómina diputados.	Para pago	Lic. Consuelo Gómez Román Lic. María de los Ángeles Pérez
		Pago de proveedores.		
	UNIDAD DE RECURSOS HUMANOS	Contratación y Alta de personal	No se cuentan	Yeri Ruíz Ruíz Carolina Ochoa García Karina Herrera Obregon
		Trámites de altas y bajas en el IMSS y pagos de cuotas obrero patronal	Para ser ingresados a los servicios de salud del Instituto Mexicano del Seguro Social	José Luis Ramírez Hernández

[2] Comisionado Javier Diez de Urdanivia, inai, Conferencia en "La Ruta de la Privacidad 2022", 26 de enero de 2022.

		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 de nomina	Elaboración de nomina Pago de salario de trabajadores	Lic. Carolina Ochoa García Cp. José Isidro Ovando Pérez
		Inscripción al INFONAVIT.	Movimientos de afiliación al INFONAVIT	Tomas Morales San Cristóbal
		Créditos ante INFONAVIT.	Descuento por crédito INFONAVIT	Tomas Morales San Cristóbal
		Certificación a INFONACOT.	Alta de trabajador al INFONACOT Elaborar formatos de nomina Personal eventual	
		Solicitudes de información y obligaciones de la plataforma nacional.	Dar cumplimiento a las obligaciones de transparencia	
		Timbrado de nómina.	Timbrado de nomina	David Paredes Trinidad
		Elaboración de constancias.	Declaración anual	
	UNIDAD DE RECURSOS MATERIALES	Contratación y prestación de servicios y compras.	Para realizar acciones de cotizaciones, compras y/o adquisiciones con los proveedores	Ing. José Alfredo Jiménez Reyes, Ing. Laura Daniela Cáceres Morales
		Orden de pago.	Para realizar acciones de trámite de pago de factura	

	UNIDAD DE CONTABILIDAD	Resguardo de Información	Resguardar la información de manera digital	Pedro Antonio, Gallardo Simuta, Carlos Alberto López Consospo, Norma Edith Gómez Hernández, Cesar Augusto Licea Sánchez
		Procesos contables.	Realizar procesos contables y resguardo de información	Dulce Esmeralda Gómez Molina, Mayra del Carmen Moreno Albores, Cesar Trinidad Saldaña Mayorga, Leticia Cecilia García Morales, Cristóbal Moisés Fernández Ruíz, Sergio Alejandro Cruz Cruz, Juan Luis Molina Santiago
	UNIDAD DE PLANEACIÓN Y PRESUPUESTO	Elaborar el anteproyecto del Presupuesto de Egresos.	Documentación comprobatoria para elaborar el anteproyecto del presupuesto de egresos	Lic. María Asunción Penagos Román, C.P. Erika del Socorro Alfaro Solís, C.P Martha Elena Mendoza C.P Alma Delia López Reyes, Lic. Lorenzo Alberto Aguilar Centeno, Lic. Christian Miguel Salinas, Lic. José Negrete Marín, C. Margarita Concepción Ramón Levet, C.P. Laura Lilia Arrevillaga Cano.
		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	Registro de las personas que solicitan audiencia, para generar un control de las mismas.	Para tener un registro de personas que solicitan información o requieren un servicio de cobertura. Para comunicación constante con el titular de los datos personales. Para envió y recepción de información.	Lic. Karla Irina Mendiola Calvo. Lic. Arturo Tomas Torres Guzmán
		Agenda de los posibles eventos.		
CONTRALORÍA INTERNA	CONTRALORÍA INTERNA	Proceso de Acta-Entrega Recepción de Servidores Públicos.	Forman parte del contenido del Acta Entrega Recepción, en el apartado de identificación del servidor publico	Lic. Carlos Ernesto Ozuna Hodich.
		Atención y seguimiento al buzón de sugerencias y quejas del H. Congreso del Estado de Chiapas	Recibir y dar seguimiento a las sugerencias, quejas y denuncias ciudadanas, con respecto a la actuación de los servidores públicos adscritos al poder legislativo.	Jorge David Barragán Gordillo 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	Mariana Guadalupe Domínguez López
		Declaración patrimonial y de interés.	Cumplimiento de la Ley de Responsabilidades Administrativas para el Estado de Chiapas art 32,33 y 34	C.P María de los Ángeles Ramírez Cameras, y Personal de sistemas de la Unidad de Informática del H. Congreso del Estado de Chiapas
UNIDAD DE TRANSPARENCIA	ÁREA DE ATENCIÓN AL PÚBLICO, INTERPRETES Y TRADUCTORES EN LENGUAS INDIGENAS	Atención al portal de transparencia.	Para realizar los trámites internos para las atenciones de las solicitudes.	Lic. Silvia Molina Ruíz Lic. Magdalena Pablo Hernández Lic. Argelia Nuricumbo Escobar
		Directorio de enlaces.		

	ÁREA DE PROTECCIÓN DE DATOS PERSONALES	Directorio de enlaces para capacitación y verificación y seguimiento como parte del programa de seguridad en protección de Datos Personales. Atención a las solicitudes de derecho ARCO.	Contar con el directorio de los enlaces de cada una de las áreas. Capacitación y seguimiento Elaboración del documento de seguridad	Lic., Maria del Carmen Esteban Cariño. C. Carolina Trejo Altuzar Ing. Orbelin Galindo Mancilla.
MESA DIRECTIVA	MESA DIRECTIVA			
SERVICIOS PARLAMENTARIOS	UNIDAD DE LOS ARCHIVOS DE TRÁMITE	Recepción de solicitudes de apoyo de intervención	Turnarlo al área correspondiente	Hugo Orlando Santana Gómez y Secretarias
		Solicitudes de desincorporaciones de bienes inmuebles.	Trasmite legislativo	
		Recepción de iniciativas de Ley y puntos de acuerdo.		
		Recepción de propuestas para nombramientos de funcionarios públicos.		
	TRÁMITES LEGISLATIVOS	Tramites de las solicitudes de desincorporaciones de bienes inmuebles. Tramites de propuestas de nombramientos.	Cotejar el nombre del solicitante con su acta de nacimiento y su acta de cabildo, con la constancia de escasos recursos económicos, con la constancia de no propiedad Trámite legislativo	Lic. Alejandro Ruiz Rodríguez Lic. Fanny Manuela González Juárez Lic. Shariver Espino Cazares
INSTITUTO DE INVESTIGACIONES LEGISLATIVAS	INSTITUTO DE INVESTIGACIONES LEGISLATIVAS	Investigaciones legislativas	Verificación de requisitos para nombramientos de servidores públicos	Lic. Alejandro Ruiz Rodríguez Lic. Fanny Manuela González Juárez Lic. Shariver Espino Cazares Diputados presidentes de comisiones legislativas que intervienen.
	Instituto de investigaciones legislativas	Coordinación de visitas guiadas	Organización de visitas Recepción de personas Recorrido	Lic. Violeta de la Cruz Ramírez/Secretaria Dra. Tatyana Penagos Coello /Tituar.

		Control de oficios recibidos y emitidos por el instituto	Cumplir obligaciones.	Lic. Mildre Y. Fuentes Burguete / Jefe de Área Lic. Amelia Gómez Cruz/Asesor Lic. Luz María Cristiani Gordillo/ Asistente Maria del Socorro Ovilla García/ Capturista Lic. Karina Janet Díaz Flores/analista
		Elaboración de la agenda legislativa.	Análisis Comparación Elaboración de un documento Documento final	
	BIBLIOTECA	Control de acceso, Control de préstamos de libros, Control de equipos de cómputo.(Matutino y Vespertino)	Control de acceso Control de préstamos de libros Control de equipo de cómputo.	Dulzura Zarate Mandujano, María Teresa Galdámez Vera, Martha Laura Escobar Flores. Azucena de Camposeco, Yadira Elena Zamudio Ramírez, Rudy Alonso Ramírez Aguilar.
	HEMEROTECA	Prestamos de diarios locales para consulta.	Para identificar al titular	Lic. María Soledad Culebro Espinoza C. Martha Martínez Ballinas
	ARCHIVO HISTÓRICO	Prestamos de documentación para la consulta presencial (de usuarios internos externos al H. Congreso)	Se recaban datos personales con la finalidad de registrar a las personas que solicitan una audiencia o información y generar un control tanto de visitas como atención. Los datos personales recabados son utilizados únicamente para el acto o efecto para el cual son solicitados, posteriormente se eliminan.	Deborah Cancino Alamilla Fernando Zapata García Darwin Alberto Gutu Benavidez. Mario Eduardo López Álvarez Hugo Alberto Ruis Flores
		Implementación de la clasificación archivística de la documentación generada en las áreas que integran al H. Congreso		Hugo Alberto Ruis Flores Coordinador de las áreas de Archivo
		Brindar asesorías y capacitación en materia de archivo al personal del H. Congreso del Estado.		Hugo Alberto Ruis Flores Coordinador de las áreas de Archivo
		Atender solicitudes de información del portal de transparencia, áreas internas del H. Congreso		Deborah Cancino Alamilla Fernando Zapata García Darwin Alberto Gutu.

DIRECCIÓN DE ASUNTOS JURÍDICOS	DIRECCIÓN DE ASUNTOS JURÍDICOS	Trámites jurídicos	Para efectos jurídicos de identificación	Manuel Liar Aguilar Gómez
		Notificaciones procesos jurídicos		Gustavo Fernández García
INFORMÁTICA	ÁREA DE DESARROLLO Y SISTEMAS	Directorios de Diputados y Funcionarios Públicos del H. Congreso del estado de Chiapas	Registrar los directorios de los diputados	Alberto Salinas Trujillo. Xochilt Candelaria Torres Toledo
		Credencialización oficial del personal del H. Congreso.	La elaboración de la credencialización	Alberto Salinas Trujillo. Fidel Uresti Cantú.
		Solicitudes de servicio web del H. Congreso del Estado de Chiapas	Para dar trámite a las solicitudes	Alberto Salinas Trujillo.
		Declaración Patrimonial y de Interés		
	ÁREA DE SOPORTE TÉCNICO	Para dar trámite a las solicitudes de servicios que se hacen llegar para la revisión, mantenimiento y dictaminación del parque informático.	Para dar trámite a las solicitudes	Francisco Javier Gordillo Estrada, Nepthali Jacob Molina Arguello, Darinel Flecha Melchor, Fidel Enrique Uresti Cantú. Gustavo Adolfo Aguilar Pérez.

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

e) 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 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	✓ Identificativos ✓ Laborales ✓ Patrimoniales
Instituto Mexicano del Seguro Social IMSS	✓ Identificativos ✓ Laborales ✓ Patrimoniales ✓ Sensibles (de salud)
Instituto del Fondo Nacional para el Consumo de los Trabajadores INFONACOT	✓ Identificativos ✓ Laborales ✓ Patrimoniales
Instituto del Fondo Nacional de la Vivienda para los Trabajadores INFONAVIT	✓ Identificativos ✓ Laborales ✓ Patrimoniales
Institución bancaria	✓ Identificativo ✓ Laborales ✓ Patrimoniales
Poder Ejecutivo del Estado de Chiapas	✓ 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 intensión 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.

IX. 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

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

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

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 racia**l, **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).

En un segundo momento, para la determinación del riesgo sobre esa tipología de datos personales se valoró la probabilidad e impacto, considerando que, la Ley establece que las causas de vulneración de seguridad más recurrentes son:

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

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,

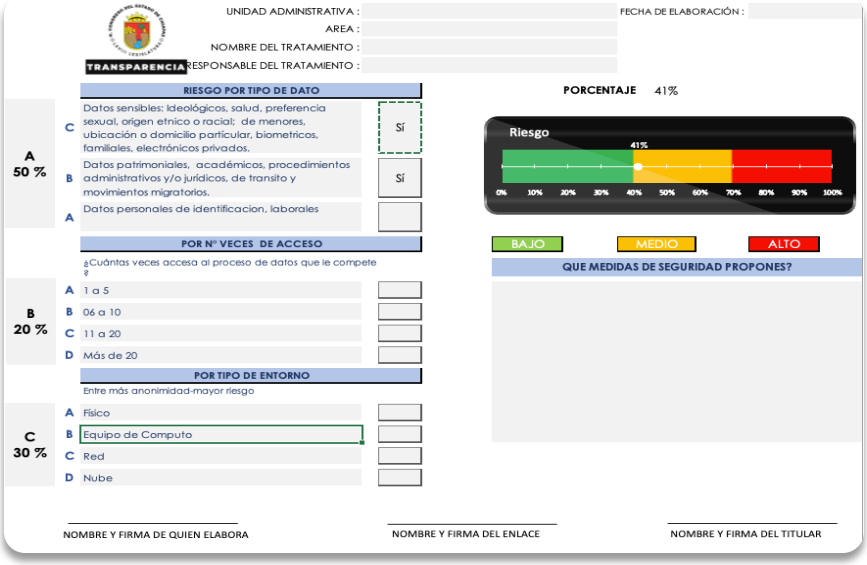
Las amenazas, que son factores externos que tienen el potencial de dañarlos y, **Los escenarios de vulneración**, que en este caso son dos: el primero, es el número de veces que se accede a la información, y el segundo, el entorno mediante el cual se accede a la información.

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 formula $Z(A+B+C)^n$, 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 $\boldsymbol{n}$, 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 $\boldsymbol{n}$) (**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 mismo; 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.



La herramienta empleada consistió en un formato denominado **Formulario de Análisis de Riesgo** (**anexo 2**) y una **gráfica de calor** (**anexo 3**), en la que cada área represento el nivel de riesgo de los tres parámetros antes descritos; resultando lo siguiente:

A.- RIESGO POR TIPO DE DATOS

A partir del tipo de dato es posible reconocer el factor de riesgo inherente como se muestra a continuación:

TIPO DE DATO	RIESGO INHERENTE	NIVEL DE RIESGO
Datos identificativos, laborales.	Bajo	A
Datos patrimoniales, académicos, procedimientos administrativos/jurídicos.	Medio	B
Datos sensibles(Salud, origen étnico o racial, ideológicos, vida sexual); así como datos de familiares o de menores; de ubicación o domicilio particular; biométricos; características físicas; electrónicos privados.	Alto	C

Cuadro 7. Riesgo por tipo de datos (verde bajo, ámbar medio, rojo alto)

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 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	2*	
MESA DIRECTIVA		
SECRETARIA DE SERVICIOS PARLAMENTARIOS Unidad de Archivo y Correspondencia	4*	
Trámites Legislativos	2*	
SECRETARÍA DE SERVICIOS ADMINISTRATIVOS Tesorería	2*	
Planeación y Presupuesto	2*	
Recursos Humanos	10*	
Recursos Materiales	2*	
Contabilidad	2*	
INSTITUTO DE INVESTIGACIONES LEGISLATIVAS	3*	1*
Biblioteca	1*	2*
Hemeroteca	1*	
Archivo Histórico	4*	
DIRECCIÓN DE ASUNTOS JURÍDICOS	2*	
CONTRALORÍA INTERNA	3*	1*
DIRECCIÓN DE COMUNICACIÓN SOCIAL	2*	
UNIDAD DE TRANSPARENCIA Área de Atención al Público, Intérpretes y Traductores e Lenguas Indígenas	2*	
Área de Protección de Datos Personales	2*	
UNIDAD DE INFORMATICA Área de Desarrollo y Sistemas	3*	1*
Área de Soporte Técnico		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
- Nube (intranet, Dropbox, google, drive, etc.)

En este rubro, cada área expreso a que entorno 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				
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 Atención al Público, Intérpretes y Traductores en Lenguas Indígenas	✓	✓	✓	✓
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 riego latente de datos personales.

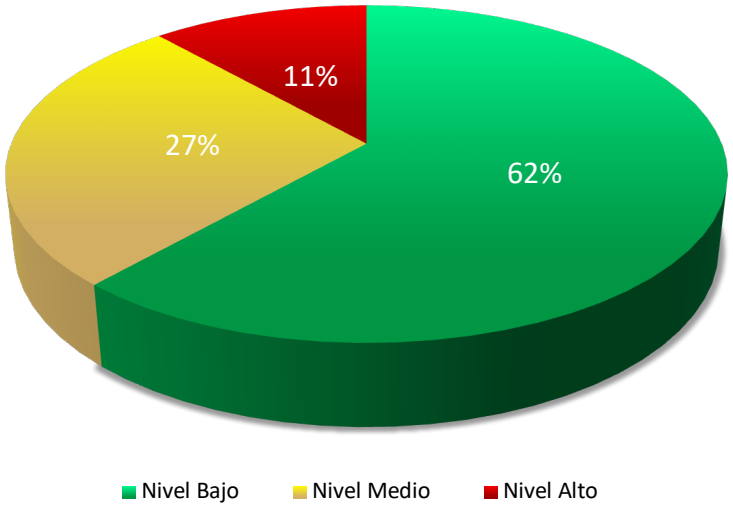
Así entonces, y considerando los tres parámetros para calcular el nivel de riesgo latente, que se obtuvo del análisis de semáforo en las gráficas de calor (**anexo 3**) de cada una de las áreas, se concluye que, las unidades administrativas que resultaron con nivel de riesgo alto (color rojo) en sus 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 intensión 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	4	INFORMATICA	1	INFORMATICA	1
HEMEROTECA	1	TRANSPARENCIA	1	CONTRALORÍA	1
BIBLIOTECA	3	CONTRALORIA INTERNA	3	DIRECCIÓN ASUNTOS JURIDICOS	2
INFORMATICA	3			RECURSOS HUMANOS	2
CONTABILIDAD	1	PARLAMENTARIOS	2		
COMUNICACIÓN SOCIAL	2	RECURSOS HUMANOS	2		
PLANEACIÓN	1	PLANEACIÓN	1		
INVESTIGACIONES LEGISLATIVAS	2	NVESTIGACIONES LEGISLATIVAS	2		
TESORERÍA	2	REURSOS MATERIALES	2		
PARLAMENTARIOS	4				
RECURSOS HUMANOS	6				
TRANSPARENCIA	3				
TOTAL DE PROCESOS					
	32		14		6

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 latente de nivel bajo.

X. 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

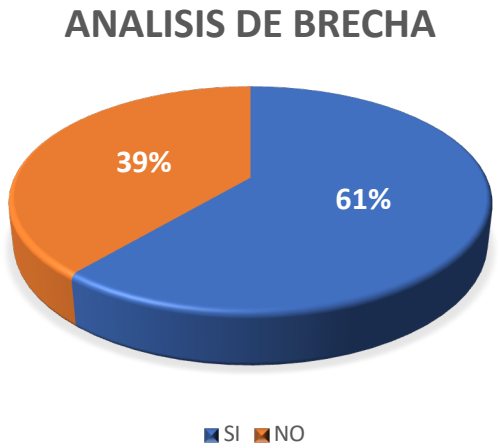
contiene una serie de medidas a manera de preguntas, para responder si se cuenta o no con ellas y un campo más de observaciones; en este instrumento se consideraron 3 rubros a saber:

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.

Este ejercicio sirvió para que cada enlace trabajara en conjunto con los responsables de los procesos (usuarios) y se dieran cuenta de las necesidades reales y de la importancia de las medidas de seguridad existentes y faltantes.

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.



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.

XI. 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 efectué, el responsable deberá establecer y mantener las medidas de seguridad que permitan proteger los datos personales contra daño, perdida, 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 los 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 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:

I. Seguimiento del programa de mantenimiento preventivo y correctivo anual de los equipos de cómputo, que implementó la Unidad de Informática;

II. 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;

Por lo que cualquier mal uso de estos medios serán 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.

III. 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.

IV. 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.

V. Implementar Directorio Activo.

VI. Implementación de niveles y esquema de privilegios, para que el usuario lleve a cabo las actividades que requiere de acuerdo con sus funciones.

VII. Borrar o eliminar de la papelera de reciclaje y del escritorio de los equipos de cómputo los documentos o archivos electrónico que no sean necesarios para el desarrollo de funciones.

VIII. Implementar técnicas de borrado seguro de la información, de acuerdo con los dispositivos que se tengan.

IX. 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.

X. Contemplar medidas adecuadas para la destrucción de los medios de almacenamiento electrónicos, como la desintegración, pulverización entre otros;

XI. 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, perdida, transmisión y acceso no autorizado, o alguna otra que vulnere la información confidencial del usuario).

Cuando se tenga que realizar 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, fotografías o bitácoras.

Cada unidad administrativa y sus áreas correspondientes elaboraran un plan de trabajo para adoptar e implementar las referidas medidas de seguridad de acuerdo a sus funciones y tratamientos que realizan en su función diaria.

b) Monitoreo de las medidas de seguridad implementadas

Una manera de mejora continua es a través del monitoreo y revisión de las medidas de seguridad implementadas, amenazas y vulneraciones, lo que permite definir nuevos controles o bien realizar actualizaciones sustentadas de los mecanismos implementados, y por su puesto de las medidas de seguridad establecidas, recordemos que todo es susceptible de mejorar; este se realizará una vez al año.

Por tal razón algunos aspectos a verificar son:

- Actualizar: Activos, procesos y/o tratamientos
- Medidas de seguridad basadas en la cultura del personal
- Medidas de seguridad en el entorno de trabajo físico
- Medidas de seguridad en el entorno digital o de sistemas de información tecnológica
- Cumplimiento de la normatividad en la materia de protección de datos personales.
- Incidentes y vulneraciones de seguridad

c) Procedimiento para actuar 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.

XII. 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).

Cuando así se amerite, se establecerán reuniones de trabajo con 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.

En la ejecución de este Documento de Seguridad, se estableció un calendario anual para la impartición de los cursos de capacitación (**Anexo 7**), dando a conocer de forma anticipada las fechas a los titulares de las distintas áreas involucradas en los tratamientos de datos personales de este Poder Legislativo.

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.

XIII. ACTUALIZACIONES

Conforme al artículo 51 de la ley estatal de la materia, el presente documento de seguridad deberá ser actualizado por la ocurrencia de alguno de 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.

XIV. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

El presente documento de seguridad es aprobado en forma unánime por los integrantes del Comité de Transparencia del Honorable Congreso del Estado de Chiapas, conforme a sus atribuciones; firmando al calce todos los que intervinieron. a los dos días del mes de diciembre del año dos mil veintidós.

ING. GUADALUPE MORALES MARÍN
Presidenta

DR. FRANCISCO CHACÓN SÁNCHEZ
Vocal

LIC. JOSÉ LUIS RUÍZ RODRÍGUEZ
Vocal

MTRO. JULIO CÉSAR RIZO CASTELLANOS
Secretario

XV. ANEXOS

1. Formato de combinaciones para obtener el nivel de riesgo latente.

2. Formulario de Análisis de Riesgo.

3. Gráfica de calor.

4. Formulario de "Análisis de Brecha".

5. Formato de reporte de incidencias.

6. Formato de seguimiento de incidentes y acciones correctivas.

7. Cronograma de capacitación.

Formato de combinaciones para obtener el nivel de riesgo latente.

A continuación, se detallan los niveles de riesgo de los datos personales tratados al interior de las áreas que conforman el H. Congreso del Estado, obtenidos mediante la fórmula $\mathbf{Z}(\boldsymbol{A}+\boldsymbol{B}+\boldsymbol{C})^{\boldsymbol{n}}$, 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 $\boldsymbol{n}$, es el número de combinaciones posibles entre las mismas.
Riesgo inherente **Nivel Bajo**, ocurre cuando:

1. El nivel de riesgo por **tipo de datos** sea **de clase A, el** nivel de riesgo por **número de veces** de acceso sea **rango A, e**l nivel de riesgo por **tipo de entorno** sea **clase A.**

2. El nivel de riesgo por **tipo de datos** sea **de clase A o B,** el nivel de riesgo por **número de veces** de acceso sea **rango A, e**l nivel de riesgo por **tipo de entorno** sea **clase A o B.**

3. El nivel de riesgo por **tipo de datos** sea **de clase A + B,** el nivel de riesgo por **número de veces** de acceso sea **rango A o B, e**l nivel de riesgo por **tipo de entorno** sea **clase A + B.**

4. El nivel de riesgo por **tipo de datos** sea **de clase A,** el nivel de riesgo por **número de veces** de acceso sea **rango B o C, e**l nivel de riesgo por **tipo de entorno** sea **clase A o A + B.**

Riesgo inherente **Nivel Medio**, ocurre cuando:

1. El nivel de riesgo por **tipo de datos** sea **de clase A+B, el** nivel de riesgo por **número de veces** de acceso sea **rango A o B, e**l nivel de riesgo por **tipo de entorno** sea **clase A +B+C.**

2. El nivel de riesgo por **tipo de datos** sea **de clase A+B, el** nivel de riesgo por **número de veces** de acceso sea **rango C, e**l nivel de riesgo por **tipo de entorno** sea **clase A +B.**

3. El nivel de riesgo por **tipo de datos** sea **de clase A+B+C, el** nivel de riesgo por **número de veces** de acceso sea **rango A o B o C, e**l nivel de riesgo por **tipo de entorno** sea **clase B+C.**
4. El nivel de riesgo por **tipo de datos** sea **de clase A, el** nivel de riesgo por **número de veces** de acceso sea **rango C, e**l nivel de riesgo por **tipo de entorno** sea **clase B+C+D.**

5. El nivel de riesgo por **tipo de datos** sea **de clase C, el** nivel de riesgo por **número de veces** de acceso sea **rango A o B o C, e**l nivel de riesgo por **tipo de entorno** sea **clase A+B+C.**

Riesgo inherente por **Nivel de Alto**, ocurre cuando:

1. El nivel de riesgo por **tipo de datos** sea **de clase A+B+C+D,** el nivel de riesgo por **número de veces** de acceso sea **rango C o D,** el nivel de riesgo por **tipo de entorno** sea **clase A+B+C+D.**

2. El nivel de riesgo por **tipo de datos** sea **de clase A+C,** el nivel de riesgo por **número de veces** de acceso sea **rango C o D,** el nivel de riesgo por **tipo de entorno** sea **clase A+B+C+D.**

3. El nivel de riesgo por **tipo de datos** sea **de clase A+C,** el nivel de riesgo por **número de veces** de acceso sea **rango C o D,** el nivel de riesgo por **tipo de entorno** sea **clase B+C+D.**

4. El nivel de riesgo por **tipo de datos** sea **de clase A+D,** el nivel de riesgo por **número de veces** de acceso sea **rango C o D,** el nivel de riesgo por **tipo de entorno** sea **clase B+C.**

Formulario de Análisis de Riesgo.

Unidad Administrativa:
Área:
Tratamiento:

Riesgo por tipo de dato

1. Seleccione todas las categorías de datos personales que trata.

A	Datos identificativos	
B	Datos electrónicos	
A	Datos laborales	
B	Datos patrimoniales	
B	Datos sobre procedimientos administrativos y/o Jcos.	
B	Datos académicos	
B	Datos de tránsito y movimiento migratorio	
C	**Datos sensibles**	
B	Datos biométricos	
C	Datos menores	
C	Datos de familiares	

Riesgo por número de veces de acceso

2. Seleccione el número de veces que se accede a la base de datos personales que se pretende proteger en un intervalo de 24 horas.

No. de accesos

A	1 a 5 veces	
B	06 a 10 veces	
C	11 a 20 veces	
D	Más de 20	

Riesgo por tipo de entorno

3. Seleccione los entornos desde los cuales se acceden a los datos personales

A	Físico (archiveros de la unidad)	
B	Equipo de computo	
C	Red	
D	Nube (intranet, Dropbox, google drive, etc.)	

Gráfica de calor.

ANEXO 3

TRANSPARENCIA

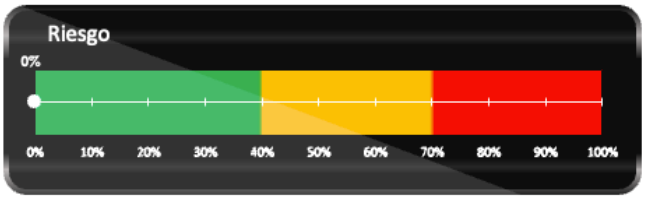
UNIDAD ADMINISTRATIVA :
AREA :
NOMBRE DEL TRATAMIENTO :
RESPONSABLE DEL TRATAMIENTO :
FECHA DE ELABORACIÓN :

	RIESGO POR TIPO DE DATO	
C	Datos sensibles: Ideológicos, salud, preferencia sexual, origen etnico o racial; de menores, ubicación o domicilio partícular, biometricos, familiales, electrónicos privados.	
B	Datos patrimoniales, académicos, procedimientos administrativos y/o jurídicos, de transito y movimientos migratorios.	
A	Datos personales de identificacion, laborales	

	POR N° VECES DE ACCESO	
	¿Cuántas veces accesa al proceso de datos que le compete ?	
A	1 a 5	
B	06 a 10	
C	11 a 20	
D	Más de 20	

	POR TIPO DE ENTORNO	
	Entre más anonimidad-mayor riesgo	
A	Físico	
B	Equipo de Computo	
C	Red	
D	Nube	

PORCENTAJE 0%



BAJO MEDIO ALTO

QUE MEDIDAS DE SEGURIDAD PROPONES?

NOMBRE Y FIRMA DE QUIEN ELABORA

NOMBRE Y FIRMA DEL ENLACE

NOMBRE Y FIRMA DEL TITULAR

Formulario de "Análisis de Brecha".

ANEXO 4

ÁREA :	
ANALISIS DE BRECHA.	
(MEDIDAS DE SEGURIDAD EXISTENTES VS MEDIDAS DE SEGURIDAD FALTANTES).	
MEDIDAS DE SEGURIDAD BASADAS EN LA CULTURA DEL PERSONAL	

PREGUNTA O CONTROL	SI	NO	PROPUESTA/OBSERVACIONES.
¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?			
Política de escritorio limpio			
Hábitos de cierre y resguardo			
Impresoras, escáneres, copiadoras y buzones limpios			
¿Tienes mecanismos para eliminar de manera segura la información en equipo de cómputo y medios de almacenamiento electrónico?			
Destrucción segura de documentos			
Tienen periodos de retención y destrucción de información			
Toman precauciones con los procedimientos de reutilización de documentos (reciclables).			
Informan al personal sobre sus deberes mínimos de seguridad y protección de datos.			
Fomentan la cultura de la seguridad de la información.			
¿Tienes procedimientos para actuar ante las vulneraciones a la seguridad de los datos personales?			
¿Tienes un procedimiento de notificación de vulneraciones?			
¿Realizas respaldos periódicos de los datos personales?			
Mencione otro:			

MEDIDAS DE SEGURIDAD EN EL ENTORNO DE TRABAJO FISICO			
PREGUNTA O CONTROL	SI	NO	OBSERVACIONES
¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?			
Mantener registros del personal con acceso al entorno de trabajo.			
¿Tienes medidas de seguridad para evitar el robo?			
Cerraduras, chapas y candados			
Elementos disuasorios (alarmas)			
¿Cuidas el movimiento de información en entornos de trabajo físico?			
Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico.			
Mantener en movimiento solo copias de la información, no el elemento original.			
El espacio físico es seguro para el resguardo de la información.			
Usar mensajería certificada			

MEDIDAS DE SEGURIDAD EN EL ENTORNO DE TRABAJO DIGITAL			
PREGUNTA O CONTROL	SI	NO	OBSERVACIONES
¿Realizas actualizaciones al equipo de cómputo?			
¿Revisa periódicamente el software instalado en el equipo de cómputo?			
¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?			
Uso de contraseñas y/o cifrado.			
Bloqueo y cierre de sesiones.			
Administrar usuarios y accesos.			
¿Revisas la configuración de seguridad del equipo de cómputo?			
¿Tienes medidas de seguridad para navegar en entornos digitales?			
Reglas de navegación segura.			
Uso de conexiones seguras.			
¿Cuidas el movimiento de información en entornos de trabajo digitales?			
Seguridad de la información enviada y recibida			

Enlace

Visto Bno. del titular

Formato de reporte de incidencias.

ANEXO 5

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS
JUNTA DE COORDINACIÓN POLÍTICA
UNIDAD DE TRANSPARENCIA

INFORMACIÓN GENERAL

INFORMACIÓN DE QUIEN DETECTA EL INCIDENTE			
NOMBRE:			
CARGO:			
TELÉFONO:		CELULAR:	

INFORMACIÓN SOBRE EL INCIDENTE			
FECHA:		HORA:	
LUGAR DONDE SE DETECTO EL INCIDENTE:			
NOMBRE DEL RESPONSABLE DEL PROCESO			
TIPO DE DATOS PERSONALES AFECTADOS			

RESUMEN TECNICO DEL INCIDENTE			
TIPO DE INDICENTE	☐ Denegación de servicio	☐ Uso no autorizado	☐ Espionaje
	☐ Código malicioso	☐ Acceso no autorizado	☐ Robo, pérdida o extravió
	☐ Ingeniería social	☐ Otro:	

TIPO DE SOPORTE DE TRATAMIENTO	☐ Físico	☐ Electrónico

DESCRIPCIÓN DETALLADA ENTORNO AL INCIDENTE OCURRIDO

FIRMA	
NOMBRE Y FIRMA DE QUIEN DETECTA EL INCIDENTE	NOMBRE Y FIRMA DEL ENLACE

Formato de seguimiento de incidentes y acciones correctivas

ANEXO 6

HONORABLE CONGRESO DEL ESTADO DE CHIAPAS
JUNTA DE COORDINACIÓN POLÍTICA
UNIDAD DE TRANSPARENCIA

ACCIONES CORRECTIVAS

1.- AISLAMIENTO DEL TRATAMIENTO DE DATOS AFECTADOS:

EL TRATAMIENTO FUE SUSPENDIDO/BLOQUEADO/RESGUARDADO	☐ SÍ	☐ NO

ACCIÓN REALIZADA	

SÍ	HORA		FECHA	
NO	DESCRIBIR LA RAZON			

EVIDENCIA DE LA ACCIÓN REALIZADA	*Señale si se anexa alguna evidencia como pueden ser: Videos, fotografías, declaraciones,etc.*
PERSONA QUE REALIZO LA ACCIÓN:	
CARGO:	
TELÉFONO:	CELULAR:

2.- OTRAS ACCIONES CORRECTIVAS IMPLEMENTADAS:

ACCIÓN REALIZADA			
HORA		FECHA	
EVIDENCIA DE LA ACCIÓN REALIZADA	*Señale si se anexa alguna evidencia como pueden ser: Videos, fotografías, declaraciones,etc.*		
PERSONA QUE REALIZO LA ACCIÓN:			
CARGO:			
TELÉFONO:		CELULAR:	

ACCIÓN REALIZADA			
HORA		FECHA	
EVIDENCIA DE LA ACCIÓN REALIZADA	*Señale si se anexa alguna evidencia como pueden ser: Videos, fotografías, declaraciones,etc.*		
PERSONA QUE REALIZO LA ACCIÓN:			
CARGO:			
TELÉFONO:		CELULAR:	

CONTACTOS INTERNOS					
JEFE INMEDIATO					
NOMBRE:					
CARGO:			CORREO ELECTRÓNICO:		
TELÉFONO:		CELULAR:		TÉLEFONO ALTERNOS.	
TIPO DE INCIDENTE	☐ Físico		☐ Electrónico		☐ Administrativo

JEFE DE INFORMATICA					
NOMBRE:					
CARGO:			CORREO ELECTRÓNICO:		
TELÉFONO:		CELULAR:		TÉLEFONO ALTERNOS.	

JEFE RECURSOS MATERIALES					
NOMBRE:					
CARGO:			CORREO ELECTRÓNICO:		
TELÉFONO:		CELULAR:		TÉLEFONO ALTERNOS.	

JEFE DE SERVICIOS ADMINISTRAVICOS					
NOMBRE:					
CARGO:			CORREO ELECTRÓNICO:		
TELÉFONO:		CELULAR:		TÉLEFONO ALTERNOS.	

JEFE UNIDAD DE TRANSPERENCIA					
NOMBRE:					
CARGO:			CORREO ELECTRÓNICO:		
TELÉFONO:		CELULAR:		TÉLEFONO ALTERNOS.	

ANEXO 7

Programa de capacitación 2022-2023

TEMAS	FECHAS/GRUPO 2022-2023																														
	diciembre				enero			febrero				marzo					abril			mayo				junio				julio			
	13	14	16	19	13	19	26	9					2	9	16	23	13	20	27	4				1	8	15	22	7	14	21	28
Derechos Arco (acceso, rectificación, cancelación, oposición).	1	2	3	4																											
Normatividad en materia de Datos Personales y clasificación de Datos Personales.					1	2	3	4																							
Principios, deberes y obligaciones.													1	2	3	4															
Aviso de Privacidad (integral y simplificado).													1	2	3	4															
Inventario de datos personales y los rubros que lo integran.																	1	2	3	4											
Información confidencial/reservada. Versión Pública.																								1	2	3	4				
Medidas de Seguridad.																												1	2	3	4

XVI. 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://transparencia.congresochiapas.gob.mx/bibliografias/los_7_principios_fundamentales.pdf